

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
DSG	CRSG	PERSREP	Live Tracks	Battlespace Information Services	COI Services
DSG	CRSG	Convoy Tracks	Live Tracks	Battlespace Information Services	COI Services
DSG	CRSG	MATDEM	Requests & Responses	Logistics Services	COI Services
DSG	CRSG	ES Request	Requests & Responses	Logistics Services	COI Services
BI-DIRECTIONAL					
DSG	CRSG	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
DSG	CRSG	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
DSG	CRSG	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
DSG	CRSG	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
DIVISIONAL SUPPORT GROUP (DSG) - BRIGADE SUPPORT GROUP (BSG)					
DSG	BSG	LOGASSESSREP	Reports	Logistics Services	COI Services
BSG	DSG	LOGREP	Reports	Logistics Services	COI Services
BSG	DSG	PERSREP	Reports	Logistics Services	COI Services
BSG	DSG	Convoy Tracks	Live Tracks	Battlespace Information Services	COI Services
BSG	DSG	MATDEM	Requests & Responses	Logistics Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BSG	DSG	ES Request	Requests & Responses	Logistics Services	COI Services
BI-DIRECTIONAL					
DSG	BSG	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
DSG	BSG	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
DSG	BSG	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
DSG	BSG	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
DSG	BSG	LOGASSESSREP	Reports	Logistics Services	COI Services
MAINTENANCE COMPANY (MC)/EQUIPMENT SUPPORT SERVICES (ES) - BACKLOADING POINT (BP)					
BI-DIRECTIONAL					
MC/ES	BP	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
MC/ES	BP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
MC/ES	BP	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
MAINTENANCE COMPANY (MC)/EQUIPMENT SUPPORT SERVICES (ES) - EQUIPMENT COLLECTION & COORDINATION POINT (ECCP)					
MC/ES	ECCP	ES Tasking	Tasking & Orders	Logistics Services	COI Services
ECCP	MC/ES	LOGREP	Reports	Logistics Services	COI Services
ECCP	MC/ES	MATDEM	Requests & Responses	Logistics Services	COI Services
BI-DIRECTIONAL					
MC/ES	ECCP	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
MC/ES	ECCP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
MC/ES	ECCP	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
EQUIPMENT COLLECTION & COORDINATION POINT (ECCP) - BACKLOADING POINT (BP)					
BI-DIRECTIONAL					
ECCP	BP	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
ECCP	BP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ECCP	BP	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
EQUIPMENT COLLECTION & COORDINATION POINT (ECCP) - FORWARD REPAIR TEAMS (FRT)					
ECCP	FRT	ES Tasking	Tasking & Orders	Logistics Services	COI Services
FRT	ECCP	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
BI-DIRECTIONAL					
ECCP	FRT	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
ECCP	FRT	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ECCP	FRT	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
EQUIPMENT COLLECTION & COORDINATION POINT (ECCP) - A2 ECHELON BATTLE GROUP LEVEL (A2 Ech)					
BI-DIRECTIONAL					
ECCP	A2 Ech	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
ECCP	A2 Ech	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ECCP	A2 Ech	Movement & Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
BRIGADE SUPPORT GROUP (BSG) - A2 ECHELON BATTLE GROUP LEVEL (A2 Ech)					
A2 Ech	BSG	LOGREP	Reports	Logistics Services	COI Services
A2 Ech	BSG	PERSREP	Reports	Logistics Services	COI Services
A2 Ech	BSG	Convoy Tracks	Live Tracks	Battlespace Information Services	COI Services
A2 Ech	BSG	MATDEM	Requests & Responses	Logistics Services	COI Services
A2 Ech	BSG	ES Request	Requests & Responses	Logistics Services	COI Services
BI-DIRECTIONAL					
BSG	A2 Ech	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
BSG	A2 Ech	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BSG	A2 Ech	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
BSG	A2 Ech	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
BSG	A2 Ech	LOGASSESSREP	Reports	Logistics Services	COI Services
A2 ECHELON BATTLE GROUP LEVEL (A2 Ech) - A1 ECHELON COMPANY LEVEL (A1 Ech)					
A1 Ech	A2 Ech	LOGREP	Reports	Logistics Services	COI Services
A1 Ech	A2 Ech	PERSREP	Reports	Logistics Services	COI Services
A1 Ech	A2 Ech	Convoy Tracks	Live Tracks	Battlespace Information Services	COI Services
A1 Ech	A2 Ech	MATDEM	Requests & Responses	Logistics Services	COI Services
A1 Ech	A2 Ech	ES Request	Requests & Responses	Logistics Services	COI Services
BI-DIRECTIONAL					
A2 Ech	A1 Ech	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
A2 Ech	A1 Ech	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
A2 Ech	A1 Ech	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
A2 Ech	A1 Ech	LOGASSESSREP	Reports	Logistics Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
A1 ECHELON COMPANY LEVEL (A1 Ech) - FORWARD REPAIR TEAM (FRT)					
BI-DIRECTIONAL					
A1 Ech	FRT	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
A1 Ech	FRT	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
A1 Ech	FRT	Movement &Transportation Information (M&T Info)	Situational Awareness	Logistics Services	COI Services
A1 ECHELON COMPANY LEVEL (A1 Ech) - FRONTLINE TROOPS (FLT)					
FLT	A1 Ech	LOGREP	Reports	Logistics Services	COI Services
FLT	A1 Ech	PERSREP	Reports	Logistics Services	COI Services
FLT	A1 Ech	Convoy Tracks	Live Tracks	Battlespace Information Services	COI Services
FLT	A1 Ech	MATDEM	Requests & Responses	Logistics Services	COI Services
FLT	A1 Ech	ES Request	Requests & Responses	Logistics Services	COI Services
BI-DIRECTIONAL					
A1 Ech	FLT	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
A1 Ech	FLT	Instant Message	Instant Messaging	Text-Based Collaboration Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
A1 Ech	FLT	LOGASSESSREP	Reports	Logistics Services	COI Services
NATIONAL SUPPORT ELEMENT (NSE) - NATIONAL SUPPORT ELEMENT (NSE)					
NSE	NSE	National Responsibility			
NATIONAL SUPPORT ELEMENT (NSE) - TROOP CONTRIBUTING NATIONS FORWARD SUPPORT GROUP (TCN FSG)					
NSE	TCN FSG	National Responsibility			

Table C-7: Logistics Support in a MJO+ Scenario Product Dissemination and Consumption

VJTF(L) AIR SUPPORT IER

22. Specific C2 and H2H information product exchange to enable the effective Air Support to be provided in the land environment during a VJTF(L) scenario is depicted in Figure C-9. The unidirectional red and green arrows represent products either consumed or disseminated from entities involved in the Air Support process within the land environment. The bi-directional black arrows represent products that are both disseminated and consumed by Air Support entities deployed in support of a Land based deployment:

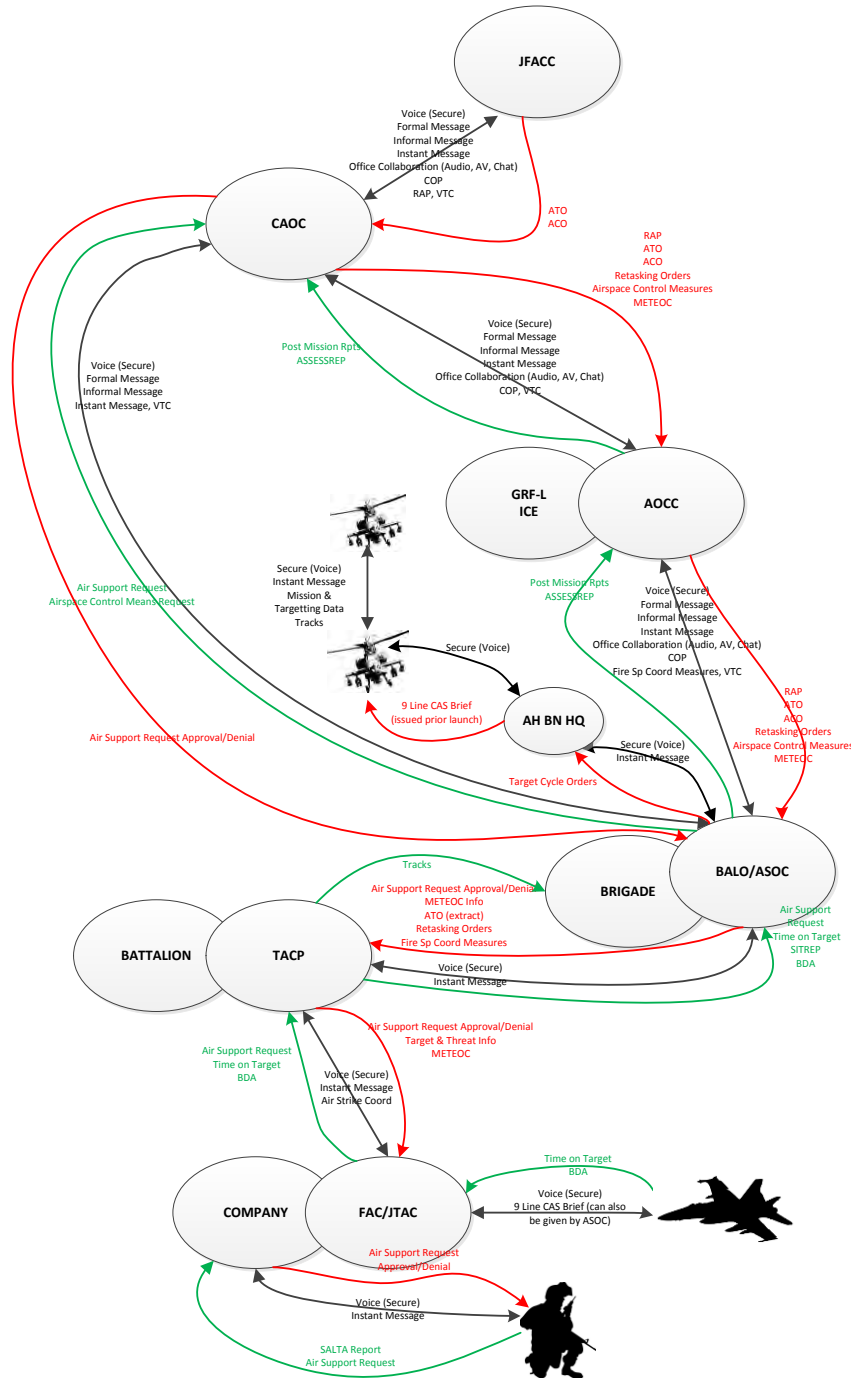


Figure C-9: VJTF(L) Air Support Product Dissemination/Consumption

23. As introduced in Figure C-9, the products depicted in the Table C-8 detail the unidirectional and bi-directional products relating to the Air Support process within a land environment under a VJTF(L) scenario. The column 'IER From' and 'IER To' details the C2 entities which the information products are exchanged with, the third column lists the product that is exchanged. Column 4 lists the operational capability that the product supports and columns 5 - 6 map the product to the service type as detailed in the C3 taxonomy nomenclature:

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JOINT FORCE AIR COMPONENT COMMAND (JFACC) - COMBINED AIR OPERATIONS CENTRE (CAOC)					
JFAC	CAOC	ATO	ATO Services	Air Services	COI Services
JFAC	CAOC	ACO	ACO Services	Air Services	COI Services
BI-DIRECTIONAL					
JFAC	CAOC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
JFAC	CAOC	Formal Message	Formal Messaging	Military Messaging Service	Core Services
JFAC	CAOC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
JFAC	CAOC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
JFAC	CAOC	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JFAC	CAOC	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
JFAC	CAOC	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
JFAC	CAOC	VTC	VTC	Video Based Collaboration Services	Core Services
JFAC	CAOC	COP	Recognized Picture Services	Situation Awareness Services	COI Services
JFAC	CAOC	RAP	RAP Services	Air Services	COI Services
COMBINED AIR OPERATIONS CENTRE (CAOC) - AIR OPERATIONS COORDINATION CENTRE (AOCC)					
CAOC	AOCC	RAP	RAP Services	Air Services	COI Services
CAOC	AOCC	ATO	ATO Services	Air Services	COI Services
CAOC	AOCC	ACO	ACO Services	Air Services	COI Services
CAOC	AOCC	Airspace Control Measures	Air Space Management Services	Air Services	COI Services
CAOC	AOCC	METEOC	Meteorology Services	Environmental Services	COI Services
CAOC	AOCC	Retasking Orders	Targeting Services	Tasking and Order Services	COI Services
AOCC	CAOC	Post Mission Reports	Reports	Operations Planning Services	COI Services
AOCC	CAOC	ASSESSREP	Reports	Operations Planning Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
CAOC	AOCC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
CAOC	AOCC	Formal Message	Formal Messaging	Military Messaging Service	Core Services
CAOC	AOCC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
CAOC	AOCC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
CAOC	AOCC	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
CAOC	AOCC	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
CAOC	AOCC	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
CAOC	AOCC	VTC	VTC	Video Based Collaboration Services	Core Services
CAOC	AOCC	COP	Recognized Picture Services	Situation Awareness Services	COI Services
AIR OPERATIONS COORDINATION CENTRE (AOCC) - BRIGADE AIR LIAISON OFFICER (BALO)					
AOCC	BALO	RAP	RAP Services	Air Services	COI Services
AOCC	BALO	ATO	ATO Services	Air Services	COI Services
AOCC	BALO	ACO	ACO Services	Air Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
AOCC	BALO	Retasking Orders	Targeting Services	Tasking and Order Services	COI Services
AOCC	BALO	Airspace Control Measures	Air Space Management Services	Air Services	COI Services
AOCC	BALO	METEOC	Meteorology Services	Environmental Services	COI Services
BALO	AOCC	Post Mission Reports	Reports	Operations Planning Services	COI Services
BALO	AOCC	ASSESSREP	Reports	Operations Planning Services	COI Services
BI-DIRECTIONAL					
AOCC	BALO	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
AOCC	BALO	Formal Message	Formal Messaging	Military Messaging Service	Core Services
AOCC	BALO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
AOCC	BALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
AOCC	BALO	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
AOCC	BALO	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
AOCC	BALO	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
AOCC	BALO	VTC	VTC	Video Based Collaboration Services	Core Services
AOCC	BALO	COP	Recognized Picture Services	Situation Awareness Services	COI Services
AOCC	BALO	Fire Sp Coord Measures	Targeting Services	Operations Planning Services	COI Services
COMBINED AIR OPERATIONS CENTRE (CAOC) - AIR SUPPORT OPERATIONS CENTRE (located at Brigade) (ASOC(B))					
ASOC(B)	CAOC	Air Support Request	ATO Services	Air Services	COI Services
ASOC(B)	CAOC	Airspace Control Means Request	Air Space Management Services	Air Services	COI Services
CAOC	ASOC(B)	Air Support Request Accept/Denial	ATO Services	Air Services	COI Services
BI-DIRECTIONAL					
ASOC(B)	CAOC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
ASOC(B)	CAOC	Formal Message	Formal Messaging	Military Messaging Service	Core Services
ASOC(B)	CAOC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
ASOC(B)	CAOC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ASOC(B)	CAOC	VTC	VTC	Video Based Collaboration Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BRIGADE AIR LIAISON OFFICER (BALO) - TACTICAL AIR CONTROL PARTY (TACP)					
BALO	TACP	METEOC	Meteorology Services	Environmental Services	COI Services
BALO	TACP	ATO (extract)	ACO Services	Air Services	COI Services
BALO	TACP	Retasking Orders	Targeting Services	Tasking and Order Services	COI Services
BALO	TACP	Fire Sp Coord Measures	Targeting Services	Operations Planning Services	COI Services
BALO	TACP	Air Support Request Accept/Denial	ATO Services	Air Services	COI Services
TACP	BALO	Air Support Request	ATO Services	Air Services	COI Services
TACP	BALO	Time on Target	Targeting Services	Tasking and Order Services	COI Services
TACP	BALO	SITREP	Reports	Joint Services	COI Services
TACP	BALO	BDA	Reports	Tasking and Order Services	COI Services
BI-DIRECTIONAL					
TACP	BALO	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
TACP	BALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
BRIGADE HEADQUARTERS - TACTICAL AIR CONTROL PARTY (TACP)					
TACP	BDE HQ	Tracks	Track Services	Battlefield Information Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BRIGADE AIR LIAISON OFFICER (BALO) - ATTACK HELICOPTER BATTALION HEADQUARTERS (AH BN HQ)					
BALO	AH BN HQ	Target Cycling Orders	Targeting Services	Tasking and Order Services	COI Services
BI-DIRECTIONAL					
BALO	AH HQ	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
BALO	AH HQ	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ATTACK HELICOPTER BATTALION HEADQUARTERS (AH BN HQ) - ATTACK HELICOPTER (AH) (given prior to launch)					
AH BN HQ	AH	9 Line CAS Brief	ATO Services	Air Services	COI Services
ATTACK HELICOPTER (AH) - ATTACK HELICOPTER (AH)					
BI-DIRECTIONAL					
AH	AH	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
AH	AH	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
AH	AH	Mission & Targeting Data	Targeting Services	Tasking and Order Services	COI Services
AH	AH	Tracks	Requests & Responses	Air Services	COI Services
TACTICAL AIR CONTROL PARTY (TACP) - FORWARD AIR CONTROLLER (FAC)					
TACP	FAC	Target & Threat Info	Targeting Services	Tasking and Order Services	COI Services
TACP	FAC	METEOC	Meteorology Services	Environmental Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
TACP	FAC	Air Support Request Accept/Denial	ATO Services	Air Services	COI Services
FAC	TACP	Air Support Request	ATO Services	Air Services	COI Services
FAC	TACP	Time on Target	Targeting Services	Tasking and Order Services	COI Services
FAC	TACP	BDA	Reports	Tasking and Order Services	COI Services
BI-DIRECTIONAL					
TACP	FAC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
TACP	FAC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
TACP	FAC	Air Strike Coord	Targeting Services	Operations Planning Services	COI Services
FRONTLINE TROOPS (FLT) - COMPANY HEADQUARTERS (Coy HQ)					
FLT	COY HQ	SALTA	Reports	Tasking & Order Services	COI Services
FLT	COY HQ	Air Support Request	ATO Services	Air Services	COI Services
Coy HQ	FLT	Air Support Request Accept/Denial	ATO Services	Air Services	COI Services
BI-DIRECTIONAL					
FLT	COY HQ	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
FLT	COY HQ	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
FORWARD AIR CONTROLLER (FAC) - FAST JET					
Fast Jet	FAC	Time on Target	Targeting Services	Tasking and Order Services	COI Services
Fast Jet	FAC	BDA	Reports	Tasking and Order Services	COI Services
BI-DIRECTIONAL					
FAC	Fast Jet	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
FAC	Fast Jet	9 Line CAS Brief (can also be given by ASOC)	ATO Services	Air Services	COI Services

Table C-8: Air Support in a VJTF(L) Scenario Product Dissemination and Consumption

MJO+ AIR SUPPORT IER

24. Specific C2 and H2H information product exchange to enable the effective Air Support to be provided in the land environment during a MJO+ scenario is depicted in Figure C-10. The unidirectional red and green arrows represent products either consumed or disseminated from entities involved in the Air Support process within the land environment. The bi-directional black arrows represent products that are both disseminated and consumed by Air Support entities deployed in support of a Land based deployment:

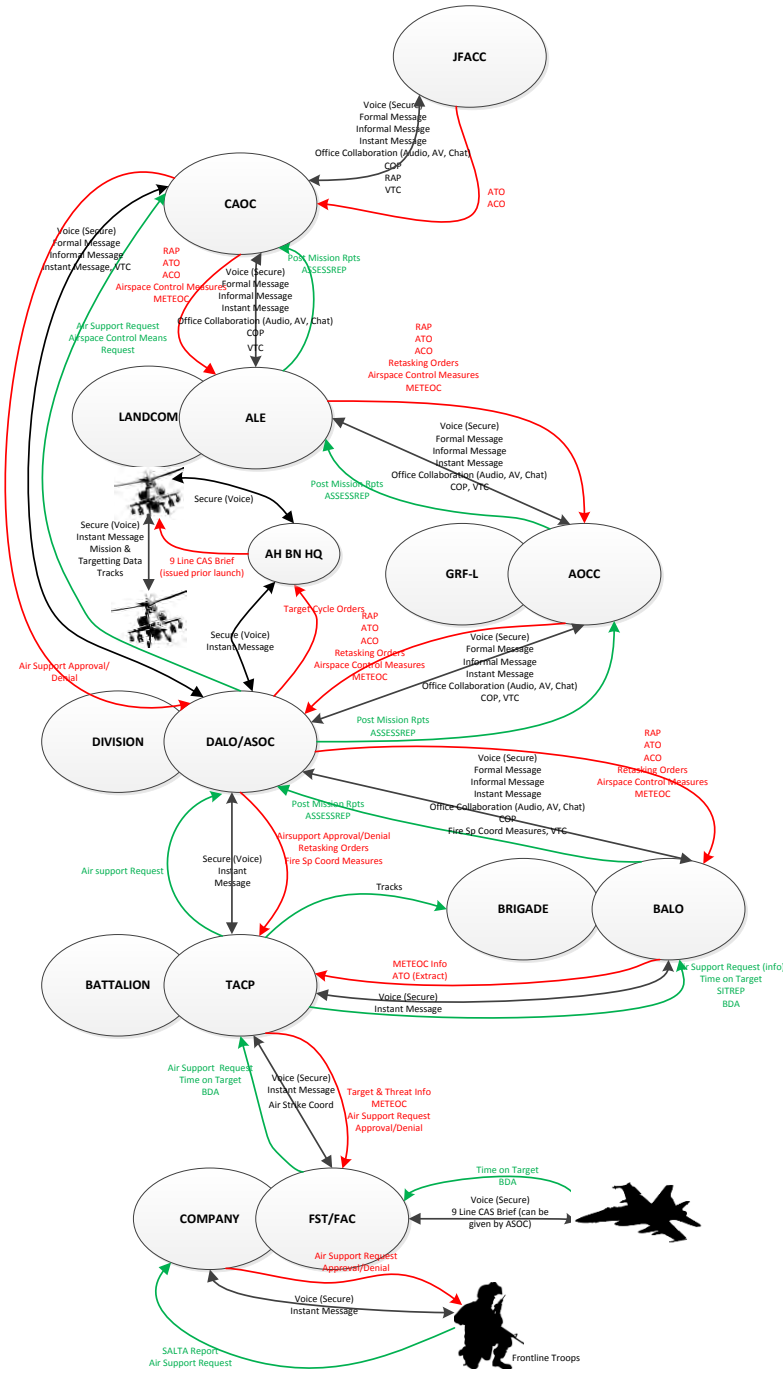


Figure C-10: MJO+ Air Support Product Dissemination/Consumption

25. As introduced in Figure C-10, the products depicted in the Table C-9 detail the unidirectional and bi-directional products relating to the Air Support process within a land environment under a MJO+ scenario. The column 'IER From' and 'IER To' details the C2 entities which the information products are exchanged with, the third column lists the product that is exchanged. Column 4 lists the operational capability that the product supports and columns 5 - 6 map the product to the service type as detailed in the C3 Taxonomy nomenclature:

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JOINT FORCE AIR COMPONENT COMMAND (JFACC) - COMBINED AIR OPERATIONS CENTRE (CAOC)					
JFAC	CAOC	ATO	ATO Services	Air Services	COI Services
JFAC	CAOC	ACO	ACO Services	Air Services	COI Services
BI-DIRECTIONAL					
JFAC	CAOC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
JFAC	CAOC	Formal Message	Formal Messaging	Military Messaging Service	Core Services
JFAC	CAOC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
JFAC	CAOC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
JFAC	CAOC	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JFAC	CAOC	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
JFAC	CAOC	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
JFAC	CAOC	VTC	VTC	Video Based Collaboration Services	Core Services
JFAC	CAOC	COP	Recognized Picture Services	Situation Awareness Services	COI Services
JFAC	CAOC	RAP	RAP Services	Air Services	COI Services
COMBINED AIR OPERATIONS CENTRE (CAOC) - AIR LIAISON ELEMENT (ALE)					
CAOC	ALE	RAP	RAP Services	Air Services	COI Services
CAOC	ALE	ATO	ATO Services	Air Services	COI Services
CAOC	ALE	ACO	ACO Services	Air Services	COI Services
CAOC	ALE	Airspace Control Measures	Air Space Management Services	Air Services	COI Services
CAOC	ALE	METEOC	Meteorology Services	Environmental Services	COI Services
ALE	CAOC	Post Mission Reports	Reports	Operations Planning Services	COI Services
ALE	CAOC	ASSESSREP	Reports	Operations Planning Services	COI Services
BI-DIRECTIONAL					
CAOC	ALE	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
CAOC	ALE	Formal Message	Formal Messaging	Military Messaging Service	Core Services
CAOC	ALE	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
CAOC	ALE	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
CAOC	ALE	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
CAOC	ALE	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
CAOC	ALE	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
CAOC	ALE	VTC	VTC	Video Based Collaboration Services	Core Services
CAOC	ALE	COP	Recognized Picture Services	Situation Awareness Services	COI Services
COMBINED AIR OPERATIONS CENTRE (CAOC) - AIR SUPPORT OPERATIONS CENTRE (located at Division) (ASOC(D))					
ASOC(D)	CAOC	Air Support Request	ATO Services	Air Services	COI Services
ASOC(D)	CAOC	Airspace Control Means Request	Air Space Management Services	Air Services	COI Services
CAOC	ASOC(D)	Air Support Request Accept/Denial	ATO Services	Air Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
ASOC(D)	CAOC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
ASOC(D)	CAOC	Formal Message	Formal Messaging	Military Messaging Service	Core Services
ASOC(D)	CAOC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
ASOC(D)	CAOC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ASOC(D)	CAOC	VTC	VTC	Video Based Collaboration Services	Core Services
AIR LIAISON ELEMENT (ALE) - AIR OPERATIONS COORDINATION CENTRE (AOCC)					
ALE	AOCC	RAP	RAP Services	Air Services	COI Services
ALE	AOCC	ATO	ATO Services	Air Services	COI Services
ALE	AOCC	ACO	ACO Services	Air Services	COI Services
ALE	AOCC	Retasking Orders	Targeting Services	Tasking and Order Services	COI Services
ALE	AOCC	Airspace Control Measures	Air Space Management Services	Air Services	COI Services
ALE	AOCC	METEOC	Meteorology Services	Environmental Services	COI Services
AOCC	ALE	Post Mission Reports	Reports	Operations Planning Services	COI Services
AOCC	ALE	ASSESSREP	Reports	Operations Planning Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
ALE	AOCC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
ALE	AOCC	Formal Message	Formal Messaging	Military Messaging Service	Core Services
ALE	AOCC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
ALE	AOCC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ALE	AOCC	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
ALE	AOCC	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
ALE	AOCC	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
ALE	AOCC	VTC	VTC	Video Based Collaboration Services	Core Services
ALE	AOCC	COP	Recognized Picture Services	Situation Awareness Services	COI Services
AIR OPERATIONS COORDINATION CENTRE (AOCC) - DIVISION AIR LIAISON OFFICER Division (DALO)					
AOCC	DALO	RAP	RAP Services	Air Services	COI Services
AOCC	DALO	ATO	ATO Services	Air Services	COI Services
AOCC	DALO	ACO	ACO Services	Air Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
AOCC	DALO	Retasking Orders	Targeting Services	Tasking and Order Services	COI Services
AOCC	DALO	Airspace Control Measures	Air Space Management Services	Air Services	COI Services
AOCC	DALO	METEOC	Meteorology Services	Environmental Services	COI Services
DALO	AOCC	Post Mission Reports	Reports	Operations Planning Services	COI Services
DALO	AOCC	ASSESSREP	Reports	Operations Planning Services	COI Services
BI-DIRECTIONAL					
AOCC	DALO	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
AOCC	DALO	Formal Message	Formal Messaging	Military Messaging Service	Core Services
AOCC	DALO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
AOCC	DALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
AOCC	DALO	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
AOCC	DALO	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
AOCC	DALO	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
AOCC	DALO	VTC	VTC	Video Based Collaboration Services	Core Services
AOCC	DALO	COP	Recognized Picture Services	Situation Awareness Services	COI Services
DIVISION AIR LIAISON OFFICER (DALO)/AIR SUPPORT OPERATIONS CENTRE - TACTICAL AIR CONTROL PARTY (TACP)					
TACP	ASOC	Air support Request	ATO Services	Air Services	COI Services
ASOC(D)	TACP	Air support Approval/Denial	ATO Services	Air Services	COI Services
ASOC(D)	TACP	Retasking Orders	ATO Services	Air Services	COI Services
ASOC(D)	TACP	Fire Support Coord Measures	Targeting Services	Operations Planning Services	COI Services
BI-DIRECTIONAL					
ASOC(D)	TACP	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
ASOC(D)	TACP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
DIVISION AIR LIAISON OFFICER (DALO) - ATTACK HELICOPTER BATTALION HEADQUARTERS (AH BN HQ)					
DALO	AH BN HQ	Target Cycle Orders	Targeting Services	Tasking and Order Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
DALO	AH BN HQ	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
ATTACK HELICOPTER BATTALION HEADQUARTERS (AH BN HQ) - ATTACK HELICOPTER (AH) (given prior to launch)					
AH BN HQ	AH	9 Line CAS Brief	ATO Services	Air Services	COI Services
ATTACK HELICOPTER (AH) - ATTACK HELICOPTER (AH)					
BI-DIRECTIONAL					
AH	AH	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
AH	AH	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
AH	AH	Mission & Targeting Data	Targeting Services	Tasking and Order Services	COI Services
AH	AH	Tracks	Requests & Responses	Air Services	COI Services
DIVISION AIR LIAISON OFFICER (DALO) - BRIGADE AIR LIAISON OFFICER (BALO)					
DALO	BALO	RAP	RAP Services	Air Services	COI Services
DALO	BALO	ATO	ATO Services	Air Services	COI Services
DALO	BALO	ACO	ACO Services	Air Services	COI Services
DALO	BALO	Retasking Orders	Targeting Services	Tasking and Order Services	COI Services
DALO	BALO	Airspace Control Measures	Air Space Management Services	Air Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
DALO	BALO	METEOC	Meteorology Services	Environmental Services	COI Services
BALO	DALO	Post Mission Reports	Reports	Operations Planning Services	COI Services
BALO	DALO	ASSESSREP	Reports	Operations Planning Services	COI Services
BI-DIRECTIONAL					
DALO	BALO	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
DALO	BALO	Formal Message	Formal Messaging	Military Messaging Service	Core Services
DALO	BALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
DALO	BALO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
DALO	BALO	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
DALO	BALO	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
DALO	BALO	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
DALO	BALO	VTC	VTC	Video Based Collaboration Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
DALO	BALO	COP	Recognized Picture Services	Situation Awareness Services	COI Services
DALO	BALO	Fire Sp Coord Measures	Targeting Services	Operations Planning Services	COI Services
BRIGADE AIR LIAISON OFFICER (BALO) - TACTICAL AIR CONTROL PARTY (TACP)					
BALO	TACP	METEOC	Meteorology Services	Environmental Services	COI Services
BALO	TACP	ATO (Extract)	ACO Services	Air Services	COI Services
BALO	TACP	Retasking Orders	Targeting Services	Tasking and Order Services	COI Services
BALO	TACP	Fire Sp Coord Measures	Targeting Services	Operations Planning Services	COI Services
TACP	BALO	Air Support Request (Info)	ATO Services	Air Services	COI Services
TACP	BALO	Time on Target	Targeting Services	Tasking and Order Services	COI Services
TACP	BALO	SITREP	Reports	Joint Services	COI Services
TACP	BALO	BDA	Reports	Tasking and Order Services	COI Services
BI-DIRECTIONAL					
TACP	BALO	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
TACP	BALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BRIGADE HEADQUARTERS - TACTICAL AIR CONTROL PARTY (TACP)					
TACP	BDE HQ	Tracks	Track Services	Battlefield Information Services	COI Services
TACTICAL AIR CONTROL PARTY (TACP) - FORWARD AIR CONTROLLER (FAC)					
TACP	FAC	Target & Threat Info	Targeting Services	Tasking and Order Services	COI Services
TACP	FAC	METEOC	Meteorology Services	Environmental Services	COI Services
TACP	FAC	Air Support Request Approval/Denial	ATO Services	Air Services	COI Services
FAC	TACP	Air Support Request	ATO Services	Air Services	COI Services
FAC	TACP	Time on Target	Targeting Services	Tasking and Order Services	COI Services
FAC	TACP	BDA	Reports	Tasking and Order Services	COI Services
BI-DIRECTIONAL					
TACP	FAC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
TACP	FAC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
TACP	FAC	Air Strike Coord	Targeting Services	Operations Planning Services	COI Services
FORWARD AIR CONTROLLER (FAC) - FAST JET					
Fast Jet	FAC	Time on Target	Targeting Services	Tasking and Order Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
Fast Jet	FAC	BDA	Reports	Tasking and Order Services	COI Services
BI-DIRECTIONAL					
FAC	Fast Jet	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
FAC	Fast Jet	9 Line CAS Brief (can also be given by ASOC)	ATO Services	Air Services	COI Services
FRONTLINE TROOPS (FLT) - COMPANY HEADQUARTERS (Coy HQ)					
FLT	COY HQ	SALTA	Reports	Tasking & Order Services	COI Services
FLT	COY HQ	Air Support Request	ATO Services	Air Services	COI Services
BI-DIRECTIONAL					
FLT	COY HQ	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
FLT	COY HQ	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services

Table C-9: Air Support in a MJO+ Scenario Product Dissemination and Consumption

VJTF(L) MEDICAL SUPPORT IER

26. Specific C2 and H2H information product exchange to enable the effective Medical Support to be provided in the land environment during a VJTF(L) scenario is depicted in Figure C-11. The unidirectional red and green arrows represent products either consumed or disseminated from entities involved in the Medical Evacuation process within the land environment. The bi-directional black arrows represent products that are both disseminated and consumed by Air Support entities deployed in support of a Land based deployment:

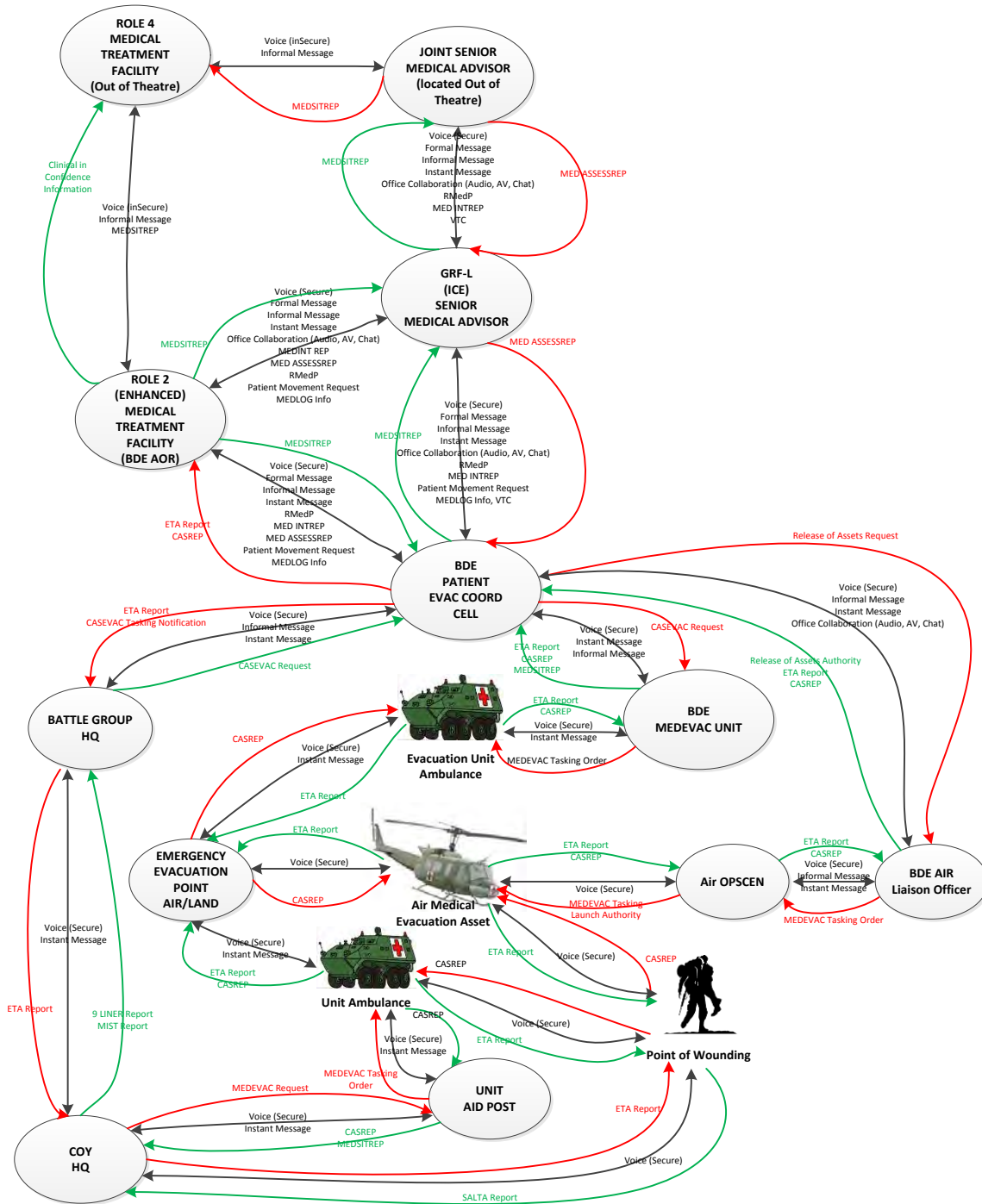


Figure C-11: VJTF(L) Medical Support Product Dissemination/Consumption

27. As introduced in Figure C-11, the products depicted in the Table C-10 detail the unidirectional and bi-directional products relating to the Medical Evacuation process within a land environment under a VJTf(L) scenario. The column 'IER From' and 'IER To' details the C2 entities which the information products are exchanged with; the third column lists the product that is exchanged. Column 4 lists the operational capability that the product supports and columns 5 - 6 map the product to the service type as detailed in the C3 Taxonomy nomenclature:

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JOINT SENIOR MEDICAL ADVISOR (JSMA) - ROLE 4 MEDICAL TREATMENT FACILITY (R4 MTF) (Out of Theatre) (Troop Contributing Nations (TCN) Provided)					
JSMA	R4 MTF	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
JSMA	R4 MTF	Voice (InSecure)	Voice	Audio-Based Communication Services	Core Services
JSMA	R4 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
JSMA	R4 MTF	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
JSMA	R4 MTF	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JSMA	R4 MTF	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
JOINT SENIOR MEDICAL ADVISOR (JSMA) - GRADUATED RESPONSE FORCE LAND (INITIAL COMMAND ELEMENT) SENIOR MEDICAL ADVISOR (GRF-L (ICE) (SMA))					
JSMA	GRF-L (ICE) (SMA)	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	JSMA	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
JSMA	GRF-L (ICE) (SMA)	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
JSMA	GRF-L (ICE) (SMA)	Formal Message	Formal Messaging	Military Messaging Service	Core Services
JSMA	GRF-L (ICE) (SMA)	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
JSMA	GRF-L (ICE) (SMA)	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
JSMA	GRF-L (ICE) (SMA)	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JSMA	GRF-L (ICE) (SMA)	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
JSMA	GRF-L (ICE) (SMA)	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
JSMA	GRF-L (ICE) (SMA)	VTC	VTC	Video Based Collaboration Services	Core Services
JSMA	GRF-L (ICE) (SMA)	RMedP	MEDICAL	LOGISTICS Services	COI Services
JSMA	GRF-L (ICE) (SMA)	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
GRADUATED RESPONSE FORCE LAND (INITIAL COMMAND ELEMENT) SENIOR MEDICAL ADVISOR (GRF-L (ICE) (SMA)) - BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC)					
GRF-L (ICE) (SMA)	B PECC	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
B PECC	GRF-L (ICE) (SMA)	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
GRF-L (ICE) (SMA)	B PECC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
GRF-L (ICE) (SMA)	B PECC	Formal Message	Formal Messaging	Military Messaging Service	Core Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
GRF-L (ICE) (SMA)	B PECC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
GRF-L (ICE) (SMA)	B PECC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
GRF-L (ICE) (SMA)	B PECC	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
GRF-L (ICE) (SMA)	B PECC	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
GRF-L (ICE) (SMA)	B PECC	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
GRF-L (ICE) (SMA)	B PECC	VTC	VTC	Video Based Collaboration Services	Core Services
GRF-L (ICE) (SMA)	B PECC	RMedP	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	B PECC	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	B PECC	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	B PECC	MEDLOG Info	MEDICAL	LOGISTICS Services	COI Services

DRAFT

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
ROLE 4 MEDICAL TREATMENT FACILITY (R4 MTF) - ROLE 2 MEDICAL TREATMENT FACILITY (R2 MTF) -					
R4 MTF	R2 MTF	Clinical In Confidence Information	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
R4 MTF	R2 MTF	Voice (Insecure)	Voice	Audio-Based Communication Services	Core Services
R4 MTF	R2 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Services
R4 MTF	R2 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
R4 MTF	R2 MTF	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
GRADUATED RESPONSE FORCE LAND (INITIAL COMMAND ELEMENT) SENIOR MEDICAL ADVISOR (GRF-L (ICE) (SMA)) - ROLE 2 MEDICAL TREATMENT FACILITY (R2 MTF)					
R2 MTF	GRF-L (ICE) (SMA)	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
GRF-L (ICE) (SMA)	R2 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
GRF-L (ICE) (SMA)	R2 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Enterprise Services

DRAFT

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
GRF-L (ICE) (SMA)	R2 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
GRF-L (ICE) (SMA)	R2 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
GRF-L (ICE) (SMA)	R2 MTF	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
GRF-L (ICE) (SMA)	R2 MTF	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
GRF-L (ICE) (SMA)	R2 MTF	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
GRF-L (ICE) (SMA)	R2 MTF	RMedP	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	R2 MTF	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	R2 MTF	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	R2 MTF	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
GRF-L (ICE) (SMA)	R2 MTF	MEDLOG Info	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - ROLE 2 MEDICAL TREATMENT FACILITY (R2 MTF)					
B PECC	R2 MTF	ETA Report	Requests & Responses	LAND Services	COI Services
B PECC	R2 MTF	CASREP	MEDICAL	LOGISTICS Services	COI Services
R2 MTF	B PECC	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	R2 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	R2 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Enterprise Services
B PECC	R2 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	R2 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
B PECC	R2 MTF	RMedP	MEDICAL	LOGISTICS Services	COI Services
B PECC	R2 MTF	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
B PECC	R2 MTF	MED INTREP	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
B PECC	R2 MTF	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
B PECC	R2 MTF	MEDLOG Info	MEDICAL	LOGISTICS Services	COI Services
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - AIR LIAISON OFFICER (ALO)					
B PECC	ALO	Release of Assets Request	Requests & Responses	Air Services	COI Services
ALO	B PECC	Release of Assets Authority	Requests & Responses	Air Services	COI Services
ALO	B PECC	ETA Report	Requests & Responses	LAND Services	COI Services
ALO	B PECC	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	ALO	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	ALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
B PECC	ALO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	ALO	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
B PECC	ALO	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
B PECC	ALO	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
AIR LIAISON OFFICER (ALO) - AIR OPSCEN (AO)					
ALO	AO	MEDEVAC Tasking Order	Tasking & Orders	Air Services	COI Services
AO	ALO	ETA Report	Requests & Responses	LAND Services	COI Services
AO	ALO	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
ALO	AO	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
ALO	AO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
ALO	AO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
Air OPERATIONS CENTRE (AO) - AIR MEDICAL EVACUATION ASSET (AMEA)					
AO	AMEA	MEDEVAC Tasking Order	Tasking & Orders	Air Services	COI Services
AO	AMEA	Launch Authority	Tasking & Orders	Air Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
AMEA	AO	ETA Report	Requests & Responses	LAND Services	COI Services
AMEA	AO	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
AO	AMEA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
AIR MEDICAL EVACUATION ASSET (AMEA) - POINT OF WOUNDING (POW)					
AMEA	POW	ETA Report	Requests & Responses	LAND Services	COI Services
POW	AMEA	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
AMEA	POW	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
AIR MEDICAL EVACUATION ASSET (AMEA) - EMERGENCY EVACUATION POINT (EEP)					
AMEA	EEP	ETA Report	Requests & Responses	LAND Services	COI Services
EEP	AMEA	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
AMEA	EEP	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - BATTLE GROUP HEADQUARTERS (BG HQ)					
B PECC	BG HQ	ETA Report	Requests & Responses	LAND Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
B PECC	BG HQ	MEDEVAC Tasking Notification	MEDICAL	LOGISTICS Services	COI Services
BG HQ	B PECC	MEDEVAC Request	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	BG HQ	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	BG HQ	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	BG HQ	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
BATTLE GROUP HEADQUARTERS (BG HQ) - COMPANY HEADQUARTERS (Coy HQ)					
BG HQ	Coy HQ	ETA Report	Requests & Responses	Tasking & Order Services	COI Services
Coy HQ	BG HQ	9 Liner Report	Reports	Tasking & Order Services	COI Services
Coy HQ	BG HQ	MIST Report	Reports	Tasking & Order Services	COI Services
BI-DIRECTIONAL					
BG HQ	Coy HQ	Voice (secure)	Voice	Audio-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BG HQ	Coy HQ	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
COMPANY HEADQUARTERS (Coy HQ) - UNIT AID POST (UAP)					
Coy HQ	UAP	MEDEVAC Request	MEDICAL	LOGISTICS Services	COI Services
UAP	Coy HQ	CASREP	MEDICAL	LOGISTICS Services	COI Services
UAP	Coy HQ	MEDSITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
Coy HQ	UAP	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
Coy HQ	UAP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
COMPANY HEADQUARTERS (Coy HQ) - POINT OF WOUNDING (POW)					
Coy HQ	POW	ETA Report	Requests & Responses	Tasking & Order Services	COI Services
POW	Coy HQ	SALTA Report	Reports	Tasking & Order Services	COI Services
BI-DIRECTIONAL					
Coy HQ	POW	Voice (secure)	Voice	Audio-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
UNIT AID POST (UAP) - UNIT AMBULANCE (UA)					
UAP	UA	MEDEVAC Tasking Order	Tasking & Orders	Air Services	COI Services
UA P	UAP	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
UAP	UA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
UAP	UA	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
UNIT AID POST - EMERGENCY EVACUATION POINT AIR/LAND AIR/LAND (EEP)					
UA	EEP	ETA Report	Requests & Responses	Tasking & Order Services	COI Services
UA	EEP	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
UA	EEP	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
UA	EEP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - BRIGADE MEDEVAC UNIT (BMU)					
B PECC	BMU	MEDEVAC Request	Tasking & Orders	LAND Services	COI Services
BMU	B PECC	ETA Report	Requests & Responses	LAND Services	COI Services
BMU	B PECC	CASREP	MEDICAL	LOGISTICS Services	COI Services
BMU	B PECC	MEDSITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	BMU	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	BMU	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	BMU	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
BRIGADE MEDEVAC UNIT (BMU)- EVACUATION UNIT AMBULANCE (EUA)					
BMU	EUA	MEDEVAC Tasking Order	Tasking & Orders	LAND Services	COI Services
EUA	BMU	ETA Report	Requests & Responses	LAND Services	COI Services
EUA	BMU	CASREP	MEDICAL	LOGISTICS Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
BMU	EUA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
BMU	EUA	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
EMERGENCY EVACUATION POINT Air/Land (EEP) - EVACUATION UNIT AMBULANCE (EUA)					
EEP	EUA	CASREP	MEDICAL	LOGISTICS Services	COI Services
EUA	EEP	ETA Report	Requests & Responses	LAND Services	COI Services
BI-DIRECTIONAL					
EEP	EUA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
EEP	EUA	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
POINT OF WOUNDING (POW) - UNIT AMBULANCE (UA)					
POW	UA	CASREP	MEDICAL	LOGISTICS Services	COI Services
UA	POW	ETA Report	Requests & Responses	LAND Services	COI Services
BI-DIRECTIONAL					
POW	UA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services

Table C-1-11: Medical Support in a VJTF(L) Scenario Product Dissemination and Consumption

MJO+ MEDICAL SUPPORT IER

28. Specific C2 and H2H information product exchange to enable the effective Medical Support to be provided in the land environment during a MJO+ scenario is depicted in Figure C-12. The unidirectional red and green arrows represent products either consumed or disseminated from entities involved in the Medical Evacuation process within the land environment. The bi-directional black arrows represent products that are both disseminated and consumed by Air Support entities deployed in support of a Land based deployment:

29. As introduced in Figure C-12, the products depicted in the table C-11 detail the unidirectional and bi-directional products relating to the Medical Evacuation process within a land environment under a MJO+ scenario. The column 'IER From' and 'IER To' details the C2 entities which the information products are exchanged with; the third column lists the product that is exchanged. Column 4 lists the operational capability that the product supports and columns 5 - 6 map the product to the service type as detailed in the C3 Taxonomy nomenclature:

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JOINT SENIOR MEDICAL ADVISOR (JSMA) - ROLE 4 MEDICAL TREATMENT FACILITY (R4 MTF) (Out of Theatre) (Troop Contributing Nations (TCN) Provided)					
R4 MTF	JSMA	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
JSMA	R4 MTF	Voice (InSecure)	Voice	Audio-Based Communication Services	Core Services
JSMA	R4 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
JSMA	R4 MTF	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
JSMA	R4 MTF	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
JSMA	R4 MTF	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
JOINT SENIOR MEDICAL ADVISOR (JSMA) - LANDCOM SENIOR MEDICAL ADVISOR (LSMA)					
JSMA	LSMA	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
JSMA	LSMA	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
LSMA	JSMA	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
LSMA	JSMA	MED INCREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
JSMA	LSMA	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
JSMA	LSMA	Formal Message	Formal Messaging	Military Messaging Service	Core Services
JSMA	LSMA	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
JSMA	LSMA	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
JSMA	LSMA	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
JSMA	LSMA	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
JSMA	LSMA	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
JSMA	LSMA	VTC	VTC	Video Based Collaboration Services	Core Services
JSMA	LSMA	RMedP	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
LANDCOM MEDICAL OPERATIONS (LMO) - GRF-L PATIENT EVACUATION COORDINATION CELL (G PECC)					
LMO	G PECC	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
LMO	G PECC	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
G PECC	LMO	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
G PECC	LMO	MED INCREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
LMO	G PECC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
LMO	G PECC	Formal Message	Formal Messaging	Military Messaging Service	Core Services
LMO	G PECC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
LMO	G PECC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
LMO	G PECC	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
LMO	G PECC	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
LMO	G PECC	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
LMO	G PECC	VTC	VTC	Video Based Collaboration Services	Core Services
LMO	G PECC	RMedP	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
ROLE 4 MEDICAL TREATMENT FACILITY (R4 MTF) - ROLE 3 MEDICAL TREATMENT FACILITY (R3 MTF) -					
R4 MTF	R3 MTF	Clinical in Confidence Information	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
R4 MTF	R3 MTF	Voice (Insecure)	Voice	Audio-Based Communication Services	Core Services
R4 MTF	R3 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
R4 MTF	R3 MTF	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
GRF-L PATIENT EVACUATION COORDINATION CELL (G PECC) - DIVISION PATIENT EVACUATION COORDINATION CELL (G PECC) (D PECC)					
G PECC	D PECC	ETA Report	Requests & Responses	LAND Services	COI Services
G PECC	D PECC	MEDEVAC Tasking Notification	MEDICAL	LOGISTICS Services	COI Services
G PECC	D PECC	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
D PECC	G PECC	Mass CASEVAC Request	MEDICAL	LOGISTICS Services	COI Services
D PECC	G PECC	MED INCREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
G PECC	D PECC	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
G PECC	D PECC	Formal Message	Formal Messaging	Military Messaging Service	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
G PECC	D PECC	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
G PECC	D PECC	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
G PECC	D PECC	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
G PECC	D PECC	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
G PECC	D PECC	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
G PECC	D PECC	VTC	VTC	Video Based Collaboration Services	Core Services
G PECC	D PECC	RMedP	MEDICAL	LOGISTICS Services	COI Services
G PECC	D PECC	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
G PECC	D PECC	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
G PECC	D PECC	MEDLOG Information	MEDICAL	LOGISTICS Services	COI Services
GRF-L PATIENT EVACUATION COORDINATION CELL (G PECC) - ROLE 3 MEDICAL TREATMENT FACILITY (R3 MTF)					
G PECC	R3 MTF	ETA Report	Requests & Responses	LAND Services	COI Services
G PECC	R3 MTF	CASREP	MEDICAL	LOGISTICS Services	COI Services
R3 MTF	G PECC	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
R3 MTF	G PECC	MED INTREP	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
G PECC	R3 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
G PECC	R3 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Services
G PECC	R3 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
G PECC	R3 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
G PECC	R3 MTF	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
G PECC	R3 MTF	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
G PECC	R3 MTF	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
G PECC	R3 MTF	VTC	VTC	Video Based Collaboration Services	Core Services
G PECC	R3 MTF	RMedP	MEDICAL	LOGISTICS Services	COI Services
G PECC	R3 MTF	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
G PECC	R3 MTF	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
G PECC	R3 MTF	MEDLOG Information	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
GRF-L PATIENT EVACUATION COORDINATION CELL (G PECC) - AIR LIAISON OFFICER (ALO)					
G PECC	ALO	Release of Assets Request	Requests & Responses	Air Services	COI Services
ALO	G PECC	Release of Assets Authority	Requests & Responses	Air Services	COI Services
ALO	G PECC	ETA Report	Requests & Responses	LAND Services	COI Services
ALO	G PECC	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
G PECC	ALO	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
G PECC	ALO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
G PECC	ALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
G PECC	ALO	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
G PECC	ALO	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
G PECC	ALO	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
DIVISION PATIENT EVACUATION COORDINATION CELL (D PECC) - ROLE 3 MEDICAL TREATMENT FACILITY (R3 MTF)					
D PECC	R3 MTF	ETA Report	Requests & Responses	LAND Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
D PECC	R3 MTF	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
D PECC	R3 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
D PECC	R3 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Services
D PECC	R3 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
D PECC	R3 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
D PECC	R3 MTF	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
D PECC	R3 MTF	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
D PECC	R3 MTF	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
D PECC	R3 MTF	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
D PECC	R3 MTF	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
D PECC	R3 MTF	MEDLOG Information	MEDICAL	LOGISTICS Services	COI Services
D PECC	R3 MTF	Recognized Medical Picture	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
DIVISION PATIENT EVACUATION COORDINATION CELL (D PECC) - ROLE 2 MEDICAL TREATMENT FACILITY (R2 MTF)					
D PECC	R2 MTF	ETA Report	Requests & Responses	LAND Services	COI Services
D PECC	R2 MTF	CASREP	MEDICAL	LOGISTICS Services	COI Services
R2 MTF	D PECC	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
R2 MTF	D PECC	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
D PECC	R2 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
D PECC	R2 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Services
D PECC	R2 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
D PECC	R2 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
D PECC	R2 MTF	RMedP	MEDICAL	LOGISTICS Services	COI Services
D PECC	R2 MTF	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
D PECC	R2 MTF	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
D PECC	R2 MTF	MEDLOG Information	MEDICAL	LOGISTICS Services	COI Services
DIVISION PATIENT EVACUATION COORDINATION CELL (D PECC)- BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC)					
D PECC	B PECC	ETA Report	Requests & Responses	LAND Services	COI Services
D PECC	B PECC	MEDEVAC Tasking Notification	MEDICAL	LOGISTICS Services	COI Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
B PECC	D PECC	MEDINC REP	MEDICAL	LOGISTICS Services	COI Services
D PECC	B PECC	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
D PECC	R3 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
D PECC	R3 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Services
D PECC	R3 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
D PECC	R3 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
D PECC	R3 MTF	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
D PECC	R3 MTF	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
D PECC	R3 MTF	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
D PECC	R3 MTF	VTC	VTC	Video Based Collaboration Services	Core Services
D PECC	R3 MTF	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
D PECC	R3 MTF	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
D PECC	R3 MTF	MEDLOG Information	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - ROLE 3 MEDICAL TREATMENT FACILITY (R3 MTF)					
B PECC	R3 MTF	ETA Report	Requests & Responses	LAND Services	COI Services
B PECC	R3 MTF	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	R3 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	R3 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Enterprise Services
B PECC	R3 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	R3 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
ROLE 3 MEDICAL TREATMENT FACILITY (R3 MTF) - ROLE 2 MEDICAL TREATMENT FACILITY (R2 MTF)					
R2 MTF	R3 MTF	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
R3 MTF	R2 MTF	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
R3 MTF	R2 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
R3 MTF	R2 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Enterprise Services
R3 MTF	R2 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
R3 MTF	R2 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
R3 MTF	R2 MTF	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
R3 MTF	R2 MTF	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
R3 MTF	R2 MTF	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
R3 MTF	R2 MTF	RMedP	MEDICAL	LOGISTICS Services	COI Services
R3 MTF	R2 MTF	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - ROLE 2 MEDICAL TREATMENT FACILITY (R2 MTF)					
B PECC	R2 MTF	ETA Report	Requests & Responses	LAND Services	COI Services
B PECC	R2 MTF	CASREP	MEDICAL	LOGISTICS Services	COI Services
B PECC	R2 MTF	MED ASSESSREP	MEDICAL	LOGISTICS Services	COI Services
R2 MTF	B PECC	MED SITREP	MEDICAL	LOGISTICS Services	COI Services
R2 MTF	B PECC	MED INTREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	R2 MTF	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	R2 MTF	Formal Message	Formal Messaging	Military Messaging Service	Core Enterprise Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
B PECC	R2 MTF	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	R2 MTF	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
B PECC	R2 MTF	RMedP	MEDICAL	LOGISTICS Services	COI Services
B PECC	R2 MTF	Patient Movement Request	MEDICAL	LOGISTICS Services	COI Services
B PECC	R2 MTF	MEDLOG Information	MEDICAL	LOGISTICS Services	COI Services
DIVISION PATIENT EVACUATION COORDINATION CELL (D PECC) - AIR LIAISON OFFICER(ALO)					
D PECC	ALO	Release of Assets Request	Requests & Responses	Air Services	COI Services
ALO	D PECC	Release of Assets Authority	Requests & Responses	Air Services	COI Services
ALO	D PECC	ETA Report	Requests & Responses	LAND Services	COI Services
ALO	D PECC	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
D PECC	ALO	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
D PECC	ALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
D PECC	ALO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
D PECC	ALO	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
D PECC	ALO	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services
D PECC	ALO	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - AIR LIAISON OFFICER (ALO)					
B PECC	ALO	Release of Assets Request	Requests & Responses	Air Services	COI Services
ALO	B PECC	Release of Assets Authority	Requests & Responses	Air Services	COI Services
ALO	B PECC	ETA Report	Requests & Responses	LAND Services	COI Services
ALO	B PECC	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	ALO	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	ALO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
B PECC	ALO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	ALO	Office Collaboration (Audio)	Collaboration	Audio-Based Communication Services	Core Services
B PECC	ALO	Office Collaboration (AV)	Collaboration	Video-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
B PECC	ALO	Office Collaboration (Chat)	Collaboration	Text-Based Collaboration Services	Core Services
AIR LIAISON OFFICER (ALO)- AIR OPERATIONS CENTRE (AO)					
ALO	AO	MEDEVAC Tasking Order	Tasking & Orders	Air Services	COI Services
AO	ALO	ETA Report	Requests & Responses	LAND Services	COI Services
AO	ALO	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
ALO	AO	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
ALO	AO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
ALO	AO	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
AIR OPERATIONS CENTRE (AO) - AIR MEDICAL EVACUATION ASSET (AMEA)					
AO	AMEA	MEDEVAC Tasking Order	Tasking & Orders	Air Services	COI Services
AO	AMEA	Launch Authority	Tasking & Orders	Air Services	COI Services
AMEA	AO	ETA Report	Requests & Responses	LAND Services	COI Services
AMEA	AO	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
AO	AMEA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
AIR MEDICAL EVACUATION ASSET (AMEA) - POINT OF WOUNDING (POW)					
AMEA	POW	ETA Report	Requests & Responses	LAND Services	COI Services
AMEA	POW	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
AMEA	POW	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
AIR MEDICAL EVACUATION ASSET (AMEA) - EMERGENCY EVACUATION POINTAIR/LAND (EEP)					
AMEA	EEP	ETA Report	Requests & Responses	LAND Services	COI Services
EEP	AMEA	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
AMEA	EEP	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - BATTLE GROUP HEADQUARTERS (BG HQ)					
B PECC	BG HQ	ETA Report	Requests & Responses	LAND Services	COI Services
B PECC	BG HQ	MEDEVAC Tasking Notification	MEDICAL	LOGISTICS Services	COI Services
BG HQ	B PECC	MEDEVAC Request	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	BG HQ	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	BG HQ	Informal Message	Informal Messaging	Informal Messaging Services	Core Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
B PECC	BG HQ	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
BATTLE GROUP HEADQUARTERS (BG HQ) - COMPANY HEADQUARTERS (Coy HQ)					
BG HQ	Coy HQ	ETA Report	Requests & Responses	Tasking & Order Services	COI Services
Coy HQ	BG HQ	9 Liner Report	Reports	Tasking & Order Services	COI Services
Coy HQ	BG HQ	MIST Report	Reports	Tasking & Order Services	COI Services
BI-DIRECTIONAL					
BG HQ	Coy HQ	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
BG HQ	Coy HQ	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
COMPANY HEADQUARTERS (Coy HQ) - UNIT AID POST (UAP)					
Coy HQ	UAP	MEDEVAC Request	MEDICAL	LOGISTICS Services	COI Services
UAP	Coy HQ	CASREP	MEDICAL	LOGISTICS Services	COI Services
UAP	Coy HQ	MEDSITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
Coy HQ	UAP	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
Coy HQ	UAP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
COMPANY HEADQUARTERS (Coy HQ) - POINT OF WOUNDING (POW)					
Coy HQ	POW	ETA Report	Requests & Responses	Tasking & Order Services	COI Services
POW	Coy HQ	SALTA Report	Reports	Tasking & Order Services	COI Services
BI-DIRECTIONAL					
Coy HQ	POW	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
UNIT AID POST (UAP) - UNIT AMBULANCE (UA)					
UAP	UA	MEDEVAC Tasking Order	Tasking & Orders	LAND Services	COI Services
UAP	UAP	CASREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
UAP	UA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
UAP	UA	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
UNIT AID POST - EMERGENCY EVACUATION POINT AIR/LAND AIR/LAND (EEP)					
UA	EEP	ETA Report	Requests & Responses	Tasking & Order Services	COI Services
UA	EEP	CASREP	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
UA	EEP	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
UA	EEP	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
BRIGADE PATIENT EVACUATION COORDINATION CELL (B PECC) - BRIGADE MEDEVAC UNIT (BMU)					
B PECC	BMU	MEDEVAC Request	Tasking & Orders	LAND Services	COI Services
BMU	B PECC	ETA Report	Requests & Responses	LAND Services	COI Services
BMU	B PECC	CASREP	MEDICAL	LOGISTICS Services	COI Services
BMU	B PECC	MEDSITREP	MEDICAL	LOGISTICS Services	COI Services
BI-DIRECTIONAL					
B PECC	BMU	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
B PECC	BMU	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
B PECC	BMU	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
BRIGADE MEDEVAC UNIT (BMU)- EVACUATION UNIT AMBULANCE (EUA)					
BMU	EUA	MEDEVAC Tasking Order	Tasking & Orders	Air Services	COI Services
EUA	BMU	ETA Report	Requests & Responses	LAND Services	COI Services
EUA	BMU	CASREP	MEDICAL	LOGISTICS Services	COI Services

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
BI-DIRECTIONAL					
BMU	EUA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
BMU	EUA	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
EMERGENCY EVACUATION POINT Air/Land (EEP) - EVACUATION UNIT AMBULANCE (EUA)					
EEP	EUA	CASREP	MEDICAL	LOGISTICS Services	COI Services
EUA	EEP	ETA Report	Requests & Responses	LAND Services	COI Services
BI-DIRECTIONAL					
EEP	EUA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services
EEP	EUA	Instant Message	Instant Messaging	Text-Based Collaboration Services	Core Services
POINT OF WOUNDING (POW) - UNIT AMBULANCE (UA)					
POW	UA	CASREP	MEDICAL	LOGISTICS Services	COI Services
UA	POW	ETA Report	Requests & Responses	LAND Services	COI Services
BI-DIRECTIONAL					
POW	UA	Voice (secure)	Voice	Audio-Based Communication Services	Core Services

Table C-11: Medical Support in a MJO+ Scenario Product Dissemination and Consumption

IER: LAND C2 ENTITIES TO NON-NATO ENTITIES

30. Figure 4-5 depicts bi-directional product dissemination relating to the H2H services and unidirectional product dissemination for liaison, coordination and deconfliction between land C2 entities to non NATO entities. The bi-directional black arrows represent products sent and consumed from the land C2 entities to non NATO entities. The unidirectional red and green arrows represents products sent and consumed from/to land C2 entities and non NATO entities.

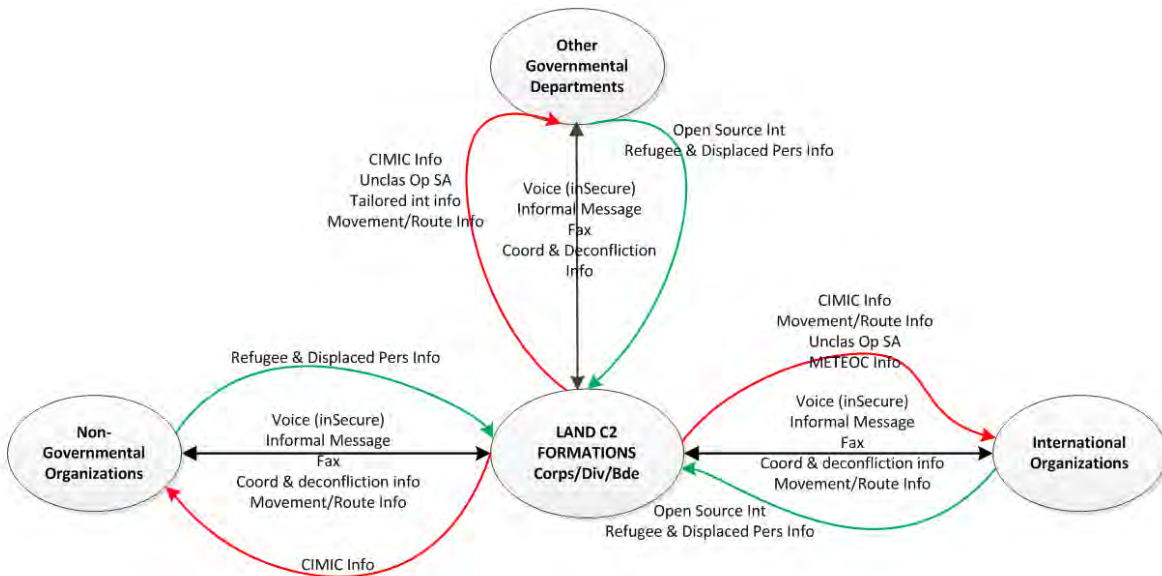


Figure 4-5: Bi-directional & Unidirectional Product Land C2 and non NATO Entities

31. Depicted in the table 4-5 are the bi-directional and unidirectional information product exchange relating to land C2 entities and non-NATO entities as introduced in Figure 4-5.

NATO UNCLASSIFIED
DRAFT

ANNEX C TO
 MC 0640

IER From	IER To	IE Product	User Service Definition Operational Capability	Technical Service Level 2	Technical Service Level 1
LAND C2 FORMATIONS (CORPS/DIVISION/BRIGADE) (LC2 FMN) - OTHER GOVERNMENTAL DEPARTMENTS (OGD)					
LC2 FMN	OGD	CIMIC INFO	Reports	CIMIC Services	COI Enabling Services
LC2 FMN	OGD	Unclassified Operational Situational Awareness	Situational Awareness	Situation Awareness Services	COI Enabling Services
LC2 FMN	OGD	Tailored intelligence information	Reports	JISR Services	COI Enabling Services
LC2 FMN	OGD	Movement/Route Information	Reports	Logistics Services	COI Enabling Services
OGD	LC2 FMN	Open Source Intelligence	Reports	JISR Services	COI Enabling Services
OGD	LC2 FMN	Refugee & Displaced Persons Information	Reports	CIMIC Services	COI Enabling Services
BI-DIRECTIONAL					
LC2 FMN	OGD	Voice (Secure)	Voice	Audio-Based Communication Services	Core Services
LC2 FMN	OGD	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
LC2 FMN	OGD	Fax	Fax	Fax Services	Core Services
LC2 FMN	OGD	Coordination & Deconfliction information	Reports	CIMIC Services	Core Services
LAND C2 FORMATIONS (CORPS/DIVISION/BRIGADE) (LC2 FMN) - INTERNATIONAL ORGANIZATIONS (IO)					
LC2 FMN	IO	CIMIC INFO	Reports	CIMIC Services	COI Enabling Services
LC2 FMN	IO	Unclassified Operational Situational Awareness	Situational Awareness	Situation Awareness Services	COI Enabling Services
LC2 FMN	IO	METEOC Information	Reports	Environmental Services	COI Enabling Services
IO	LC2 FMN	Open Source Intelligence	Reports	JISR Services	COI Enabling Services
IO	LC2 FMN	Refugee & Displaced Persons Information	Reports	CIMIC Services	COI Enabling Services
BI-DIRECTIONAL					
LC2 FMN	IO	Voice (inSecure)	Voice	Audio-Based Communication Services	Core Services
LC2 FMN	IO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
LC2 FMN	IO	Fax	Fax	Fax Services	Core Services
LC2 FMN	IO	Coordination & Deconfliction information	Reports	CIMIC Services	Core Services
LC2 FMN	IO	Movement/Route Information	Reports	Logistics Services	COI Enabling Services
LAND C2 FORMATIONS (CORPS/DIVISION/BRIGADE) (LC2 FMN) - NON-GOVERNMENTAL ORGANIZATIONS (NGO)					
LC2 FMN	NGO	CIMIC INFO	Reports	CIMIC Services	COI Enabling Services
NGO	LC2 FMN	Open Source Intelligence	Reports	JISR Services	COI Enabling Services
NGO	LC2 FMN	Refugee & Displaced Persons Information	Reports	CIMIC Services	COI Enabling Services
BI-DIRECTIONAL					
LC2 FMN	NGO	Voice (inSecure)	Voice	Audio-Based Communication Services	Core Services
LC2 FMN	NGO	Informal Message	Informal Messaging	Informal Messaging Services	Core Services
LC2 FMN	NGO	Fax	Fax	Fax Services	Core Services
LC2 FMN	NGO	Coordination & Deconfliction information	Reports	CIMIC Services	Core Services
LC2 FMN	NGO	Movement/Route Information	Reports	Logistics Services	COI Enabling Services

Table 4-5: Bi-directional & Unidirectional Product Land C2 and non NATO Entities

CONNECTIVITY DIAGRAMS FOR C2 SERVICES IMPLEMENTATION

1. Annex D depicts the user services and connectivity requirements for typical land tactical functions like Logistics, (Joint) ISR and Fire Support. For each functions, a table depicts the services and transmissions required between the tactical C2 echelons. Service and connectivity requirements are also visualized for an MJO+ and a VJTF (L) scenario.

SERVICE PROVISION FOR LOGISTICS

2. This section describes the service requirements and related transmission requirements for Logistics, focusing on the C2 elements JLSG, LANDCOM G4, Corps Rear Support Group (CRSG), Divisional Support Group (DSG), BDE Support Group (BSG), A2 Echelon (A2C) at BG and A1 Echelon (A1E) at COY Level. Table D-1-1 depicts the services matrix, Table D-1-2 shows the transmission bearer matrix. Figures D-1-1 puts both service and transmission requirements in a graphical context for an MJO+ scenario, while figure D-1-2 applies them to the VJTF (L) scenario.

SERVICE TYPE	JLSG	LC G4	CRSG	DSG	BSG	A2E	A1E	
Joint Services	X	X						
Logistics Services	X	X	X	X	X	X	X	
ERP Services	X	X	X	X	X			
Operational Planning Services	X	X	X	X	X	X	X	
Tasking and Order Services	X	X	X	X	X	X	X	
Situational Awareness Service	X	X	X	X	X	X	X	
Battlespace Information Services	X	X	X	X	X	X	X	
Audio-Based Communication Services	X	X	X	X	X	X	X	
Military Messaging Service	X	X	X	X	X			
Informal Messaging Services	X	X	X	X	X			
Text-Based Collaboration Services	X	X	X	X	X	X	X	
Video-Based Communication Services	X	X	X	X	X			
Content Management Services	X	X						
Fax Services	X	X	X	X	X			

Table D-1-1: Services in Support of Land Tactical Logistics

SERVICE TYPE	JLS G	LC G4	CRS G	DS G	BS G	A2 E	A1 E	Remarks and Examples
Transmission Services								
Wired Transmission Services								
Wired Local Area Transmission Services	X	X	X	X	X	X		This applies down to BDE Could even be BG (LAN switching)
Wired Metropolitan Area Transmission Services	X	X	X					Corps & above using leased lines to supply outdets
Wired Wide Area Transmission Services	X	X	X	(X)	(X)			Corps & above using leased line into NGCS; all elements shall be able to use wired bearers if prepared and available
Wireless Line of Sight (LOS) Static Transmission Services								
Wireless LOS Static Narrowband Transmission Services								
Wireless LOS Static Wideband Transmission Services	X	X	X					DLOS and HC-BLOS between locations
Wireless Line of Sight (LOS) Mobile Transmission Services								
Wireless LOS Mobile Narrowband Transmission Services				X	X	X	X	TACCIS at BDE & below (HF, VHF, UHF
Wireless LOS Mobile Wideband Transmission Services				X	X			HF, UHF
Wireless Beyond Line of Sight (BLOS) Static Transmission Services								
Wireless BLOS Static Narrowband Transmission Services	X	X	X					HF, TACSAT, Commercial satellite
Wireless BLOS Static Wideband Transmission Services	X	X	X	X	X			MILSATCOM (LANDCOM down to Corps) - note the static bit
Wireless Beyond Line of Sight (BLOS) Mobile Transmission Services								
Wireless BLOS Mobile Narrowband Transmission Services				X	X	X	X	HF, TACSAT Commercial satellite
Wireless BLOS Mobile Wideband Transmission Services								MILSATCOM on the move

Table D-1-2: Transmission Services in Support of Land Tactical Logistics

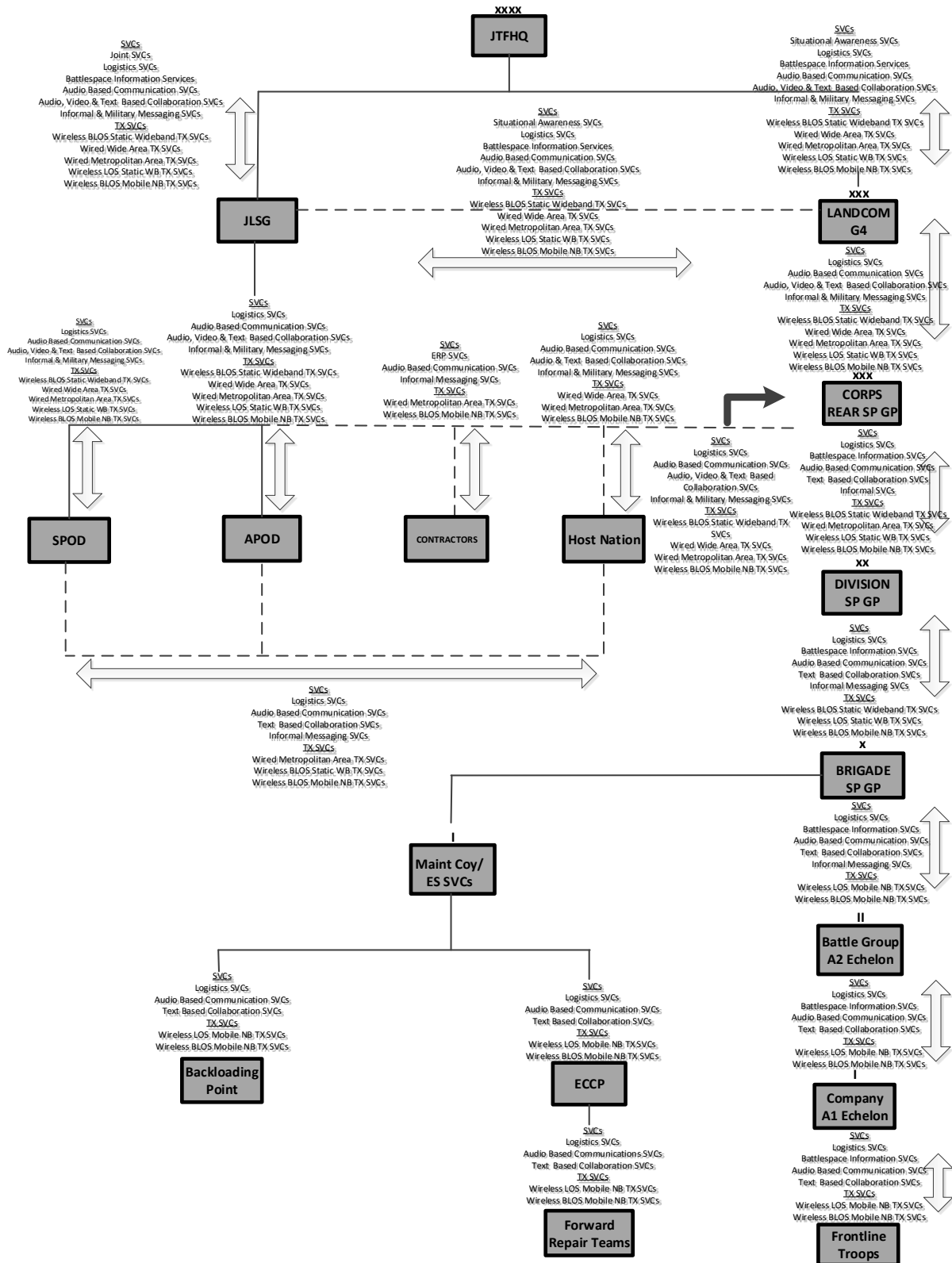


Figure D-1-1: Services and Transmission in Support of Logistics (MJO+ Scenario)

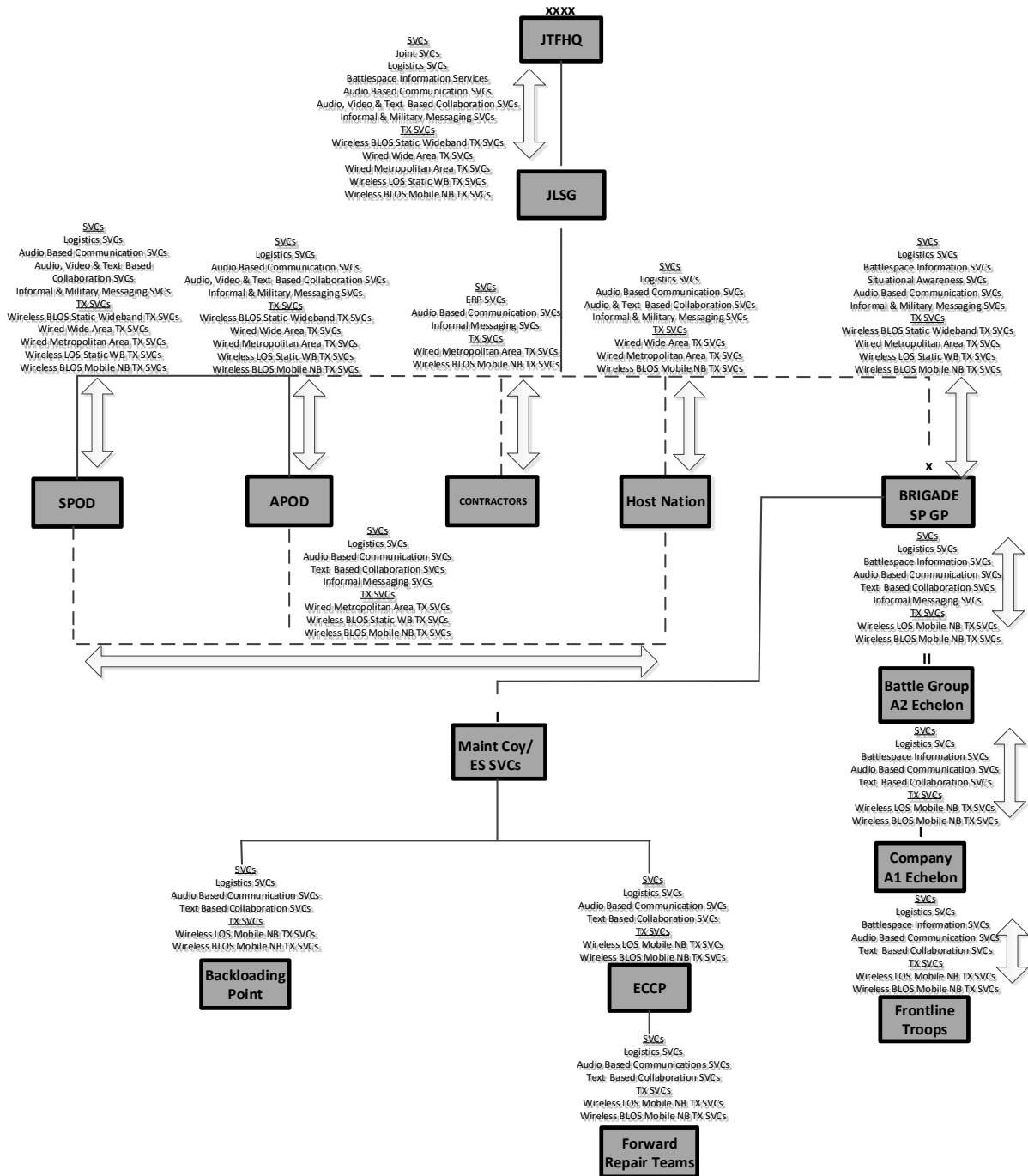


Figure D-1-2: Services and Transmission in Support of Logistics (VJTF (L) Scenario)

SERVICE PROVISION FOR INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE.

3. This section describes the service requirements and related transmission requirements for (Joint) Intelligence, Surveillance and Reconnaissance. The services matrix focuses on ISR relevant C2 elements Landcom Land Intelligence Fusion Centre (LIFC), Corps Intelligence Fusion Centre (CIFC), All Sources Analysis Cell (ASAC, at DIV and BDE level), BG Intelligence Support Section (BGISS), and COIST COY Intelligence Support Team (COIST). Table D-2-1 depicts the services matrix, Table D-2-2 shows the transmission bearer matrix. Figures D-2-1 puts both service and transmission requirements in a graphical context for an MJO+ scenario, while figure D-2-2 applies them to the VJTF scenario.

SERVICE TYPE	LIFC	CIFC	ASAC	BGISS	COIST	
Joint Services	X	X	X			
JISR Services	X	X	X	X	X	
Electronic Warfare Services	X	X	X			
Operational Planning Services	X	X	X	X	X	
Tasking and Order Services	X	X	X	X	X	
Situational Awareness Service	X	X	X	X	X	
Battlespace Information Services	X	X	X	X	X	
Environmental Services	X	X	X			
Audio-Based Communication Services	X	X	X	X	X	
Military Messaging Service	X	X	X			
Informal Messaging Services	X	X	X			
Text-Based Collaboration Services	X	X	X	X	X	
Video-Based Communication Services	X	X	X			
Content Management Services	X	X	X			
Fax Services			X			

Table D-2-1: Services in Support of Land Tactical ISR

SERVICE TYPE	LIFC	CIFC	ASAC	BGISS	COIST	Remarks and Examples
Wired Transmission Services						
Wired Local Area Transmission Services	X	X	X	X		This applies down to Bde Could even be BG (LAN switching)
Wired Metropolitan Area Transmission Services	X	X				Corps & above using leased lines to supply outlets
Wired Wide Area Transmission Services	X	X	(X)			Corps & above using leased line into NGCS; all elements shall be able to use wired bearers if prepared and available
Wireless Line of Sight (LOS) Static Transmission Services						
Wireless LOS Static Narrowband Transmission Services						
Wireless LOS Static Wideband Transmission Services	X	X	(X)			DLOS and HC-BLOS between locations
Wireless Line of Sight (LOS) Mobile Transmission Services						
Wireless LOS Mobile Narrowband Transmission Services			X	X	X	TACCIS at BDE & below (HF, VHF, UHF
Wireless LOS Mobile Wideband Transmission Services			X	X		HF, UHF
Wireless Beyond Line of Sight (BLOS) Static Transmission Services						
Wireless BLOS Static Narrowband Transmission Services	X	X				HF, TACSAT, Commercial satellite
Wireless BLOS Static Wideband Transmission Services	X	X	X			MILSATCOM (LANDCOM down to Corps) - note the static bit
Wireless Beyond Line of Sight (BLOS) Mobile Transmission Services						
Wireless BLOS Mobile Narrowband Transmission Services			X	X	X	HF, TACSAT Commercial satellite
Wireless BLOS Mobile Wideband Transmission Services						MILSATCOM on the move

Table D-2-2: Transmission Services in Support of Land Tactical ISR

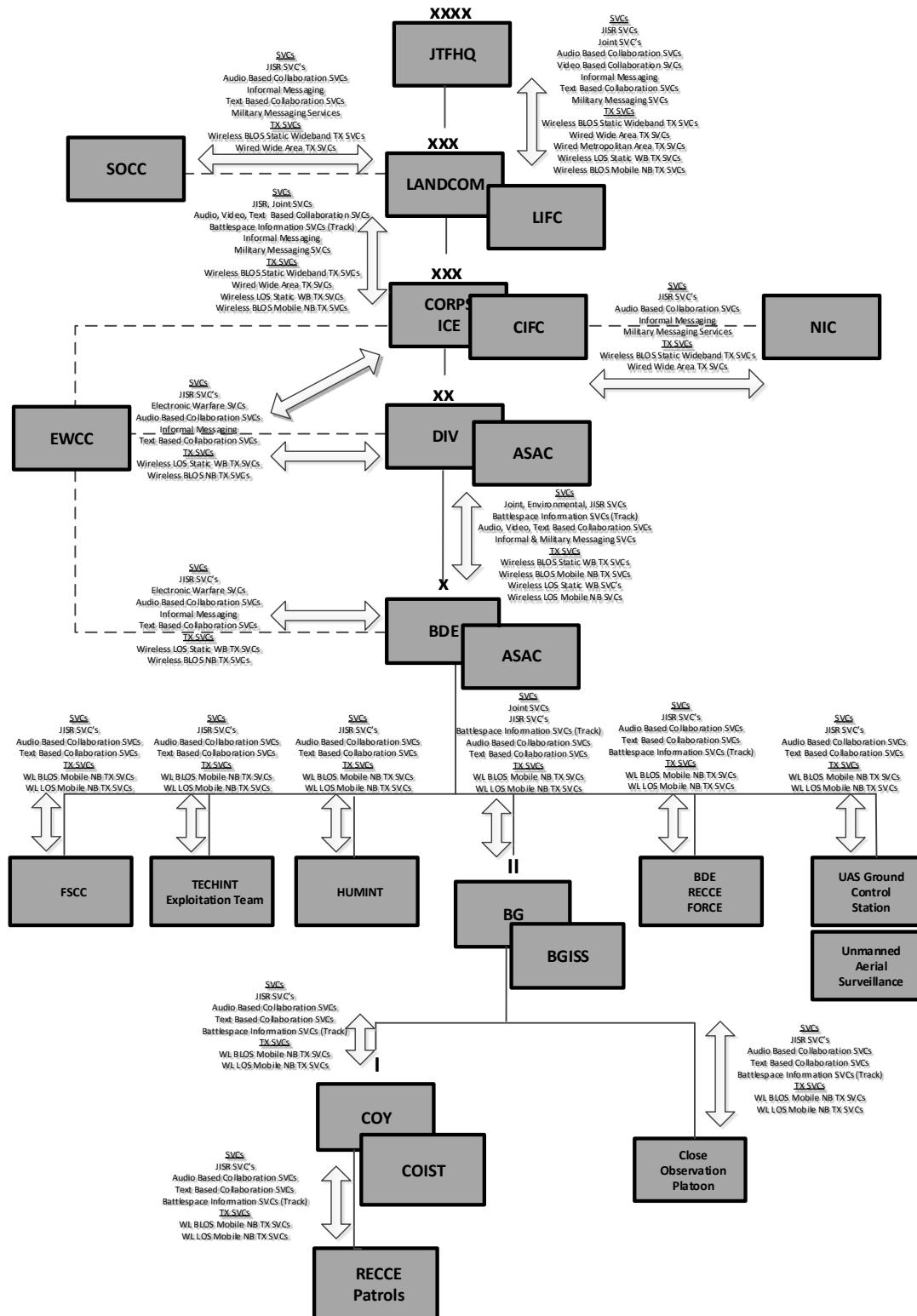


Figure D-2-1: Services and Transmission in Support of ISR (MJO+ Scenario)

SERVICE PROVISION FOR FIRE SUPPORT

4. This section describes the service requirements and related transmission requirements for (Joint) Fire support. The services matrix focuses on Fire Support relevant C2 elements Landcom (LC), the Corps Fire Sp Coord Centre/ Target Sp Cell (FSCC), the BDE level Joint Fires Cell JFCBDE, the BG Level Joint Fires Cell (JFCBG) and the COY level Fire Support Team (FST). Table D-3-1 depicts the services matrix, Table D-3-2 shows the transmission bearer matrix. Figures D-3-1 puts both service and transmission requirements in a graphical context for an MJO+ scenario, while figure D-3-2 applies them to the VJTF scenario.

SERVICE TYPE	LC	FSCC	FSpCC	JFCBGE	JFCBG	FSpT	
Operational Planning (Targeting) Services	X	X	X	X	X	X	
Land Services	X	X	X	X	X		
Airspace Management Services	X	X	X	X	X	X	
Environmental Services	X	X	X	X	X	X	
Tasking & Order Services (Operations Assessment Services)	X	X	X	X	X	X	
Audio-Based Communication Services	X	X	X	X	X	X	
Military Messaging Service	X	X	X	X			
Informal Messaging Services	X	X	X	X			
Text-Based Collaboration Services	X	X	X	X	X	X	
Video-Based Communication Services	X	X					
Content Management Services	X						

Table D-3-1: Services in Support of Fire Support

NATO UNCLASSIFIED
DRAFT

ANNEX D TO
Draft MC 0640

SERVICE TYPE	LC	FSCC	FSpCC	JFCBGE	JFCBG	FSpT	Remarks and Examples
Wired Transmission Services							
Wired Local Area Transmission Services	X	X	X	X	X		This applies down to Bde Could even be BG (LAN switching)
Wired Metropolitan Area Transmission Services	X	X					Corps & above using leased lines to supply outlets
Wired Wide Area Transmission Services	X	X	(X)	(X)			Corps & above using leased line into NGCS; all elements shall be able to use wired bearers if prepared and available
Wireless Line of Sight (LOS) Static Trans-mission Services							
Wireless LOS Static Narrowband Transmission Services							
Wireless LOS Static Wideband Transmission Services	X	X	(X)	(X)			DLOS and HC-BLOS between locations
Wireless (LOS) Mobile Transmission Services							
Wireless LOS Mobile Narrowband Transmission Services			X	X	X	X	TACCIS at BDE & below (HF, VHF, UHF
Wireless LOS Mobile Wideband Transmission Services			X	X			HF, UHF
Wireless Beyond Line Of Sight (BLOS) Static Transmission Services							
Wireless BLOS Static Narrowband Transmission Services	X	X					HF, TACSAT, Commercial satellite
Wireless BLOS Static Wideband Transmission Services	X	X	X	X			MILSATCOM (LANDCOM down to Corps) - note the static bit
Wireless BLOS Mobile Transmission Services							
Wireless BLOS Mobile Narrowband Transmission Services			X	X	X	X	HF, TACSAT Commercial satellite
Wireless BLOS Mobile Wideband Transmission Services							MILSATCOM on the move

Table D-3-2: Transmission Services in Fire Support

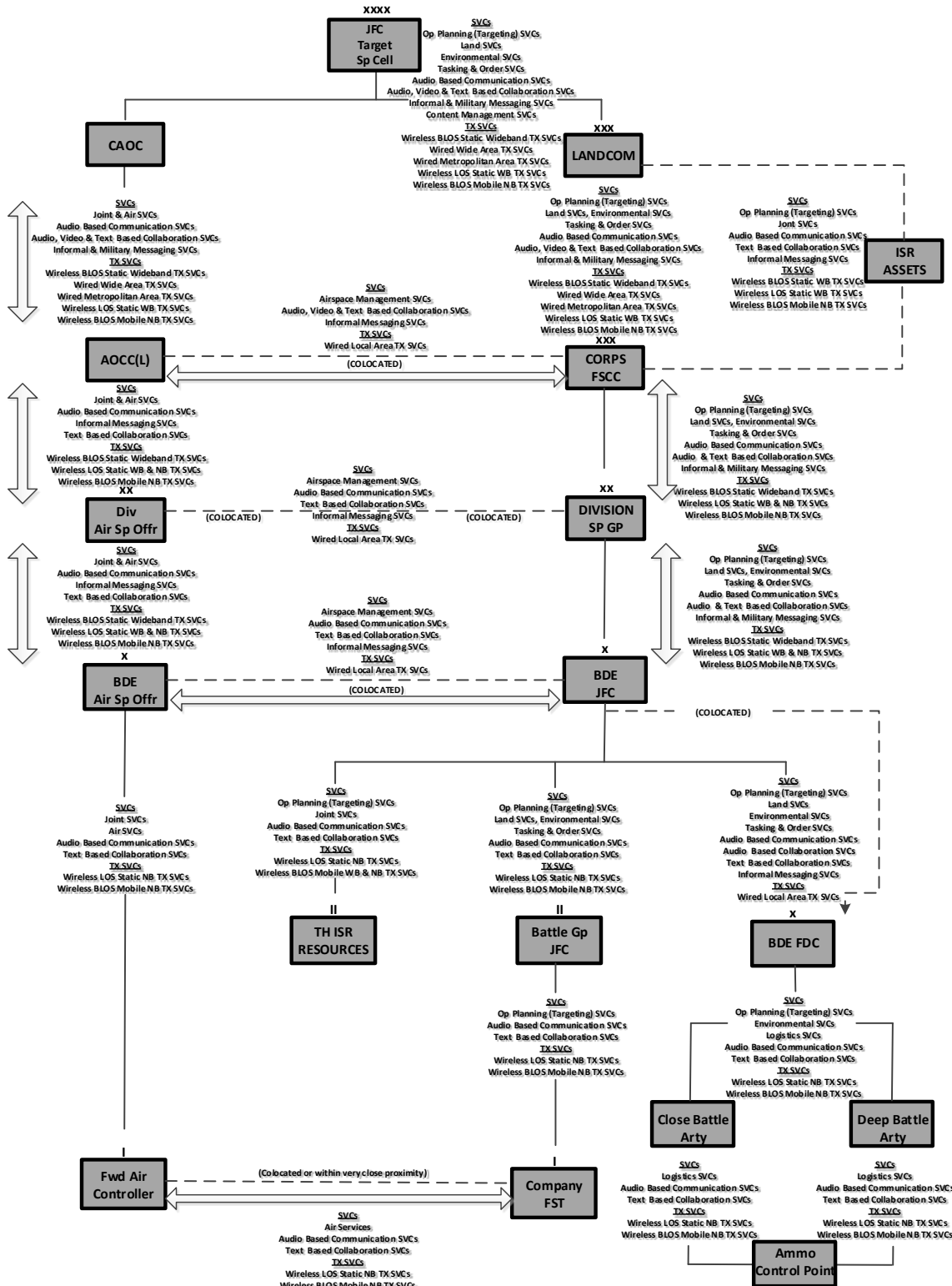


Figure D-3-1: Services and Transmission in Support of Fire Support (MJO+ Scenario)

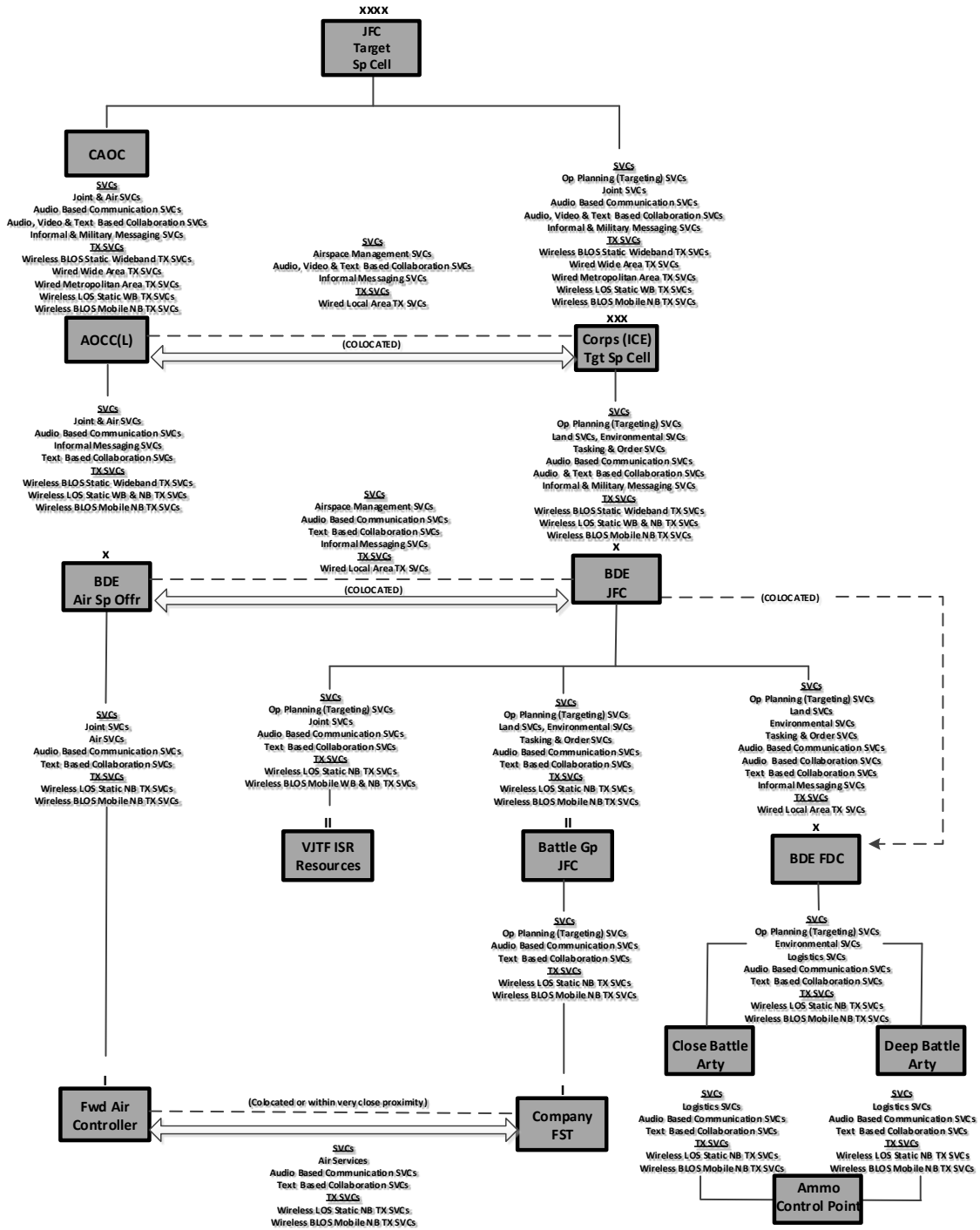


Figure D-3-2: Services and Transmission in Support of Fire Support (VJTf (L) Scenario)

SERVICE PROVISION FOR MEDICAL SUPPORT

5. This section describes the service requirements and related transmission requirements for Medical support. The services matrix focuses on relevant C2 elements in support of Medical, Landcom (LC) Senior Medical Advisor, Corps Patient Evacuation Coordination Center (CPECC), The Corps Role 3 Medical Treatment Facility (CR3MTF), the Division Patient Evacuation Coordination Centre (DPECC), the Patient Evacuation Coordination Centre at BDE level (BPECC), the Role 2 Medical Treatment Facility at BDE level (BR2MTF), BG Unit Aid Post (UAP), and the Team Medic at Point of Wounding (TM) Table D-4-1 depicts the services matrix, Table D-4-2 shows the transmission bearer matrix.

SERVICE TYPE	LC	CPECC	CR3MTF	DPECC	BPECC	BR2MTF	UAP	TM
Land Services		X	X	X	X	X	X	X
Air Services		X		X	X			
Logistics (Medical) Services	X	X	X	X	X	X	X	X
Tasking & Order Services				X	X		X	X
Audio-Based Communication Services	X	X	X	X	X	X	X	X
Military Messaging Service	X	X	X	X	X	X		
Informal Messaging Services	X	X	X	X	X	X		
Text-Based Collaboration Services	X	X	X	X	X	X	X	
Video-Based Communication Services	X	X	X	X	X	X		

Table D-4-1: Services for Medical Support

NATO UNCLASSIFIED
DRAFT

ANNEX D TO
 Draft MC 0640

SERVICE TYPE	LC	CPE CC	CR3MTF	DPECC	BPECC	BR2MTF	UAP	TM	Remarks and Examples
Wired Transmission Services									
Wired Local Area Transmission Services	X	X	X	X	X	X	X		This applies down to Bde Could even be BG (LAN switching)
Wired Metropolitan Area Transmission Services	X	X	X						Corps & above using leased lines to supply outdets
Wired Wide Area Transmission Services	X	X	X	X	X	X			Corps & above using leased line into NGCS; all elements shall be able to use wired bearers if prepared and available
Wireless Line of Sight (LOS) Static Transmission Services									
Wireless LOS Static Narrowband Transmission Services			X			X			
Wireless LOS Static Wideband Transmission Services	X	X	X	X	X	X			DLOS and HC-BLOS between locations
Wireless LOS Mobile Transmission Services									
Wireless LOS Mobile Narrowband Transmission Services				X	X		X	X	TACCIS at BDE & below (HF, VHF, UHF
Wireless LOS Mobile Wideband Transmission Services			X	X	X				HF, UHF
Wireless BLOS Static Transmission Services									
Wireless BLOS Static Narrowband Transmission Services	X	X							HF, TACSAT, Commercial satellite
Wireless BLOS Static Wideband Transmission Services	X	X	X	X	X	X			MILSATCOM (LANDCOM down to Corps) - note the static bit
Wireless BLOS Mobile Transmission Services									
Wireless BLOS Mobile Narrowband Transmission Services				X	X		X	X	HF, TACSAT Commercial satellite
Wireless BLOS Mobile Wideband Transmission Services									MILSATCOM on the move

Table D-4-2: Transmission Services in Medical Support

SERVICES REQUIREMENTS PER TYPE OF C2 ENTITY DEVELOPMENT

This Annex contains diagrams graphically depicting the minimum services expected for C2, intelligence, and support entities in the land environment. These services include Communication and Information Systems (CIS) capabilities and applications; technical services for communities of interest (CoI) (ie. mission information services); core services; and transmission services.

LANDCOM INTELLIGENCE FUSION CENTRE (LIFC)

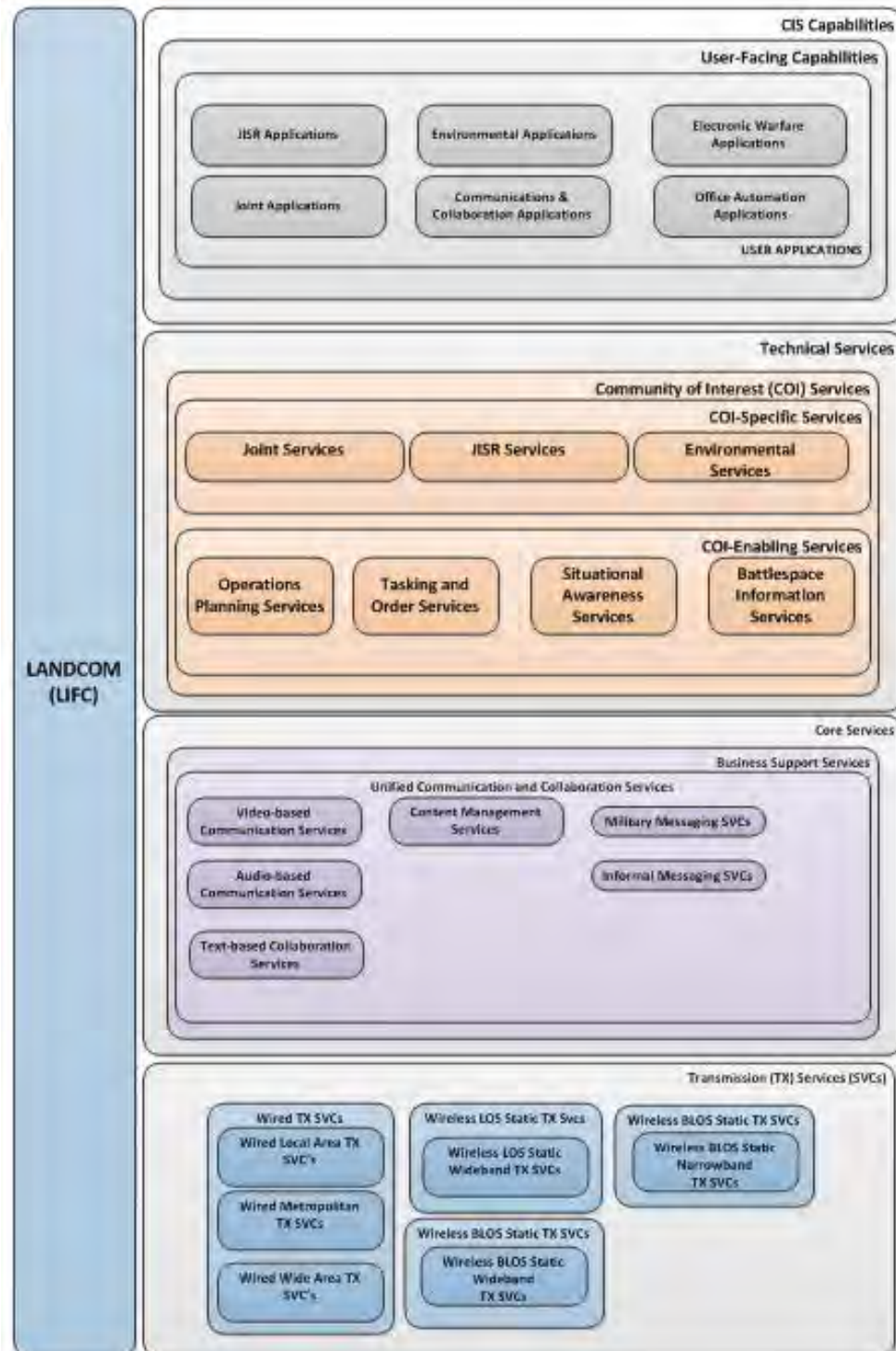


Figure E-1: LIFC Services Requirement

CORPS INTELLIGENCE FUSION CENTRE (CIFIC)

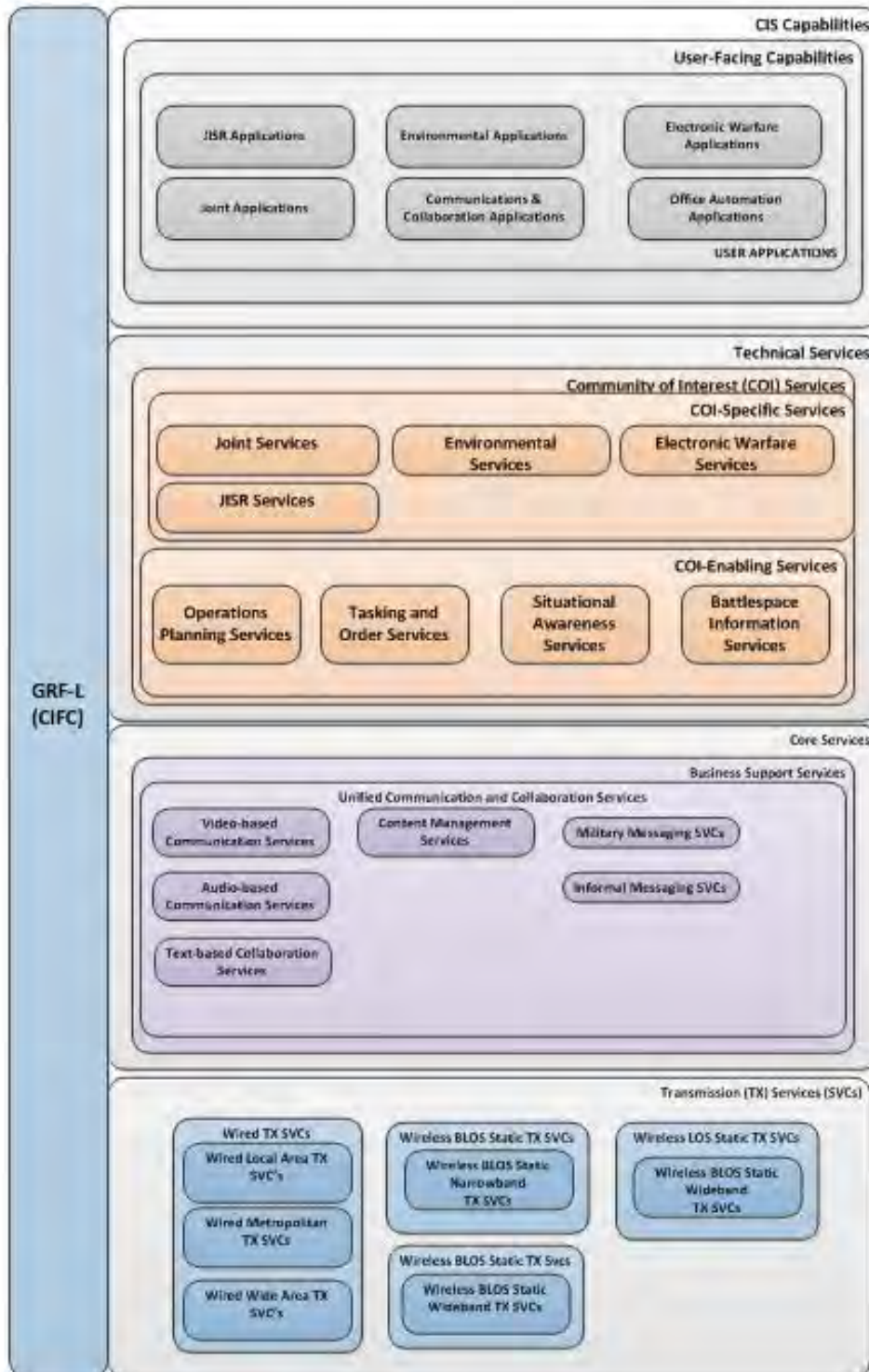


Figure E-2: CIFIC Services Requirement

DIVISION/BRIGADE (ALL SOURCES ANALYSIS CENTRE) (ASAC)

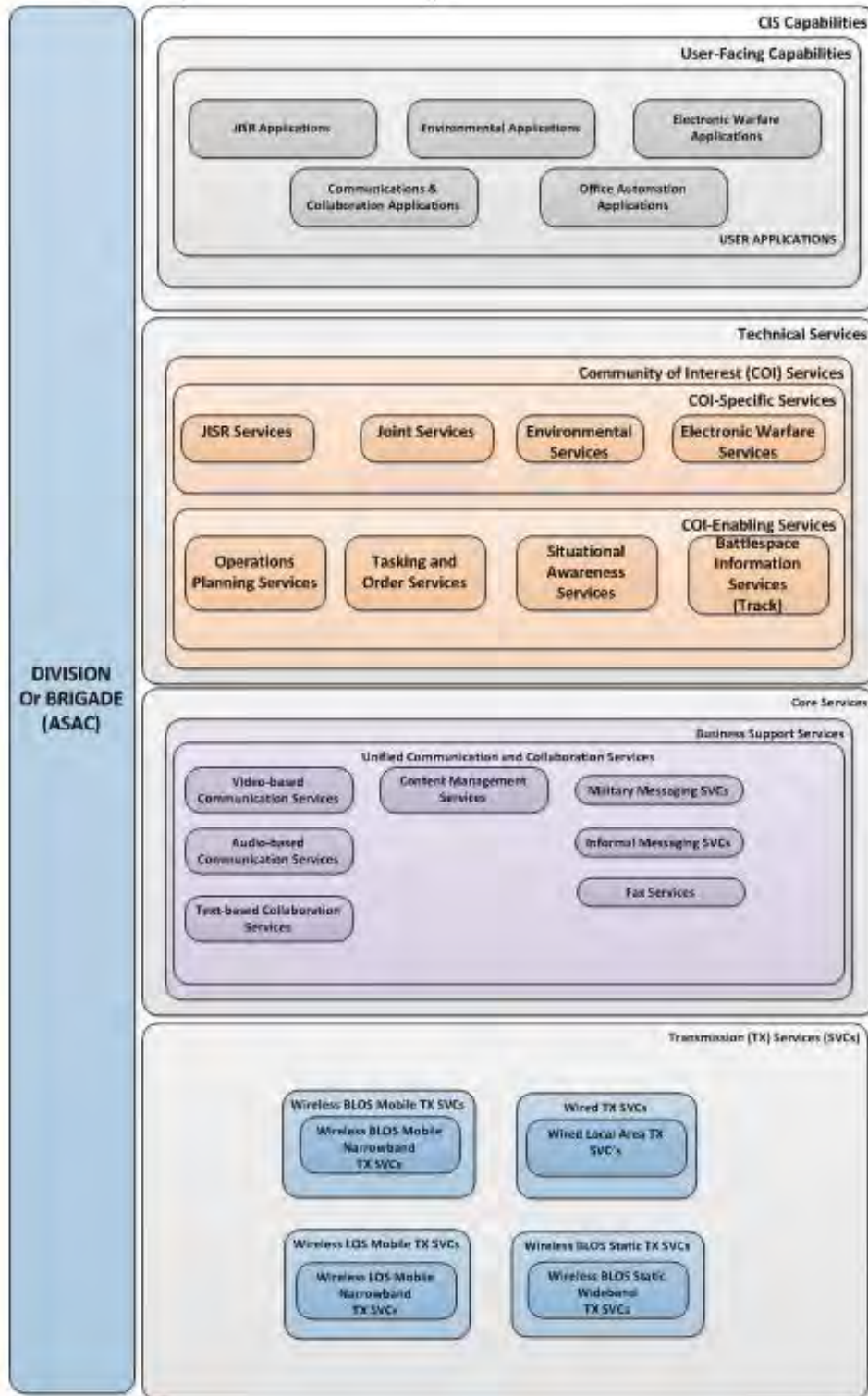


Figure E-3: ASAC Services Requirement

BATTLE GROUP INTELLIGENCE SUPPORT SECTION (BGISS)

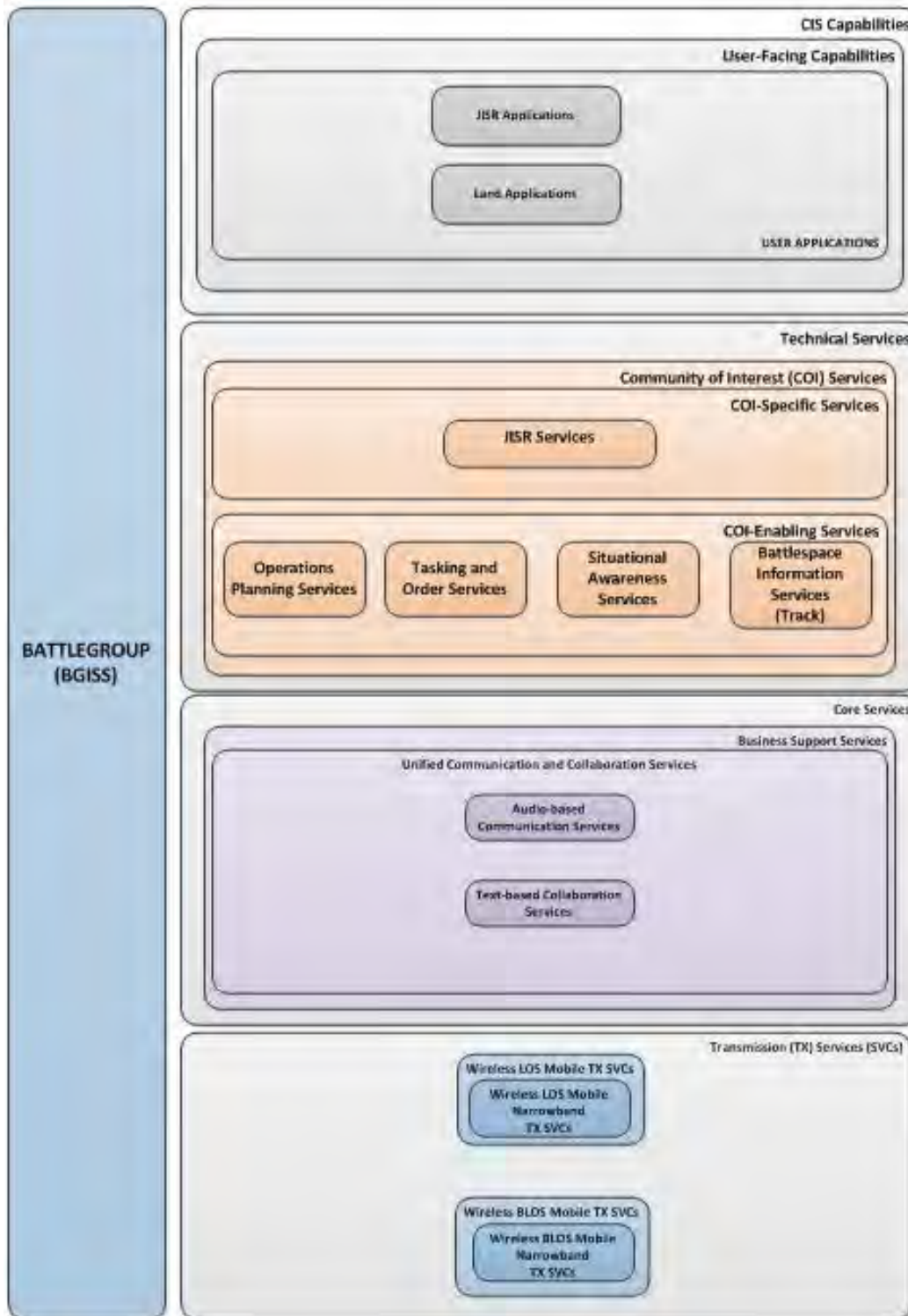


Figure E-4: BGISS Services Requirement

COMPANY INTELLIGENCE SUPPORT TEAM (COIST)

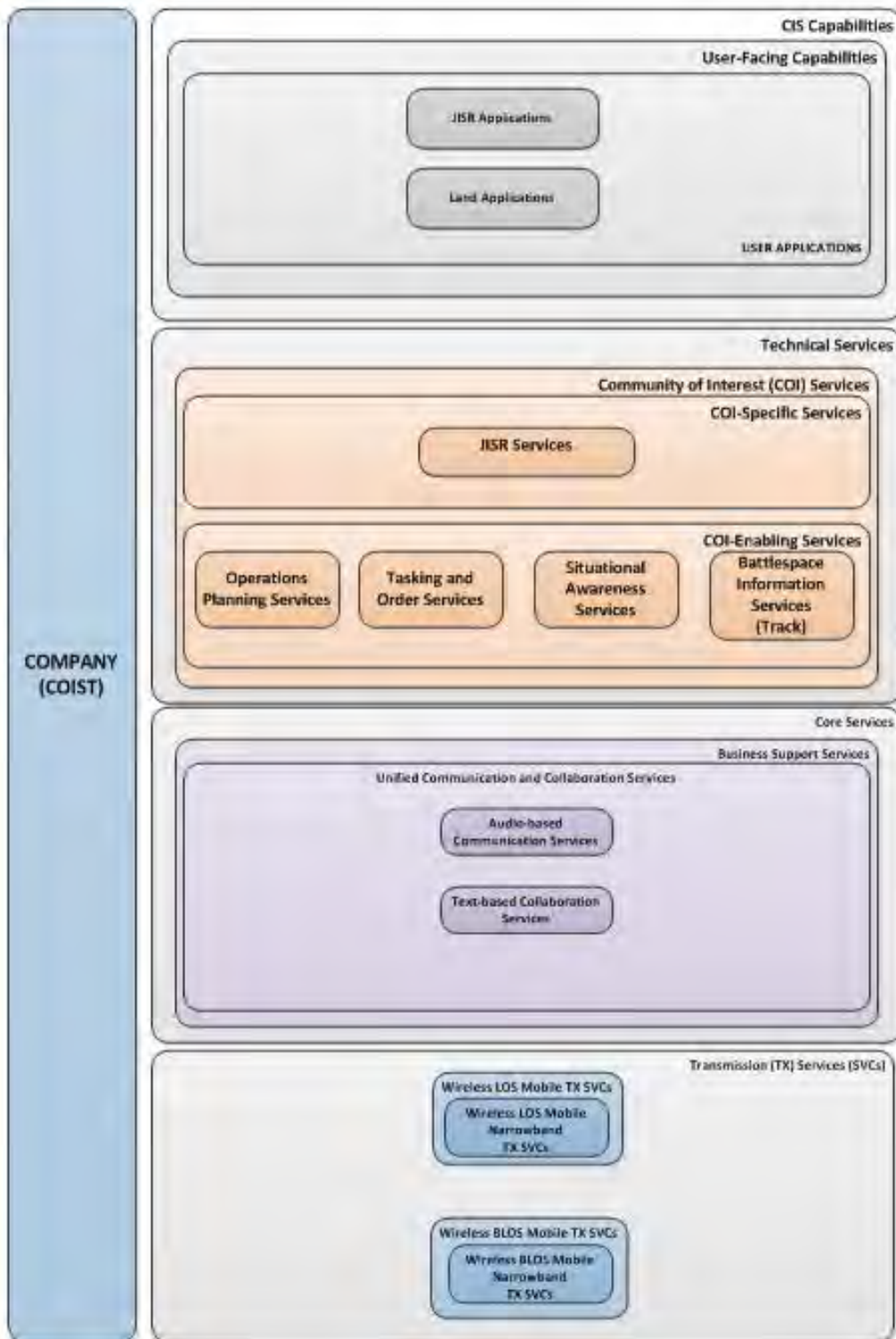


Figure E-5: COIST Services Requirement

LANDCOM FIRE SUPPORT

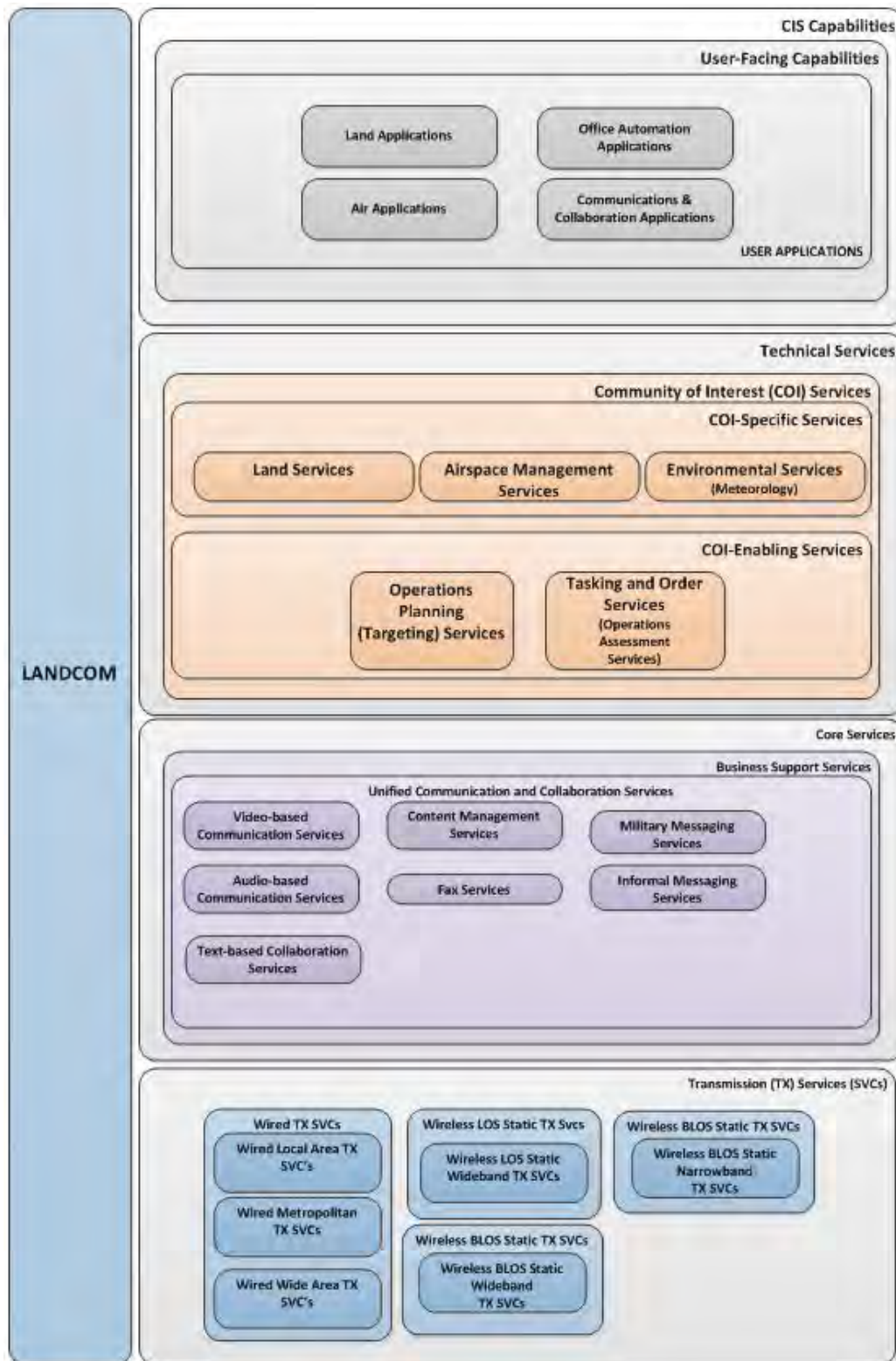


Figure E-6: LANDCOM Fire Support Services Requirement

CORPS FIRE SUPPORT CENTRE/TARGET SUPPORT CELL

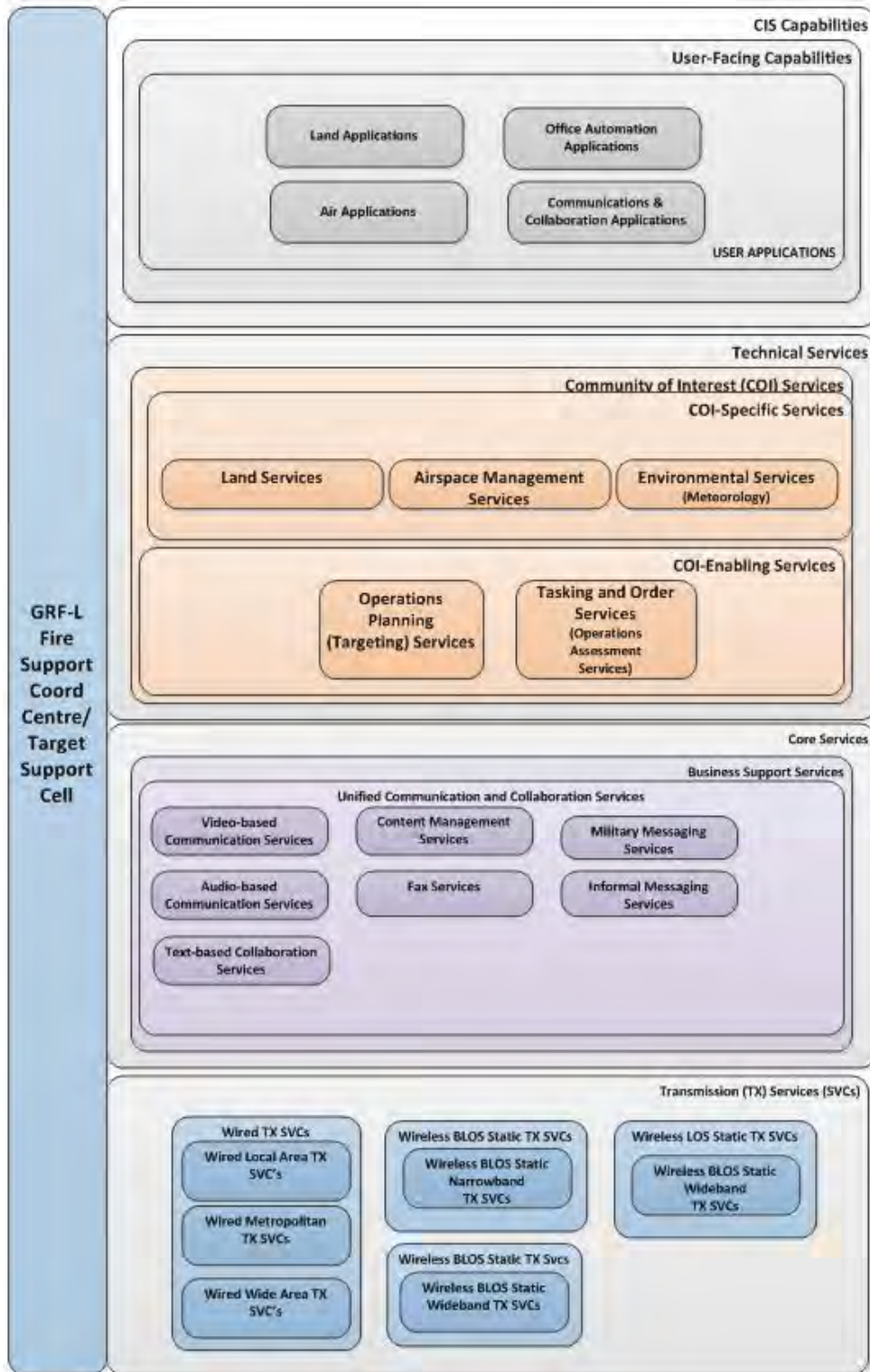


Figure E-7: Corps Fire Support Centre/Target Support Cell Services Requirement

DIVISION FIRE SUPPORT COORDINATION CENTRE

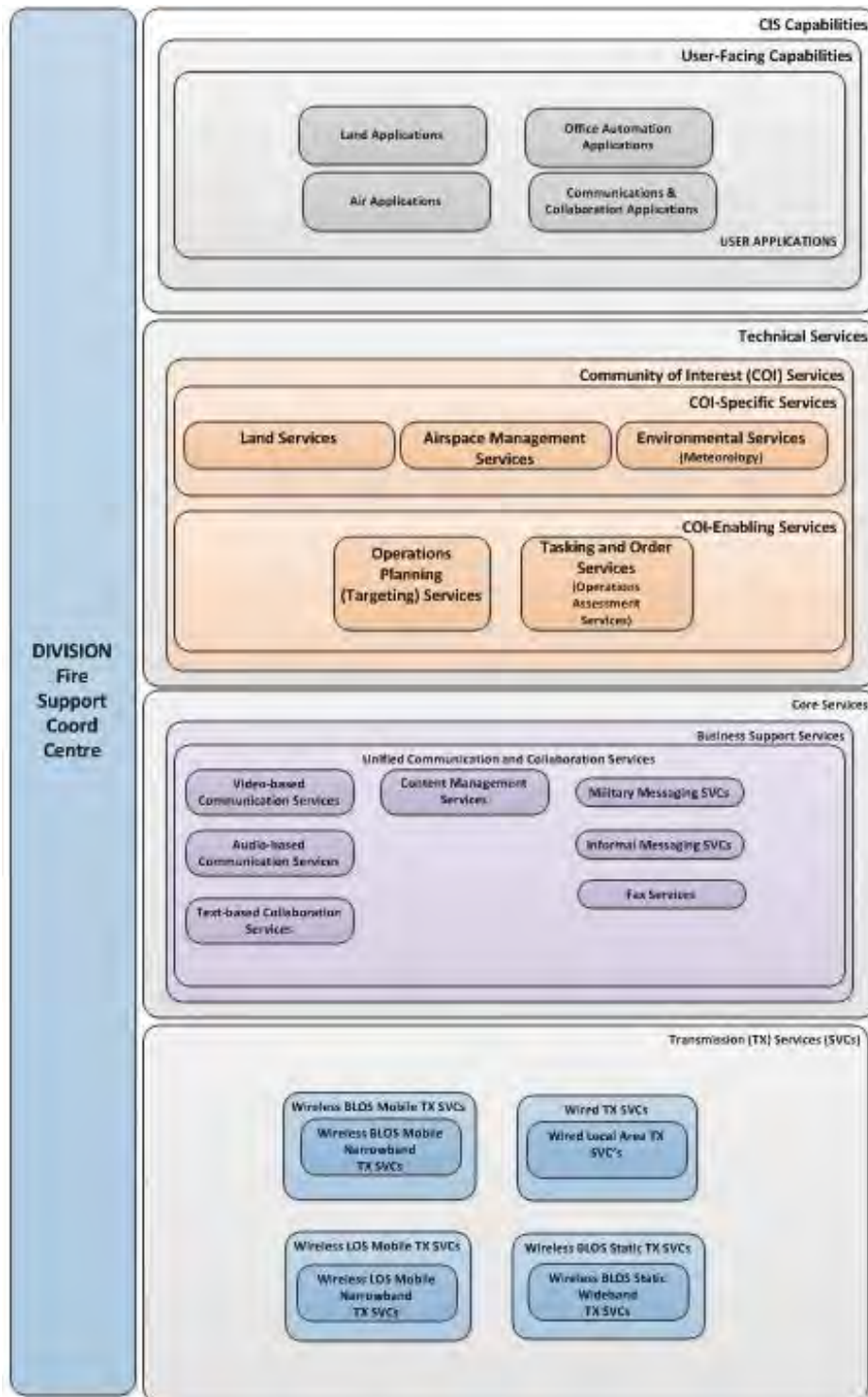


Figure E-8: Division Fire Support Coordination Centre Services Requirement

BRIGADE JOINT FIRES CELL

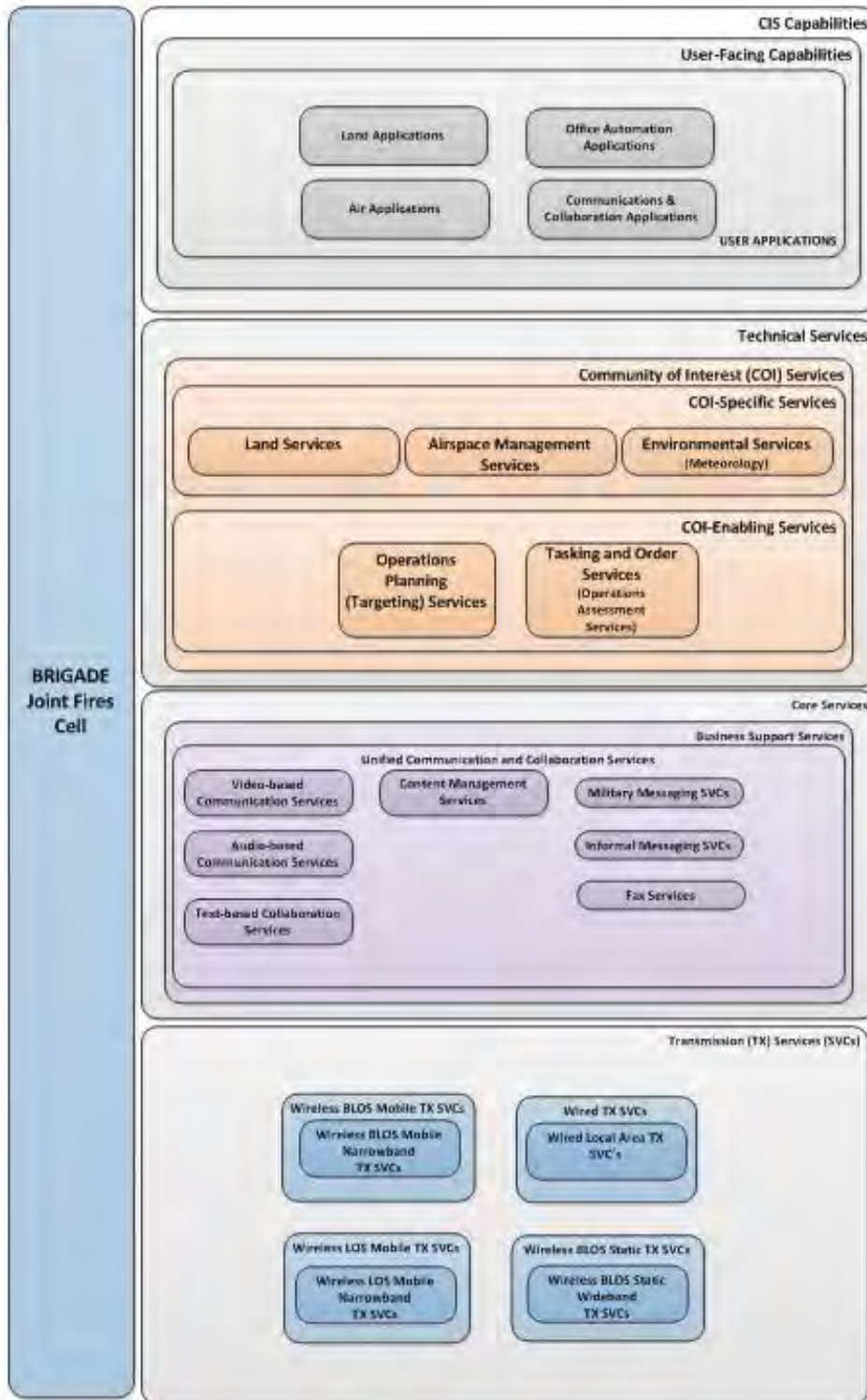


Figure E-9: Brigade Joint Fires Cell Services Requirement

BATTLE GROUP JOINT FIRES CELL

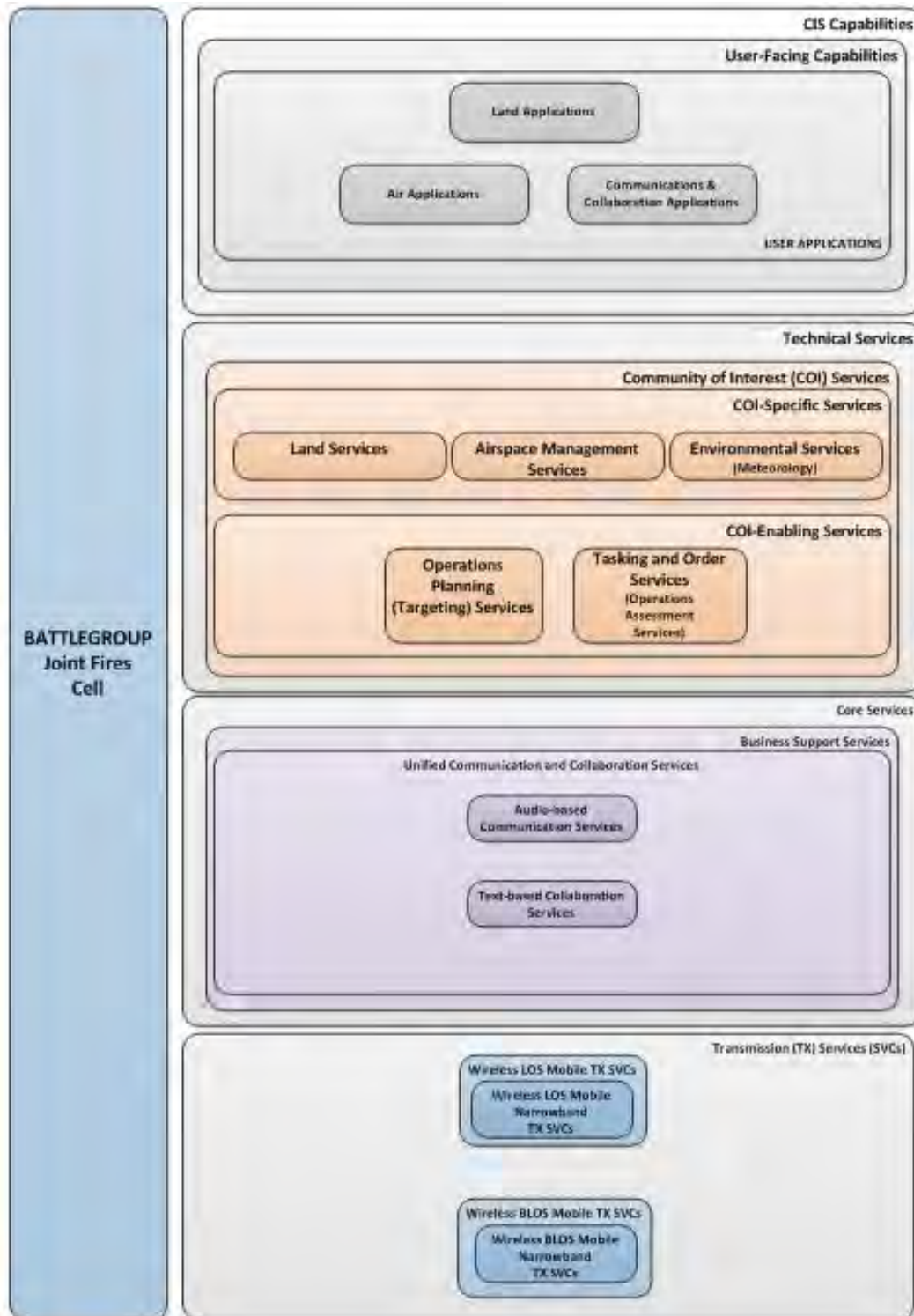


Figure E-10: Battle Group Joint Fires Cell Services Requirement

COMPANY FIRE SUPPORT TEAM

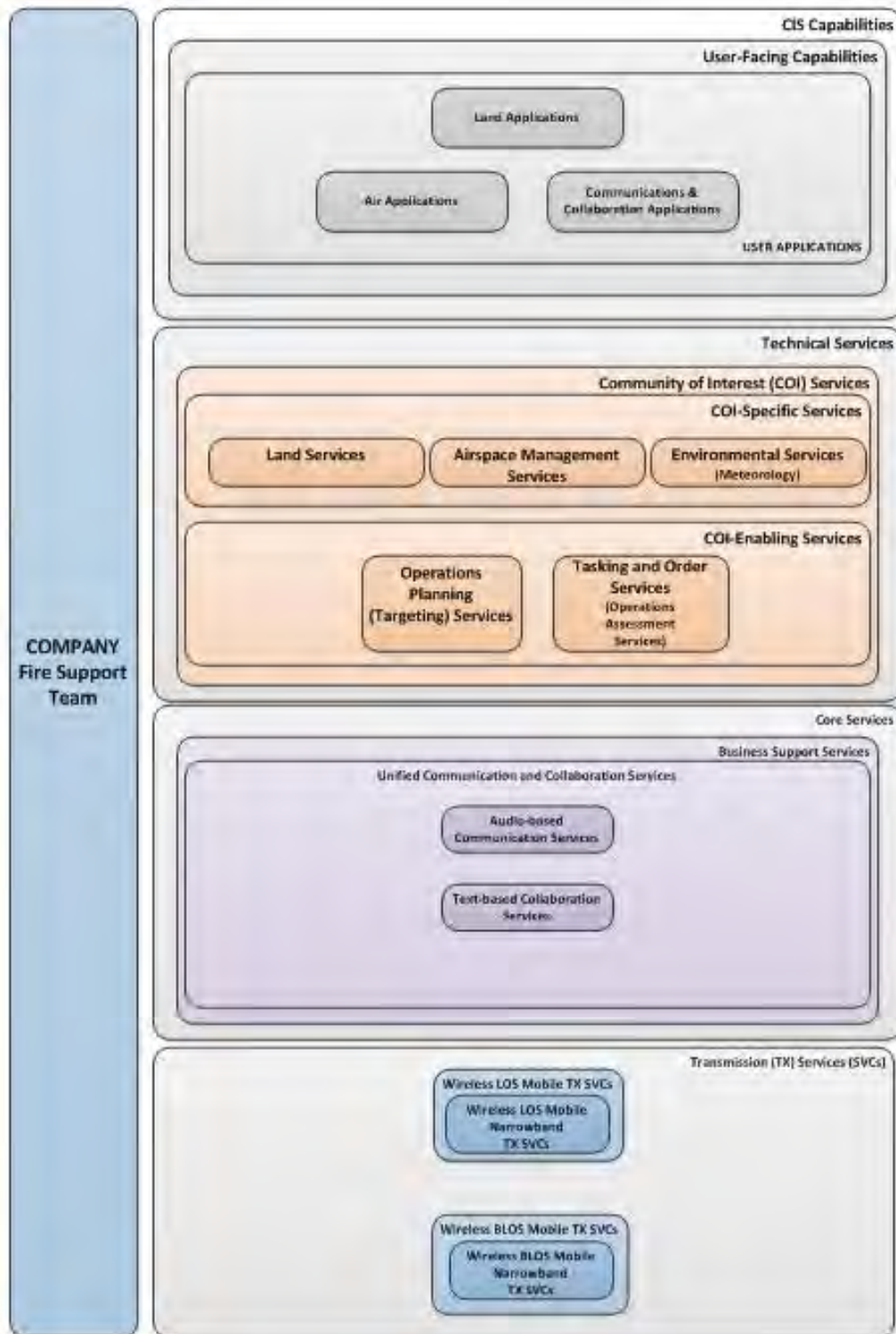


Figure E-11: Company Fire Support Team Services Requirement

JOINT LOGISTICS SUPPORT GROUP (JLSG)

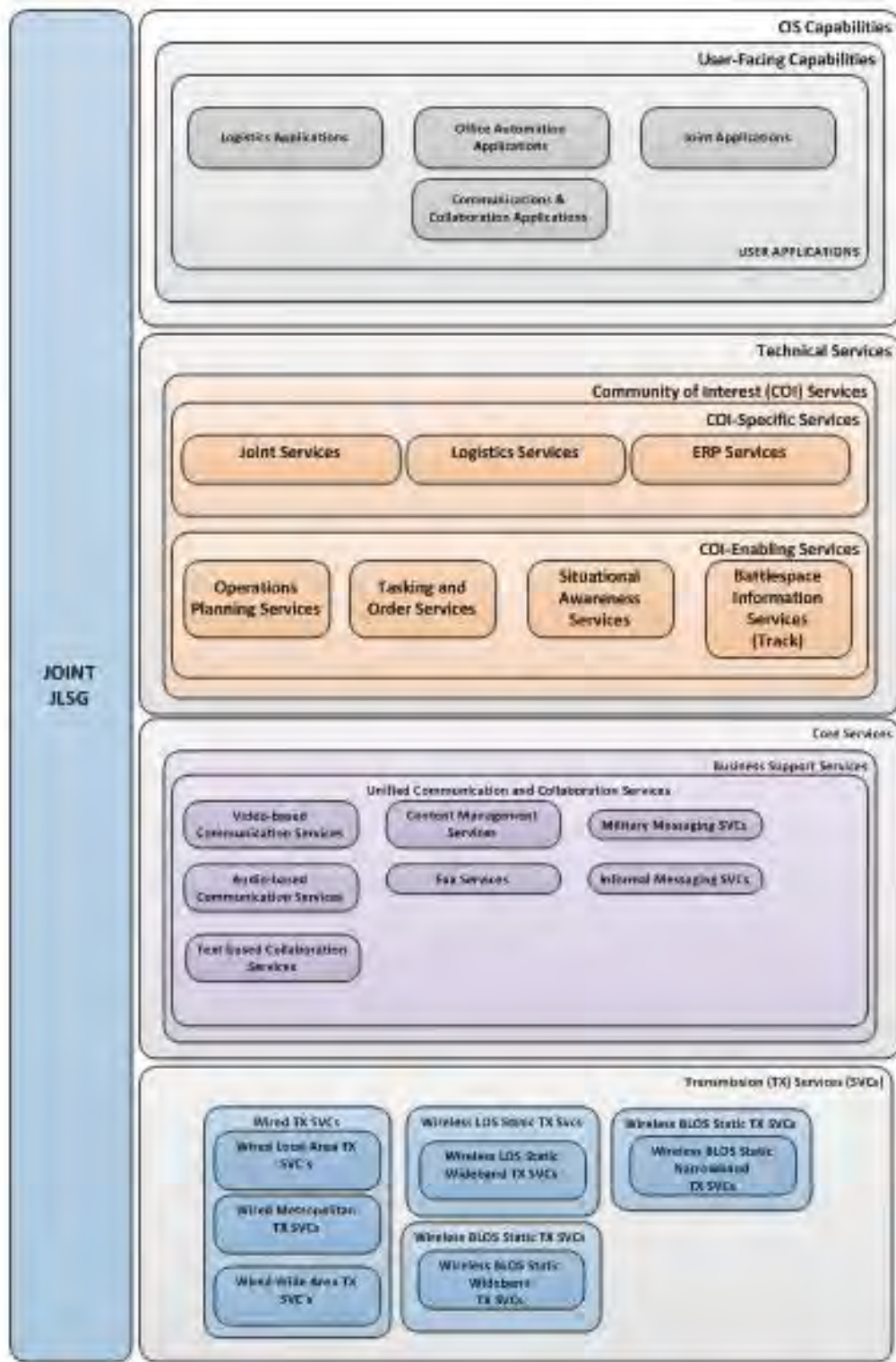


Figure E-12: JLSG Services Requirement

LANDCOM LOGISTICS

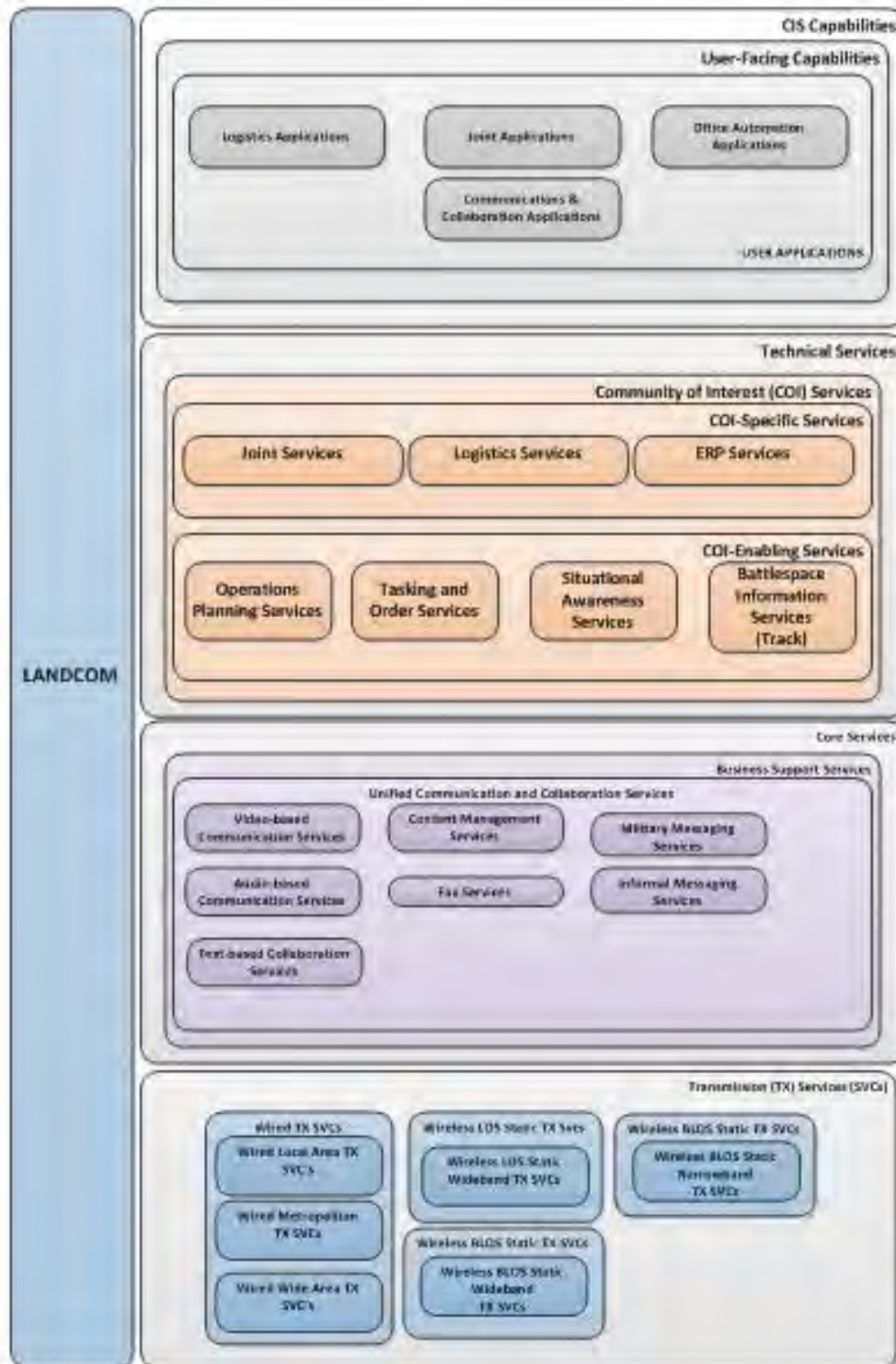


Figure E-13: LANDCOM Logistics Services Requirement

CORPS REAR SUPPORT GROUP LOGISTICS

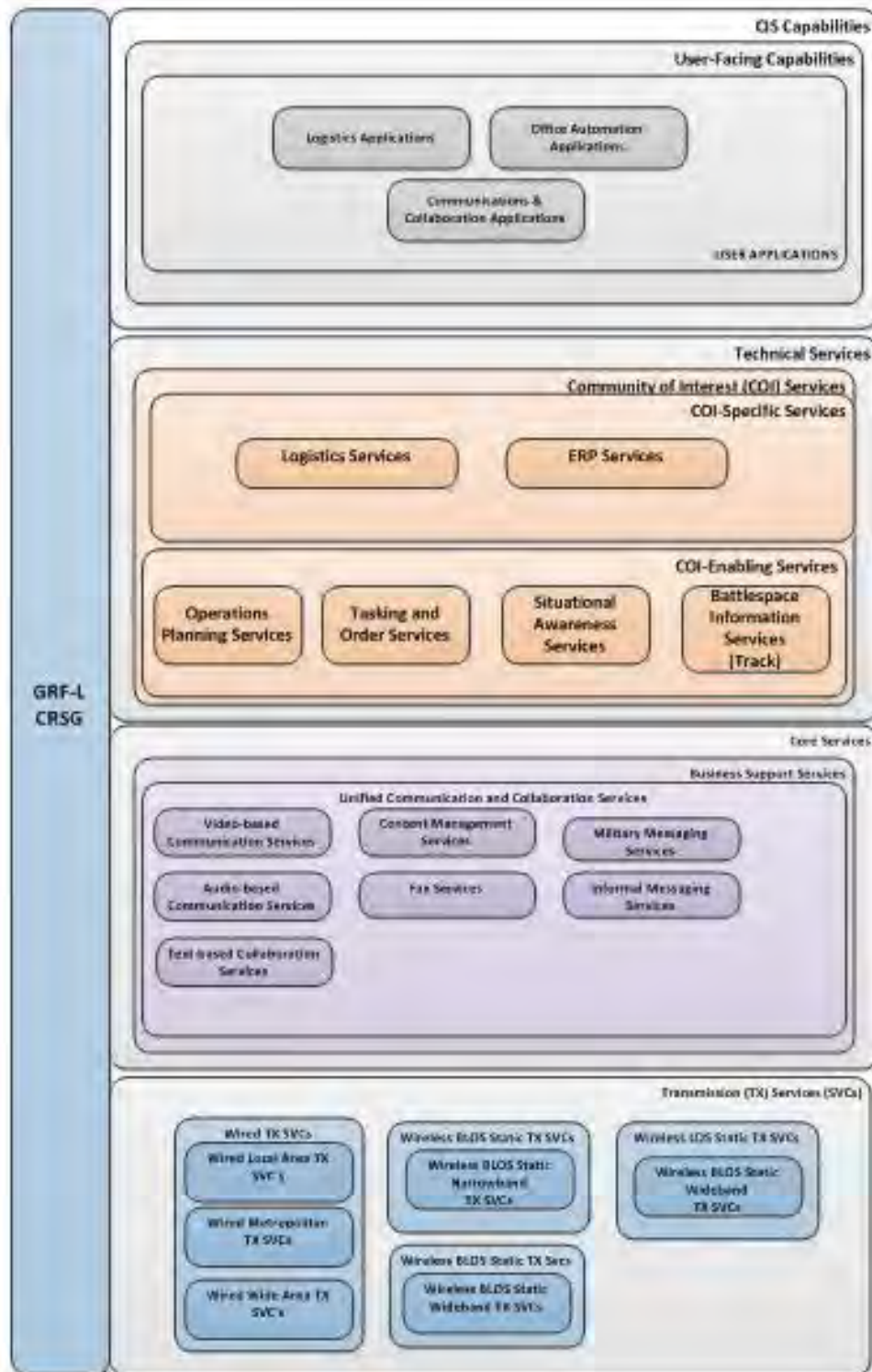


Figure E-14: Corps Rear Support Group Logistics Services Requirement

BRIGADE SUPPORT GROUP LOGISTICS

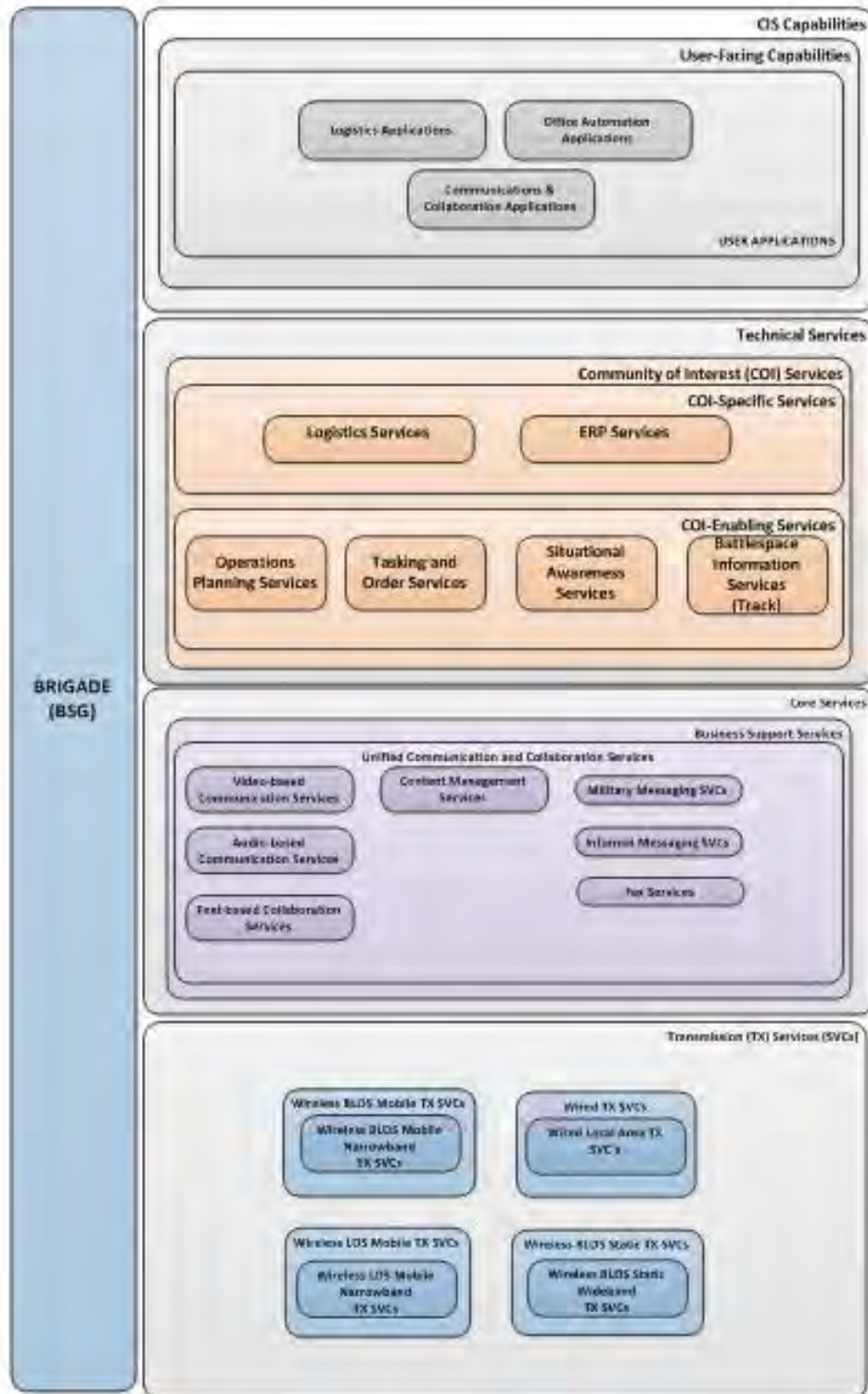


Figure E-15: Brigade Support Group Logistics Services Requirement

BATTLE GROUP LOGISTICS

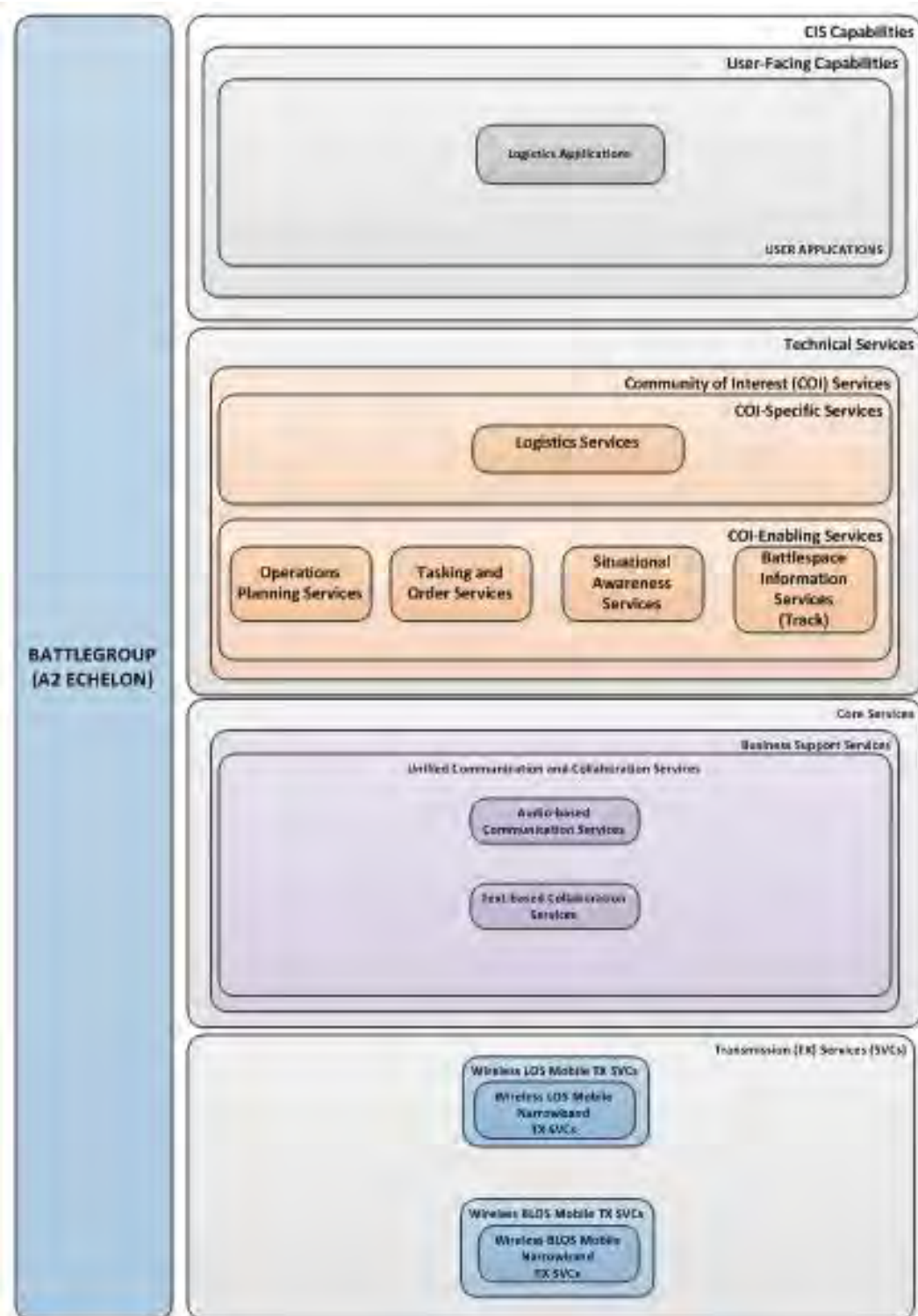


Figure E-16: Battle Group (A2 Echelon) Logistics Services Requirement

COMPANY LOGISTICS

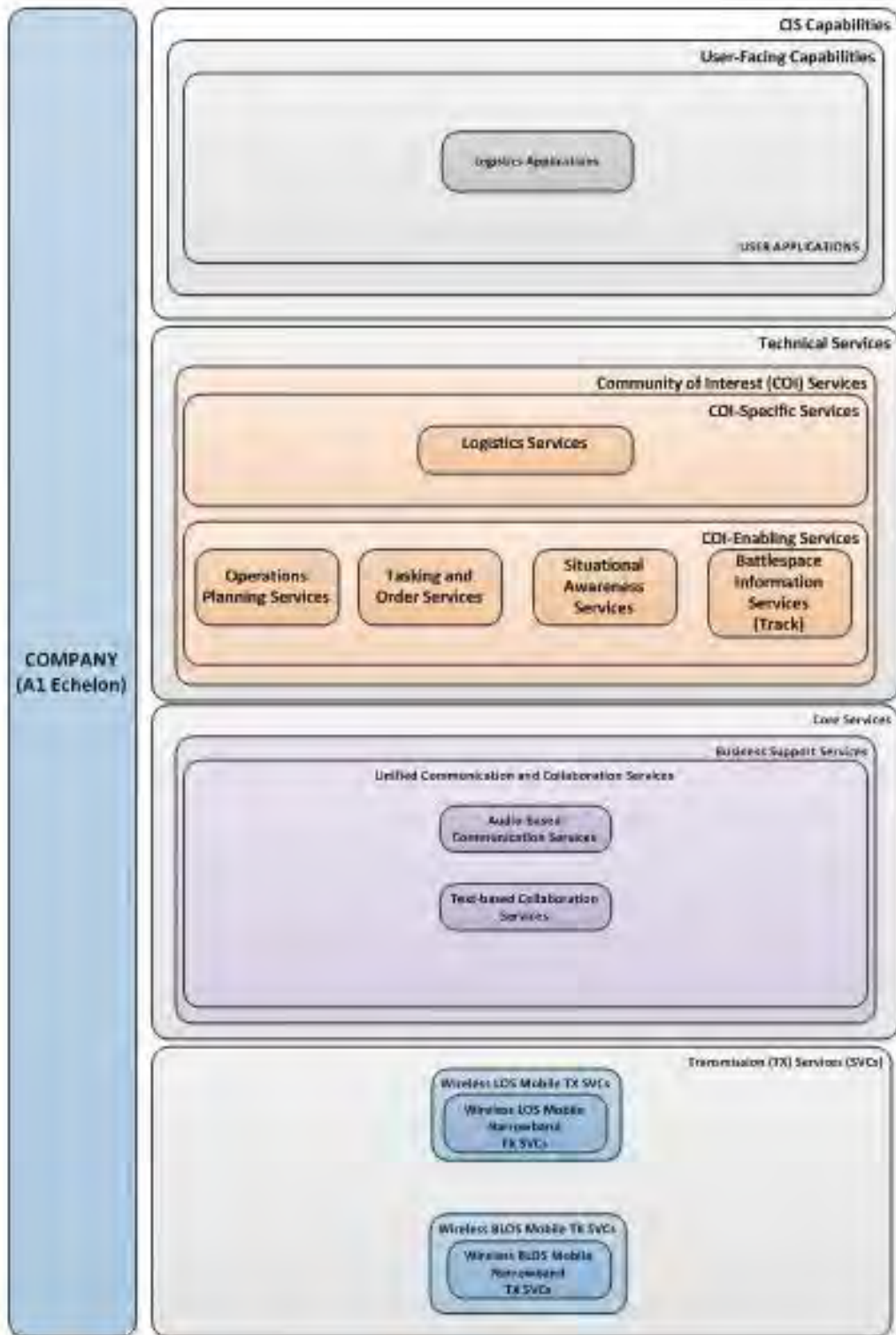


Figure E-17: Company (A1 Echelon) Logistics Services Requirement

LANDCOM MEDICAL

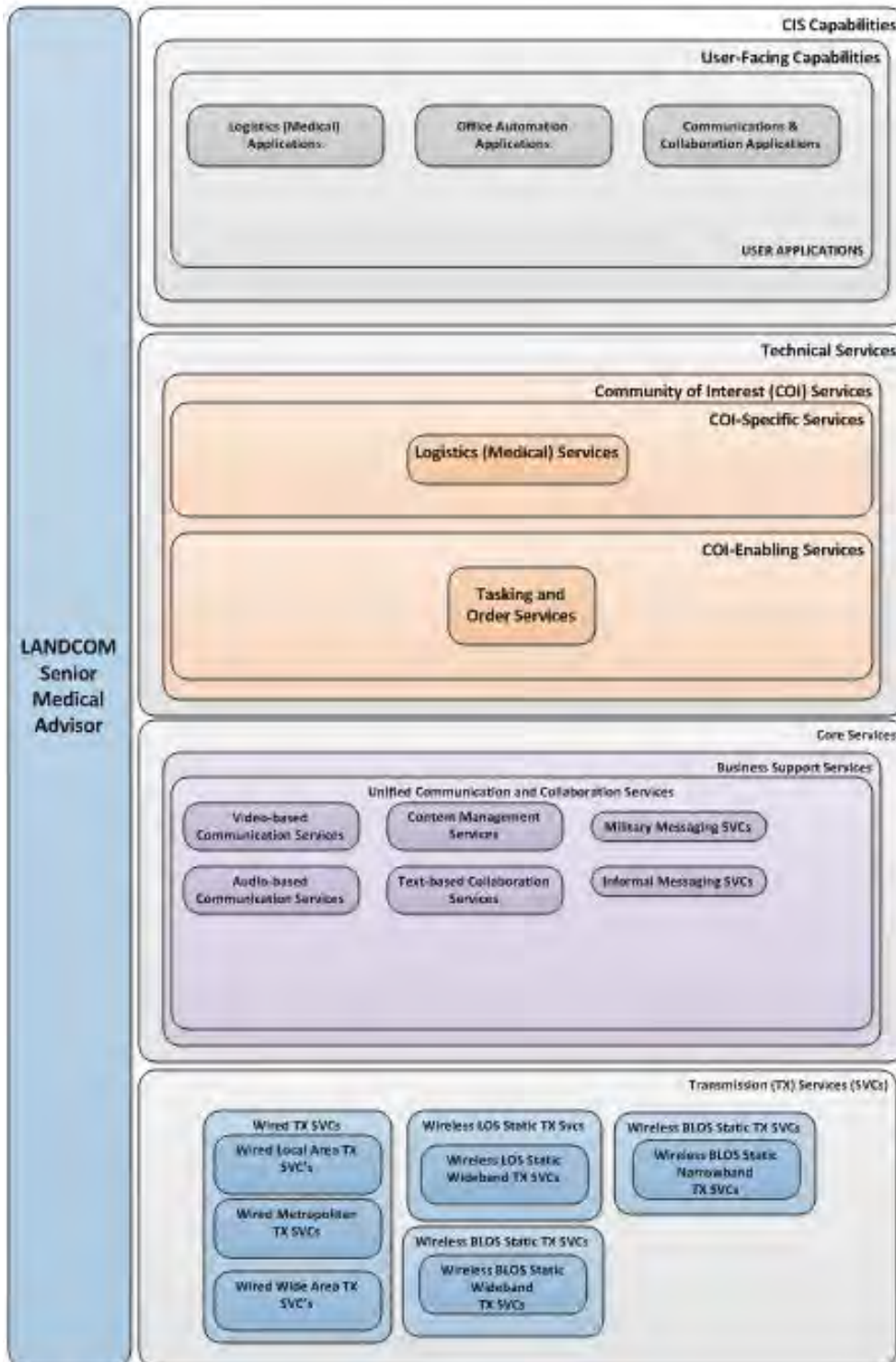


Figure E-18: LANDCOM Medical Services Requirement

CORPS MEDICAL

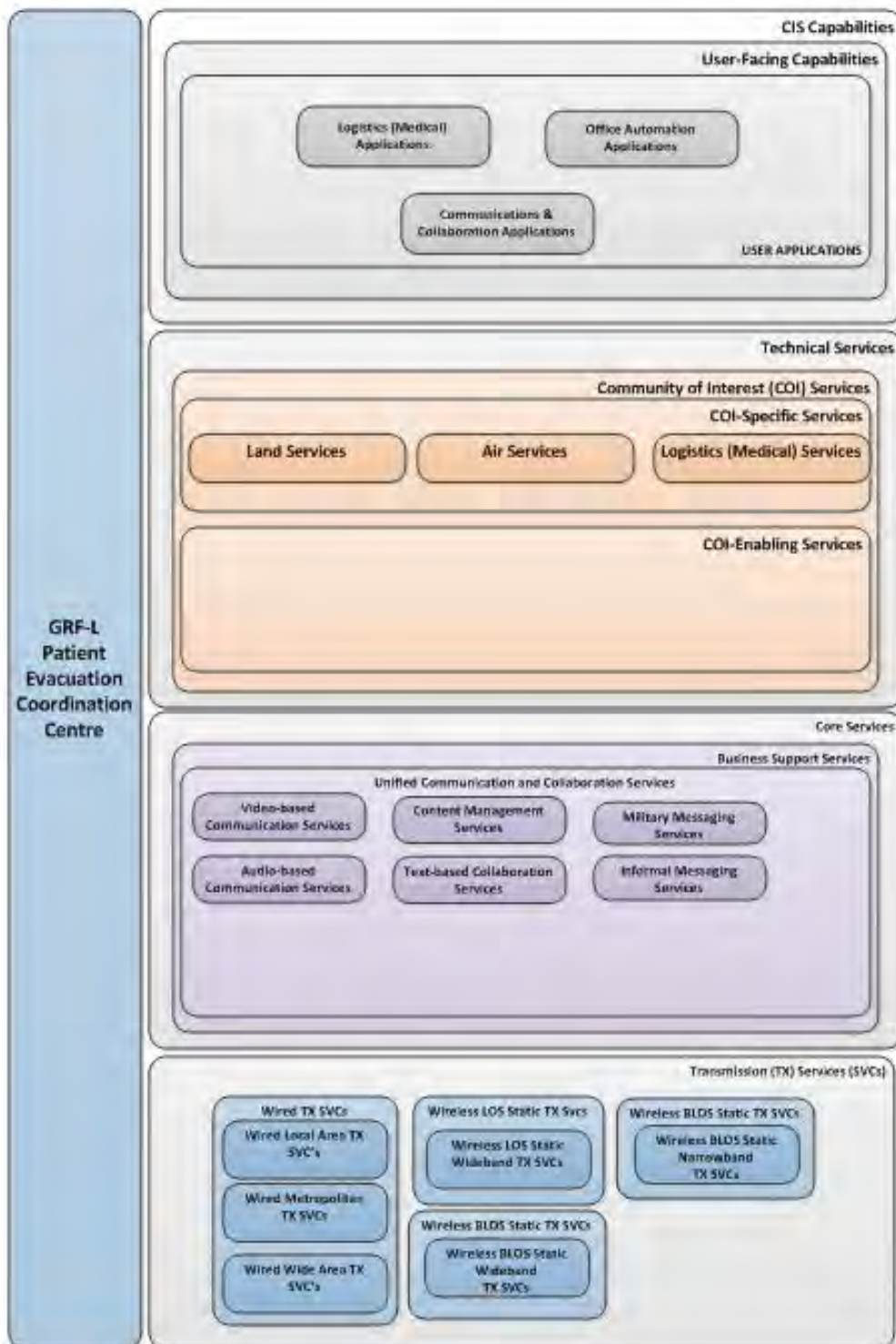


Figure E-19: Corps Medical Services Requirement

ROLE 3 MEDICAL TREATMENT FACILITY (MTF)

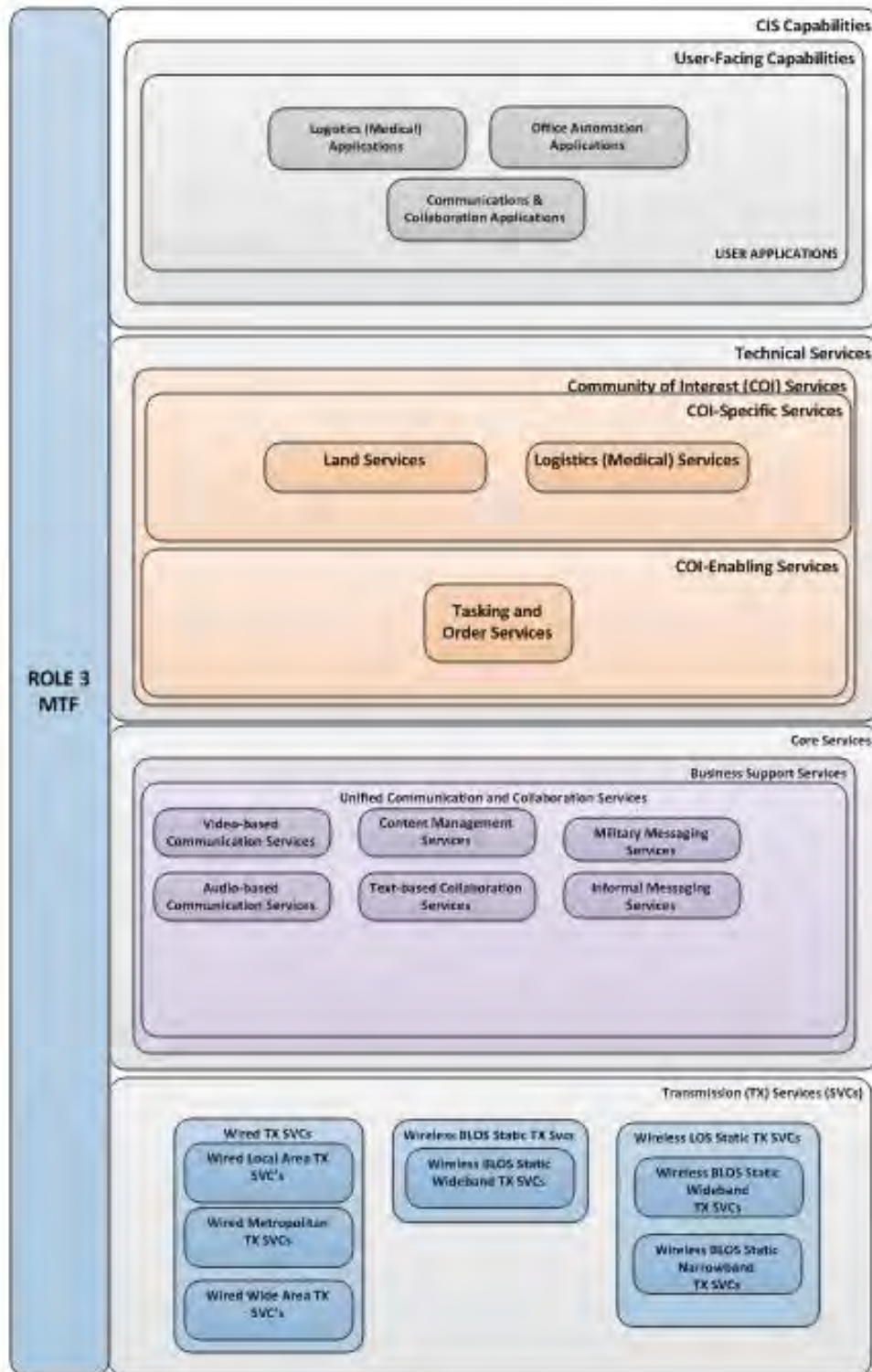


Figure E-20: Role 3 MTF Services Requirement

DIVISION PATIENT EVACUATION COORDINATION CENTRE (PACC)

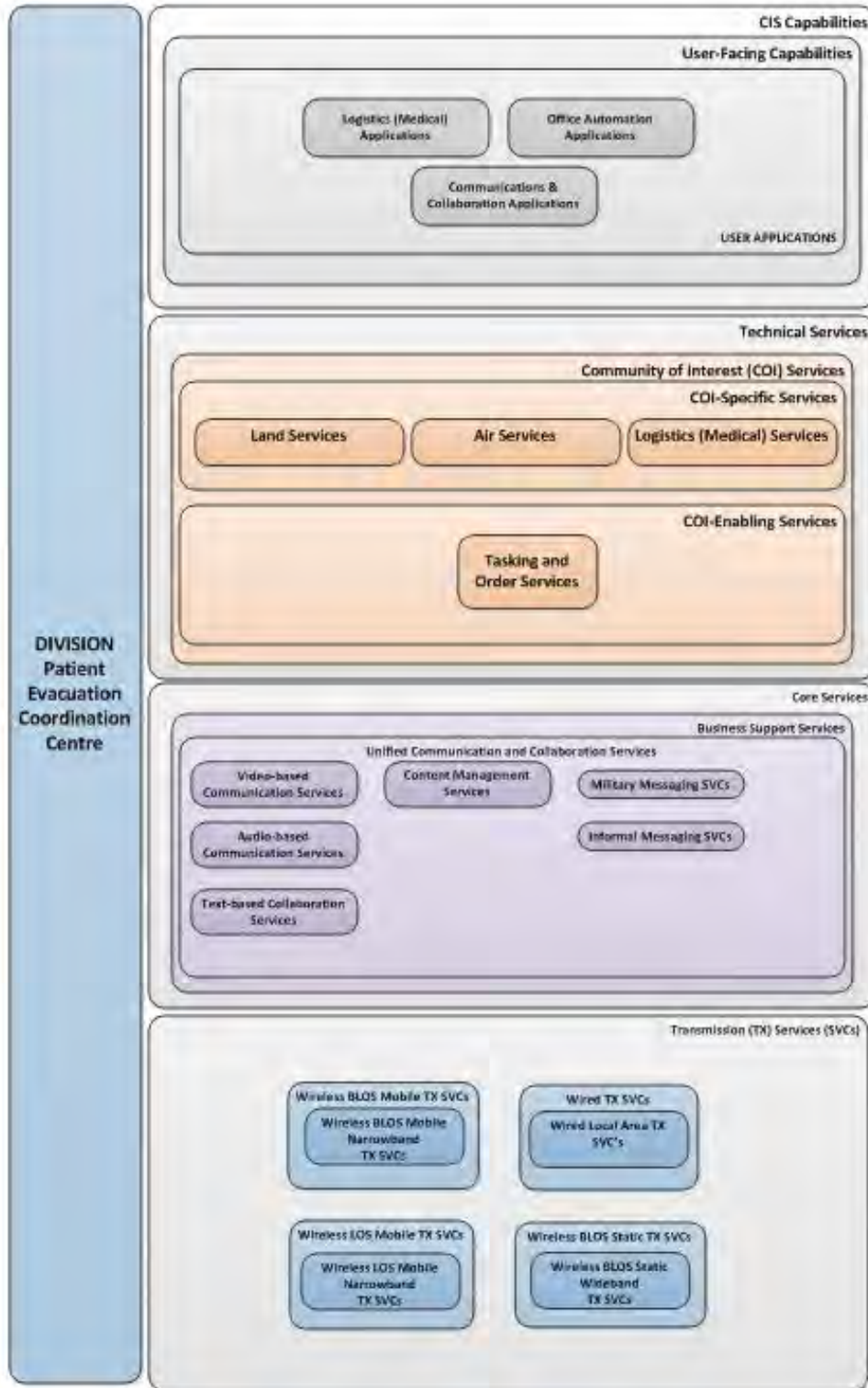


Figure E-21: Division PACC Medical Services Requirement

BRIGADE PACC

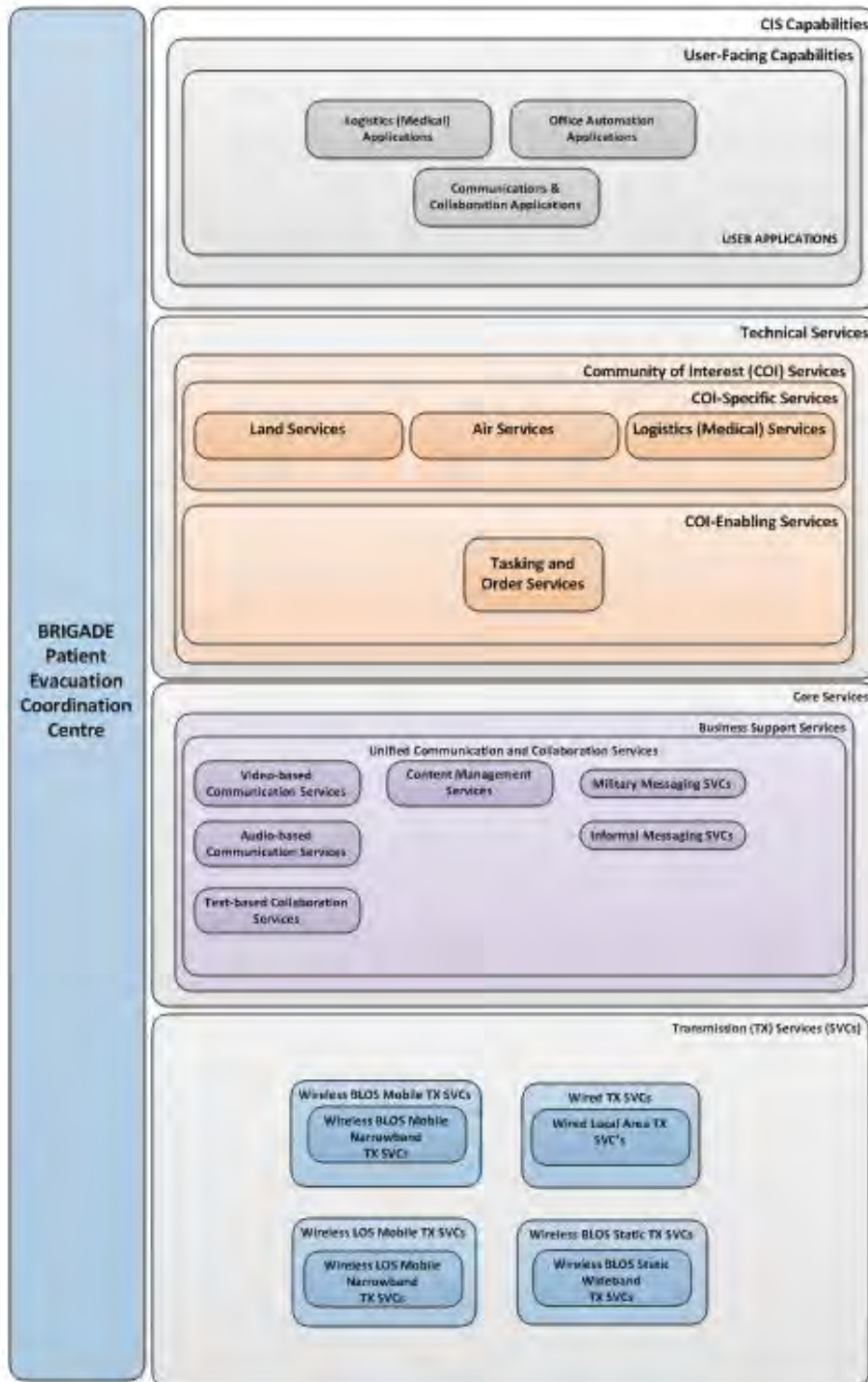


Figure E-22: Brigade PACC Medical Services Requirement

ROLE 2 MTF

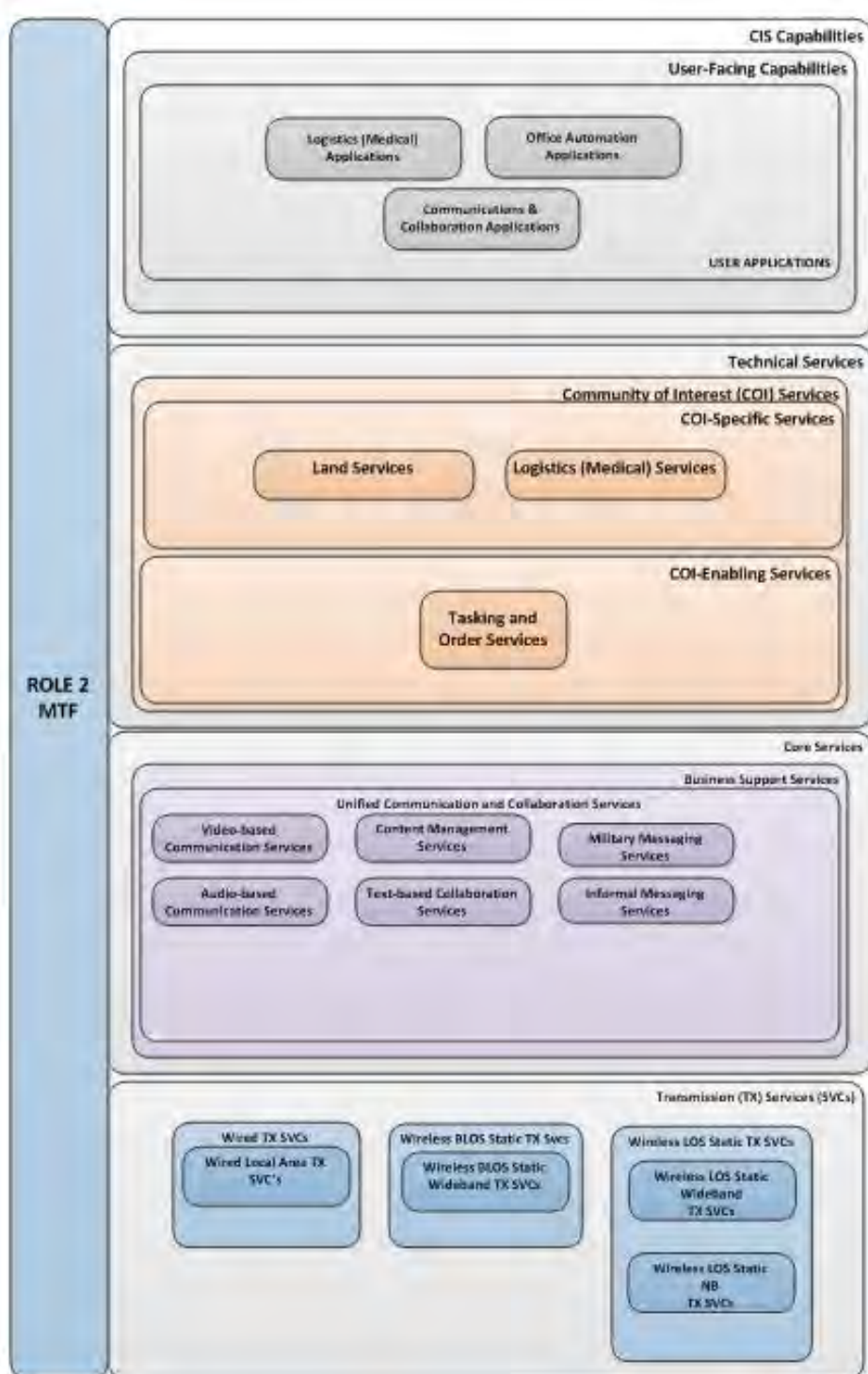


Figure E-23: Role 2 MTF Services Requirement

BATTLE GROUP UNIT AID POST

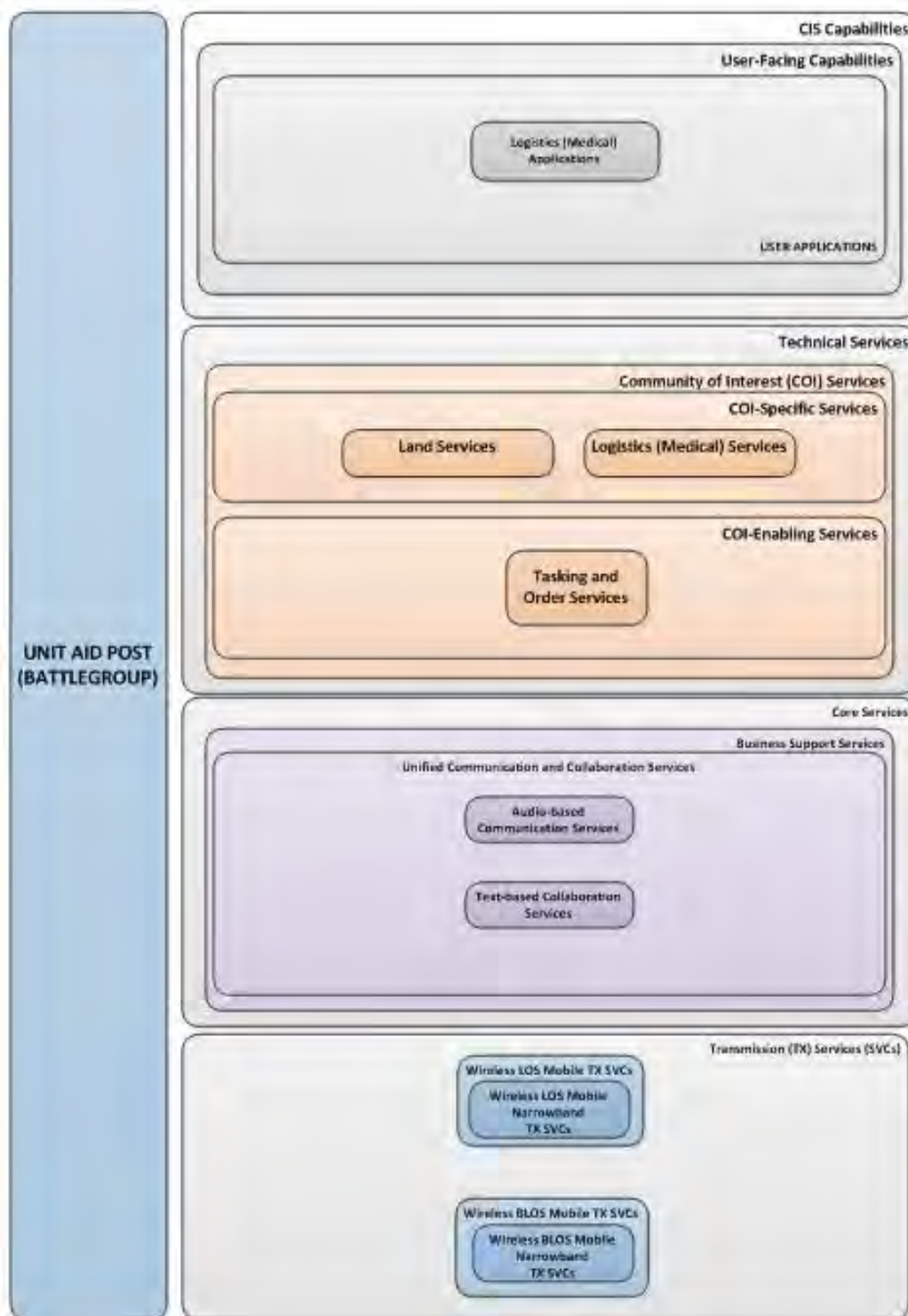


Figure E-24: Battle Group Unit Aid Post Medical Services Requirement

TEAM MEDIC

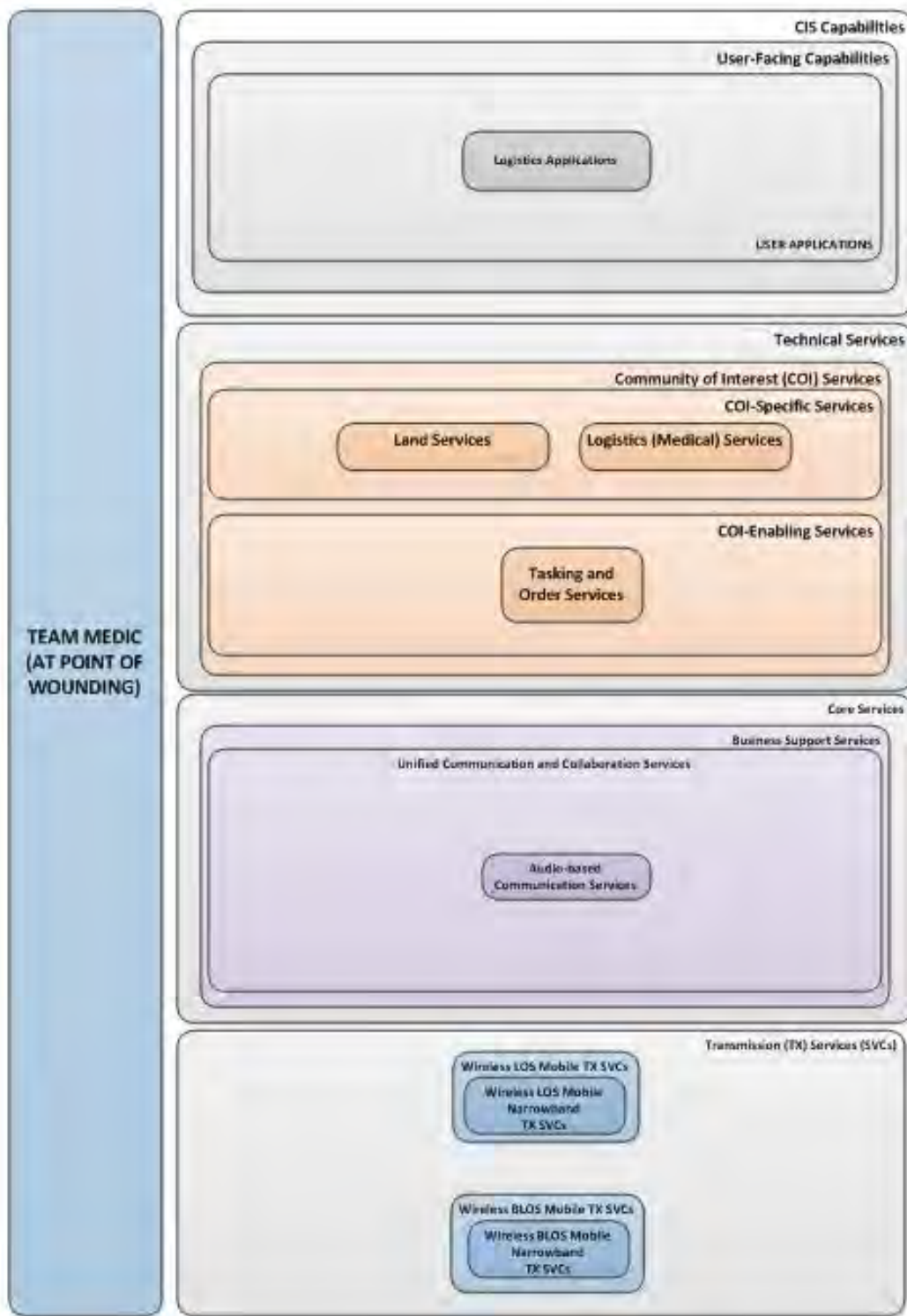


Figure E-25: Team Medic Medical Services Requirement

FEDERATED MISSION NETWORKING (FMN)

1. Purpose. This Annex further elaborates on FMN, and FMN principles that shall be applied to land tactical interoperability requirements to implement MNs. The Annex also discusses how FMN events like assessment and confirmation are related to land tactical level CIS domain, and introduces some considerations on the confidentiality levels that can be applied to tactical networks, depending on the type of mission that the tactical CIS is engaged in.

2. FMN Introduction. The FMN Concept was approved with MCM-0125-2012. That Concept (Reference T) provides overarching guidance for establishing a Federated Mission Networking capability that enables effective information sharing among NATO, NATO Nations, and/or non-NATO entities (NNE) participating in operations. Volume I of the NATO FMN Implementation Plan (NFIP) was approved with MCM-0106-2014 (Reference U), and states that “The (FMN) Concept envisions a world in which the commander of an operation effectively performs end-to-end processes and shares information in a coalition environment. This ability is enabled through a common understanding of how those processes are described and through the access to shared, secure information. The commander must be able to communicate orders, intent, and direction down to the tactical level and provide reports and recommendations up to the strategic level. Information must be available throughout the coalition force in any foreseeable operational scenario. Achievement of trust and transparency among mission participants is essential.” The mechanism to realise the above vision is a flexible and scalable CIS mission network implementation amongst mission participants that is command structure agnostic (see MCM-0125-2012 (Reference T)). On mission network level, exchange of information between the mission participants is seamless, and mission participants shall be able to leave or join the mission network without impact to the overall service provision to the other mission participants.

3. FMN Framework.

a. Following NFIP guidance, the FMN Framework was established, and the Military Committee was appointed as the FMN Governor. The Governor oversees and guides the FMN Management activities that are executed by the FMN Management Group (MG). The FMN MG is chaired by ACO DCOS CCD, and each FMN Affiliate has one seat in the Management Group. Implementing NFIP, the NATO Command Structure became one of the FMN Affiliates.

b. As stated in the FMN Concept, “The FMN Framework is a governed, managed, all-inclusive structure providing processes, plans, templates, enterprise architectures, capability components and tools needed to prepare (including planning), develop, deploy, operate and evolve and terminate

Mission Networks in support of Alliance and multinational operations in dynamic, federated environments.” In support of enduring mission network evolution, the FMN Framework process foresees a spiral approach to continuously increase the services and capabilities that can be federated within a mission network. Every two years, a new FMN Spiral Specification (FMN SpSp) is produced, based on an incremental operational requirement ambition for each spiral, agreed by all FMN Affiliates.

c. To guide above spiral implementation process, the FMN SpSp Vision document describes the vision for the next 10 years, and the FMN SpSp Roadmap (Reference A) details the spiral steps that are planned to meet the FMN vision. Every two years, a new version of the FMN SpSp is issued, aiming at a synchronized approach to improve C2 service federation across all Affiliates. Affiliates are to implement the latest FMN SpSp into the fielded systems, conduct a self-assessment on compliance, to be shared with the FMN Framework as a mandatory input for confirmation. The final step is the demonstration that the FMN service implementation is compliant with the specification, usually conducted during a FMN Readiness confirmation event, typically a multinational exercise. FMN Readiness Confirmation events cover operational, procedural and technical FMN SpSp technical requirements.

4. Mission Network (MN) Instantiation.

a. Applying the principles described above, the FMN Framework provides templated documents, processes and ready to use capabilities that allow the tailoring of FMN Framework products and services to instantiate federated networks for a specific mission. Such Mission Network provides a governed single instance of capability, including the CIS, management, processes and procedures created for the purpose of an operation, exercise, training event, or interoperability verification activity.

b. Once a MN instantiation is established using the products from FMN Framework processes, the Mission Network Instance creates its own Management Structure. In addition to the services described in the common FMN Spiral Specifications, the Mission Commander can request implementation of additional services, and thereby tailor the Mission Network Instance to the actual needs of the Mission. That can also include deviation from FMN Spiral Specifications, should the mission require so.

c. In the resulting federation all Affiliates are in principle equal. To ensure oversight for services across all Affiliates, one Affiliate is assigned the responsibility of a SMA, conducting overall federation planning and ensuring coherence. Furthermore, mission specific Security Accreditation Authority and Information Management Authority are created.

5. FMN Principles:

a. Seamless H2H communication is required across all tactical and mission network elements (This requirement is interpreted as the need to be able to provide voice, chat and basic email services between any user in the mission network to any user in the tactical networks and vice versa. As tactical networks are severely throughput constraint, the support of web services is for further study.)

b. Tactical networks need to be able to seamlessly consume the single view of the battlespace produced in the mission network (This requirement is interpreted as the capability of any tactical unit to see or request battlespace information relevant for its unit and its assigned tasks, e.g. geospatial information on the area of deployments, friendly force information or other operational picture information that of relevance for their task and location.)

c. Tactical networks need to be able to seamlessly contribute/update elements of the battlespace view (This requirement is understood as the capability of a unit to contribute unit/task specific information into the mission wide battlespace view, e.g. their position and status, intel status updates, enemy positions etc.)

6. FMN principles are applied in the implementation and fielding of Mission Networks (MN) which provide mission secret environments tailored for operational deployments of NATO and Non-NATO forces, and to allow information exchange and mission information services to be used across the applicable allied or coalition infosphere.

APPLICABILITY AT BDE AND BELOW

7. As explained in the main document, the FMN principles shall be applied to achieve interoperability down to and at BDE level. Services that are not (yet) specified in the FMN SpSp or additional MN capabilities, for which standards based interoperability cannot be implemented, interoperability based on asset sharing shall be considered. For this version of MC 0640, CIS below BDE level shall follow legacy land tactical CIS provision principles, applying asset sharing; see Figure F-1.

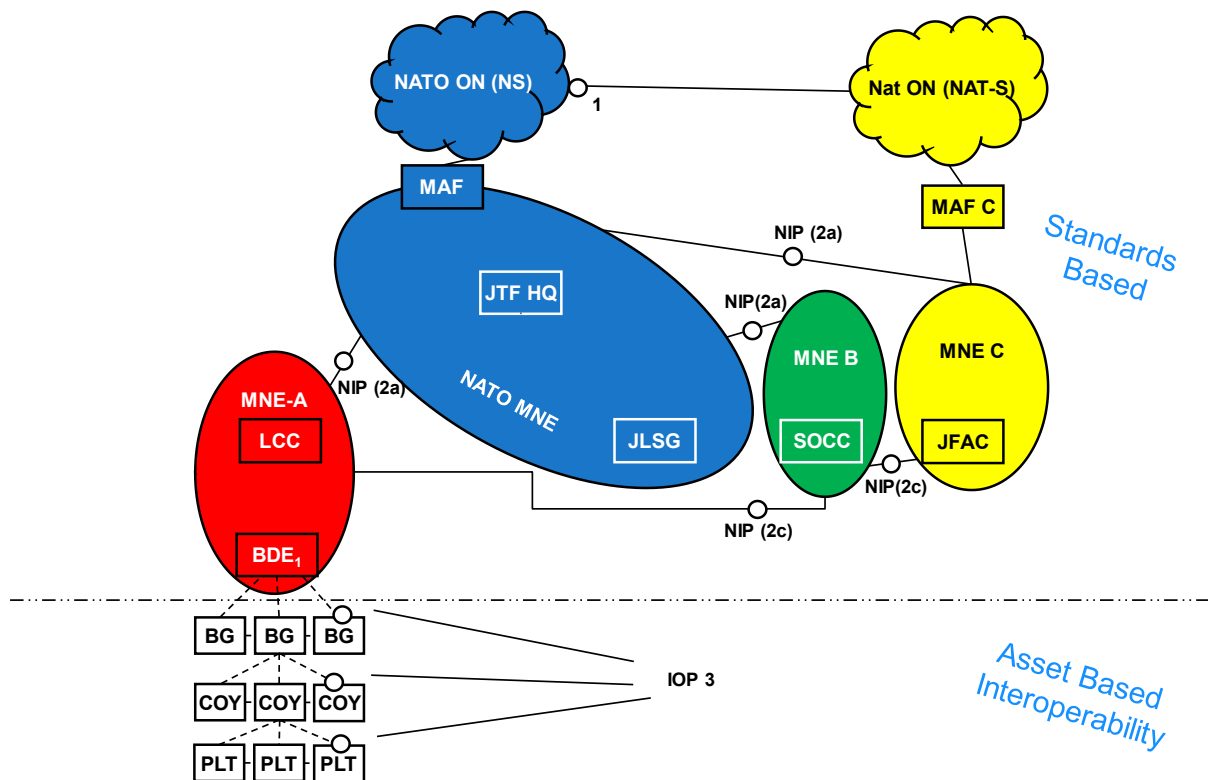


Figure F-1: CIS Provision Principles Applied

8. It is assumed that the BDE HQ, and all supporting units that are provided by the same nation, have seamless access to the MN. Units below BDE level require access to the MN for the following services:

- a. Tactical levels need to be able to participate in H2H services:
 - (1) Voice,
 - (2) Email,
 - (3) Chat.

b. Tactical units need to be able to consume relevant battlespace information:

- (1) Common Operational Picture (COP), Recognized Ground, Maritime and Air Pictures (RGP), (RMP), (RAP), etc.,
- (2) Orders and reports,
- (3) Tactical units need to be able to produce/contribute relevant battlespace information,
 - (i) Track/Position information,
 - (ii) Geospatial information,
 - (iii) Localized operational picture,
 - (iv) Reports.

9. The BDE CIS have to provide any interface/service adaptation functionality needed to interconnect/exchange services between the tactical network and the MN.

TACTICAL CIS CONFIRMATION

10. The FMN framework process foresees regular confirmation events to test and confirm that the Affiliate's capabilities are implemented in compliance with the FMN Spiral Specifications. Current confirmation assessment is focussed on the interfaces between Affiliates on the MN level between any two MNE, and between MNE and the connected MNX.

11. With the extension of FMN principles into the land tactical domain, FMN service confirmation assessment shall also include those services that have to reach across mission and tactical networks, and cross the federation-to-tactical boundary.

12. Exercises for Tactical units shall therefore also contain FMN confirmation elements. Assessment and confirmation shall be done against the services described in Paragraph 4 above, and tests shall also include service gateways between the mission and tactical networks.

TRAINING

13. The NATO FMN Strategic Training Plan (FMN STP, MCM-0261-2016(INV)) (Reference V) states "Forces that are preparing for and maintaining deployment readiness are required to be familiar and compliant with pre-agreed components of the FMN Framework Portfolio at all times."

14. It is therefore pivotal that Land Tactical units engage in and receive FMN awareness and FMN technical trainings, aligned to the FMN operational, process and service interoperability requirements as per current FMN Spiral Specification. Training foundation shall be provided as part of the affiliates operational and CIS training curricula (referred to as individual training in the FMN STP), and knowledge and skills shall be further improved through collaborative training during multinational or coalition exercises.

15. Chapter 6-5 of FMN STP (Reference V) introduces the basis for training requirements to be identified for the tactical level. As NATO, NATO Nations and other Affiliates need to seamlessly integrate the MN and the tactical level networks, all networks involved have to comply with the FMN standards profile. Predefined service instructions are therefore needed across all network implementations to ensure seamless build-up of a federated MN and the required services.

16. Tactical units must be able to provide and consume services in a federated MN environment. Through national and collective training the tactical force elements must be trained to collectively work in a federation, and the CIS operators need to understand the federated mission principles so that they can plan, establish and operate the network in response to the specific needs of the operation.

17. FMN specific aspects that shall be addressed during the training:

- a. Introduction to FMN framework processes of FMN Spiral Specification, Verification and Validation (V&V), Coalition Interoperability Assurance and Validation (CIAV) and FMN Readiness Confirmation;
- b. Understanding of the related testing and experimentation; and
- c. Integration of the tactical units CIS into a MN.

18. The FMN STP tactical level training requirement identification concludes that the FMN related content shall be injected into the various, already existing courses and exercises for tactical units on national or multinational level.

19. Departing from the considerations above, requirements for FMN related Operational user training and CIS operator training shall be developed and mandated for Affiliate provided training. To achieve the collective training effects, multinational and coalition exercise specification shall ensure that all FMN related training aspects are considered during the exercise planning and the related events scripted into the exercise execution phase.

FMN FRAMEWORK APPLIED TO LAND ENVIRONMENT CIS

20. The MC 0640 community shall validate the coverage of a FMN Service within the tactical domain for every service introduced with the current and upcoming FMN Spirals. The current FMN SpSp services that need to be extended into the land

tactical domain shall be identified by analysis, and technical interoperability requirements for land tactical units below Bde level shall be derived. That includes a validation of the services as introduced with the FMN SpSp2 (Appendix 5 to Reference N) against feasibility in the tactical domain.

21. The same shall apply to future Spiral Specifications.

22. As already indicated above, it must be ensured that the FMN related land tactical CIS services are included into the assessment criteria, and that corresponding test and evaluation events are included into the annual exercise events.

SECURITY DOMAINS AS DISCUSSED IN THE FMN FRAMEWORK ENVIRONMENT

23. In the FMN Framework it is acknowledged that not all missions would benefit from the main mission security domain (operational Mission Network) being at Secret level. Table F-1 below depicts a mapping of a mission type to the recommended confidentiality level of the operational mission network. Recognising that the confidentiality requirement on the tactical level is normally lower than the confidentiality level of the operational network, the table also suggests an adequate level for the tactical network supporting a mission. For Collective Defence, e.g. the NRF, the operational network is on Secret level, and the tactical network can be on Restricted level. A mission providing Support to Disaster Relief can be operated on Unclassified level on both operational and tactical level.

Mission Type	Operational MN	Tactical MN
Collective Defence (CD)	S	R
Antiterrorism (AT)	R	U
Consequence Management (CM)	U	U
Counter Insurgency (COIN)	S	R
Counter Terrorism (CT)	S	R
Peacekeeping (PK)	R	R
Peace Enforcement (PE)	S	R
Conflict Prevention (CP)	R	U
Peacemaking (PM)	?	?
Peacebuilding (PB)	R	U
Support to Humanitarian Assistance (SHA)	U	U
Support to Disaster Relief (DR)	U	U
Support of Non-Combatant Evacuation Operations (NEO)	S	R
Extraction Operation (EOP)	S	R
Military Aid/Support to Civil Authorities (SCA)	R	R
Enforcement of Sanctions and Embargoes (ESE)	S	R

S= Secret; R = Restricted; U= Unclassified

Table F-1: Notional Mapping of Mission Type to Information Confidentiality Requirements per Mission Type.

24. However, it will be the mission commander who assesses the mission confidentiality requirements, and finally decides on the confidentiality levels implemented for the operational and the tactical mission network.

POTENTIAL SOLUTIONS FOR INTEROPERABILITY POINTS (IOP)**OVERVIEW**

1. Purpose. This Annex describes the available and future solutions for radio level and service level interoperability for multinational Land operation to enable operational planning that supports the services identified in the appropriate IERs for the units and missions.
2. Definition. From the definition given in MC 0593/1: 'IOP 3 is connecting mobile tactical endpoints via a radio through a radio interface which requires a common waveform supported by both radios to achieve interoperability'.
3. Challenge. To enable the rapid passage of mission critical information as determined by the mission thread concept requires tactical communication systems that are compatible and interoperable with each other. It is acknowledged due to National security regulations and procurement programs it would be challenging for all NATO and Non-NATO Nations to procure a common radio platform, or one that is interoperable with every other. Whilst the Land environment await progress in this area the requirement still exists for Combat Network Radio (CNR) interoperability. Therefore, innovative solutions are required to join different national secure radio nets, containing different cryptographic keymat.

RADIO INTEROPERABILITY SOLUTIONS

4. Planning. Multiple solutions have been identified for the secure transmission of tactical services. Lead Nations have responsibility for planning the tactical networks using available resources appropriate to the units and missions undertaken. Solutions described in this annex are: Loaned Radios, Tactical Voice Bridges, Internet Protocol IOPs and Common Waveforms.
5. Loaned Radio. The loaned radio concept allows use of National radios distributed by host/framework Nation.
 - a. This concept is defined for lower Land units in the Joint Dismounted Soldier Systems (JDSS) Information Network (JDSSIN) STANAG 4677 (Reference W), approved by the NATO Conference of National Armaments Directors (CNAD).
 - b. JDSSIN defines the seamless transfer of tactical information between soldiers of different nationalities operating at the platoon or squad (group, section) level. While this standard is primarily focused at enabling interoperability for the dismounted soldier, the approach may also be applied to any situation where Battle Management System (BMS) interoperability is required using tactical radios, such as at the tactical mobility platform level.

c. The standard requires the system to secure information to a minimum classification level equivalent NATO RESTRICTED. To support the service layer, it defines a JDSS gateway from the National to mission network which includes data translation, IP header and payload security filters.

6. Tactical Voice Bridge (TVB). Bridges are interface mechanisms that achieve interoperability between different networks. Since they do not define a common waveform, they are short of the IOP 3 definition as stated above.

a. The use of a TVB may provide a cost effective solution providing an interim solution that could quickly plug a capability gap that currently exists. A number of NATO nations are already considering the benefits of employing a TVB at the tactical level.

b. TVBs will continue to be trialed at interoperability events and once a suitable model has been found and approved, the details will be promulgated to the Land community for procurement consideration. If a TVB is deployed national security accreditation is required for all the radios that will connect.

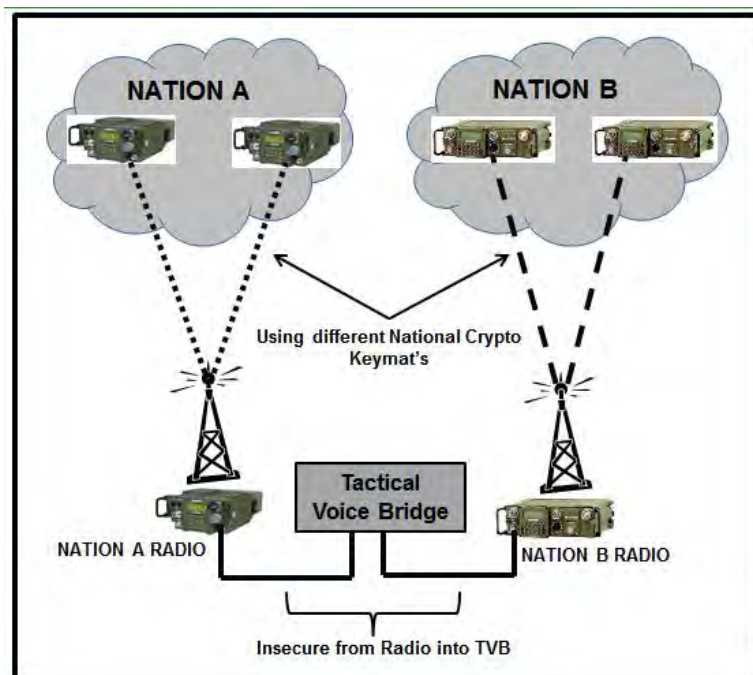


Figure 1. Example of a TVB bridging two radio nets

c. A TVB has the ability to bridge a number of nets using different national crypto keymat and waveforms (HF to VHF, VHF to UHF and HF to UHF). As shown in Figure 1, radios with national crypto fills from nation A and B are located close to the TVB. The radios are connected to the TVB. When a transmission is received by Nation A radio it will retransmit via the TVB out

onto Nation B's radio network. The only insecure connection is the wired interface between the local radios and the TVB; therefore, the national radios and TVB hardware must be operated from within a facility secured up to the highest level of classification of both radio nets.

d. TVBs that are commercially available have the capability to bridge up to eight different radio nets. TVBs with this capacity could bridge and facilitate an all informed secure BDE Command radio net, or used for range extension purposes.

e. It is acknowledged that each nation would be required to deploy a National radio within the facility of the TVB located at a BDE Headquarters in order to facilitate the 'inside leg' of the TVB. This would also require either National dispensation to locate a secure radio at the HQ or the deployment of additional personnel to operate and to perform the role of custodian of the National radio(s).

7. Internet Protocol (IP) Interoperability Point. Internet Protocol (IP) Access to Half Duplex Radio Networks, STANAG/ACoMP 5634 (Reference X), defines a standard for IP interoperability via back-to-back radio connection for two different wireless networks, or connection between a wired network and a wireless network of a different Nation or mission.

a. Supported services are defined as voice push-to-talk (PTT) and IP data forwarding. IP data forwarding can then support other tactical services such as messaging (with appropriate higher-level interfaces). Appropriate industry standard management and routing protocols are supported.

b. Voice transmission is planned to use Voice Activated Radio Control (VARC) which supports the PTT transfer of SCIP 2.4 kbps encrypted and MELPe (STANAG 4591 (Reference Y)) 2.4 kbps unencrypted voice service, with other extensions possible in future versions.

c. This mechanism defines up to voice and IP (network) layer interoperability, including inter-domain routing and service admission control.

d. This standard is under development.

8. Common Waveform. Common waveforms are those that are fielded on National or common funded radios and can interoperate at the wireless interface level. The multinational nets created by the use of common waveforms meets the definition of IOP3 per MC 0593/1.

a. Common waveforms may be either pre-installed on National radios or supplied by the Framework Nation as a download for compatible radio platforms. The compatible radio platforms for downloads would be expected

to comply to a predetermined minimum level of the Software Communications Architecture (SCA) and have a predetermined minimum performance capability to run the downloaded waveform.

b. Single channel narrowband waveform standards are currently fielded on National radios (STANAG 4204 (Reference Z) and 4205 compliant (Reference AA)), but do not implement TRANSEC and require external COMSEC. The vulnerabilities of the use of these waveforms are explained in Chapter 5 .

c. STANAG 5630 (AComP 5630-5633) Narrowband Waveform (NBWF) Edition 1 (Reference BB) is under ratification procedure in NATO. The waveform offers profiles with both voice and data transfer between radios from different manufacturers, in the VHF band for lower bit rates. NBWF offers COMSEC up to NATO RESTRICTED level within the standard, and can be supported by external COMSEC for higher classification levels. Edition 2 of the standard will incorporate EPM to provide TRANSEC.

d. A common waveform standard requires the implementation of common physical, link, and network layers; common TRANSEC; either common COMSEC or support for common external COMSEC; and appropriate signaling and management to configure and maintain the network.

e. Common key management is a major issue, and requires its own infrastructure. ACT is defining common NATO key management as part of its crypto modernization initiative.

f. All radios operate within a common mission security domain.

SUPPORT OF INTEROPERABLE SERVICES

9. Voice. NATO support for tactical voice is guided by the NATO Secure Voice Strategy (NSVS, AC/322-D(2018)0016) (Reference CC).

a. The existing NATO Services focus on one specific technology (Secure Communications Interoperability Protocol, SCIP) as being the end-goal. However in noting that many networks are already migrated to, or will migrate to IP-technology over the next years, other technologies should not be discarded beforehand especially when this may result in resource savings.

b. The translation of voice traffic between networks is managed by bridges as discussed above. Common waveforms should be able to operate using the same voice coding to ensure end-to-end operation without gateways.

10. Messaging. Messaging is primarily utilised across IP-enabled systems and platforms, and IP interoperability is supported via common waveforms or via bridges.

a. Once IP interoperability is in place, interoperable text-based collaboration services (chat) may be supported via Extensible Messaging and Presence Protocol (XMPP).

b. Machine-to-machine data exchange interoperability is possible via the JDSS Interoperability Interface.

c. Email via Simple Mail Transfer Protocol (SMTP) and header markers is possible via common markers defined in NATO Interoperability Standards and Profiles (NISP, ADatP-34) (Reference DD).

11. Friendly Force Tracking. FFT (also known as Blue Force Tracking (BFT)) is commonly regarded as one of the most important capabilities of a Command and Control Information System (C2IS).

a. An effective FFT system provides commanders at all levels with the exact location of own forces and any coalition forces in their areas of operations. This is a key factor in force protection, whilst also reducing the risk of friendly fire (fratricide). This improved situational awareness enables commanders to make use of full operational capabilities for the forces under their command.

b. In 2005, Allied Command Transformation introduced the use of a NATO Friendly Force Identification (NFFI) standard. This was in response to an urgent need to exchange friendly force tracks between national C2ISs. The NFFI standard consists of a message definition and interface protocol definitions to enable the exchange of information.

REFERENCES

- A. SH/CCD J6/FMN/148/17-317789, FMN Management Group Meeting #3 - Meeting Summary, 29 Jun 17.
- B. MC 0593/1, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations, 12 Jul 17.
- C. PO(2015)0580, Political Guidance 2015, 16 Oct 15.
- D. SH/PLANS/JCAP/FCP/16-312951, CRR 16 Bi-SC Minimum Capability Requirements (MCR16), 12 Apr 16.
- E. AC/322-D(2016)0017, C3 Taxonomy Baseline 2.0, 14 Mar 16.
- F. AJP-3.2 Edition A Version 1, Allied Joint Doctrine for Land Operations, 15 Mar 16.
- G. C-M(2002)0049, Security within the North Atlantic Treaty Organization (NATO), 17 Jun 02.
- H. MCM-0234-2015, NATO Mission Thread Capstone Concept, 13 Jan 16.
- I. IMSM-0565-2017, NATO Cryptographic Baseline and Reference Architecture Perspectives - Revision 1, 4 Dec 17.
- J. MC 0571/1, Military Concept for Cyber Defence, 30 Sep 15.
- K. PO(2014)0801, Minimum Requirements of CIS Security (Including Cyber Defence) for National CIS Critical for NATO Core Tasks, 19 Dec 14
- L. AJP-6 Edition A Version 1, Allied Joint Doctrine for Communication and Information Systems, 28 Feb 17.
- M. APP-15 Edition A Version 2, NATO Information Exchange Requirement Specification Process, 21 Nov 17.
- N. SH/CCD J6/FMN/004/18-319761, FMN Management Group Meeting #4 – Meeting Summary, 19 Jan 18.
- O. STANAG 4705 (Edition 1), International Network Numbering for Communications Systems in Use in NATO, 18 Feb 15.
- P. STANAG 5046 (Edition 4), The NATO Military Communications Directory System, 18 Feb 15.

- Q. STANAG 5066 (Edition 3), Profile for HF Radio Data Communications, 30 Mar 15.
- R. APP-11 Edition D Version 1, NATO Message Catalogue, 23 Nov 15.
- S. ACP 190 NS-1 (C), NATO Guide to Spectrum Management in Military Operations, 15 Feb 16.
- T. MCM-0125-2012, NATO Future Mission Network (FMN) Concept, 21 Nov 12.
- U. C-M(2015)0003-AS1, NATO Federated Mission Networking Implementation Plan, 30 Jan 15.
- V. C-M(2017)0009 (INV), Military Committee FMN Strategic Training Plan (FMN STP), 13 Feb 17.
- W. STANAG 4677 (Edition 1), Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability, 3 Oct 14.
- X. STANAG 5634 (Edition 1), Internet Protocol (IP) Interface to Half Duplex Radio Networks, AComP 5634 (Study Draft).
- Y. STANAG 4591 (Edition 1), The 600 Bit/s, 1200 Bit/s and 2400 Bit/s NATO Interoperable Narrow Band Voice Coder, 3 Oct 08.
- Z. STANAG 4204 (Edition 3), Technical Standards for Single Channel VHF Radio Equipment, 29 Sep 08.
- AA. STANAG 4205 (Edition 4), Technical Standards for Single Channel UHF Radio Equipment - AComP-4205 Edition A, 29 Jul 05.
- BB. STANAG 5630 (Edition 1), Narrowband Waveform (NBWF) for VHF/UHF Radios, AComP 5630-5633 Edition A (Ratification Draft).
- CC. AC/322-D(2018)0016, NATO Secure Voice Strategy (NSVS), 17 Apr 18.
- DD. AC/322-N(2017)0043-REV1, NATO Interoperability Standards and Profiles (ADatP- 34(J) (NISP v10), 19 Oct 17.

AD = ACO Directive

AJP = Allied Joint Publication

MC = Military Committee Policy Document

STANAG = NATO Standardization Agreement

NATO UNCLASSIFIED

12 October 2021

DOCUMENT

PO(2021)0360

Silence procedure ends:

19 Oct 2021 - 17:30

To : Permanent Representatives (Council)

From : Secretary General

APPROVAL OF NATO'S DATA EXPLOITATION FRAMEWORK POLICY

1. Please find attached NATO's Data Exploitation Framework Policy and enclosed the related military advice (MCM-0142-2021). This Policy should be read in conjunction with NATO's Artificial Intelligence Strategy (PO(2021)0350 (NR)).
2. On 24 September 2021, the task-limited Data Exploitation Working Group agreed to be dissolved in accordance with its Terms of Reference (PO(2019)0275 (INV)), pending the approval of the Policy.
3. On 30 September 2021, the Data Exploitation Working Group and the Consultation, Command and Control Board agreed to the Data Exploitation Framework Policy (AC/341-WP(2021)0001-REV6-MULTIREF).
4. **Unless I hear to the contrary by 17:30 hours on Tuesday, 19 October 2021**, I shall assume that the Council has approved NATO's Data Exploitation Framework Policy, has agreed to forward the document to the Defence Ministers for their endorsement, and has approved the dissolution of the Data Exploitation Working Group.

(Signed) Jens Stoltenberg

1 Annex
1 Enclosure

Original: English

NATO UNCLASSIFIED

- 1 -



DATA EXPLOITATION FRAMEWORK POLICY

REFERENCES

- A. PO(2018)0491-REV1, (NR) Functional Review of the NATO HQs, 28 November 2018
- B. PO(2019)0275 (INV), Terms of Reference for the Data Exploitation Working Group, 27 June 2019
- C. PO(2020)0208, Chief Information Officer Function for NATO, 22 June 2020
- D. PO(2021)0059, Approval of 'Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies', 15 February 2021
- E. PO(2021)0350 (NR), NATO's Artificial Intelligence Strategy, 11 October 2021
- F. MCM-0099-2021, ACT/TT3671/SACT/2021-84/NS3669 (NS), The Initial Alliance Warfare Development Agenda, 26 April 2021
- G. C-M(2007)0118, The NATO Information Management Policy, 28 January 2008
- H. C-M(2011)0043, NATO Records Policy, 28 June 2011
- I. C-M(2015)0041-REV2, Alliance Consultation, Command, and Control Policy, 14 December 2018
- J. C-M(2015)0041-REV2-Annex 13, Alliance Consultation, Command, and Control Policy: NATO Data Management Policy, 14 December 2018
- K. C-M(2002)49-REV1, Security Within the North Atlantic Treaty Organization (NATO), 20 November 2020
- L. AC/35-D/2002-REV5, Directive on the Security of NATO Classified Information, 25 November 2020
- M. C-M(2008)0116-REV1, Public Disclosure of NATO Information, 28 February 2017
- N. C-M(2002)60, The Management of Non-Classified NATO Information, 11 July 2002
- O. C-M(2009)0021, Policy on the Retention and Disposition of NATO Information, 6 February 2009
- P. AC/324-D(2014)0008-REV1, Directive on the Preservation of NATO Digital Information of Permanent Value, 20 December 2018
- Q. PO(2020)0147 MCM-0033-2020 Military Committee Advice on Strategy to Develop and Sustain a NATO Intelligence Systems Architecture, 7 May 2020
- R. PO(2021)0199 (NR), Comprehensive Cyber Defence Policy, 31 May 2021
- S. MC 0296/3 (Final), NATO Geospatial Policy, 31 October 2016
- T. PO(2018)0235, Biometrics Framework Policy, 1 June 2018
- U. PO(2020)0315, NATO Battlefield Evidence Policy, 15 October 2020
- V. MC 0647 (FINAL), Policy on Open Source Intelligence (OSINT), 23 June 2017
- W. C-M(2017)0062, NATO Enterprise Communications and Information Vision, 5 December 2017
- X. PR/CP (2021)086, 2021 Brussels Summit Communiqué, 14 June 2021
- Y. ADatP-34, NATO Interoperability Standards and Profiles (NISF), covered by STANAG 5524
- Z. PO(2021)0253 (NS), NATO Cyber Adaptation, 12 July 2021

I. INTRODUCTION

Background

1. In 2018, NATO embarked upon a major initiative to promote the use of data¹ as a strategic resource, following the NATO HQ Functional Review (Reference A). This initiative is being led by the Data Exploitation Working Group (DEWG) (Reference B), which was given the task of developing the Data Exploitation² Framework Policy (DEFP) to:
 - Set out NATO's objectives, strategy and approach to the use of data as a strategic resource building on relevant parts of NATO's Information Management Policy and NATO's Security Policy, while maintaining the integrity of these Council-approved policies.
 - Provide an overview of the potential phases of development of the Alliance's efforts.
 - Examine options on how to best ensure a robust NATO-wide governance and utilization of data as a strategic asset, including by considering the option of a Chief Data Officer role.

Approach

2. The DEFP establishes a framework to ensure that NATO is able to leverage data as a strategic resource and seeks to address challenges to data exploitation identified by Allies and members of the NATO Enterprise. Its objective is to put into place an overarching, comprehensive approach to ensure data is used responsibly and in line with core Alliance values with a focus on improving the data exploitation capabilities across all levels in the military, civilian and political domains in order to enable priority use-cases where: (1) data exists and is already being exploited, and (or) (2) where strategic data assets still needs to be built or shared to have the most immediate and beneficial impact for the Alliance.
3. The Framework Policy in Section II starts by outlining the **scope of this effort**, which includes the Alliance as a whole, support to Allies as they develop their national

¹ Throughout this Framework Policy, the term Data includes, but is not limited to "raw" data, information and data analytics resources, such as models, algorithms, reports, etc. Data and information are used interchangeably, as the definition is dependent on the perspectives and relative to the "use" context. Please see Appendix 3 for more details.

² Data Exploitation is an umbrella term to encompass the full spectrum of activities involved with enabling NATO to leverage on, gain value from, and manage data as a strategic resource. This covers existing activities with established NATO processes (please see Appendix 3 for further details), while expanding upon and including activities related to Data Use, Data Analytics development, and the application of data science and AI- techniques, such as Big Data analytics, Natural Language Processing (NLP) and machine learning (ML) to improve data exploitation capabilities.

approaches, how data exploitation can be taken forward in the NATO Enterprise, and ensuring the basis for working with partners in coalition formats.

4. In Section III, the Framework Policy outlines a proposed **Overall Vision**, from which have been derived a set of desired outcomes, **strategic goals**, and objectives which will form the basis for the work ahead. This Vision is supported by a set of **Principles** outlined in Section IV which will determine how data will be collected, stored, shared, and exploited. These are built upon existing approaches contained in Council-agreed documents.
5. In Section V, the Framework Policy then outlines a series of **Roles and Responsibilities** to implement the Policy. These build on existing structures and take into account new developments, including for example the introduction of the NATO Chief Information Officer and the Office of the Chief Information Officer (Reference C).
6. Section VI covers **Implementation Building Blocks**, introducing a set of potential Alliance application areas informed by priority use cases and highlights the importance of establishing a NATO Data Exploitation Maturity Model (NDEMM) to track progress.
7. The Policy concludes in Section VII by outlining a set of next steps, including the creation of a Strategic Plan and Implementation Guidance. A set of **Appendices** further expand on relevant issues, including a table outlining foundational principles (Appendix 1), an overview of a proposed Maturity Model (to be published separately) to help measure where we stand in our efforts and allow for constant monitoring of progress towards the desired outcomes and objectives (Appendix 2), an initial Glossary (Appendix 3), and suggested Governance and Enterprise Management Way Ahead (Appendix 4).
8. This Framework Policy was developed through engagement with data exploitation stakeholders across the Alliance. Based on the results of an initial Data Exploitation Questionnaire, five Food-for-Thought papers were produced on the following themes:
 - i) Policy Scope & Vision (AC/341(2021)0002)
 - ii) Data Exploitation and Key Data Analytics context (AC/341-N(2020)0003)
 - iii) Processes Landscape & Governance Roles (AC/341-N(2020)0004)
 - iv) Technology & Principles (AC/341-N(2021)0001)
 - v) People & Governance Structures (AC/341-N(2021)0002)

Foundational documents

9. This Framework Policy will serve as an enabler for current and future NATO initiatives, in particular the “Foster and Protect: NATO’s Coherent Implementation Strategy on Emerging and Disruptive Technologies” (Reference D), NATO’s Artificial Intelligence Strategy (Reference E), and the NATO Warfighting Capstone Concept (NWCC)/(initial)Warfare Development Agenda (iWDA) “Data Exploitation Programme” jump-starter (Reference F).

10. In accordance with the Council tasking, the Data Exploitation Framework Policy builds upon, while maintaining the integrity of, the following Council-approved foundational policies (Reference A):
 - a) NATO Information Management Policy (Reference G)
 - b) Records Policy (Reference H)
 - c) C3 Framework Policies (Reference I), including the Data Management Policy (Reference J)
 - d) Security Policy (Reference K, Reference L)
 - e) Public Disclosure Policy (Reference M)
 - f) Management of Non-Classified NATO Information Policy (Reference N)
 - g) Policy on the Retention and Disposition of NATO Information (Reference O, Reference P)
11. In addition to these foundational policies, the Data Exploitation Framework Policy incorporates Military Committee Strategies and Guidance, as well as category-specific “Data Use” Policies that are being developed or are already in place for specific categories of data, such as intelligence (Reference Q), cyber defence (Reference R), geospatial (Reference S), biometrics (Reference T), battlefield evidence (Reference U), open source intelligence (Reference V), etc. These strategies, guidance, and category-specific policies may provide additional governance, above and beyond those specified by the NATO Information Management Policy, which will need to be taken into account in specific use cases.
 - 1.
12. Figure 1 illustrates the “living” Data Exploitation Framework (DEF) Policies and Guidance Landscape, which brings these foundational documents together. This Landscape is mapped to the Data Exploitation Lifecycle³ to make sure that all will be made aware of the relevant Policies and Guidance to be referenced and applied to data as it progresses through its lifecycle. As Policies and Guidance change and new ones develop, this “living” Landscape will be managed and maintained as part of the implementation of this Policy. An initial Glossary supporting this landscape is provided at Appendix 3.

³ The Data Exploitation Lifecycle expands upon the NATO Information Management Lifecycle (Reference G), providing more granularity into the different aspects and stages of data as it progresses from “raw” data collected for a particular use case, into “curated” data that can be analysed and exploited as information. In addition, any data produced or received by NATO in pursuance of its legal obligations, missions or in the transaction of business is a record to be managed according to the Records Policy (Reference H). It should be noted that *the same* Policy or Guidance document might be applicable to multiple stages of the Data Exploitation Lifecycle, for example the Management of Non-Classified Information and Security Policy apply to both the “Secure Data” and “Securely Access and Share Data” stages.

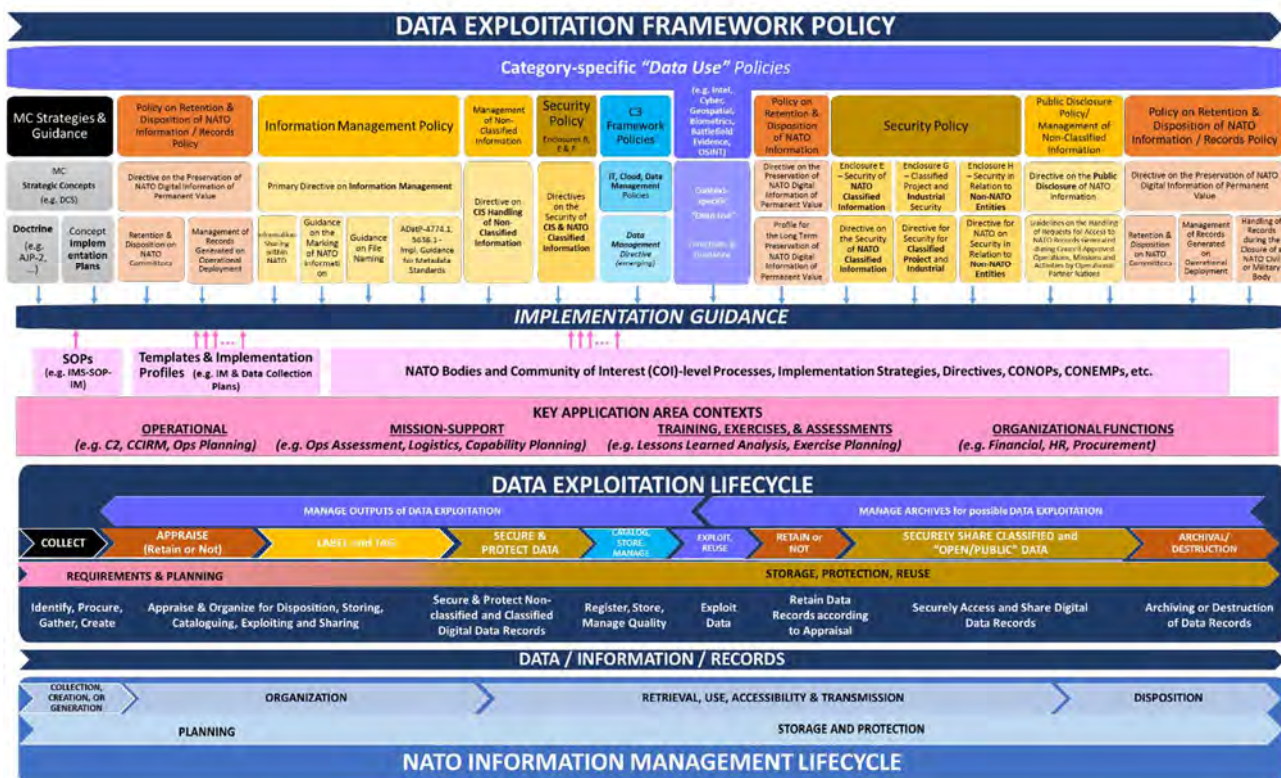


Figure 1 – Data Exploitation Policies and Guidance Landscape and Data Exploitation Lifecycle

II. SCOPE

13. The scope of the NATO Data Exploitation Framework Policy is the Alliance⁴, while the approach adopted here should help support both individual Allied national efforts, as well as provide a platform for engaging with partners in coalition formats:

- a) **Alliance:** NATO would act as a venue for Allies to share national approaches with a view to strengthening Alliance data exploitation, with a focus on scalable and interoperable data sharing, quality-assured life-cycle management of data, increased collaboration, and aligned data exploitation projects. Alliance-wide efforts are underpinned by the Vision, Desired outcomes and Objectives, and help drive the pursuit of a series of Data Exploitation enabling capabilities, concepts and policies to help support NATO in evolving into an organisation that treats data as a strategic resource.
- b) **Allied national efforts:** support Allies as they adopt and implement necessary policies, standards, capabilities and applications and identify and elicit and implement new data-exploitation projects individually, bilaterally, or multilaterally. NATO would

⁴ The Alliance are the Allies and the NATO Enterprise, as defined in Reference W.

provide the venue for Allies to discuss, exchange national good practices and align their data exploitation efforts and capabilities to foster interoperability and scalability.

- c) **NATO Enterprise**: develop specific directives, standards, capabilities, and applications for use across the NATO Enterprise entities – based on the identification of priority areas and use cases which are fundamental to how the Alliance operates.
- d) **Coalition**: develop standards profiles and service specifications to ensure interoperable data exploitation capabilities as part of a Coalition, e.g. Federated Mission Network.

14. Data Exploitation will be leadership-driven and user-led, based on a set of priority Alliance use cases that would support political and military decision making and improve NATO operational and functional processes. These priority Alliance use cases will be assessed and prioritized as part of a Data Exploitation Framework Strategic Plan.

III. OVERALL VISION

15. The following overall vision will drive data exploitation efforts:

The vision is to achieve information superiority and data-driven decision making at all levels across the Alliance by fully leveraging the value of NATO⁵ generated, national, and publicly available data.

The approach to data exploitation will be underpinned by core Alliance values and by principles of responsible development and use reflecting our shared values and consistent with applicable international law⁶. Our efforts will be built in secure, trusted, and reliable environments. These data exploitation efforts will be driven by a strong, collaborative culture which encourages sharing of data. Data exploitation expertise and tools will be made easily accessible to all.

DESIRED OUTCOMES

16. To achieve this **Vision**, a set of **Desired Outcomes** have been identified:

- Information superiority across all areas of the Alliance;
- Greater awareness, usability, and availability of quality data;
- Increased sharing of NATO, Alliance, and Coalition data and capabilities;
- Trusted, sound data, and its coherent governance to ensure data are treated as a valuable strategic asset;

⁵ Please see Glossary in Appendix 3 for definitions for NATO generated and national data.

⁶ NATO's core Alliance values are those reiterated during the 2021 Brussels Summit Communiqué (Reference X), namely individual liberty, human rights, democracy, and the rule of law, and further affirmed through para 8 of (NR) NATO's Artificial Intelligence Strategy (Reference E) as promoting democratic norms and values and ensuring respect for international law.

- Greater Alliance value from data, with increased evidence-informed decision-making within the political and military spheres;
- Better reporting on data exploitation and analysis results to decision-makers;
- Improvements in programs, policies, and capabilities development;
- Increased numbers of data science practitioners⁷ participating in a culture of innovation, learning, and experimentation to ease access to data exploitation;
- Data exploitation efforts aligned with core Alliance values, including the protection of personally identifiable information and privacy.

STRATEGIC GOALS AND OBJECTIVES

17. In order to achieve the Vision and Desired Outcomes, three key Strategic Goals have been identified in the areas of People, Processes, and Technology. These Strategic Goals and their supporting Objectives will form the basis for developing a Strategic Plan:

a) **Strategic Goal #1 (People)**

Empower our people to derive maximum value from data through a user-focused and leader driven approach.

Objective 1.1: Leadership driven integration of data exploitation into decision-making processes, in a form whereby decision makers and analysts are able to understand the context, caveats, and limitations of data-driven outputs so that they can be considered and evaluated for use;

Objective 1.2: Broadened data literacy, by providing managed, easy access to data, exploitation expertise, and tools, as well as to the policies, processes, and training to use them appropriately;

Objective 1.3: Established specialized data science competencies and increasing numbers of data science practitioners, working together to build a culture of innovation, learning, and experimentation through shared collaborative spaces, ideas incubators, managed self-service data analytics, and continuous learning opportunities;

Objective 1.4: Commitment to staff development in data exploitation and use, streamlining and improving recruitment, retention and upskilling of staff.

b) **Strategic Goal #2 (Processes)**

⁷ These are also known as “citizen data scientists” within industry. Please see Glossary in Appendix 3 for definition of citizen data scientists.

Establish a framework of coherent policies, processes, and simplified implementation guidance for leveraging Alliance, Enterprise, Coalition and public initiatives to enable data exploitation.

Objective 2.1: Principles and guidance to ensure data exploitation is underpinned by core Alliance values and principles of responsible development and use, and that data is protected and exploited in accordance with applicable national and international laws;

Objective 2.2: Robust governance and leadership across the organization to ensure coherent implementation;

Objective 2.3: Key policy enablers, such as legal frameworks, license agreements, and collaboration vehicles, that authorize the sharing of data and data exploitation frameworks;

Objective 2.4: Repeatable, simple procedures for planning, evaluating, and implementing data science projects to ensure they bring value to the decision-makers, can be leveraged by many, and are aimed to optimize the Functional and Operational Processes of NATO.

c) **Strategic Goal #3 (Technology)**

Establish a single logical environment for the Alliance, “secure and governed by design”.

Objective 3.1: Interoperable & interconnected CIS/IT, collaboration, data sharing and data exploitation services that are secure, trusted, and reliable;

Objective 3.2: Improved discoverability, availability, accessibility and interoperability of data that are of high quality, reliable, traceable, managed, and protected, preferably via managed NATO Catalogues;

Objective 3.3: Increased data science capabilities and data exploitation outcomes that are reliable, robust, traceable, reusable, responsibly developed, equitable, and governable.

IV. DATA EXPLOITATION PRINCIPLES

18. In order to ensure that all data exploitation work is guided by core Alliance values, principles of responsible use, and that the critical components of Council-approved policies concerning the sharing of data remain in place, a set of **Data Exploitation Principles**⁸ have been drawn up which will apply to all NATO’s Data Exploitation efforts. These principles collectively provide the rules of conduct that should be followed towards effective data exploitation across its full lifecycle.

⁸ These principles are built upon and maintain the integrity of Foundational Principles, as reflected in Appendix 1.

1) **Data are a Shared, Strategic Asset:**

- i) To advance common objectives, NATO Allies and the NATO Enterprise commit to share data to the greatest extent possible to address a set of priority Alliance use cases, which will be assessed and prioritized as part of a Data Exploitation Framework Strategic Plan.
- ii) NATO Enterprise will maximize data sharing and rights for data use to ensure NATO data are corporate⁹, shared, strategic assets.
- iii) Data will be made available for use through appropriate secured and protected mechanisms.

2) **Adherence to Applicable Legal and Regulatory Frameworks**

- i) Exploitation of NATO data will be governed under the aegis of the NATO Data Exploitation Framework Policy, and will respect Council-approved policies on Information Management (Reference G), Records Management (Reference H), C3 Framework (Reference I), including Data Management (Reference J), Security (Reference K, Reference L), Management of Non-Classified Information (N), and Public Disclosure (Reference M), Retention and Disposition of NATO information (Reference O, Reference P), in addition to other relevant policies approved in the future. Category-specific Data Use policies (e.g. Intelligence (Reference Q), Cyber (Reference R), Geospatial (Reference S), Biometrics Framework Policy (Reference T), Battlefield Evidence Policy (Reference U), Open Source Intelligence (Reference V), etc.) will apply, where relevant, in addition to relevant internal policies and rules applicable to the NATO Enterprise.
- ii) Data are owned by the entity (NATO nation, NATO entity, or third party) which creates, produces, or collects the data¹⁰ and maintains content, defines access rules, negotiates and agrees to release constraints, establishes disposition instructions, and is the authority for the life-cycle of information.¹¹
- iii) The collection, storage, sharing, and exploitation of data will be subject to requirements and legal restrictions specified by the information owner and will be handled in accordance to the extant policies, and their updates, as specified in principle 2.i. All action taken on the basis of shared data will be in accordance with applicable legal and regulatory frameworks. Collected data will be managed in

⁹ In support of the NATO Information Management Policy (Reference G) "Information as a corporate resource" and the Data Management Policy (Reference J) "Data as a corporate asset" foundational principles (Appendix 1).

¹⁰ With the exception of personal data in all its forms, which is covered by the personal data principles.

¹¹ Definition of the information owner, per the NATO Information Management Policy (Reference G).

accordance with the applicable policies and rules, and retention and disposition will be undertaken in consultation with the NATO Archivist and the Archives Committee.

- iv) The lifecycle of the data and the lifecycle of the information products derived or created from that data, such as intelligence products, assessment reports, etc., may take separate pathways, with potentially different category-specific Data Use policies applied, as applicable.
- v) Personal Data:
 - (1) Personal data should be accurate and kept only for as long as necessary and appropriate.
 - (2) Personal data should be protected and exploited securely; fairly and in accordance with applicable national and international law; and only for stated and limited purposes.

3) **Enabled Data Use and Custodianship:**

- i) NATO nations or NATO bodies with whom data are shared, act as custodians of the data, and shall comply with the requirements and legal restrictions of the owner for the sharing and use of the data. Data stewards¹² will support the custodians in enabling and ensuring compliance to stated requirements.
- ii) Unless otherwise specified by the information owner, data shared with NATO in NATO-led operations and exercises will be protected and handled in accordance with NATO agreed security, legal, and regulatory frameworks.
- iii) Data can be categorized as either national or NATO data, as indicated in the information owner and originator metadata that accompanies the data. The information owner and originator will facilitate proper handling by providing the appropriate originator, ownership, and confidentiality security policy metadata values, as well as any special handling rules.
- iv) In order to facilitate the digital management of data, the information owner will ensure that data is accompanied with complete and high quality metadata, as specified in the Data Management Policy (Reference J), Metadata Management Principles, and supporting directives or implementation guidance, to enable protection, handling, and management of the data throughout its full lifecycle. To ensure traceability and auditability, the following additional guidance should be followed:

¹² As defined in the Data Management Policy (Reference J) and referenced in the Glossary (Appendix 3).

- (1) Certain original metadata of the data shall be preserved throughout its lifecycle. Specifically, the Originator metadata should be specified and should become protected fields that do not change throughout the data/information lifecycle.
- (2) Ownership should be specified, and could change, but only in accordance with provided transfer of ownership rules (Reference G).
- (3) Confidentiality metadata values could change, but only with the permission of the information owner or in accordance to the specified handling rules. When these values do change, alternative metadata fields should be used if the original confidentiality metadata values have also to be maintained, to enable proper processing, such as to enable protected sharing through technical firewalls or information exchange gateways.
- (4) The confidentiality “security policy” metadata should not be used in place of the originator and ownership metadata.
- (5) If applicable, transfer of ownership rules and metadata changes should be stored electronically with the data/information.

4) **Digitized & Registered Quality Data:**

- i) To ensure the availability of data, there should be a concerted effort to digitize¹³ key¹⁴ data assets, and their accompanying metadata, and to register them within a NATO Data Catalogue, with common interface specifications, so that they can be managed, accessed, and exploited effectively.
- ii) Digitized data must be of high quality¹⁵—consistent, accurate, complete, accessible, available, and disaggregated, as necessary.
- iii) Information owners will plan for possible reuse of data, building in visibility and accessibility from the start by ensuring that data is properly marked and labelled with minimum metadata, according to the Data Management Policy (Reference J), Metadata Management Principles, and supporting directives or implementation guidance.

¹³ Digitization does not mean destruction of originals or long term preservation solution. Not all data can be digitized from a legal and contractual point of view, and certain records will still have to be kept in paper format (Reference H, and Reference O).

¹⁴ “Key” data assets can be identified as those that are needed for the prioritized Alliance use cases of the Data Exploitation Framework Strategic Plan.

¹⁵ It will be important to define and quantify the data quality factors so that they can be measured to provide an indication of the quality of the data and metadata. Some quality factors could be: "Accuracy", "Completeness", "Integrity", "Timeliness", "Relevance", "Consistency", "Reliability", "Appropriate presentation", "Accessibility", "Ease of Reusability", and "Uniqueness". Selection, definitions, and KPIs for these quality attributes are to be included as part of the Strategic Plan and Implementation Plans, as appropriate.

- iv) If the original data are not digital, information owners and custodians shall work towards ensuring that the original metadata and data are converted to a digital form conformant to NATO agreed standards, with original values preserved, if the data is to be stored and processed on a digital medium. Applicable Data Exploitation Principles should be applied to ensure metadata is provided and retained digitally regarding originator, ownership, transfer of ownership, and security handling.
- v) NATO should implement IT solutions that provide an opportunity to fully automate the data exploitation lifecycle, properly secure data, and maintain end-to-end records management, using automated data interfaces that are externally accessible and machine-readable, applying the interoperable by design principle.

5) **Governed Analytics**¹⁶:

- i) The Alliance affirms the following principles for enabling data pedigree, artificial intelligence application, and data analytics development.
 - (1) Lawfulness
 - (2) Responsibility and Accountability
 - (3) Explainability and Traceability
 - (4) Reliability
 - (5) Governability
 - (6) Bias Mitigation
- ii) Data exploitation models, algorithms, and data will be developed, documented, and used to support operationalisation of and compliance to the NATO AI Strategy's Principles of Responsible Use for AI in Defence (Reference E). Data should be timely, relevant, and accurate; and data should be subject to processes to maintain its quality and trustworthiness.

6) **Interoperable by Design**:

- i) The design of NATO's data exploitation models, algorithms, and data collection, storage and use should ensure interoperability among Allies.
- ii) All NATO entities will work with the Enterprise Coherence Authority to establish a data architecture approach that will allow the registration and sharing of data, models and algorithms across different systems, geographies, and functional silos

¹⁶ These Principles are drawn from the AI Strategy (Reference E), to ensure that the use of data for analysis and in the development of data analytics models and algorithms will facilitate compliance to the NATO Principles of Responsible Use for Artificial Intelligence in Defence.

using common agreed NATO standards, implementation profiles and service specifications. If it is not possible to share metadata conformant to the NATO agreed metadata standards, the appropriate mapping and transformation rules to the NATO agreed metadata standard are to be provided.

- iii) Technical standards and solutions for data and metadata should first be selected from the NATO Interoperability Standards and Profiles (NISP) standard (Reference Y), and then with international open standards and solutions adopted where necessary and added to the NISP, as required.

7) **Appropriately handled Unattributed data:**

- i) If previously shared data does not have any ownership or originator metadata associated with it, and they are marked or labelled with a NATO classification, it will be protected and handled as NATO data.
- ii) Applicable Data Exploitation Principles should be applied to ensure metadata is made available and retained digitally regarding originator, ownership, transfer of ownership, and security handling.

V. ROLES AND RESPONSIBILITIES

19. To drive forward NATO's Data Exploitation Efforts, the following roles and responsibilities will apply, covering overall governance and Enterprise management.

Alliance Governance

- a) Allies, through the North Atlantic Council, will exercise governance over this policy, related policies, and directives, to:
 - i) monitor compliance with, and ensure execution of, this Policy and supporting Directives by NATO Enterprise civil and military bodies;
 - ii) delegate these responsibilities of monitoring compliance with, ensuring execution of, consulting with relevant committees, including, inter alia: the Security Committee, Archives Committee, Cyber Defence Committee, as appropriate, and maintaining this Policy and subsequent related directives and strategies, to the Consultation, Command and Control Board (C3B), suitably reinforced, to act as the lead Council Committee for Data Exploitation.

Enterprise Management

20. In order to pursue the implementation of the overall vision, desired outcomes and objectives, as well as to ensure compliance with the Data Exploitation Principles and other foundational documents, and develop relevant Policies, directives, and strategies

for Data Exploitation, the following Enterprise Management function are being considered. The Data Exploitation Framework Strategic Plan will further define and assess the operationalisation of these roles.

- a) Enterprise Data Exploitation Board: The Enterprise Data Exploitation Board will be the Senior Enterprise management body overseeing NATO Enterprise Data Exploitation programmes, projects, and capabilities. The Board will have access to the appropriate advisory authorities, including Legal, Ethics, and Data Protection Advisors, NATO Information Management Authority (NIMA), NATO Archivist, and NATO Technical Authority. The Board would work closely with the Senior Executive Group (SEG) created as part of the NATO Chief Information Officer (NATO CIO) construct. The Board will be chaired by the NATO CIO to facilitate coherent Enterprise governance and management of this Policy's implementation with relevant initiatives.
- b) Data Exploitation Office:
 - i) Maximising use of existing resources and working across organisational boundaries, a NATO Data Exploitation Office would bring together relevant staff elements from across the Enterprise, under the potential leadership of a Chief Data Officer (CDO), to exercise data exploitation implementation responsibilities, as described below, and would work under the strategic leadership of the NATO CIO. An analysis of alternatives will be carried out to determine the need for a potential CDO function and additional personnel required to support the DEFP implementation. The creation of new functions will require an assessment by the Resources Policy and Planning Board (RPPB) and will be subject to RPPB's approval to ensure appropriate allocation of resources.
 - ii) The way in which the Data Exploitation Office (DEO) responsibilities are to be fulfilled is meant to be flexible, and should evolve as NATO matures as a data-driven Alliance and as a coherent Enterprise under the NATO CIO. These functions should initially be filled by existing staff members and Enterprise functional units¹⁷. Informed by the agreed priority Alliance use cases and aligned to the needs identified by the NDEMM analysis in maturing NATO in its data exploitation people, processes, and technology, the Data Exploitation Framework Strategic Plan¹⁸ would assess and recommend how these roles should be assigned, and would further refine and recommend how the roles and responsibilities are to be taken forward, including future resource requirements and planning. This Office will support the Data Exploitation Board with respect to coherent implementation of the Data Exploitation Framework Policy.

¹⁷ Including, inter alia, the Emerging Security Challenges Division, the Consultation, Command and Control (C3) Staff, Office of the Chief Information Officer, and representatives from the Strategic Commands.

¹⁸ In this way, "how" these roles are filled can be reviewed, assessed and agreed, as needed, with updates to the Strategic Plan.

- iii) Responsibilities for a potential CDO and/or a Data Exploitation Office may include:
 - (1) acting as the NATO analytics lead for the Enterprise, coordinating and advocating requirements for Data Exploitation in close cooperation with all stakeholders;
 - (2) ensuring coherent Enterprise management and implementation of this Policy, including the People, Processes, and Technology objectives, across the Enterprise bodies and organizational functional units, to achieve the DEFP Vision, Objectives, and Desired Outcomes;
 - (3) leading critical data exploitation efforts such as running data analytics pilot projects, improving data literacy, selecting and prioritizing analytics tools and services, establishing and managing a NATO Data Catalogue, reference and master data;
 - (4) defining Enterprise data exploitation inputs in the strategy associated with the management and governance of data and information, its effective exploitation, and related quality assurance and protection, in line with NATO's Digital Transformation Action Plan (Reference E);
 - (5) liaising and coordinating with Alliance data exploitation teams to facilitate and maximize sharing of data and data analytics resources to support the prioritized Alliance use cases;
 - (6) reporting implementation progress using the NATO Data Exploitation Maturity Model (NDEMM), analysing outcomes, and providing inputs to the Data Exploitation Framework Strategic Plans and annual Implementation Plans and Status Reports;
 - (7) maintaining and updating the NDEMM, as required.
- c) NATO Chief Information Officer (NATO CIO): In addition to the responsibilities delegated to the NATO CIO in Reference C, Reference Z, and above, the Office of the CIO will have a critical role to play to facilitate Data Exploitation, including in the following areas:
 - i) Governance & management on topics related to providing NATO capabilities to support Data Exploitation and automated Data Management;
 - ii) Contributing functional and non-functional requirements to provide the DEFP enablers and establish a single, logical environment for the Alliance that is secured and governed by design;
 - iii) Services to enable seamless and secured Data Sharing, Data Analytics & Visualisation, Data Management, Information Management, & Archiving.
- d) NATO Archivist: In addition to the responsibilities delegated to the NATO Archivist in Reference G, H, M, O, and above, the NATO Archivist will have a critical role to play to facilitate Data Exploitation of archived NATO data.

VI. IMPLEMENTATION BUILDING BLOCKS

Key Alliance Application Areas

21. The potential scope of applying Data Exploitation is all encompassing. In order to bring these into context, Key Alliance Application Areas for Data Exploitation are identified in Figure 2, taking into consideration various contexts, including:

- a) The three Alliance core tasks (Collective Defence, Co-operative Security, and Crisis Management);
- b) NATO core areas (Operational, Mission Support, Training, Exercises, and Assessments, and Organizational Functions);
- c) Recognized Operational and Functional Domains.

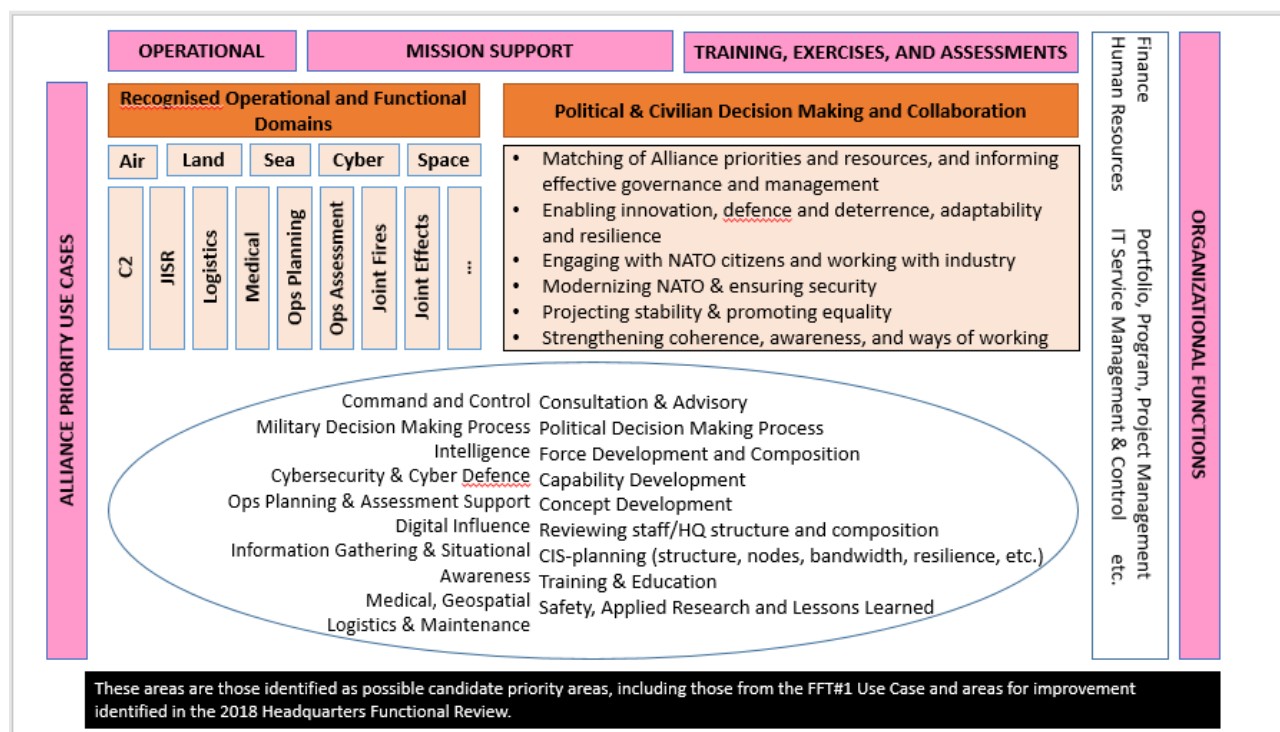


Figure 2 Key Alliance Application Areas¹⁹ for Data Exploitation

22. These Key Alliance Application Areas are not meant to be exhaustive, but to help identify opportunities and allow future activities to be prioritized without inhibiting the potential for data initiatives in non-Key Application Areas. These Key Alliance Application Areas could be used by leaders and users to guide the identification of specific Focus Areas and Use Cases Natural Language Processing in subsequent Strategy documents.

¹⁹ Some possible use cases identified in FFT #1 included AWACS predictive maintenance, real-time situational awareness, such as would be possible from processing Alliance Ground Surveillance (AGS) data, etc.

23. Data Exploitation projects will be leadership-driven and user-led, and include those that support priority Alliance use cases.

NATO Data Exploitation Maturity Model

24. Introducing a NATO Data Exploitation Maturity Model (NDEMM) will be key to measuring the progress and development of NATO’s data exploitation efforts. A maturity model provides an approach to measure and monitor progress on the maturity of NATO in its Data Exploitation activities in achieving the stated Vision, Strategic Goals and Objectives, and Desired Outcomes. It will help focus attention on key parts of the Enterprise and provide a basis for the targeted allocation of resources over time. Appendix 2 outlines the first version of this Model, which will be continuously reviewed and updated.

VII. NEXT STEPS AND RECOMMENDATIONS

25. The Data Exploitation Framework (DEF) expands upon the Framework Policy by identifying additional documents that will have to be developed and implemented next, in order to assist with the Policy’s implementation. Specifically:

- a. Data Exploitation Framework (DEF) Strategic Plan, will provide more concrete, practical steps to implement the Policy and will be reviewed and updated, as needed, every 4 years. The Strategic Plan, which may consolidate multiple Strategies, to achieve each of the Objectives of the Policy, will provide the initial strategic approach to implement the DEFP, prioritizing the Key Application Area Use Cases for the Alliance, and laying down the groundwork of activities needed to achieve the next level of Data Exploitation Maturity.
- b. DEF Implementation Plans, to be developed and reported on an annual basis, to enable the governance authorities to monitor and control the implementation of the Strategic Plan.



Figure 3 Components of the Data Exploitation Framework

26. This Data Exploitation Framework, shown in Figure 3, provides the strategy and approach to enable NATO to monitor and control its initiatives to use data as a strategic

resource. The next steps with anticipated timelines for the development of these documents, and their maintenance cycle, are the following:

- a) **Q1 2022** – Run a first assessment of NATO Enterprise Maturity, using the NATO Data Exploitation Maturity Model (see Appendix 2), which is to be reviewed and updated annually;
- b) **Q2 2022** – DEF Strategic Plan for 2023-2024; reviewed and updated in 2024, in-line with the review cycle and update of the AI Strategy (Reference E), and every 4 years after;
- c) **Q1 2023** – DEF Implementation Plan(s), reviewed and updated annually, to plan and report on implementation of the Strategic Plan.

27. The next steps to support the transfer of accountability from the Data Exploitation Working Group to the C3 Board will be to set up an interim Data Exploitation Office made up of relevant bodies of the International Staff Emerging Security Challenges division, C3 Staff, Office of the Chief Information Officer, and the Strategic Commands, with support from the Legal Advisors, NATO Archivist, and NATO Technical Authorities. These will support the C3 Board in updating its mandate to accommodate Data Exploitation and in developing the Data Exploitation Framework Strategic Plan (see Appendix 4 for more details).

RECOMMENDATIONS

28. Allies are invited to:

- a) Approve the NATO Data Exploitation Framework Policy contained in Annex 1;
- b) Note the Appendices attached to this policy, with a view to their further refinement and development as a basis for the Data Exploitation Framework Strategic Plan.

APPENDIX 1: FOUNDATIONAL PRINCIPLES

1. As identified in the Principles section of the Data Exploitation Framework Policy, the Data Exploitation foundational documents express a series of Foundational Principles that have to be adhered to across the Data Exploitation Lifecycle. The key foundational principles are captured and referenced in Table A.1:

NATO Information Management Policy (Reference G)	Records Policy (Reference H)	Data Management Policy – Data Management Principles (Reference J)	Data Management Policy – Metadata Management Principles (Reference J)
Information is a Corporate Resource	Ownership and custodianship	Data as a corporate asset	Metadata use
Information Ownership and Custodianship	Access to national information	Data Visibility	NATO core metadata
Leadership and Organisational Structure	Authenticity and integrity of records	Data Accessibility	Metadata schemas
Information Sharing	Preservation and accessibility	Data Preservation	Metadata classification
Information Standardisation	Usability and completeness	Data Interoperability	Metadata evolution and life-cycle
Information Assurance	Retention	Data Assurance and Security Management	Marking, labelling and binding
Information Needs	Release	Data Quality	Automation.
	Disclosure	Data Architectures	Data management principles applicability
NATO Security Policy (Reference K) – Directive on the Security of NATO Classified Information (Reference L)		Data as an Enterprise Resource	
All Basic Principles in Enclosure “B”		Master Data	
Aggregation Principle		Data Stewards	
Changing NATO Security Classification or Declassifying NATO Classified Information			

2. Table A.1: Foundational principles of the DEFP

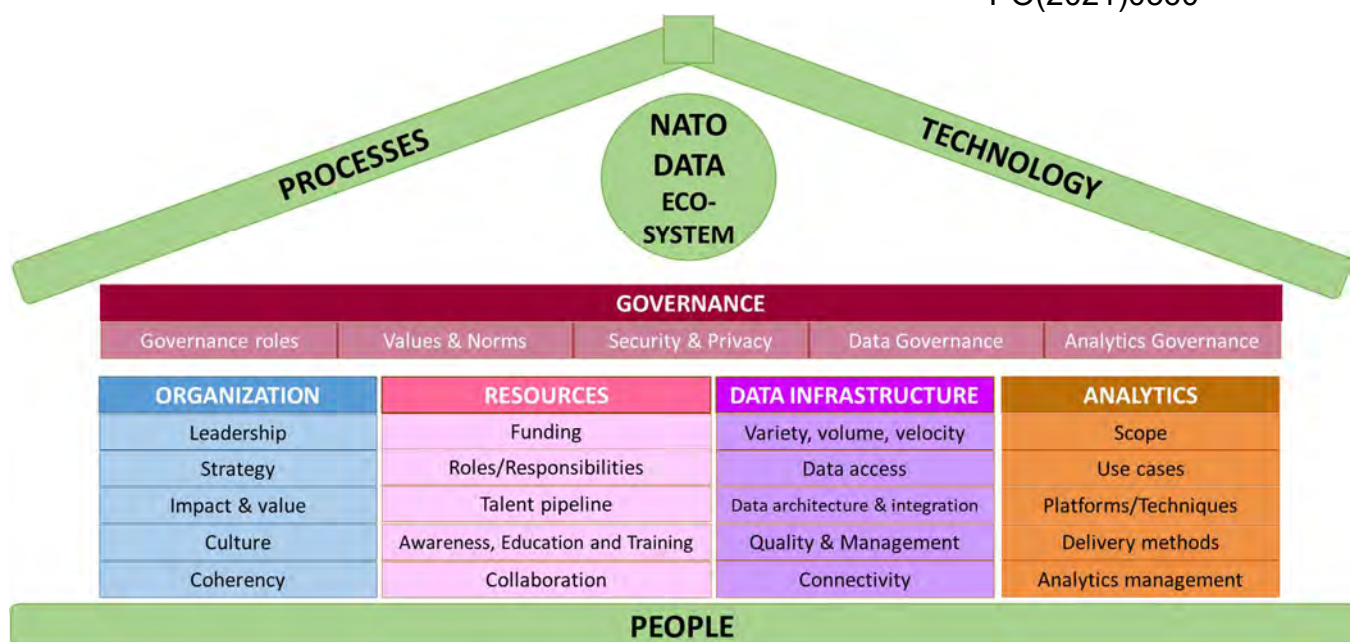
2.1.

3.

APPENDIX 2: NATO DATA EXPLOITATION MATURITY MODEL (NDEMM)

1. The NATO Data Exploitation Maturity Model (NDEMM) will be the means by which development of the maturity of the NATO Enterprise in treating data as a strategic resource will be understood over time. This NDEMM was developed by adopting the Transforming Data With Intelligence (TDWI) Analytics Maturity Model²⁰, and adapting it for use within NATO. The TDWI model was selected as it was the most mature, complete, and easy to use, and TDWI provided their consent for the employment of their Questions and Answers for NATO.
2. The NDEMM, shown at Figure B.1 below, is a 2-tier model to address both Alliance and NATO Enterprise contexts. Around the outside, we have the 1st tier Enablers of People, Processes, and Technology. These three Enablers are aligned with the DEFP objectives, respectively, as these are what the Alliance will strive to provide to enable data exploitation across NATO. To provide more guidance on how to deliver these Enablers, we have the 2nd-tiered Factors of Governance, Organization, Resources, Data Infrastructure, and Analytics. These Factors could apply to one or more of the 1st tier Enablers, and are the additional aspect of what the Alliance and Enterprise will need to focus on to mature and provide those Enablers.
3. Finally, for each of these 2nd Tier Factors there are Dimensions, which provide an even more detailed look into each Factor. For example, the Leadership, Strategy, Impact and Value, Culture and Coherency dimensions, are specific aspects of the Organization factor. These dimensions can describe characteristics, elements, or activities desired at each level, which can then be used to assess our maturity.
4. —
- 5.

²⁰ Maturity Models and Assessments | Transforming Data with Intelligence (tdwi.org)
<https://tdwi.org/pages/research/maturity-models-and-assessments.aspx>



- 6.
7. Figure B.1: The NATO Data Exploitation Maturity Model (NDEMM)
4. The maturity indicators, in the form of the questions and answers to assess these enablers, factors, and dimensions, mostly come from the TDWI Analytics Maturity Model. These were adapted into the NATO context, whereby some factors, dimensions, questions and answers were added or updated, and then grouped together to assess the People, Processes, and Technology Enablers aligned to each of the DEFP strategic goals and objectives. The details of the NDEMM maturity indicators and assessment calculations can be made available upon request, and will be managed and maintained by the Chief Data Officer as part of the implementation of this Policy.
5. Please contact the NATO HQ IS-ESC Data Policy Unit at mbx.isescdatapolicyunit@HQ.NATO.INT to get more in-depth analysis and information regarding the NDEMM, such as the answers to these indicators that serve as the basis for calculating the maturity level, or Indicators per Dimension, Indicators per themed-Objective, Assessment calculations, etc.
- 8.

APPENDIX 3: GLOSSARY

1. In order to facilitate the implementation of this Policy, an initial understanding of various terms are captured to maximise common understanding. Recognising the wider importance of securing standardised interpretations, these terms will be further refined²¹ in order to secure their formal submittal and inclusion in the NATO Terms standard²². In the meantime, this initial working Glossary, as set out below, should facilitate work to progress on key aspects, such as the Data Exploitation Framework Strategic Plan, including but not limited to the following:
 - a. **Analytics/Exploitation Teams**: There are a number of roles and responsibilities required at the Data Exploitation implementation layer that are specific to data analytics and data science activities, and reflect disciplines under the heading of “Data Scientists”. These could include roles such as Data Engineers, Business Intelligence Analysts, Data Analysts, Big Data Experts, AI or Machine Learning Experts, Software Developers, etc.
 - b. **Citizen Data Scientist**: Citizen data scientist is a term used in industry to describe when existing business roles are “trained up” to fill the “data scientist expertise gaps” so that they can support the Analytics/Exploitation teams in analysing data, and creating data and business models for their companies with the help of big data tools and technologies. Citizen data scientists do not necessarily need to be data science or business intelligence “experts”; rather, this role can be assigned to employees in an organization who learn how to use the big data tools and technology and apply them within their day-to-day work.
 - c. **Data**: The term Data includes, but is not limited to “raw” data, information and data analytics resources, such as models, algorithms, reports, etc. Data and information are used interchangeably, as the definition is dependent on the perspectives and relative to the “use” context. “Data” is considered unorganized, while “information” is considered organized, structured, etc. However, as it is dependent on the use context, “data” could be considered the *input* to a data exploitation process while “information” could be considered its *output*. One process’ output (i.e. information) could be considered another process’ input (i.e. data), and vice versa
 - d. **Data Analysis/Analytics Lifecycle**: The Data Analytics Lifecycle is a subset of the Data Exploitation Lifecycle, focused on the detailed steps in the “collecting, preparing and processing” of data so that it can be analyzed with the goal of deriving useful information from it. Data analysis focuses on human analysis of the data; data analytics add computing tools and AI techniques, or machine-enabled analysis, such as machine-learning, natural language processing, statistical analysis, and/or computer-based models and simulation, to enhance the processing and analysis of the data to improve the insight that can be gained from it and to support better decision making.

²¹ To include looking into aligning agreed terms from the Data Management Association (DAMA) dictionary of terms, where applicable.

²² AAP-06, NATO Glossary of Terms and Definitions, covered by STANAG 3680.

- e. **Data Analytics:** There are “four types of data analytics,”-- “Descriptive”, “Diagnostic”, “Predictive”, and “Prescriptive” – which provide scaled improvements in the machine-enabled analysis (or analytics) of the data, therefore impacting the types of insights that can be gained and types of questions that can be answered.
 - i) Descriptive and Diagnostic analytics typically focus on understanding the past, typically used for canned and ad-hoc reporting, queries and drilldowns, and discovery and alerts. These normally answer questions such as, “What happened?”, “How many, when, and where?”, “Why did it happen?”, and “Where should we look?”
 - ii) Predictive and Prescriptive analytics focus on the future, typically using statistical and predictive modelling, random testing, and optimization methods. These normally are used to answer questions such as, “What is the pattern?”, “What will happen next?”, “What if we try this?”, or “What is the best action?”
- f. **Data Analytics Deployment:** the roll out and application of data analytics in a live environment using actual operational or organisational data.
- g. **Data Exploitation:** Data Exploitation is an umbrella term to encompass the full spectrum of activities involved with enabling NATO to leverage on, gain value from, and manage data as a strategic resource. This covers existing activities with established processes, such as Data Requirements setting and Planning, CIS Management and Protection, Data Collection, Information Analysis, Information Management, and Archival-related Records management; while expanding upon and including activities related to Data Use, Data Analytics development, and the application of data science and AI- techniques, such as Big Data analytics, Natural Language Processing (NLP) and machine learning (ML).
- h. **Data Exploitation Lifecycle:** The Data Exploitation Lifecycle builds upon the NATO Information Management Lifecycle (Reference G), providing more granularity into the different aspects and stages of data exploitation as it progresses from “raw” data/information²³ into collected, catalogued, curated and enriched data for data analytics and records²⁴ managed for archival purposes.
- i. **Data/Information Management Teams:** These teams are focused on managing the data/information through its lifecycle to ensure that the data and information management processes are followed. In general, they are a cohort responsible for custodianship of data or information irrespective of its perceived or actual quality, intended or likely uses and management of the data enabling its exploitation. These could include roles such as Data Collectors, Data Stewards, Data Quality Assurance, Information Managers, Archivists, etc.
- j. **Data Scientist:** Of note is the role of “Data Scientist”, which many consider in the private sector as a “mystical, rare unicorn”, as it is very difficult to find a single person who can fulfil this role. A data scientist is an individual, organization or application

²³ Please note that we consider data and information as interchangeable, as the definition is dependent on the perspectives and relative to the “use” context. “Data” could be considered the input to a data exploitation process for a particular use case, while “information” could be considered its output. One process’ information could be considered another process’ data, and vice versa.

²⁴ We distinguish data/information from records only in the context of the records management processes – whereby data/information should be appraised early in its lifecycle (Reference N) as potential “NATO records” to be managed according to Reference H.

that performs statistical analysis, data mining and retrieval processes on a large amount of data to identify trends, figures and other relevant information. A data scientist performs data analysis on data stored in data warehouses or data centers to solve a variety of business problems, optimize performance and gather business intelligence. This “data scientist” role would be expected to be able to cover all aspects from the analytics team, from software development, data collection through to the business analyst roles. In reality, a data scientist would only be able to cover a subset of these roles, and would rely on a team made up of mix of data stewards, data engineers, data analysts, machine-learning experts, and operational/business analysts to support them.

- k. **Leaders & Decision Makers**: Irrespective of seniority, from squad leader to 4-star general/admiral, or from team leads to the ASG, leaders and decision-makers are the ultimate end-users of the analysis/analytical outputs provided by data exploitation. They are responsible for managing data exploitation activities within their team, including through prioritisation efforts and leadership driven integration of data into their decision-making processes.
- l. **National data**: Data produced by a nation or national unit not operating in a NATO context and which carry national markings, and may be marked released to NATO, if it is sharable with NATO. Typically, if the data is shared with NATO, it may be subject to requirements and legal restrictions specified by the information owner, such as specific legal and regulatory frameworks.
- m. **NATO data**: NATO data is defined as data that originates from or is produced by NATO entities using NATO or National information systems, and which carry the NATO marking. If data shared with NATO does not have any originator or ownership marking, and carries NATO marking, then it will be considered NATO data.
- n. **NATO Data Eco-system**: NATO’s virtual socio-technical network construct, which brings together the People, Processes, and Technology aspects of the data network to enable actors to interact and collaborate to find, archive, publish, consume, or reuse data as well as to foster innovation, create value, improve functional and operational processes, and develop new concepts. There will be two separate NATO eco-system concepts, namely:
 - i) **NATO Partners Public / Open Data Eco-system**: which will be the NATO Data Eco-system limited to only handling public and publicly disclosable NATO data, with appropriate governance, people, processes, and technology enablers,
 - ii) **NATO Protected Data Eco-system**: which is the NATO Data Eco-system which will also allow exploitation of protected and classified data
- o. **NATO entities**: These are the NATO bodies and organizational units that participate within the NATO Data Ecosystem. These could be the
 - i) NATO Bodies, such as Allied Command Operations, Allied Command Transformation, International Staff, etc.,
 - ii) NATO Support Agencies and Organizations, such as the NCI Agency, Science and Technology Organization, NSPA, etc., or the
 - iii) Other types of organisation, national and multinational units that are actively supporting a NATO context or responsible to a NATO command, such as the Munitions Safety and Information Analysis Centre (MSISAC), Rapidly Deployable Corps forces, etc.

- p. **NATO Individuals**: All NATO Individuals play a vital role in enabling the use of data as a strategic resource and in making NATO a data-driven digital enterprise. In particular, as participants in the Data Exploitation Lifecycle and Information Management Lifecycle (Reference G), they must understand the importance of acting in accordance to the roles and responsibilities set out in previously agreed documents (References G, H, I) in their day-to-day work activities. Therefore, the DEFP highlights and reconfirms the importance that everyone has the roles and responsibilities to potentially act as:
- i) Data Collectors and Stewards (Reference I [Annex 13])
 - ii) Originators (Reference G, J, H)
 - iii) Information Owners (Reference G, H)
 - iv) Information Custodians (Reference G, H)
- q. **Operational Functions/Units**: In the corporate world, the term business units and business functions are typically used for the organizational structures on an entity. Since NATO is not a commercial business, the term operational functions and operational units may be used instead, especially for organizational structures set up for supporting military operations. Organizational functions and operational functions may be used interchangeably.
- r. **Organizational Functions/Functional Units**: In the corporate world, the term business units and business functions are typically used for the organizational structures on an entity. Since NATO is not a commercial business, the term organizational functions and functional units may be used instead, especially for organizational structures set up for non-military operations. Organizational functions and operational functions may be used interchangeably.
2. To ensure consistency, key terms already defined in foundational documents or the NATO Terms standard will be used and referenced here. Specifically, the following terms are used:
- a. **Data Steward (Reference I, Reference J)**: Role within the NATO Enterprise responsible for utilising the data related processes, policies, directives, and with responsibilities for administering data in compliance with approved policy. The responsibilities of data stewards shall include the inception of data elements, the extension of data elements across data lifecycle, the population of data repositories, the authorisation for data use and the retirement of data elements. They shall also be responsible for identifying duplication of data elements and taking the corrective actions, and for data quality, security and availability of the data for which he or she is data steward.
 - b. **Information Custodian (Reference G)**: The nation or organisation which receives information and makes it visible and is responsible to the information owner for the agreed level of safe-keeping and availability of information.
 - c. **Information Owner (Reference G)**: The nation or organisation which creates and maintains content, defines access rules, negotiates and agrees to release constraints, establishes disposition instructions, and is the authority for the life-cycle of information.
 - d. **Originator (Reference G, K)**: The nation or international organisation under whose authority the information has been produced or introduced into NATO.

APPENDIX 4: Suggested Governance and Enterprise Management Way Ahead²⁵

1. To date, a working level coalition between the Data Policy Unit (DPU) in IS-Emerging Security Challenges Division, ACT, IS-Office of Legal Affairs, C3 Staff, NATO Office of Security (NOS), OCIO and NATO Archivist has prepared the Data Exploitation Working Group (DEWG) agreement of the DEFP – the sole task for which the DEWG was established.
2. The transition away from drafting Policy and Directives at a high level to implementing the Data Exploitation Operating Model, however, demands a more robust organisation with clearer lines of authority, responsibility and accountability.
3. The Data Exploitation Office (DEO) would be established under the oversight of the C3 Board in its role to govern NATO’s Data Exploitation efforts and would draw upon the expertise from relevant NATO bodies to deliver v1.0 of the DEF Strategic Plan.
4. Based on guidance outlined in paragraph 20, the Strategic Plan will include a recommendation on how the Enterprise Management functions should be filled and indicate resource requirements for the management and implementation teams, based on Alliance Priority Use Cases, NDEMM maturity assessment, and Target Maturity goals to ensure that they will address the needs of the Alliance, with a suggested model shown in Figure D.1.

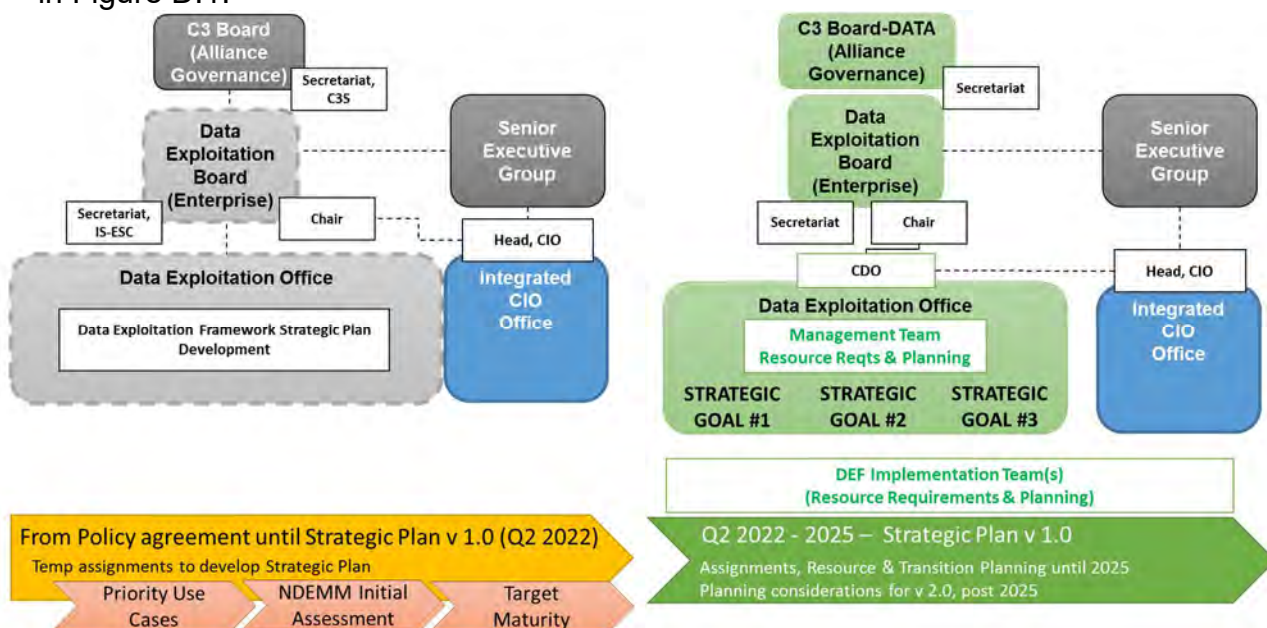


Figure D.1: Suggested Governance and Enterprise Management Way Ahead

²⁵ The suggested governance and enterprise management way ahead follows a similar approach to organizational arrangements for IM, and is adapted from the agreed NATO Information Management Authority (C-M(2009)0035 (INV)) setup.

5. The DEO would comprise those Data Exploitation stakeholders each of whom has formally assigned specific responsibilities to develop each of the three Strategic Goals.
6. The DEO working methods to deliver v1.0 of the DEF Strategic Plan would be set out in co-ordination with relevant stakeholders through a Terms of Reference to be agreed by January 2022.
7. The DEO would be responsible for implementation of the DEFP and the Data Exploitation Strategic Plan across the Enterprise and be accountable to the Enterprise Data Exploitation Board.
8. Relevant elements from across the NATO Enterprise would need to nominate an appropriate single point of contact within that organization to be responsible for co-ordinating with the DEO and for ensuring that their respective Data exploitation plans and programmes are implemented in accordance with the DEFP and the Strategic Plan.

NATO UNCLASSIFIED



7 October 2021

MCM-0142-2021

SECRETARY GENERAL, NORTH ATLANTIC TREATY ORGANIZATION

MILITARY COMMITTEE ADVICE ON NATO DATA EXPLOITATION FRAMEWORK POLICY

References:

- A. AC/341-WP(2021)0001-REV6-AS1, Data Exploitation Framework Policy, 1 Oct 21.
- B. AC/322-WP(2021)0015-REV2-AS1, Data Exploitation Framework Policy, 1 Oct 21.
- C. MCM-0200-2020, MCM-0200-2020 to NATO Warfighting Capstone Concept, 28 Jan 21.
- D. PO(2021)0042, Political-Military Advice on the NATO Warfighting Capstone Concept, 15 Feb 21.
- E. MCM-0099-2021, Initial Warfare Development Agenda, 18 Jun 21.
- F. PO(2021)0059, Approval of 'Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies', 15 Feb 21.
- G. IMSM-0149-2019 (INV), Data Centric Security Vision and Strategy Proposal for the Alliance Federation including the NATO Enterprise, 17 May 19.
- H. DPRC-N(2021)0033-REV6-AS1, NATO's Artificial Intelligence Strategy, 30 Jul 21.
- I. PO(2020)0147, MCM-0033-2020 Military Committee Advice on Strategy to Develop and Sustain a NATO Intelligence Systems Architecture, 24 Apr 20.

BACKGROUND

1. As tasked by the Council, the Data Exploitation Working Group (DEWG) produced and approved the Data Exploitation Framework (DEF) Policy (Reference A). The Consultation, Command and Control (C3) Board also approved the DEF Policy (Reference B). The DEF Policy will now be forwarded for Council's approval along with this military advice.

2. The DEF Policy articulates NATO's objectives, strategy and approach for the use of data as a strategic resource building on relevant parts of NATO's extant policy framework and maintaining the integrity of these Council-approved policies. The DEF Policy also examines options on how best to ensure a robust NATO-wide governance and utilization of data as a strategic asset.

NATO UNCLASSIFIED



NATO UNCLASSIFIED

3. The Military Committee (MC) at Chiefs of Defence level approved the NATO Warfighting Capstone Concept (NWCC) on 28 Jan 21 (Reference C). The Council then approved it on 15 Feb 21 and Defence Ministers endorsed NWCC on 17 Feb 21 (Reference D) as the Alliance's military strategic warfare development concept, planning the way for the next 20 years. NWCC articulates 25 lines of delivery and the Warfare Development Agenda (WDA) is the vehicle to achieve them. SACT delivered the initial Warfare Development Agenda (iWDA) on 26 Apr 2021, which the MC endorsed and submitted to the Council for notation (Reference E).

4. Both Reference C and Annex E of Reference E stress the importance of the exploitation of data in support of the employment of the military instrument and its development, through both the NATO Data Exploitation Programme line of delivery and the emphasising of data as a critical enabler across capability development efforts. The military strategic framework of NWCC and WDA describes a clear military imperative for the DEF Policy and its guiding principles and efforts.

5. The Council agreed NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies (EDTs) (Reference F), which confirms data as a foundational EDT and data exploitation as a key enabler for rapidly adopting EDTs, including Artificial Intelligence (AI) and autonomy.

6. The MC has already initiated an ambitious data centric programme with Reference G. A Data Centric Security (DCS) Implementation Plan, to be updated regularly, intends to turn the DCS Vision and Strategy into reality.

AIM

7. To provide the military advice on the DEF Policy at References A and B to inform Council decision.

CONSIDERATIONS

8. Building on extant Policies. The MC recognizes that NATO is not starting its data exploitation effort from a static position, but rather from a situation where there is already an extant and comprehensive policy framework shaping the management and usage of information and data, from multiple dimensions and for several communities of interest (COI). The DEF Policy correctly referenced several key MC strategies and guidance pertaining to information or data management for specific military COI. The MC therefore welcomes that the DEF Policy explicitly recognizes the existence of this rich set of extant policies, from which to build NATO's data exploitation framework. Moving forward it will be important to ensure coherence across this expanding policy framework. From a military perspective, the NATO Data Exploitation Programme line of delivery of the WDA could be used for this purpose.

NATO UNCLASSIFIED

9. Roles and Responsibilities - Governance. The MC supports the recommendation for Council to delegate governance of data exploitation to the C3 Board to ensure coherence with extant data related efforts and other underpinning digital enablers. As NATO advances with data exploitation and other EDT, it needs to establish a consistent set of digital responsibilities. The MC also welcomes the principle of “leadership-driven and user-led, based on a set of priority Alliance use cases” and asks to be consulted when the time comes to prioritize military use cases. The MC will task the strategic commands to lead the development of military use cases.

10. Roles and Responsibilities - Management. MC recommends preserving the digital coherence authority with the newly established NATO Chief Information Officer (CIO) for the NATO Enterprise and the CIO should therefore have a leading role in data exploitation services in the NATO Enterprise. The scattering argument made for governance also applies for management. Given the data exploitation ambitions associated with the NWCC and required to support the EDT implementation strategy (Reference F), the MC also believes SACT and ASG ESC will have important roles to play.

11. Enabler for Multiple NATO initiatives. This DEF Policy needs to enable and facilitate current and future NATO initiatives, in particular the NATO Data Exploitation Programme jump - starter in the WDA (Reference E, Annex E), and the critical enabler “Data” (the detailed description is expected in the next iteration of the WDA). It should also be an enabler for NATO’s emerging AI Strategy (Reference H).

12. Scope of Data. The MC understands that this policy pertains to all data sources: public, NATO owned and Allies and Partners shared; classified and non-classified. This is the correct scope as military insight supporting command and control and other essential military functions will increasingly rely on a growing amount of data complemented by other EDTs such as AI. As such, it is important that the DEF Policy and future associated plans and directives enables the sharing of larger amounts of data.

13. Implementation. Beyond the DEF Policy approval, implementation will be crucial. From a military perspective, data exploitation is foundational in building-up Cognitive Superiority over potential adversaries. In particular, data exploitation enables the NWCC influence and power projection and multi-domain defence imperatives. The MC recognizes that stakeholders’ collaboration is key, and, among others, HQ SACT and ESC’s Data Policy Unit should continue to collaborate closely when developing implementation plans for the WDA’s Data Exploitation Programme and the DEF Policy thus ensuring a coherent approach, helping to avoid redundancies and to exploit synergies with and amongst other programmes and projects. The WDA should be the main vehicle to implement Data Exploitation. The MC encourages, where appropriate, the DEF Policy to influence programmes such as Allied Future Surveillance Capability (AFSC), Joint Multi-Domain Command and Control (JMDC2), NATO Intelligence Systems Architecture (Reference I), and Federated Mission Networking (FMN). The MC also invites the Strategic Commands to facilitate the implementation of this policy through warfare development efforts including the development of common funded capabilities.

NATO UNCLASSIFIED

14. Data Centricity. As stated in the iWDA (Reference E), the MC is convinced that a shift towards data centricity is a condition sine qua non for NATO to remain a successful alliance. In addition to the DEF Policy, the DCS Vision and Strategy (Reference G) is a step in that direction, which must be reinforced and accelerated as much as possible. In this context, the DEF implementation efforts must be synchronized with on-going DCS implementation efforts.

CONCLUSIONS

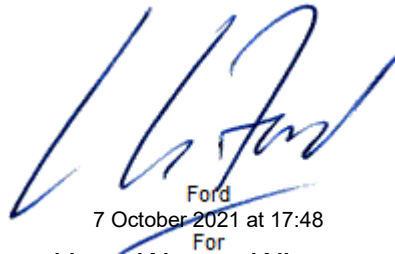
15. Based on the above considerations, the MC:
- a. Agrees leveraging extant policy framework and complementing it over time with the necessary directive, guidance and standards to achieve data exploitation goals and objectives. The MC will contribute to this framework as required.
 - b. Supports the C3 Board having delegated governance responsibilities over data exploitation, recognizing the C3 Board's extant leading role for information and data management and ensuring coherence across the C3 domain.
 - c. Also supports preserving the NATO CIO coherence function by assigning leadership role for data exploitation. For the NATO Enterprise, in particular for the NATO Command Structure and in support of the Alliance, coherent management of information and communications technology, cyber and data exploitation is imperative.
 - d. Emphasises the need for synchronization with the projects, programmes and initiatives that will feed from or contribute to data exploitation.
 - e. Understands the scope of the DEF Policy to be all data, as detailed in Paragraph 12, and highlights that military decision-making needs to be supported by enhanced data exploitation. The DEF Policy and subsequent documents must continue to encourage and facilitate the sharing of data among Allies and Partners in all military domains.
 - f. Underlines that the WDA should be the main vehicle to implement the DEF Policy and that cooperation among multiple stakeholders will be key.
 - g. Reinforces the importance of a shift of culture, mind-set and capability development approach towards data centricity. The MC endeavours to accelerate on-going work on Data Centric Security.

NATO UNCLASSIFIED

RECOMMENDATIONS

16. The MC recommends the Council to note this military advice to inform its deliberations and decision on the DEF Policy.

17. This document clears IMSWM-0237-2021 and all SDs thereto.

FOR THE MILITARY COMMITTEE:

Ford
7 October 2021 at 17:48
For

Hans-Werner Wiermann
Lieutenant General, German Army
Director General
International Military Staff

Copy to: IMS SDL CG+MR+SC+SCR+DIV, IMS-LS.

Originating Office: NHQC3S

Action Officer: LtCol Duemichen (5309) (TT+2021-03536)

Taxonomy: Information and Knowledge Management (INF) - INF - Policy

NATO STANDARD

ADatP-4774

**CONFIDENTIALITY METADATA
LABEL SYNTAX**

Edition A Version 1

DECEMBER 2017



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED DATA PROCESSING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

20 December 2017

1. The enclosed Allied Data Processing Publication ADatP-4774, Edition A, Version 1, CONFIDENTIALITY METADATA LABEL SYNTAX, which has been approved by the nations in the Consultation, Command, and Control Board (C3B), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4774.
2. ADatP-4774, Edition A, Version 1, is effective upon receipt.
3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.
4. This publication shall be handled in accordance with C-M(2002)60.



Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

INTENTIONALLY BLANK

INTENTIONALLY BLANK

TABLE OF CONTENTS

1	Introduction	1-1
1.1	Background	1-1
1.2	Objective	1-2
1.3	Scope	1-2
1.4	Assumptions.....	1-2
2	Confidentiality Metadata Label Requirements	2-1
2.1	Overview	2-1
2.2	Common Security Policy	2-1
2.3	Requirements.....	2-3
3	Terms and Definitions	3-1
3.1	Abbreviations	3-2
4	Labelling	4-1
4.1	Introduction	4-1
4.2	Concepts and Terminology	4-1
4.3	Succession Handling.....	4-3
4.4	Syntax	4-3
5	Policy	5-1
5.1	Introduction	5-1
6	References	6-1
	APPENDIX 1: Confidentiality Metadata Label Schema	App 1-1
	ANNEX A: Schema	App 1-A1
	ANNEX B: Examples.....	App 1-B1
	APPENDIX 2: NATO Security Policy Confidentiality Labels.....	App 2-1
	ANNEX A: Example Clearances for Nations	App 2-A1
	ANNEX B: Security Policy Information File	App 2-B1
	ANNEX C: PUBLIC Security Policy Confidentiality Labels.....	App 2-C1
	ANNEX D: PUBLIC Security Policy Information File	App 2-D1

INTENTIONALLY BLANK

1 Introduction

1.1 Background

The NATO Information Management Policy [C-M(2007)0118] guides the establishment of an IM Framework for efficient and effective information management, enabling decision-making by the sharing of information within and between NATO, the Nations and their respective Communities of Interest. The NATO Security Policy [C-M(2002)0049] and supporting directives cover all aspects concerning the secure handling of information.

In accordance with the NATO Interoperability Policy [Source C-M(2009)0145] standards are to support interoperability between NATO, the Nations and their respective Communities of Interest to act together coherently, effectively and efficiently to achieve allied tactical, operational and strategic objective, especially to support the achievement of Information Superiority within an information sharing networked environment.

This ADatP-4774 is published by the Consultation, Command and Control Board (C3B) and is authorized for public disclosure. It supports the cooperation with external actors in line with the Lisbon Summit decisions on the Comprehensive Approach as well as the following principles of the NATO Information Management Policy and NATO Network Enabled Capability (NNEC) Strategies for Data and Technical Services [AC/322-D(2005)0053-REV2, dated 14 Sept 2009]:

Information Ownership and Custodianship. Information shall have an originator, and clearly defined ownership and custodianship assigned throughout its life-cycle.

Information Sharing. Information shall be managed with an emphasis on the 'responsibility-to-share' balanced by the security principle of 'need-to-know', and managed to facilitate access, optimise information sharing and re-use, and reduce duplication, all in accordance with security, legal and privacy obligations.

Information Standardisation. Information shall have standardised structures and consistent representations to enable interoperability, cooperation and more effective and efficient processes.

Information Assurance. Information shall be protected by applying the principle of Information Assurance, which is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication.

Data Assurance. The authority of the source and integrity of the data can be determined and assessed because of the history, security level, and access control level of each data asset is known and available.

The Military Committee recommendation on the Implementation of the NATO Federated Mission Networking Capability [MCM-0106-2014] provides the framework for establishing information sharing in a federated networked environment in support of coalition operations. The NATO mission environment is evolving from network-centric based security architecture to Data-Centric based security architecture.

1.2 Objective

The objective of this document is to provide common XML-based formats and syntax for security policies and confidentiality metadata. Information objects and data assets can be labelled to support access and release decisions in a manner that is understandable to all coalition partners.

This document provides the semantics for a common security policy based on agreed NATO Security Policy and supporting directives.

1.3 Scope

This document addresses aspects of information management that are required to enable the security of information sharing. Technical implementation of this standard will require detailed implementation profiles specific to usage scenarios where technology permits. These profiles are published in ADatP-34 (NATO Interoperability Standards and Profiles).

1.4 Assumptions

This document was developed using the following assumptions and constraints:

- National Security Policies will not change through the application of this standard;
- This standard must reflect National Security Policies;
- Information sharing in a federated networked environment is based on an agreed Common Security Policy;
- A Common Security Policy must be adjustable to reflect event specific requirements; and
- Equivalencies between National Security Policies and a commonly agreed security policy can be defined.

2 Confidentiality Metadata Label Requirements

2.1 Overview

Nations and some organisations implement organisational specific information security policies. Typically these policies support one or more of the following objectives:

- Achieve and maintain protection of information determined by its confidentiality;
- Ensure that information receives an appropriate level of protection;
- Prevent unauthorized disclosure, modification, removal or destruction of information, and interruption to the organisation's activities.

In the physical paper-based information environment, confidentiality is represented by markings¹, usually at the top and bottom of a page, and sometimes also applied to portions of the information such as titles or paragraphs, also known as portion-marking. Those markings are typically specific to the language and context of the originating organisation and not universally understood (e.g. CONFIDENTIAL, ПОВЕРИТЕЛНО, 机密). Under NATO policy, marking shall be displayed in English or French, see Ref 1.

In the digital environment, confidentiality must be encoded as a machine-readable *confidentiality metadata label*. A confidentiality metadata label may be used to:

- Determine access limitations;
- Support appropriate protection during transmission of information;
- Enable appropriate markings to be rendered for display, printing, etc.;
- Support the selection of the appropriate retention and disposition procedures;
- Support the redaction and sanitization of information.

Typically, the information owner has the authority for setting the rules for handling the information and for protecting the integrity and confidentiality throughout its lifecycle. If the information owner shares the information with another entity, that entity (information custodian) is responsible to the information owner for the agreed level of protection of the received information.

2.2 Common Security Policy

When information is shared between different entities three general scenarios are possible:

1. Sharing of information between entities governed by different security policies;
2. Sharing of information between entities governed by the same security policies;

¹ Security Markings are defined in Reference 2, Appendix A. These are often referred to as Security Markings with no differentiation in meaning or intent.

3. Sharing of information with entities not governed by a formally defined security policy.

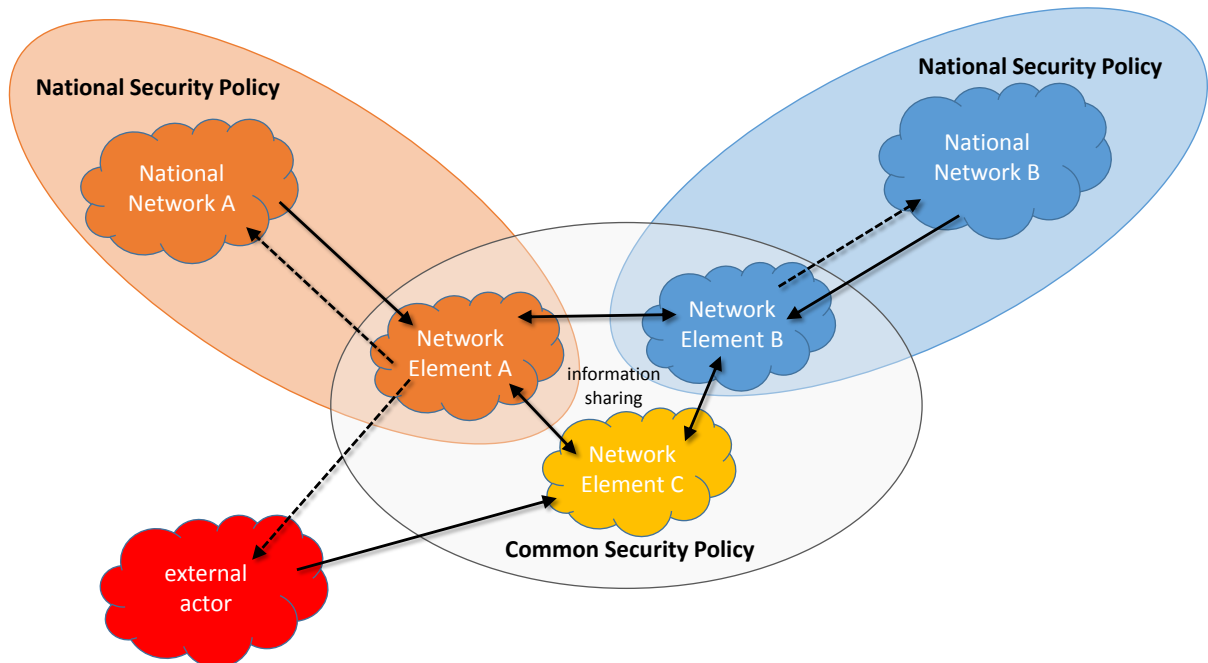


Figure 1: Information sharing scenarios

Before information is shared between entities that are governed by different security policies, formal agreements for the exchange of information are established. Information Exchange Agreements typically include a minimum set of security or protection controls that reflect the organisational information security policies and the type of the information involved. These agreements are the prerequisite to information sharing and thereby contribute to the establishment of a trust between entities; however, they must be enabled through a common understanding, by all entities, of each other's confidentiality metadata labels.

If there are multiple entities (n = number of entities) that want to share information the approach of individual bilateral agreements would result in each entity would need to understand n confidentiality metadata labels, i.e. $n*(n-1)/2$ agreements. When a new entity enters this circle of trust all existing entities are affected and n new bilateral agreements would have to be established. Even for a group as small as three entities it would be more effective to establish a single common security policy for that group, each entity would then only have to understand its own and the common policy and would be unaffected by new entities joining the group.

Note that in the common security policy case, information may be exchanged in a circular way, which would result in an information owner receiving their own information from another entity. This situation leads to a requirement for information to permanently maintain its original confidentiality metadata label.

2.3 Requirements

To enable information sharing in the different scenarios described above, this standard meets the following minimum requirements:

1. Express the confidentiality requirements throughout the IM lifecycle, regardless of the format of the information, or the medium on which it is processed and transmitted;
2. Provide the ability to express security policies in a common syntax;
3. Provide the ability to designate the security policies to be applied to the handling of information (i.e. policy identifier) (See Appendix 1);
4. Support at least two security policies in parallel (See Appendix 1 and the Alternative Confidentiality Label);
5. Express agreed equivalency relationship between different security policies to support the concept of Alternative Confidentiality Label(s) (See Appendix 1);
6. Provide a security policy for information from external actors that do not have a recognized security policy (See Appendix 2, Annex C and D);
7. Provide the ability to indicate the ownership of the information (See Appendix 1 and the concept of Context or Ownership);
8. Provide the ability to indicate categories required to specify protection and distribution in accordance with the approved security policies including classification, releasability, privacy mark, need-to-know, Community of Interest and administrative designators (See Appendix 2);
9. Provide the ability for applications and services to create confidentiality metadata labels at any point in the information life-cycle;
10. Provide the ability to render human readable markings consistent with the respective security policies (See Appendix 1 and Appendix 2);
11. Support automated handling decisions including release of information (See Appendix 2 and the Release To category type); and
12. Provide the ability to indicate changes to protection of the confidentiality of the information due to succession requirements such as downgrading and distribution reduction or expansion (See Appendix 1).

INTENTIONALLY BLANK

3 Terms and Definitions

Alternative Confidentiality Label: An Alternative Confidentiality Label is assigned to a data object when that data object is shared across boundaries that have different Governing Security Policies. In this case, the Alternative Confidentiality Label provides the equivalent labelling information in the recipient Governing Security Policy. The Alternative Confidentiality Label is provided in addition to the Originator Confidentiality Label.

Attributes: Named properties of an element that may carry different values depending upon the context in which they occur. Attributes modify the meaning of the elements to which they apply. [Library of Congress/Society of American Archivists].

Binding: A relationship between information and its metadata such as confidentiality metadata labels that provides an appropriate level of assurance of the integrity of the association between the information and the metadata.

Community of Interest: A collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions or business processes and who therefore must have shared vocabulary for the information they exchange. [Source: C-M(2008)0113]

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes. [Source: C-M(2007)0118]

Confidentiality Metadata Label: A set of metadata representing the collection of confidentiality elements and attributes that indicate the sensitivity of the information. It is represented with a structure and a controlled Value Domain that can be automatically processed to determine the sensitivity of the information to which it refers.

Need-to-Know (Principle): The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services [Source: C-M(2009)0035 (INV)].

Information: Any communications or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms. [Source: C-M(2007)0118]

Information Custodian: The nation or organisation which receives information and makes it visible and is responsible to the information owner for the agreed level of safe-keeping and availability of information. [Source: C-M(2007)0118]

Information Owner: The nation or organisation which creates and maintains content, defines access rules, negotiates and agrees to release constraints, establishes disposition instructions and is the authority for the life-cycle of information. [Source: C-M(2007)0118]

Integrity: The property that information (including data) has not been altered or destroyed in an unauthorized manner. [Source: C-M(2008)0113]

Metadata: Structured information that describes, explains, locates and otherwise makes it easier to retrieve and use an information resource (i.e. data object). The structure consists of 'elements', each of which contains 'values'. The values relate to the resource itself; there may be controls over what the actual values can be. [C-M(2002)049]

Security Marking: A visual (i.e. displayable) representation of the sensitivity of an object intended for human processing e.g. the Security Marking associated with a document as indicated by information inserted in the header and footer, a visual marking attached to a device, etc. A Security Marking may be rendered from the Confidentiality Metadata Label associated with an object.

Value Domain: The set of permissible values for an element or attribute. Value domains for Confidentiality Metadata Labels and Security Markings are specified in Reference 1 that is considered the authoritative source.

3.1 Abbreviations

C3	Consultation, Command and Control
COI	Community of Interest
NNEC	NATO Network Enabled Capability
NATO	North Atlantic Treaty Organization
URL	Uniform Resource Locator
XML	eXtensible Markup Language
JPEG	Joint Photographic Experts Group

4 Labelling

4.1 Introduction

This chapter addresses the labelling requirements specified in the References. It defines the syntax for confidentiality metadata labels that satisfy the following primary requirements:

- Can be bound to any type of information;
- Is adaptable to Security Policy changes;
- Supports the recognized security requirements for all types of information (unmarked, unclassified and classified);
- Supports the protection of information from creation to deletion, regardless of the format of the information, or the medium on which it is processed and transmitted;
- Supports Alliance coalitions, missions and exercises;
- Indicates the security policy to be applied (i.e. policy identifier);
- Indicates the classification of the information;
- Indicates categories required to specify distribution in accordance with the approved security policy including ownership, releasability, dissemination limitation, need-to-know and administrative designators;
- Indicates the succession requirements for future information handling e.g. downgrading and reduced or expanded distribution; and
- Supports the handling of information originating from other security domains.

This chapter uses the key words (e.g., SHALL, SHOULD, MAY) defined in RFC 2119 [10] to define the requirement levels for specific parts of confidentiality metadata label syntax.

4.2 Concepts and Terminology

Security Marking: Physical objects (documents, devices and equipment) carry a security marking that identifies the sensitivity of the information and, in the case of a document, is normally written on the front coversheet and in page headers and footers. Some documents carry additional marking abbreviations (e.g. NU, NR, NS) at the start of each paragraph, diagram or section. Problematically, these security markings are manually applied and therefore subject to variation.

A Confidentiality Metadata Label is a set of metadata representing the collection of confidentiality elements and attributes of the information that indicate the security safeguards applied to the information. A Confidentiality Metadata Label is represented with a structure and a controlled Value Domain that can be

electronically processed. The Confidentiality Metadata Label which is the subject of this standard is detailed in Appendix 1.

Confidentiality Metadata Labels may be bound to portions of the information, including paragraphs, sections, figures and tables. The following primary elements are included in the Confidentiality Metadata Label:

- a. Governing Security Policy – the Security Policy Authority is identified within each label;
- b. Classification – since information may be classified, unclassified or unmarked, every label includes a single value identifying the classification level of the information;
- c. Privacy Mark – is used to convey operational instructions, warnings or notifications of significance to the user or custodian of the data object. Privacy Mark is a legacy element that is used for backward compatibility;
- d. Category – provides restriction and/or expansion of the dissemination within the scope of the classification of the information.

The categories are:

- Restrictive – e.g. BOHEMIA
- Permissive – e.g. RELEASABLE TO ISAF
- Informative – e.g. PERSONAL

The definition of these categories can be seen in Table 7: Category Types. The Category element allows subcategories to be defined. The subcategories defined for the purpose of this standard are identified in Table 1: Defined Subcategories below.

Table 1: Defined Subcategories

Context	In combination with the Governing Security Policy context indicates the “Ownership”, as defined in (Reference 1). Information can be created in the context of co-operative activities, e.g. EAPC, in which the Governing Security Policy is applied.
Releasable To	Used to expand the dissemination of information to additional entities outside of the context for which that information was created.

Only	Used to restrict or limit the dissemination of information to specific entities and a sub-set of the entities within the context for which that information was created.
Additional Sensitivity	Used to indicate the sensitive nature of certain NATO information not conveyed by the Ownership or Classification; meaning that it is subject to additional stringent security regulations and procedures.
Administrative	Used to indicate discretionary handling according to local, non-automated procedures or provide guidance about the disposition of information

4.3 Succession Handling

The Succession Handling provides a mechanism to indicate the confidentiality metadata label that will be applicable at a certain time in the future. This can be used to meet Information Management requirement to capture the expected downgrading of the data object prior to the policy default (e.g. 30 years)

The access control decision, in accordance with the Governing Security Policy, may need to take into account the Succession Handling.

In the absence of any *SuccessionHandling* element, a *ReviewDateTime* SHALL be specified to indicate when the confidentiality metadata label shall be reviewed.

The review process SHOULD append Succession Handling elements in order to maintain a confidentiality metadata label history.

The Succession Handling consequently also includes the confidentiality metadata label history, including the original confidentiality metadata label that was specified.

4.4 Syntax

The Confidentiality Metadata Label Syntax is based upon the label description from IETF RFC 2634 (Reference [8]) and includes additional refinements to support requirements for Information Assurance and Information Management (i.e. succession handling for disposition and retention).

The Confidentiality Metadata Label Syntax utilises the eXtensible Markup Language (XML) to represent a confidentiality metadata label.

An XML representation provides an open and flexible mechanism that can be integrated with a wide variety of data types and is aligned with the federation approach for Alliance coalitions.

An XML schema is defined which contains each of the elements of the Confidentiality Metadata Label.

The elements of the XML schema are described in the Appendix 1.

INTENTIONALLY BLANK

5 Policy

5.1 Introduction

For confidentiality metadata labels to be used effectively and consistently within a networking environment, there must be a well-defined mapping of the security policy onto the appropriate confidentiality metadata label elements. This ensures that the appropriate semantics (according to the security policy) are observed and applied.

This chapter describes the Value Domains for the *ConfidentialityInformation* and its child elements in order to support effective and consistent application.

The NATO Security Policy has been adopted as the basis for the Governing Security Policy for this chapter and subsequent appendixes.

A second Security Policy is defined to support the ingestion of information from public sources or private sources where confidentiality metadata labels are not provided. This decision supports the initiation of a coalition, mission or exercise at Day-0.

ConfidentialityInformation

Table 2 specifies the *ConfidentialityInformation* elements and the defined *Category* elements, in support of the NATO Security Policy. The Value Domains for these elements are provided in Reference 1.

Table 2: Confidentiality Information Elements in the NATO Security Policy

Element	
<i>PolicyIdentifier</i>	
<i>Classification</i>	
<i>Privacy Mark</i>	
<i>Category</i>	tagName
	"Context"
	"Only"
	"Releasable To"
	"Additional Sensitivity"
	"Administrative"

Table 3: Value Domains for Confidentiality Information Elements in the PUBLIC Policy

Element		Value Domain
<i>PolicyIdentifier</i>		"PUBLIC"
<i>Classification</i>		"UNMARKED"
<i>Privacy Mark</i>		Not Used
<i>Category</i>	tagName	
	"Administrative"	Reference 1 & C-M(2002)60 Para 9

All values within the *ConfidentialityInformation* element are treated as case insensitive during processing.

For example, "Top Secret" and "TOP SECRET" are equivalent.

All values used in the *ConfidentialityInformation* element use the English terms.

NATO policy states that markings must be English or French however the confidentiality metadata label will enable security markings to be generated in any alternate language through the appropriate conversion of label values.

Each of the *ConfidentialityInformation* elements as used for the NATO Security Policy are described in further detail in Appendix 2.

For specific coalitions, missions or exercises, it is expected that the Value Domain for the Context subcategory will be extended. Value domain extensions may also be provided for the Releasable To, Limited Dissemination, Additional Sensitivity or Administrative categories.

Within the NATO enterprise, the Context along with the Governing Security Policy, indicates the dissemination of NATO information to NATO nations, or non-NATO nations depending upon the context in which the NATO information was created.

The use of the "NATO Security Policy" as the "Governing Security Policy" has the following constraints:

- The *CreationDateTime* element SHALL be present in a confidentiality metadata label;
- In the absence of any *SuccessionHandling* element, a *ReviewDateTime* SHALL be specified to indicate when the confidentiality metadata label shall be reviewed;
- The *ReviewDateTime* attribute SHALL be present when no *SuccessionHandling* element is present;

- If the *ReviewDateTime* attribute does not impact the validity of the Confidentiality Metadata Label i.e. if the *ReviewDateTime* attribute specifies a date in the past, the *ConfidentialityLabel* element SHALL still be deemed valid.; and
- The URI, if it is present, SHALL use the urn scheme with an oid namespace identifier to provide an equivalent of the policy identified by the *PolicyIdentifier* element content.

If the *SuccessionHandling* element is not present then the *ReviewDateTime* attribute SHALL be present.

INTENTIONALLY BLANK

6 References

- [1] Guidance on the Marking of NATO Information, June 2011, AC/322-N(2011)0130 REV1.
- [2] The Primary Directive on Information Management, 18 December 2008, C-M(2008)0113 (INV).
- [3] Security Within the North Atlantic Treaty Organisation, 17 June 2002, C-M(2002)049.
- [4] C-M(2002)60 The management of Non-Classified NATO Information, 11 July 2002
- [5] Directive on the Security of Information, 17 January 2012, AC/35-D/2002-REV4.
- [6] AC/322-D(2004)0021 (INV), "INFOSEC Technical and Implementation Guidance for Electronic Labelling of NATO Information", March 2004
- [7] NATO Core Metadata Specification (NCMS), AC/322-D(2014)0010, 14 January 2014.
- [8] IETF RFC 2634, "Enhanced Security Services for S/MIME", at <http://tools.ietf.org/html/rfc2634>, June 1999.
- [9] IETF RFC 5913, "Clearance Attribute and Authority Clearance Constraints Certificate Extension", at <http://tools.ietf.org/html/rfc5913>, June 2010.
- [10] IETF RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", at <http://tools.ietf.org/html/rfc2119>, March 1997.
- [11] STANAG 4406 Edition 2, "Military Message Handling System (MMHS)", Brussels, Belgium, (NATO/EAPC Unclassified)

INTENTIONALLY BLANK

APPENDIX 1: Confidentiality Metadata Label Schema

Introduction

This appendix defines the syntax of the Confidentiality Metadata Label for use within NATO Alliance coalitions, operations, exercises and training.

Metadata that uses the Confidentiality Metadata Label syntax SHALL be appropriately bound to the information to which it relates.

The Confidentiality Metadata Label syntax can be used to specify the *originatorConfidentialityLabel*, *metadataConfidentialityLabel* and an *alternativeConfidentialityLabel* metadata associated with Information.

The *originatorConfidentialityLabel* Element

The *originatorConfidentialityLabel* element is of type *ConfidentialityLabelType*. It contains the confidentiality label which the originator of a data object associated with that data object.

The *originatorConfidentialityLabel* element may be used by reference in other XML schemas, or within XML documents whose schemas allow any XML elements.

The *alternativeConfidentialityLabel* Element

The *alternativeConfidentialityLabel* element is of type *ConfidentialityLabelType*. It contains an equivalent representation, in an alternative policy, of the *originatorConfidentialityLabel*

The *alternativeConfidentialityLabel* element may be used by reference in other XML schemas, or within XML documents whose schemas allow any XML elements.

The *MetadataConfidentialityLabel* Element

The *metadataConfidentialityLabel* element is of type *ConfidentialityLabelType*. It contains the confidentiality label that is assigned to the metadata set associated with the data object.

The *metadataConfidentialityLabel* element may be used by reference in other XML schemas, or within XML documents whose schemas allow any XML elements.

The *ConfidentialityLabelType* Type

The *ConfidentialityLabelType* type is an extension of the *ConfidentialityLabelBaseType* type. It extends the *ConfidentialityLabelBaseType* by adding two optional attributes; *Id* and *ReviewDateTime* (see Figure 2).

The optional *Id* attribute can be used to provide a unique identifier for the confidentiality metadata label. Uniqueness is only guaranteed within one instance XML document.

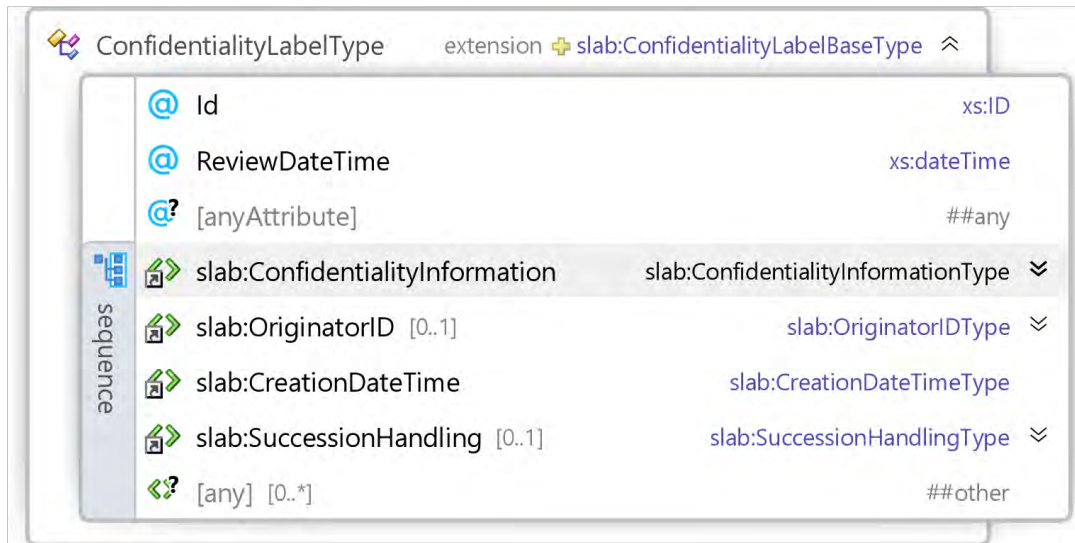


Figure 2: The ConfidentialityLabelType Type

The optional *ReviewDateTime* attribute, refers to the date when the confidentiality metadata label should be manually reviewed i.e. in support of archiving and disposition of the data object.

The *ReviewDateTime* attribute SHALL be present when no *SuccessionHandling* element is present.

The *ReviewDateTime* attribute SHALL not impact the validity of the confidentiality metadata label i.e. if the *ReviewDateTime* attribute specifies a date in the past, the confidentiality metadata label SHALL still be deemed valid.

Table 4: Attributes of the *ConfidentialityLabelType* Type prescribes the use of attributes of the *ConfidentialityLabelType* type:

Table 4: Attributes of the ConfidentialityLabelType Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
<i>Id</i>	Optional	Unique identifier of this element instance	“Label-3”, “958700be-280a-4758-a3c5-303c2d898b3e”

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
<i>ReviewDateTime</i>	Optional	XML schema type 'dateTime' . This attribute is mandatory if SuccessionHandling is not present.	"2015-01- 01T09:00:00", "2013-04- 01T11:59:59"

The *ConfidentialityLabelBaseType* Type

The *ConfidentialityLabelBaseType* type contains a mandatory *ConfidentialityInformation* (of type *ConfidentialityInformationType*) and *CreationDateTime* (of type *CreationDateTimeType*) elements and optional *OriginatorID* (of type *OriginatorIDType*) and *SuccessionHandling* (of type *SuccessionHandlingType*) elements (see Figure 3).

The *OriginatorID* element SHOULD contain information about the originator of the confidentiality metadata label.

Note that the *OriginatorID* element may be different to the creator of the Information (for example, a service may create and bind a confidentiality metadata label to information created by another user or service).

The *CreationDateTime* element can be used to express the date and time of the original classification by the originator.

Note that the *CreationDateTime* of the confidentiality metadata label may be different to the time at which the information itself was created.

The *SuccessionHandling* element allows the originator to define a confidentiality metadata label that will succeed the current confidentiality metadata label at the specified date and time.

This meets the information management requirement for appraisal, retention and disposition of information and the operational requirement to indicate information that may have a temporal or transient value.

Additional elements may be included in the *ConfidentialityLabel* element to support COI and National features and requirements.

These additional elements are for local use and MAY be ignored by other systems.

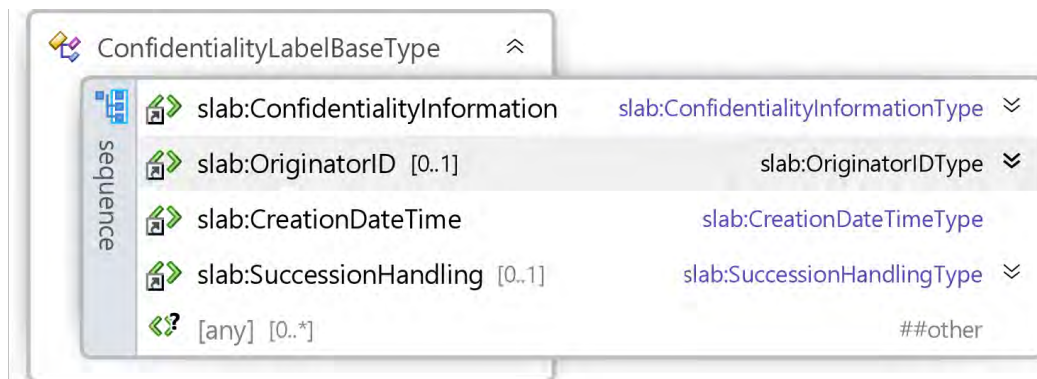


Figure 3: The ConfidentialityLabelBaseType Type

The ConfidentialityInformationType Type

The *ConfidentialityInformationType* type contains mandatory *PolicyIdentifier* (of type *PolicyIdentifierType*) and *Classification* (of type *ClassificationType*) elements and optional *PrivacyMark* (of type *PrivacyMarkType*) and *Category* (of type *CategoryType*) elements (see Figure 4).

The *PolicyIdentifier* element is used to uniquely identify the Governing Security Policy Authority which manages the security policy to which the confidentiality label relates and indicates the semantics of the other confidentiality label elements and attributes

The *PolicyIdentifier* element also provides an indication of the information domain that governed creation of the data item.

The set of values for the *Classification* element, and the use of these values, are defined by the Security Policy Authority (identified in the *PolicyIdentifier* element).

The set of values for the *PrivacyMark* element may be defined by the Governing Security Policy Authority (identified in the *PolicyIdentifier* element) in force (which may define a list of values to be used) or determined by the originator of the confidentiality label. The element may be used to convey information concerning operational instructions, warnings, notifications or other issues identified in the transmission or storage of the object.

The *PrivacyMark* content MAY be COI specific values (e.g. “CLEAR”) or an arbitrary string defined by the originator.

The *Category* elements provide further granularity for the sensitivity of the information, but may be conditional on the value of the *Classification* element, as determined by the Security Policy Authority (identified in the *PolicyIdentifier* element).

Additional elements may be included in the *ConfidentialityInformationType* type to support COI and National features and requirements.

These additional elements are for local use and MAY be ignored by other systems.

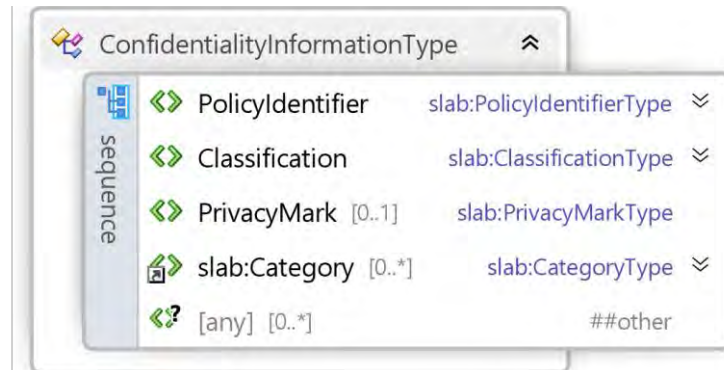


Figure 4: The ConfidentialityInformationType Type

The PolicyIdentifierType Type

The *PolicyIdentifierType* content is a textual identifier for the security policy.

The *PolicyIdentifierType* type contains a single optional attribute; *URI* (see Figure 5).



Figure 5: The PolicyIdentifierType Type

Additional attributes may be included in the *PolicyIdentifier* element to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

The *URI* attribute provides the opportunity to use a unique identification of the policy without any ambiguity that may be associated with a textual identifier.

The *URI* attribute MAY be present, and if it is present, it SHALL use the urn scheme with an oid namespace identifier to provide an equivalent of the policy identified by the *PolicyIdentifier* element content.

Table 5 prescribes the use of attributes of the *PolicyIdentifierType* type:

Table 5: Attributes of the *PolicyIdentifierType* Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
<i>URI</i>	Optional	The URI SHALL follow the “urn” scheme using an “oid” namespace identifier.	“urn:oid:1.3.26.1.3.1” “urn:oid:1.2.840.113549.1.9.16.7.1”

The *ClassificationType* Type

The *ClassificationType* content is a registered textual identifier for the classification within the security policy.



Figure 6: The *ClassificationType* Type

The *Classification* element contains a single optional attribute; URI (see Figure 6). The optional URI attribute SHALL NOT be used.

Additional attributes may be included in elements of type *ClassificationType* to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

Table 6 prescribes the use of attributes of the *ClassificationType* type:

Table 6: Attributes of the *ClassificationType* Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
“URI”	Prohibited		N/A

The *PrivacyMarkType* Type

The *PrivacyMarkType* type is a simple string which contains no additional elements or attributes. The string contains the privacy mark value.



Figure 7: The *PrivacyMarkType* Type

The *CategoryType* Type

The *CategoryType* type contains one optional *CategoryValue* element.

The *CategoryType* type contains two mandatory attributes, *Type* and *TagName*, and one optional attribute, *URI* (see Table 8).

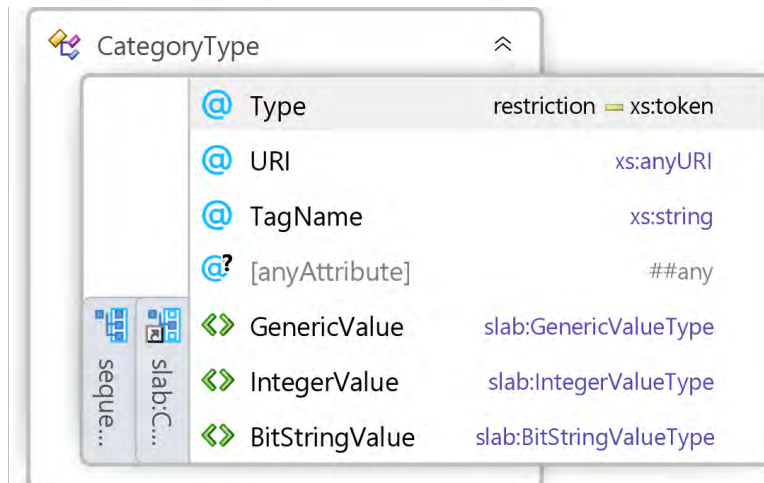


Figure 8: The *CategoryType* Type

Additional attributes may be included in elements of type *CategoryType* to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

The mandatory *Type* attribute can take one of the three values; “RESTRICTIVE”, “PERMISSIVE” or “INFORMATIVE”.

Table 7: Category Types

Category Type	Description
RESTRICTIVE	Restrictive category types reduce the scope of dissemination. This type is used for access control decisions.
PERMISSIVE	Permissive category types are used to provide explicit inclusion sets for the purpose of access control

INFORMATIVE	Informative category types are not used for access control decisions and are provided to improve information handling.
-------------	--

The mandatory *TagName* attribute contains the name of the category tag that is applicable as specified in Table 2.

The set of values for the *TagName* attribute, and the use of these values, are defined by the security policy in force (identified in the *PolicyIdentifier* element) and generally refer to a grouping of categories (Table 2). The values for *TagName* attribute are addressed in Chapter 5.

The *URI* attribute provides the opportunity to use a unique identification of the category tag name without any ambiguity that may be associated with a textual identifier.

The *URI* attribute MAY be present and if it is present, it SHALL use the urn scheme with an OID namespace identifier to provide an equivalent of the policy identified by the *PolicyIdentifier* element content.

Table 8 prescribes the use of attributes of the *CategoryType* type:

Table 8: Attributes of the *CategoryType* Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
<i>Type</i>	Mandatory		“PERMISSIVE”, “RESTRICTIVE”, “INFORMATIVE”
<i>TagName</i>	Mandatory		“Releasable to”, “Context”, “Only”, “Additional Sensitivity”, “Administrative”
<i>URI</i>	Optional	The URI SHALL adhere to the “urn” scheme using an “oid” namespace identifier to provide a machine-readable equivalent to the applicable category tag set.	“urn:oid:1.3.26.1.4.1”, “urn:oid:1.3.26.1.4.3”

The *CategoryValueType* Type

The *CategoryValueType* type is declared to be abstract and so cannot be present in a confidentiality label directly.

The *CategoryValueType* type contains three elements in a substitution group; *GenericValue*, *IntegerValue* and *BitStringValue*.

The *GenericValue* element SHALL be used as the substitution for the *CategoryValueType* of a *CategoryValue* element.

The *IntegerValue* and *BitStringValue* elements SHALL NOT be used as a substitution for the *CategoryValue* element.

The set of values for the *GenericValue* elements, and the use of these values, are defined by the security policy in force (identified in the *PolicyIdentifier* element) and the category tag (identified in the *TagName* attribute).

The *OriginatorIDType* Type

The *OriginatorIDType* type contains one mandatory attribute, *IDType* (see Figure 9).



Figure 9: The *OriginatorIDType* Type

Additional attributes may be included in the elements of type *OriginatorIDType* to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

The allowed values for the *IDType* attribute, together with a brief description and an example for the *OriginatorID* value are shown below:

Table 9: Values for the *IDType* Attribute of *OriginatorID*

IDType	Description	Example Value
"rfc822Name"	An Internet electronic mail address.	john.doe@ncia.nato.int
"dNSName"	An Internet domain name.	ncia.nato.int
"directoryName"	A distinguished name encoded as a string.	cn=John Doe, ou=NCIA, o=NATO

IDType	Description	Example Value
"uniformResource Identifier"	A Uniform Resource Identifier (URI) for the World Wide Web.	http://www.ncia.nato.int/
"IPAddress"	An Internet Protocol address.	192.168.0.1
"x400Address"	An O/R address encoded as a string.	/cn=John Doe /OU=NCIA /O=NATO /PRMD=NMS /C=OO/
"jID"	An XMPP address.	doe@ncia.nato.int/mobile
"userPrincipalName"	An Internet-style user name format defined by Microsoft.	john.doe@nr.ncia.nato.int

The SuccessionHandlingType Type

The SuccessionHandlingType type contains mandatory *SuccessionDateTime* (of type *SuccessionDateTimeType*) and *SuccessorConfidentialityLabel* (of type *ConfidentialityLabelBaseType*) elements (see Figure 10).

Additional elements may be included to support COI and National features and requirements.

These additional elements are for local use and MAY be ignored by other systems.

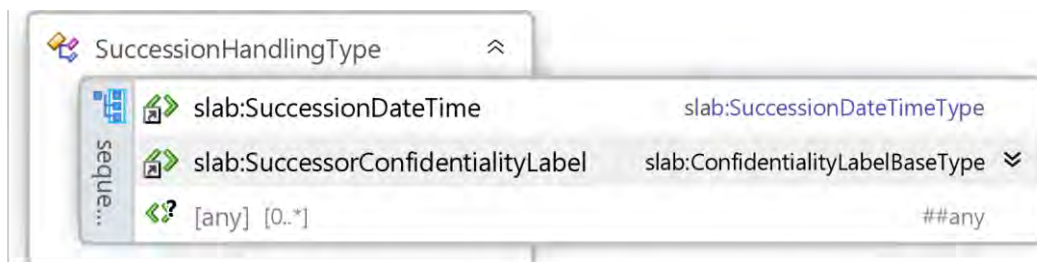


Figure 10: The SuccessionHandlingType Type

The SuccessionDateTime Type

The *SuccessionDateTime* type is an XML datetime string which contains no additional elements or attributes (see Figure 11). The datetime string contains the succession date time value.



Figure 11: The *SuccessionDateTime* Type

The *CreationDateTime* Type

The *CreationDateTime* type is an XML datetime string which contains no additional elements or attributes (see Figure 12). The datetime string contains the creation date time value.

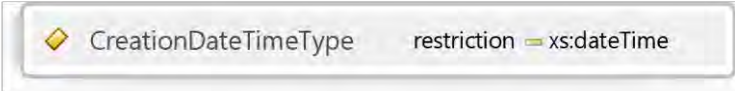


Figure 12: The *CreationDateTime* Type

INTENTIONALLY BLANK

ANNEX A: Schema

A schema has been defined that may be used to verify the validity of the confidentiality label.

The schema has the following namespace
<urn:nato:stanag:4774:confidentialitymetadatalabel:1:0>.

The schema is registered in the NATO Metadata Registry and Repository (NMRR) and also the U.S. Metadata Repository (US MDR) using the above namespace.

The schema for the Confidentiality Metadata Label is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>

<!--
*****

NATO UNCLASSIFIED

XML Schema for capturing the Confidentiality Label specification for
confidentiality labels and their succession history.

    |
    /\
    -< + >-
    \ /
    |      NCI AGENCY
    ## # ##### # P.O. box 174
    ## # # # # 2501 CD The Hague
    ## # # # #
    # # # # # # Core Enterprise Services
    # ## ##### #
    A G E N C Y

*****
-->

<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
  targetNamespace="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
  version="1.3"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
        urn:nato:stanag:4774:confidentialitymetadatalabel:1:0
      </UniqueIdentifier>
      <Name>Confidentiality Label Schema</Name>
      <Definition>Schema for a confidentiality label</Definition>
      <VersionIndicator>1.3</VersionIndicator>
      <UsageGuidance>
        Used within NATO for representing a confidentiality label.
      </UsageGuidance>
      <RestrictionType/>
    </xs:appinfo>
  </xs:annotation>
</xs:schema>
```

```

<RestrictionValue/>
<ConfidentialityLabel ReviewDateTime="2019-04-01T09:00:00Z">
  <ConfidentialityInformation>
    <PolicyIdentifier>NATO</PolicyIdentifier>
    <Classification>UNCLASSIFIED</Classification>
    <Category Type="PERMISSIVE" TagName="Context">
      <GenericValue>NATO</GenericValue>
    </Category>
  </ConfidentialityInformation>
  <CreationDateTime>2014-04-01T09:00:00Z</CreationDateTime>
</ConfidentialityLabel>
</xs:appinfo>
<xs:documentation>
  The schema can be used with the metadata binding schema to bind confidentiality label metadata (such as
  those defined in the NATO Core Metadata Specification NCMS)) to data objects.
</xs:documentation>
</xs:annotation>

<xs:complexType name="ConfidentialityLabelType" id="confidentialityLabelType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:confidentialityLabelType
      </UniqueIdentifier>
      <Name>Confidentiality Label Type</Name>
      <Definition>
A type that is used as the base for the confidentiality label metadata elements.
      </Definition>
      <VersionIndicator>1.3</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
  </xs:documentation>
</xs:annotation>
<xs:complexContent>
  <xs:extension base="slab:ConfidentialityLabelBaseType">
    <xs:attribute name="Id" type="xs:ID"/>
    <xs:attribute name="ReviewDateTime" type="xs:dateTime"/>
    <xs:anyAttribute processContents="lax"/>
  </xs:extension>
</xs:complexContent>
</xs:complexType>

<!-- For backwards compatibility only -->
<xs:element name="ConfidentialityLabel" type="slab:ConfidentialityLabelType"/>

<!-- Standard NCMS metadata -->
<xs:element name="originatorConfidentialityLabel"
  type="slab:ConfidentialityLabelType"/>
<xs:element name="alternativeConfidentialityLabel"
  type="slab:ConfidentialityLabelType"/>
<xs:element name="metadataConfidentialityLabel"
  type="slab:ConfidentialityLabelType"/>

<xs:complexType name="ConfidentialityLabelBaseType"
  id="confidentialityLabelBaseType">

```

```

<xs:annotation>
  <xs:appinfo>
    <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:confidentialityLabelBaseType
    </UniqueIdentifier>
    <Name>Confidentiality Label Base Type</Name>
    <Definition>
A type that is used as the base for the confidentiality label and successor confidentiality label elements.
    </Definition>
    <VersionIndicator>1.3</VersionIndicator>
    <UsageGuidance></UsageGuidance>
    <RestrictionType></RestrictionType>
    <RestrictionValue></RestrictionValue>
  </xs:appinfo>
  <xs:documentation>

  </xs:documentation>
</xs:annotation>
<xs:sequence>
  <xs:element ref="slab:ConfidentialityInformation"/>
  <xs:element ref="slab:OriginatorID" minOccurs="0"/>
  <xs:element ref="slab:CreationDateTime"/>
  <xs:element ref="slab:SuccessionHandling" minOccurs="0"/>
  <xs:any processContents="lax" namespace="##other" minOccurs="0"
    maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:element name="ConfidentialityInformation"
  type="slab:ConfidentialityInformationType"/>

<xs:complexType name="ConfidentialityInformationType"
  id="confidentialityInformationType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:confidentialityInformationType
      </UniqueIdentifier>
      <Name>Confidentiality Information Type</Name>
      <Definition>
A type that describes the basic sensitivity information of policy, classification, privacy mark and categories.
      </Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
    <xs:documentation>

    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="PolicyIdentifier" type="slab:PolicyIdentifierType"/>
    <xs:element name="Classification" type="slab:ClassificationType"/>
    <xs:element name="PrivacyMark" type="slab:PrivacyMarkType" minOccurs="0"/>
    <xs:element ref="slab:Category" minOccurs="0" maxOccurs="unbounded"/>
    <xs:any processContents="lax" namespace="##other" minOccurs="0"
      maxOccurs="unbounded"/>
  </xs:sequence>

```

```
</xs:complexType>

<xs:element name="PolicyIdentifier" type="slab:PolicyIdentifierType"/>

<xs:complexType name="PolicyIdentifierType" id="policyIdentifierType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:policyIdentifierType
      </UniqueIdentifier>
      <Name>Policy Identifier Type</Name>
      <Definition>
The Security Policy Authority, which in turn defines the value domain for the other elements within the
Confidentiality Information.
      </Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
    <xs:documentation>

    </xs:documentation>
  </xs:annotation>
  <xs:simpleContent>
    <xs:extension base="slab:RequiredToken">
      <xs:attribute name="URI" type="xs:anyURI"/>
      <xs:anyAttribute processContents="lax"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="RequiredToken" id="requiredToken">
  <xs:restriction base="xs:token">
    <xs:minLength value="1"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="Classification" type="slab:ClassificationType"/>

<xs:complexType name="ClassificationType" id="classificationType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:classificationType
      </UniqueIdentifier>
      <Name>Classification Type</Name>
      <Definition>The basic hierarchical indication of sensitivity.</Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
    <xs:documentation>

    </xs:documentation>
  </xs:annotation>
  <xs:simpleContent>
    <xs:extension base="slab:RequiredToken">
```



```
<xs:attribute name="URI" type="xs:anyURI"/>
<xs:anyAttribute processContents="lax"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:element name="PrivacyMark" type="slab:PrivacyMarkType"/>

<xs:simpleType name="PrivacyMarkType" id="privacyMarkType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:privacyMarkType
      </UniqueIdentifier>
      <Name>Privacy Mark Type</Name>
      <Definition>
Additional information for the end user on the handling of the associated data object.
      </Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
    <xs:documentation>

  </xs:documentation>
</xs:annotation>
  <xs:restriction base="xs:string"/>
</xs:simpleType>

<xs:element name="Category" type="slab:CategoryType"/>

<xs:complexType name="CategoryType" id="categoryType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:categoryType
      </UniqueIdentifier>
      <Name>Category Type</Name>
      <Definition>
The more granular indication of sensitivity, over and above the classification.
      </Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
    <xs:documentation>

  </xs:documentation>
</xs:annotation>
  <xs:sequence minOccurs="0" maxOccurs="unbounded">
    <xs:element ref="slab:CategoryValue"/>
  </xs:sequence>
  <xs:attribute name="Type" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:token">
        <xs:enumeration value="RESTRICTIVE"/>
        <xs:enumeration value="PERMISSIVE"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:complexType>
```

```
<xs:enumeration value="INFORMATIVE"/>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="URI" type="xs:anyURI" use="optional"/>
<xs:attribute name="TagName" type="xs:string" use="required"/>
<xs:anyAttribute processContents="lax"/>
</xs:complexType>

<xs:element name="CategoryValue" type="slab:CategoryValueType" abstract="true"/>

<xs:simpleType name="CategoryValueType" id="categoryValueType">
  <xs:restriction base="xs:string"/>
</xs:simpleType>

<xs:element name="GenericValue" type="slab:GenericValueType"
  substitutionGroup="slab:CategoryValue"/>

<xs:simpleType name="GenericValueType" id="genericValueType">
  <xs:restriction base="slab:CategoryValueType"/>
</xs:simpleType>

<xs:element name="IntegerValue" type="slab:IntegerValueType"
  substitutionGroup="slab:CategoryValue"/>

<xs:simpleType name="IntegerValueType" id="integerValueType">
  <xs:restriction base="slab:CategoryValueType">
    <xs:pattern value="[0-9]+"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="BitStringValue" type="slab:BitStringValue"
  substitutionGroup="slab:CategoryValue"/>

<xs:simpleType name="BitStringValue" id="bitStringValue">
  <xs:restriction base="slab:CategoryValueType">
    <xs:pattern value="[0-1]+"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="OriginatorID" type="slab:OriginatorIDType"/>

<xs:complexType name="OriginatorIDType" id="originatorIDType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:originatorIDType
      </UniqueIdentifier>
      <Name>Originator ID Type</Name>
      <Definition>
The originator of the confidentiality label, which may be different to the originator of the data object.
      </Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
  </xs:documentation>
</xs:complexType>
```

```

</xs:documentation>
</xs:annotation>
<xs:simpleContent>
  <xs:extension base="xs:string">
    <xs:attribute name="IDType" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="rfc822Name" />
          <xs:enumeration value="dNSName" />
          <xs:enumeration value="directoryName" />
          <xs:enumeration value="uniformResourceIdentifier" />
          <xs:enumeration value="iPAddress" />
          <xs:enumeration value="x400Address" />
          <xs:enumeration value="userPrincipalName" />
          <xs:enumeration value="jID" />
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
    <xs:anyAttribute processContents="lax"/>
  </xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:element name="CreationDateTime" type="slab:CreationDateTimeType"/>

<xs:simpleType name="CreationDateTimeType" id="creationDateTime">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:creationDateType
      </UniqueIdentifier>
      <Name>Creation Date Time Type</Name>
      <Definition>The time at which the confidentiality label was created, which may be different to the time the
data object was created.</Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
  </xs:annotation>
  <xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<xs:element name="SuccessionHandling" type="slab:SuccessionHandlingType"/>

<xs:complexType name="SuccessionHandlingType" id="successionHandlingType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:successionHandlingType
      </UniqueIdentifier>
      <Name>Classification Type</Name>
      <Definition>
The proposed confidentiality label at a subsequent date.
      </Definition>
      <VersionIndicator>1.2</VersionIndicator>
    </xs:appinfo>
  </xs:annotation>
  <xs:restriction base="xs:string">
    <xs:enumeration value="Classification Type" />
  </xs:restriction>
</xs:complexType>

```

```
<UsageGuidance></UsageGuidance>
<RestrictionType></RestrictionType>
<RestrictionValue></RestrictionValue>
</xs:appinfo>
<xs:documentation>

</xs:documentation>
</xs:annotation>
<xs:sequence>
  <xs:element ref="slab:SuccessionDateTime"/>
  <xs:element ref="slab:SuccessorConfidentialityLabel"/>
  <xs:any namespace="##any" processContents="skip" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:element name="SuccessionDateTime" type="slab:SuccessionDateTimeType"/>

<xs:simpleType name="SuccessionDateTimeType" id="successionDateTimeType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:successionDateTimeType
      </UniqueIdentifier>
      <Name>Succession Date Time Type</Name>
      <Definition>
The proposed date at which a proposed successorConfidentialityLabel should come in to force.
      </Definition>
      <VersionIndicator>1.2</VersionIndicator>
      <UsageGuidance></UsageGuidance>
      <RestrictionType></RestrictionType>
      <RestrictionValue></RestrictionValue>
    </xs:appinfo>
    <xs:documentation>

    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<xs:element name="SuccessorConfidentialityLabel" type="slab:ConfidentialityLabelBaseType"/>

</xs:schema>
```

ANNEX B: Examples

This section contains fictitious examples that illustrate the use of the confidentiality label.

The values shown in these examples follow those defined in Reference 1

This example shows the use of permissive categories with the *GenericValue* elements grouped according to the category tag name:

```
<slab:originatorConfidentialityLabel
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <slab:ConfidentialityInformation>
    <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
    <slab:Classification>UNCLASSIFIED</slab:Classification>
    <slab:Category Type="PERMISSIVE" TagName="Releasable to">
      <slab:GenericValue>SWE</slab:GenericValue>
      <slab:GenericValue>FIN</slab:GenericValue>
      <slab:GenericValue>RUS</slab:GenericValue>
    </slab:Category>
  </slab:ConfidentialityInformation>
  <slab:CreationDateTime>2015-08-29T16:15:00Z</slab:CreationDateTime>
</slab:originatorConfidentialityLabel>
```

This example shows the use of restrictive and informative categories; the *GenericValue* elements are grouped according to category tag name:

```
<slab:originatorConfidentialityLabel
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <slab:ConfidentialityInformation>
    <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
    <slab:Classification>CONFIDENTIAL</slab:Classification>
    <slab:Category Type="RESTRICTIVE" TagName="Special Category Designators">
      <slab:GenericValue>ATOMAL</slab:GenericValue>
      <slab:GenericValue>CRYPTO</slab:GenericValue>
    </slab:Category>
    <slab:Category Type="INFORMATIVE" TagName="Administrative">
      <slab:GenericValue>MEDICAL</slab:GenericValue>
    </slab:Category>
  </slab:ConfidentialityInformation>
  <slab:CreationDateTime>2015-08-29T16:15:00Z</slab:CreationDateTime>
</slab:originatorConfidentialityLabel>
```

This example shows the use of the *OriginatorID* elements.

```
<slab:originatorConfidentialityLabel
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
  Id="ID_1" ReviewDateTime="2001-12-17T09:30:47Z">
  <slab:ConfidentialityInformation>
    <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
    <slab:Classification>RESTRICTED</slab:Classification>
    <slab:Category TagName="Releasable To" Type="PERMISSIVE">
      <slab:GenericValue>SWE</slab:GenericValue>
      <slab:GenericValue>FIN</slab:GenericValue>
    </slab:Category>
  </slab:ConfidentialityInformation>
  <slab:OriginatorID IDType="rfc822Name">lunt@ncia.nato.int</slab:OriginatorID>
  <slab:CreationDateTime>2015-01-01T09:00:00Z</slab:CreationDateTime>
</slab:originatorConfidentialityLabel>
```

This example shows the use of the *SuccessionHandling* element.

```
<slab:originatorConfidentialityLabel
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <slab:ConfidentialityInformation>
    <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
    <slab:Classification>SECRET</slab:Classification> </slab:ConfidentialityInformation>
  <slab:CreationDateTime>2015-08-29T16:15:00Z</slab:CreationDateTime>
  <slab:SuccessionHandling>
    <slab:SuccessionDateTime>2015-01-01T09:00:00Z</slab:SuccessionDateTime>
    <slab:SuccessorConfidentialityLabel>
      <slab:ConfidentialityInformation>
        <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
        <slab:Classification>RESTRICTED</slab:Classification>
      </slab:ConfidentialityInformation>
    </slab:SuccessorConfidentialityLabel>
  </slab:SuccessionHandling>
</slab:originatorConfidentialityLabel>
```

APPENDIX 2: NATO Security Policy Confidentiality Labels

Introduction

The confidentiality label schema defined in Appendix 1 of this ADatP specifies the syntax for confidentiality labels and provides the semantics for the values a confidentiality label may contain. In other words, the confidentiality label schema is a generic framework for storing any confidentiality label values that supports multiple different security policies.

PolicyIdentifier

The *PolicyIdentifier* element indicates the security policy authority and the semantics of the values of the other *ConfidentialityInformation* elements.

A single policy is used across NATO and all North Atlantic Council (NAC)-approved activities and has the value “NATO”².

The corresponding attributes for Policy element are:

Table 10: Attributes for the Policy Element

Attribute	Value
URI	“urn:oid:1.3.26.1.3.1”

For example,

```
<PolicyIdentifier>NATO</PolicyIdentifier>
```

Classification

The *Classification* element indicates the sensitivity of the content of the data object to which the confidentiality label is bound.

The Value Domain for the Classification element within the NATO Security Policy are specified in Reference 1.

For example,

```
<Classification>RESTRICTED</Classification>
```

The *Category* elements that are valid within a *ConfidentialityInformation* element are dependent upon the selected values in the *Classification* element, as provided in Reference 1.

Note that when generating a security marking from a Confidentiality Label containing a “TOP SECRET” classification, the *PolicyIdentifier* element MUST be displayed as “COSMIC” instead of “NATO”

² When rendering the *PolicyIdentifier* element as a marking, if the *Classification* element is “Top Secret”, it is rendered as “COSMIC” rather than “NATO”.

PrivacyMark

The Value Domain of the privacy mark is the single value “CLEAR”

The “CLEAR” value is defined to support the Clear Service specified in STANAG 4406 Ed. 2 [11].

The privacy mark is used for information only and not used to make an access control decision.

For example,

```
<PrivacyMark>CLEAR</PrivacyMark>
```

Categories

Introduction

The NATO Security Policy [1] defines five Security categories:

Table 11: Security Categories for the NATO Security Policy

Value	Definition
“Context”	The context under which the NATO information was originated including NAC-approved activities.
“Releasable To”	Further dissemination of NATO information beyond the context in which it was created.
“Only”	Restriction of the dissemination of the NATO Information by the originator to some of the non-NATO members of the context.
“Additional Sensitivity”	Additional handling requirements.
“Administrative”	The type of the NATO Information and the corresponding need for limited access.

The “Context”, “Only” and “Releasable To” Category tags support the dissemination of NATO information Nations and groupings.

Figure 13 shows how these Categories and the PolicyIdentifier are used to support the dissemination of NATO information to Nations, together with example security markings.

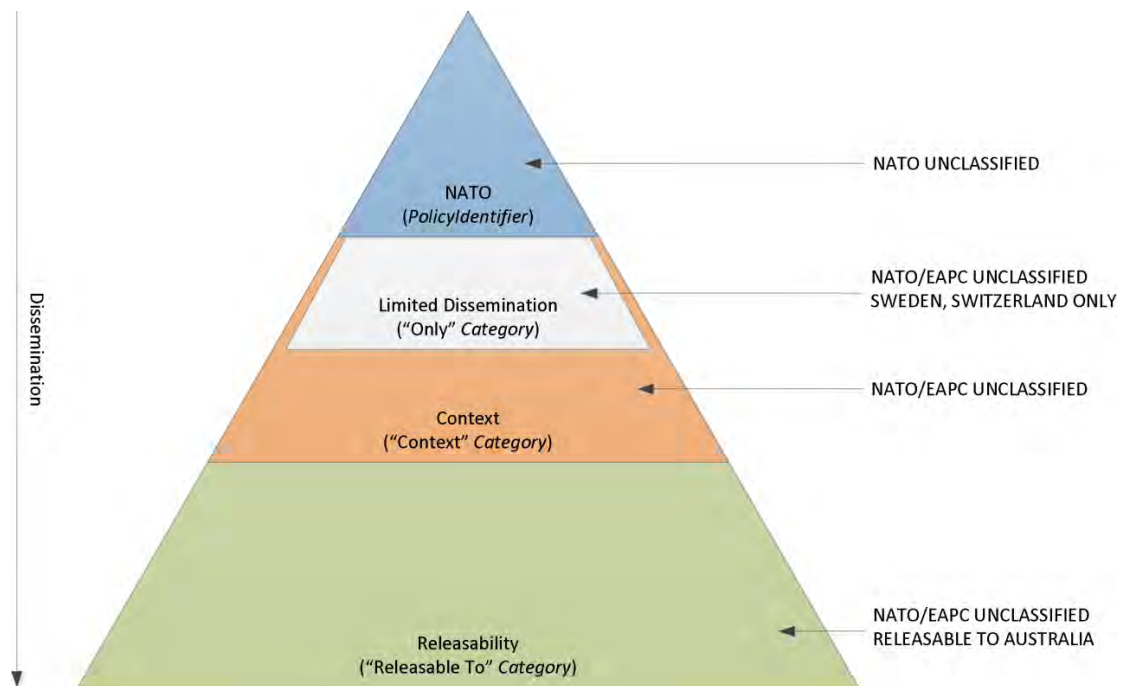


Figure 13: Category and PolicyIdentifier Role for Information Dissemination

The area of the triangle in Figure 13 represents the scope of the dissemination of the NATO information for the corresponding confidentiality label.

The *PolicyIdentifier* sets the dissemination to a core set of Nations, the NATO Nations.

The “Context” *Category* may refine the dissemination to a subset of the NATO Nations and a set of Non-NATO Entities.

The “Only” *Category* limits the dissemination to a sub-set of the Nations identified by the “Context” *Category*.

The “Releasable To” *Category* expands the dissemination to include additional Nations and grouping, in addition the Nations identified by the “Context” *Category*.

All of the categories are described in the following sections.

Context

NATO information may be originated in the context of a NAC approved activity with Nations, and in which the NATO Security Policy is still to be applied.

The context in which the NATO information is originated may determine the dissemination of the information, beyond the set of NATO Nations.

The combination of the NATO policy identifier and the context constitutes the “Ownership”, as defined in Reference 4.

The context is held within a “Context” category within the *ConfidentialityInformation* element.

The corresponding attributes for the “Context” category element are:

Table 12: Attributes for the Context Category Element

Attribute	Value
tagName	“Context”
type	“PERMISSIVE”
URI	“urn:oid:1.3.26.1.4.4”

The “Context” category **MUST** be present within a NATO Security Policy *ConfidentialityInformation* element.

The “Context” category Value Domain relate to two specific elements:

1. A mandatory context identifying a set of Nations and optional a set of Non-NATO Entities;
2. An optional indication that the information may be released beyond the context.

The values in the “Context” Value Domain represent the context in which the information was created.

As the membership of NATO and NAC-approved activities has changed over time (and may again in the future) the dissemination of the NATO information originated in that context will also change.

For example, information generated before a Nation became a member of NATO should not automatically be disseminated to that Nation when it becomes a member of NATO.

Each value in the “Context” Value Domain therefore includes a suffix which distinguishes between the different memberships of NATO or the NAC-approved activities.

In general use, only the “Context” Category value for NATO or a NAC-approved activity with the highest suffix shall be used.

The Value Domain³ of the “Context” Category within the NATO Security Policy is specified in Reference 1.

The “Context” Category **SHALL** contain a single value from the Value Domain.

Where a *ConfidentialityInformation* element contains a “Releasable To” Category the “Context” Category **SHALL** include the additional value “Releasable”.

³ Note that these values within this value domain still need to be verified to ensure that all historical contexts have been identified.

For example,

```
<ConfidentialityInformation>
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <Classification>RESTRICTED</Classification>
  <Category tagName="Context" type="PERMISSIVE">
    <GenericValue>EAPC</GenericValue>
    <GenericValue>Releasable</GenericValue>
  </Category>
  <Category tagName="Releasable To" type="PERMISSIVE">
    <GenericValue>EAPC</GenericValue>
    <GenericValue>JPN</GenericValue>
  </Category>
</ConfidentialityInformation>
```

Note, the “Releasable” value supports the release decision process and is not displayed with any corresponding security marking.

Only

The dissemination of information generated by NATO or a NATO approved activity may be limited by the originator to a subset of the Nations identified by the context.

The Limited Dissemination values are grouped into an “Only” category within the *ConfidentialityInformation* element.

The corresponding attributes for the Limited Dissemination category element are:

Table 13: Attributes for the Limited Dissemination Category Element

Attribute	Value
tagName	“Only”
type	“PERMISSIVE”
URI	“urn:oid:1.3.26.1.4.5”

The Value Domain for the “Only” category are those Nations that are members of the context identified by the “Context” *Category* together with the NATO Context values and the “Releasable To” category values.

For example, the following confidentiality label limits the distribution to only the NATO member Nations together with Armenia and Austria (and not the other Nations identified by the EAPC context).

```
<ConfidentialityInformation>
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <Classification>RESTRICTED</Classification>
  <Category tagName="Context", type="PERMISSIVE">
    <GenericValue>EAPC</GenericValue>
  </Category>
  <Category tagName="Only" type="PERMISSIVE">
    <GenericValue>ARM</GenericValue>
```

```

    <GenericValue>AUT</GenericValue>
    <GenericValue>NATO</GenericValue>
  </Category>
</ConfidentialityInformation>

```

There may be zero, one or more “Only” Category values within a NATO policy *ConfidentialityInformation* element.

Releasable To

NATO information that is intended to be further disseminated outside the context within which it was created shall include Releasability values.

The Releasability values are grouped into category element within the *ConfidentialityInformation* element.

The corresponding attributes for the Releasability category element are:

Table 14: Attributes for Releasability Category Element

Attribute	Value
tagName	“Releasable To”
type	“PERMISSIVE”
URI	“urn:oid:1.3.26.1.4.2”

The Value Domain for the “Releasable To” category are those Nations that are not members of the context, together with approved grouping of entities including entities in an accompanying “Only” category (see Reference 1).

For example, the following confidentiality label extends the dissemination to Georgia and New Zealand as well as the EAPC member Nations.

```

<ConfidentialityInformation>
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <Classification>RESTRICTED</Classification>
  <Category TagName="Context", Type="Permissive">
    <GenericValue>EAPC</GenericValue>
    <GenericValue>Releasable</GenericValue>
  </Category>
  <Category TagName="Releasable To" Type="PERMISSIVE">
    <GenericValue>EAPC</GenericValue>
    <GenericValue>GEO</GenericValue>
    <GenericValue>NZL</GenericValue>
  </Category>
</ConfidentialityInformation>

```

There may be zero, two⁴ or more “Releasable To” Category values within a NATO policy Confidentiality Label element.

Additional Sensitivity

The sensitive nature of certain NATO information means that it is subject to additional stringent security regulations and procedures.

The Additional Sensitivity values are grouped into an “Additional Sensitivity” category within the *ConfidentialityInformation* element.

The corresponding attributes for the “Additional Sensitivity” category element are:

Table 15: Attributes for the Additional Sensitivity Category Element

Attribute	Value
tagName	“Additional Sensitivity”
type	“RESTRICTIVE”
URI	“urn:oid:1.3.26.1.4.1”

Note that the tagName “Additional Sensitivity” corresponds to the “Category Designator” in Reference 4.

Reference 1 specifies the Value Domains for the “Additional Sensitivity” category.

For example,

```
<Category TagName="Additional Sensitivity" Type="RESTRICTIVE">
  <GenericValue>ATOMAL</GenericValue>
  <GenericValue>BOHEMIA</GenericValue>
</Category>
```

There may be zero, one or more “Additional Sensitivity” category values within a NATO policy *ConfidentialityInformation* element.

Administrative

Administrative markings indicate discretionary handling according to local, non-automated procedures or provide information about the disposition of information.

Administrative values may only be applied to NATO information by the originator.

The Administrative values are grouped into an “Administrative” category within the *ConfidentialityInformation* element.

The corresponding attributes for the “Administrative” category element are:

⁴There will be at least one value to identify the context, and one value to identify the additional dissemination.

Table 16: Attributes for the Administrative Category Element

Attribute	Value
tagName	"Administrative"
type	"INFORMATIVE"
URI	"urn:oid:1.3.26.1.4.3"

Administrative Markings are defined in Reference 2 and are consequently valid only within *ConfidentialityInformation* elements that have a *Classification* element of "UNCLASSIFIED".

Note that the *tagName* "Administrative" corresponds to the "Administrative Marking" in Reference 4.

Reference 1 specifies the Value Domain for the "Administrative" category.

For example,

```
<Category TagName="Administrative" Type="INFORMATIVE">
  <GenericValue>COMMERCIAL</GenericValue>
  <GenericValue>MANAGEMENT</GenericValue>
</Category>
```

There may be zero, one or more "Administrative" category values within a NATO policy *ConfidentialityInformation* element.

Examples

Table 17 shows example markings from Reference 4, together with the equivalent confidentiality label.

Table 17: Example - Security Marking and Equivalent Confidentiality Label

Marking	Confidentiality Label
NATO UNCLASSIFIED Releasable to ISAF, KFOR, RESOLUTE SUPPORT	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>UNCLASSIFIED</Classification> <Category tagName="Context" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName="Releasable To" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> <GenericValue>ISAF</GenericValue> <GenericValue>KFOR</GenericValue> <GenericValue>RESOLUTE SUPPORT</GenericValue> </Category> </ConfidentialityInformation>
NATO UNCLASSIFIED	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>UNCLASSIFIED</Classification> <Category tagName="Context" type="PERMISSIVE">

Marking	Confidentiality Label
	<pre><GenericValue>NATO</GenericValue> </Category> </ConfidentialityInformation></pre>
<p>NATO UNCLASSIFIED – STAFF</p>	<pre><ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>UNCLASSIFIED</Classification> <Category tagName="Context" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> </Category> <Category tagName="Administrative" type="INFORMATIVE"> <GenericValue>STAFF</GenericValue> </Category> </ConfidentialityInformation></pre>
<p>NATO RESTRICTED Releasable to Japan, Switzerland, Ukraine</p>	<pre><ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>RESTRICTED</Classification> <Category tagName="Context" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName="Releasable To" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> <GenericValue>JPN</GenericValue> <GenericValue>CHE</GenericValue> <GenericValue>UKR</GenericValue> </Category> </ConfidentialityInformation></pre>
<p>NATO/EAPC CONFIDENTIAL Releasable to ISAF</p>	<pre><ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>CONFIDENTIAL</Classification> <Category tagName="Context" type="PERMISSIVE"> <GenericValue>EAPC</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName="Releasable To" type="PERMISSIVE"> <GenericValue>EAPC</GenericValue> <GenericValue>ISAF</GenericValue> </Category> </ConfidentialityInformation></pre>
<p>NATO/KFOR CONFIDENTIAL NATO, Ireland, Sweden, Ukraine Only</p>	<pre><ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>CONFIDENTIAL</Classification> <Category tagName="Context" type="PERMISSIVE"> <GenericValue>KFOR</GenericValue> </Category> <Category tagName="Only" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> <GenericValue>IRL</GenericValue> <GenericValue>SWE</GenericValue> <GenericValue>UKR</GenericValue> </Category> </ConfidentialityInformation></pre>

The following table shows a further example of markings, together with the equivalent confidentiality label, which shows the use of both the Only and Releasable To categories.

Table 18: Using Both Releasable To and Only Categories

Marking	Confidentiality Label
<p>NATO RESTRICTED Canada, Germany, Spain, France, Italy, Netherlands, Norway, UK, USA Only</p> <p>Releasable to Sweden</p>	<pre> <ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>RESTRICTED</Classification> <Category tagName="Context" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName="Only" type="PERMISSIVE"> <GenericValue>CAN</GenericValue> <GenericValue>DEU</GenericValue> <GenericValue>ESP</GenericValue> <GenericValue>FRA</GenericValue> <GenericValue>ITA</GenericValue> <GenericValue>NLD</GenericValue> <GenericValue>NOR</GenericValue> <GenericValue>GBR</GenericValue> <GenericValue>USA</GenericValue> </Category> <Category tagName="Releasable To" type="PERMISSIVE"> <GenericValue>NATO</GenericValue> <GenericValue>SWE</GenericValue> </Category> </ConfidentialityInformation> </pre>

ANNEX A: Example Clearances for Nations

Introduction

This Annex presents a number of example clearances that may be used when evaluating a confidentiality label in support of an access control decision.

The example clearances illustrate how the restrictive categories (Additional Sensitivity) and permissive categories (Only, Releasable To) are used to support the access control decision.

Clearances do not, in general, include informative categories (Administrative) as informative categories are not considered in the access control decision.

A clearance contains the same security marking elements as a confidentiality label, with the exception that a clearance contains multiple classification elements, where a confidentiality label contains a single element.

The example clearances consider:

1. A NATO member nation,
2. A partner nation and
3. A non-member, non-partner nation.

An XML schema for representing the example clearances used in this Annex is defined below. The clearance syntax is based upon the clearance attribute description from Clearance Attribute and Authority Clearance Constraints Certificate Extension RFC 5913 (Reference [9]) and imports the necessary security marking elements from the *ConfidentialityInformation* element required to represent a clearance.

Schema

A schema has been defined to represent a clearance.

The schema has the following namespace:
urn:nato:stanag:4774:confidentialityclearance:1:0.

The schema for the Confidentiality Clearance is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!--  
*****
```

```
        NATO UNCLASSIFIED
```

XML Schema for representing a Confidentiality Clearance.

```
        |  
        /\  
    -< + >-  
        \/  
        |      NCI AGENCY  
    ## # ##### #   P.O. box 174  
    ## # # # #   2501 CD The Hague
```


Core Enterprise Services

A G E N C Y

-->

```
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
targetNamespace="urn:nato:stanag:4774:confidentialityclearance:1:0"
version="1.2" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:annotation>
<xs:appinfo>
<UniqueIdentifier/>
<Name>Confidentiality Clearance Schema</Name>
<Definition>Schema for a confidentiality clearance</Definition>
<VersionIndicator>1.0</VersionIndicator>
<UsageGuidance>
Used within NATO for representing a confidentiality clearance.
</UsageGuidance>
<RestrictionType/>
<RestrictionValue/>
<ConfidentialityLabel ReviewDateTime="2020-03-24T00:00:00Z">
<ConfidentialityInformation>
<PolicyIdentifier>NATO</PolicyIdentifier>
<Classification>UNCLASSIFIED</Classification>
<Category Type="PERMISSIVE" TagName="Context">
<GenericValue>NATO</GenericValue>
</Category>
</ConfidentialityInformation>
<CreationDateTime>2015-03-24T00:00:00Z</CreationDateTime>
</ConfidentialityLabel>
</xs:appinfo>
<xs:documentation>
The schema can be used to convey X.501 clearance attribute Access Control Information (ACI) in XML.
</xs:documentation>
</xs:annotation>

<!-- Import STANAG 4774 Confidentiality Metadata Label Schema -->
<xs:import namespace="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
schemaLocation="nl-cl.xsd"/>

<xs:element name="ConfidentialityClearance" id="confidentialityClearance">
<xs:annotation>
<xs:appinfo>
<UniqueIdentifier> urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:confidentialityClearance
</UniqueIdentifier>
<Name>Confidentiality Clearance</Name>
<Definition>
Confidentiality Clearance importing types from ConfidentialityLabel
</Definition>
<VersionIndicator>1.2</VersionIndicator>
<UsageGuidance>Used to represent the ACI of any entity.</UsageGuidance>
<RestrictionType/>
<RestrictionValue/>
</xs:appinfo>
```

```
</xs:annotation>
<xs:complexType>
  <xs:complexContent>
    <xs:extension base="sclr:ConfidentialityClearanceType">
      <xs:anyAttribute processContents="lax"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
</xs:element>
<xs:complexType name="ConfidentialityClearanceType" id="confidentialityClearanceType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier> urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:confidentialityClearanceType
    </UniqueIdentifier>
    <Name>Confidentiality Clearance Type</Name>
    <Definition>
      A type that is used as the base for the confidentiality clearance elements.
    </Definition>
    <VersionIndicator>1.0</VersionIndicator>
    <UsageGuidance/>
    <RestrictionType/>
    <RestrictionValue/>
  </xs:appinfo>
</xs:annotation>
<xs:sequence>
  <xs:element ref="slab:PolicyIdentifier"/>
  <xs:element ref="sclr:ClassificationList"/>
  <xs:element ref="slab:Category" minOccurs="0" maxOccurs="unbounded"/>
  <xs:element ref="sclr:ConfidentialityClearanceExtensions" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:element name="ClassificationList" type="sclr:ClassificationListType"/>
<xs:complexType name="ClassificationListType" id="classificationListType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:classificationListType
    </UniqueIdentifier>
    <Name>ClassificationList Type</Name>
    <Definition>A type that enumerates the classifications.</Definition>
    <VersionIndicator>1.0</VersionIndicator>
    <UsageGuidance/>
    <RestrictionType/>
    <RestrictionValue/>
  </xs:appinfo>
</xs:annotation>
<xs:sequence>
  <xs:element ref="slab:Classification" maxOccurs="unbounded"/>
  <xs:element ref="sclr:ConfidentialityClearanceExtensions" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:element name="ConfidentialityClearanceExtensions" type="sclr:ConfidentialityClearanceExtensionsType"/>
<xs:complexType name="ConfidentialityClearanceExtensionsType"
id="confidentialityClearanceExtensionsType">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:confidentialityClearanceExtensionsType
    </UniqueIdentifier>
    <Name>ConfidentialityClearanceExtensions Type</Name>
```

```
<Definition>A type that allows for extensibility.</Definition>
<VersionIndicator>1.0</VersionIndicator>
<UsageGuidance/>
<RestrictionType/>
<RestrictionValue/>
</xs:appinfo>
</xs:annotation>
<xs:sequence>
  <xs:any processContents="lax" namespace="##other" minOccurs="0" \
    maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:schema>
```

NATO Member Nation

Introduction

The following sections discuss the category values a nation will have in their clearance if they are a current member of NATO.

Context Category

A nation which is a member of NATO will have a “Context” category value in their clearance for NATO and all NAC-approved activities of which they are a member.

Releasable To Category

A nation will have a “Releasable To” category value in their clearance for NATO and all NAC-approved activities of which they are a member, as well as their own national value.

Only Category

A nation will have an “Only” category value in their clearance for NATO as well as their own national value.

Additional Sensitivity Category

A nation will have the appropriate “Additional Sensitivity” categories values in their clearance.

Example

An example clearance for the United Kingdom, a founding member of NATO:

```
<sclr:ConfidentialityClearance
  xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
  xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <sclr:ClassificationList>
    <Classification>UNCLASSIFIED</Classification>
    <Classification>RESTRICTED</Classification>
    <Classification>CONFIDENTIAL</Classification>
    <Classification>SECRET</Classification>
    <Classification>TOP SECRET</Classification>
  </sclr:ClassificationList>
  <Category TagName="Context" Type="PERMISSIVE">
    <GenericValue>NATO</GenericValue>
```

```
<GenericValue>EAPC</GenericValue>
<GenericValue>GEORGIA</GenericValue>
<GenericValue>ISAF</GenericValue>
<GenericValue>KFOR</GenericValue>
<GenericValue>PFP</GenericValue>
<GenericValue>RUSSIA</GenericValue>
<GenericValue>UKRAINE</GenericValue>
<GenericValue>Releasable</GenericValue>
</Category>
<Category TagName="Releasable To" Type="PERMISSIVE">
  <GenericValue>NATO</GenericValue>
  <GenericValue>EAPC</GenericValue>
  <GenericValue>ISAF</GenericValue>
  <GenericValue>KFOR</GenericValue>
  <GenericValue>PFP</GenericValue>
  <GenericValue>GBR</GenericValue>
</Category>
<Category TagName="Only" Type="PERMISSIVE">
  <GenericValue>NATO</GenericValue>
  <GenericValue>GBR</GenericValue>
</Category>
<Category TagName="Additional Sensitivity" Type="RESTRICTIVE">
  <GenericValue>ATOMAL</GenericValue>
  <GenericValue>BOHEMIA</GenericValue>
  <GenericValue>CRYPTO</GenericValue>
</Category>
</sclr:ConfidentialityClearance>
```

Partner Nation

Introduction

The following sections discuss the category values a nation will have in their clearance if they are not a member of NATO, but are a NATO partner nation.

Context Category

A nation should have the “Context” category value in their clearance for each NAC approved activity in which they are a partner nation.

A nation should also have the “Context” category value of “Releasable” in their clearance, to support confidentiality labels generated outside of the NAC approved activities of which of the nation is a partner nation.

Releasable To Category

A nation should also have a “Releasable To” category value in their clearance for each NAC approved activity in which they were a partner nation.

A nation should have a “Releasable To” category value in their clearance for their nation, to support confidentiality labels generated outside of the NAC approved activities of which of the nation is a partner nation.

Only Category

A nation should have an “Only” category value in their clearance for their nation.

Additional Sensitivity Category

A nation will have the appropriate “Additional Sensitivity” category values in their clearance.

Example

An example clearance for the New Zealand, which is a partner nation in the ISAF NAC approved activity:

```
<sclr:ConfidentialityClearance
xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
<PolicyIdentifier>NATO</PolicyIdentifier>
<sclr:ClassificationList>
<Classification>UNCLASSIFIED</Classification>
<Classification>RESTRICTED</Classification>
<Classification>CONFIDENTIAL</Classification>
<Classification>SECRET</Classification>
</sclr:ClassificationList>
<Category TagName="Context" Type="PERMISSIVE">
<GenericValue>ISAF</GenericValue>
<GenericValue>Releasable</GenericValue>
</Category>
<Category TagName="Releasable To" Type="PERMISSIVE">
<GenericValue>NZL</GenericValue>
<GenericValue>ISAF</GenericValue>
</Category>
<Category TagName="Only" Type="PERMISSIVE">
<GenericValue>NZL</GenericValue>
</Category>
</sclr:ConfidentialityClearance>
```

Non-NATO, Non-Partner Nation

Introduction

The following sections discuss the category values a nation will have in their clearance if they are neither a member of NATO nor a NATO partner nation.

Context Category

A nation should have the “Context” category value of “Releasable” in their clearance.

Releasable To Category

A nation should have a “Releasable To” category value in their clearance for their nation.

Only Category

A nation should have no “Only” category values in their clearance, as they are not part of any NAC approved activities.

Additional Sensitivity Category

A nation will have the appropriate “Additional Sensitivity” category values in their clearance.

Example

An example clearance for the Samoa:

```
<sclr:ConfidentialityClearance
  xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
  xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <sclr:ClassificationList>
    <Classification>UNCLASSIFIED</Classification>
    <Classification>RESTRICTED</Classification>
    <Classification>CONFIDENTIAL</Classification>
    <Classification>SECRET</Classification>
  </sclr:ClassificationList>
  <Category TagName="Context" Type="PERMISSIVE">
    <GenericValue>Releasable</GenericValue>
  </Category>
  <Category TagName="Releasable To" Type="PERMISSIVE">
    <GenericValue>WSM</GenericValue>
  </Category>
</sclr:ConfidentialityClearance>
```

INTENTIONALLY BLANK

ANNEX B: Security Policy Information File

Introduction

A Security Policy Information File (SPIF) describes all of the allowable values within a security policy and the relationships between them.

The SPIF can also include information that defines how the allowable values should be rendered as a security marking.

The SPIF can include information for rendering in different languages.

An XML schema for representing a SPIF is defined at www.xmlspif.org.

Validation

The confidentiality label syntax defined in Appendix 2 allows a confidentiality label to be represented in a wide range of security policies including both NATO security policies and National security policies.

The confidentiality label syntax supports the Principle of Consistent Labelling by defining a schema for the confidentiality label, but does not, of itself, support the consistent application of a security policy.

In order to support the consistent generation of confidentiality labels with registered values, additional information is required about the specific policies that are being used.

Validation Approaches

There are number of validation languages and tools that can be implemented to make assertions about the presence or absence of patterns within XML documents. One such example of this is Schematron which is a rules based validation language which can be defined for specific security policy to ensure that all of the values present with a confidentiality label lie within the correct Value Domain.

Example

The following example SPIF uses the XMLSPIF schema to encapsulate the elements of the NATO Security Policy. The complete, up to date SPIF for the NATO Security Policy is held in the NMRR.

NATO SPIF

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- $Id: NATO Security Policy.xml 79 2015-11-06 15:54:38Z g.lunt $ -->
<spif:SPIF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:spif="http://www.xmlspif.org/spif"
  schemaVersion="2.1" version="79" creationDate="201511061430200Z"
  originatorDN="CN=Graeme Lunt,O=SMHS Ltd,C=GB"
  keyIdentifier="6AA4BA9F66BFCD44" privilegeId="2.16.840.1.101.2.1.8.3"
  rbaId="2.16.840.1.101.2.1.8.3">
  <spif:securityPolicyId name="NATO" id="1.3.26.1.3.1"/>
```

```
<spif:securityClassifications>
  <spif:securityClassification name="UNCLASSIFIED" lacv="1" hierarchy="1">
    <spif:markingData xml:lang="fr" phrase="SANS CLASSIFICATION">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="RESTRICTED" lacv="2" hierarchy="2">
    <spif:markingData xml:lang="fr" phrase="DIFFUSION RESTREINTE">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="CONFIDENTIAL" lacv="3" hierarchy="3">
    <spif:markingData xml:lang="fr" phrase="CONFIDENTIEL">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="SECRET" lacv="4" hierarchy="4">
    <spif:markingData xml:lang="fr" phrase="SECRET">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="TOP SECRET" lacv="5" hierarchy="5">
    <spif:markingData phrase="COSMIC">
      <spif:code>replacePolicy</spif:code>
    </spif:markingData>
    <spif:markingData xml:lang="fr" phrase="TRES SECRET">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
</spif:securityClassifications>
<spif:securityCategoryTagSets>
  <spif:securityCategoryTagSet name="Additional Sensitivity" id="1.3.26.1.4.1">
    <spif:securityCategoryTag name="Additional Sensitivity" tagType="restrictive"
      singleSelection="false">
      <spif:tagCategory name="ATOMAL" lacv="1">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
        <spif:excludedClass>RESTRICTED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="CRYPTO" lacv="2">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
        <spif:excludedClass>RESTRICTED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="SIOP" lacv="3"/>
      <spif:tagCategory name="SIOP ESI" lacv="4" obsolete="true"/>
      <spif:tagCategory name="EXCLUSIVE" lacv="5" obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="INTELLIGENCE" lacv="6" obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="LOGISTICS" lacv="7" obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="OPERATIONS" lacv="8" obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="BOHEMIA" lacv="9" >
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
    </spif:securityCategoryTagSet>
</spif:securityCategoryTagSets>
```

```
<spif:markingQualifier markingCode="pageTop">
  <spif:qualifier markingQualifier=" " qualifierCode="separator"/>
</spif:markingQualifier>
</spif:securityCategoryTag>
</spif:securityCategoryTagSet>
<spif:securityCategoryTagSet name="Releasable To" id="1.3.26.1.4.2">
  <spif:securityCategoryTag name="Releasable To" tagType="enumerated"
  enumType="permissive" singleSelection="false">
    <spif:tagCategory name="ALB" lacv="008">
      <spif:markingData phrase="Albania">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Albanie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="DZA" lacv="012">
      <spif:markingData phrase="Algeria">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Algérie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="ARM" lacv="051">
      <spif:markingData phrase="Armenia">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Arménie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="AUS" lacv="036">
      <spif:markingData phrase="Australia">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Australie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="AUT" lacv="040">
      <spif:markingData phrase="Austria">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Autriche">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="AZE" lacv="031">
      <spif:markingData phrase="Azerbaijan">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Azerbaïdjan">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
    </spif:tagCategory>
  </spif:securityCategoryTag>
</spif:securityCategoryTagSet>
```

```
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BAH" lacv="048">
  <spif:markingData phrase="Bahrain">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bahreïn">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BLR" lacv="112">
  <spif:markingData phrase="Belarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bélarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BEL" lacv="056">
  <spif:markingData phrase="Belgium">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Belgique">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="BIH" lacv="070">
  <spif:markingData phrase="Bosnia and Herzegovina">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bosnie-Herzégovine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BGR" lacv="100">
  <spif:markingData phrase="Bulgaria">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bulgarie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="CAN" lacv="124">
  <spif:markingData phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="HRV" lacv="191">
```

```
<spif:markingData phrase="Croatia">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:markingData xml:lang="fr" phrase="Croatie">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="CZE" lacv="203">
  <spif:markingData phrase="Czech Republic">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tchèque, République">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DNK" lacv="208">
  <spif:markingData phrase="Denmark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Danemark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="EGY" lacv="818">
  <spif:markingData phrase="Egypt">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Égypte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="EST" lacv="233">
  <spif:markingData phrase="Estonia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Estonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FIN" lacv="246">
  <spif:markingData phrase="Finland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Finlande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FRA" lacv="250">
  <spif:markingData phrase="France">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="France">
```

```
<spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GEO" lacv="268">
  <spif:markingData phrase="Georgia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Géorgie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DEU" lacv="276">
  <spif:markingData phrase="Germany">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Allemagne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GRC" lacv="300">
  <spif:markingData phrase="Greece">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Grèce">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="HUN" lacv="348">
  <spif:markingData phrase="Hungary">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Hongrie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISL" lacv="352">
  <spif:markingData phrase="Iceland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Islande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="IRL" lacv="372">
  <spif:markingData phrase="Ireland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Irlande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
```

```
<spif:tagCategory name="ISR" lacv="376">
  <spif:markingData phrase="Israel">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Israël">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ITA" lacv="380">
  <spif:markingData phrase="Italy">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Italie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JPN" lacv="392">
  <spif:markingData phrase="Japan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Japon">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JOR" lacv="400">
  <spif:markingData phrase="Jordan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Jordanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KAZ" lacv="398">
  <spif:markingData phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KOR" lacv="410">
  <spif:markingData phrase="Korea, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Corée, République de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KWT" lacv="414">
  <spif:markingData phrase="Kuwait">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Koweït">
```

```
<spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KGZ" lacv="417">
  <spif:markingData phrase="Kyrgyzstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kirghizistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LVA" lacv="428">
  <spif:markingData phrase="Latvia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lettonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LTU" lacv="440">
  <spif:markingData phrase="Lithuania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lituanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LUX" lacv="442">
  <spif:markingData phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="MLT" lacv="470">
  <spif:markingData phrase="Malta">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Malte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MRT" lacv="478">
  <spif:markingData phrase="Mauritania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mauritanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
```



```
</spif:tagCategory>
<spif:tagCategory name="MDA" lacv="498">
  <spif:markingData phrase="Moldova, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Moldova, République de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNG" lacv="496">
  <spif:markingData phrase="Mongolia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mongolie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNE" lacv="499">
  <spif:markingData phrase="Montenegro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Monténégro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MAR" lacv="504">
  <spif:markingData phrase="Morocco">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Maroc">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NLD" lacv="528">
  <spif:markingData phrase="Netherlands">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pays-Bas">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NZL" lacv="554">
  <spif:markingData phrase="New Zealand">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Nouvelle-Zélande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NOR" lacv="578">
  <spif:markingData phrase="Norway">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
<spif:markingData xml:lang="fr" phrase="Norvège">
  <spif:code>documentStart</spif:code>
</spif:markingData>
</spif:tagCategory>

<spif:tagCategory name="POL" lacv="616">
  <spif:markingData phrase="Poland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pologne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PRT" lacv="620">
  <spif:markingData phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="QAT" lacv="634">
  <spif:markingData phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ROU" lacv="642">
  <spif:markingData phrase="Romania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Roumanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RUS" lacv="643">
  <spif:markingData phrase="Russian Federation">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Russie, Fédération de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SRB" lacv="688">
  <spif:markingData phrase="Serbia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Serbie">
```

```
<spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SVK" lacv="703">
  <spif:markingData phrase="Slovakia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Slovaquie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SVN" lacv="705">
  <spif:markingData phrase="Slovenia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Slovénie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="ESP" lacv="724">
  <spif:markingData phrase="Spain">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Espagne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SWE" lacv="752">
  <spif:markingData phrase="Sweden">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Suède">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>

<spif:tagCategory name="CHE" lacv="756">
  <spif:markingData phrase="Switzerland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Suisse">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="TJK" lacv="762">
  <spif:markingData phrase="Tajikistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tadjikistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="FYR" lacv="807">
```

```
<spif:markingData phrase=" the former Yugoslav Republic of Macedonia">
  <!--Turkey recognises the Republic of Macedonia with its constitutional name-->
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:markingData xml:lang="fr" phrase="l'ex-République yougoslave de Macédoine">
  <!-- La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.-->
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TUN" lacv="788">
  <spif:markingData phrase="Tunisia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tunisie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TUR" lacv="792">
  <spif:markingData phrase="Turkey">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Turquie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TKM" lacv="795">
  <spif:markingData phrase="Turkmenistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Turkménistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UKR" lacv="804">
  <spif:markingData phrase="Ukraine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Ukraine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ARE" lacv="784">
  <spif:markingData phrase="United Arab Emirates">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Émirats Arabes Unis">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GBR" lacv="826">
  <spif:markingData phrase="United Kingdom">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
```

```
<spif:markingData xml:lang="fr" phrase="Royaume-Uni">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="USA" lacv="840">
  <spif:markingData phrase="United States of America">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="États-Unis">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UZB" lacv="860">
  <spif:markingData phrase="Uzbekistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Ouzbékistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NATO" lacv="1001">
  <spif:markingData phrase="NATO">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="EAPC" lacv="1101">
  <spif:markingData phrase="EAPC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISAF" lacv="1201">
  <spif:markingData phrase="ISAF">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="IP" lacv="1301">
  <spif:markingData phrase="IP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ICI" lacv="1401">
  <spif:markingData phrase="ICI">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
</spif:tagCategory>
```

```
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KFOR" lacv="1501">
  <spif:markingData phrase="KFOR">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MD" lacv="1601">
  <spif:markingData phrase="MD">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PATG" lacv="1701">
  <spif:markingData phrase="PATG">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PFP" lacv="1801">
  <spif:markingData phrase="PFP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RESOLUTE SUPPORT" lacv="1901">
  <spif:markingData phrase="RESOLUTE SUPPORT">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PARP" lacv="2001">
  <spif:markingData phrase="PARP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NGC" lacv="2101">
  <spif:markingData phrase="NGC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NUC" lacv="2201">
  <spif:markingData phrase="NUC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
```

```
<spif:tagCategory name="NRC" lacv="2301">
  <spif:markingData phrase="NRC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:markingQualifier markingCode="pageTop">
  <spif:qualifier markingQualifier="Releasable To "
    qualifierCode="prefix"/>
  <spif:qualifier xml:lang="fr" markingQualifier="Communicable a "
    qualifierCode="prefix"/>
  <spif:qualifier markingQualifier="/" qualifierCode="separator"/>
</spif:markingQualifier>
</spif:securityCategoryTag>
</spif:securityCategoryTagSet>
<spif:securityCategoryTagSet name="Only" id="1.3.26.1.4.5">
  <spif:securityCategoryTag name="Only" tagType="enumerated"
    enumType="permissive" singleSelection="false">
>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="ALB" lacv="008">
    <spif:markingData phrase="Albania">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:markingData xml:lang="fr" phrase="Albanie">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="DZA" lacv="012">
    <spif:markingData phrase="Algeria">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:markingData xml:lang="fr" phrase="Algérie">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="ARM" lacv="051">
    <spif:markingData phrase="Armenia">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:markingData xml:lang="fr" phrase="Arménie">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="AUS" lacv="036">
    <spif:markingData phrase="Australia">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:markingData xml:lang="fr" phrase="Australie">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
    <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="AUT" lacv="040">
    <spif:markingData phrase="Austria">
      <spif:code>documentStart</spif:code>
    </spif:code>
  </spif:code>

```

```
</spif:markingData>
<spif:markingData xml:lang="fr" phrase="Autriche">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="AZE" lacv="031">
  <spif:markingData phrase="Azerbaijan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Azerbaïdjan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BAH" lacv="048">
  <spif:markingData phrase="Bahrain">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bahreïn">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BLR" lacv="112">
  <spif:markingData phrase="Belarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bélarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BEL" lacv="056">
  <spif:markingData phrase="Belgium">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Belgique">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="BIH" lacv="070">
  <spif:markingData phrase="Bosnia and Herzegovina">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bosnie-Herzégovine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BGR" lacv="100">
  <spif:markingData phrase="Bulgaria">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bulgarie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```



```
</spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="CAN" lacv="124">
  <spif:markingData phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="HRV" lacv="191">
  <spif:markingData phrase="Croatia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Croatie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="CZE" lacv="203">
  <spif:markingData phrase="Czech Republic">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tchèque, République">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DNK" lacv="208">
  <spif:markingData phrase="Denmark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Danemark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="EGY" lacv="818">
  <spif:markingData phrase="Egypt">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Égypte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="EST" lacv="233">
  <spif:markingData phrase="Estonia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Estonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FIN" lacv="246">
  <spif:markingData phrase="Finland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
<spif:markingData xml:lang="fr" phrase="Finlande">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FRA" lacv="250">
  <spif:markingData phrase="France">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="France">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GEO" lacv="268">
  <spif:markingData phrase="Georgia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Géorgie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DEU" lacv="276">
  <spif:markingData phrase="Germany">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Allemagne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GRC" lacv="300">
  <spif:markingData phrase="Greece">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Grèce">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="HUN" lacv="348">
  <spif:markingData phrase="Hungary">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Hongrie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISL" lacv="352">
  <spif:markingData phrase="Iceland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Islande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
```

```
<spif:tagCategory name="IRL" lacv="372">
  <spif:markingData phrase="Ireland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Irlande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISR" lacv="376">
  <spif:markingData phrase="Israel">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Israël">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ITA" lacv="380">
  <spif:markingData phrase="Italy">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Italie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JPN" lacv="392">
  <spif:markingData phrase="Japan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Japon">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JOR" lacv="400">
  <spif:markingData phrase="Jordan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Jordanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KAZ" lacv="398">
  <spif:markingData phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KOR" lacv="410">
  <spif:markingData phrase="Korea, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
<spif:markingData xml:lang="fr" phrase="Corée, République de">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KWT" lacv="414">
  <spif:markingData phrase="Kuwait">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Koweït">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KGZ" lacv="417">
  <spif:markingData phrase="Kyrgyzstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kirghizistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LVA" lacv="428">
  <spif:markingData phrase="Latvia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lettonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LTU" lacv="440">
  <spif:markingData phrase="Lithuania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lituanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LUX" lacv="442">
  <spif:markingData phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="MLT" lacv="470">
  <spif:markingData phrase="Malta">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Malte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
```

```
</spif:tagCategory>
<spif:tagCategory name="MRT" lacv="478">
  <spif:markingData phrase="Mauritania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mauritanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MDA" lacv="498">
  <spif:markingData phrase="Moldova, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Moldova, République de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNG" lacv="496">
  <spif:markingData phrase="Mongolia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mongolie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNE" lacv="499">
  <spif:markingData phrase="Montenegro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Monténégro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MAR" lacv="504">
  <spif:markingData phrase="Morocco">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Maroc">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NLD" lacv="528">
  <spif:markingData phrase="Netherlands">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pays-Bas">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NZL" lacv="554">
  <spif:markingData phrase="New Zealand">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
```

```
<spif:markingData xml:lang="fr" phrase="Nouvelle-Zélande">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NOR" lacv="578">
  <spif:markingData phrase="Norway">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Norvège">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="POL" lacv="616">
  <spif:markingData phrase="Poland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pologne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PRT" lacv="620">
  <spif:markingData phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="QAT" lacv="634">
  <spif:markingData phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ROU" lacv="642">
  <spif:markingData phrase="Romania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Roumanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RUS" lacv="643">
  <spif:markingData phrase="Russian Federation">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Russie, Fédération de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
<spif:excludedClass>TOP SECRET</spif:excludedClass>  
</spif:tagCategory>
```

```
<spif:tagCategory name="SRB" lacv="688">  
  <spif:markingData phrase="Serbia">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:markingData xml:lang="fr" phrase="Serbie">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:excludedClass>TOP SECRET</spif:excludedClass>  
</spif:tagCategory>
```

```
<spif:tagCategory name="SVK" lacv="703">  
  <spif:markingData phrase="Slovakia">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:markingData xml:lang="fr" phrase="Slovaquie">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:excludedClass>TOP SECRET</spif:excludedClass>  
</spif:tagCategory>
```

```
<spif:tagCategory name="SVN" lacv="705">  
  <spif:markingData phrase="Slovenia">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:markingData xml:lang="fr" phrase="Slovénie">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:excludedClass>TOP SECRET</spif:excludedClass>  
</spif:tagCategory>
```

```
<spif:tagCategory name="ESP" lacv="724">  
  <spif:markingData phrase="Spain">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:markingData xml:lang="fr" phrase="Espagne">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:excludedClass>TOP SECRET</spif:excludedClass>  
</spif:tagCategory>
```

```
<spif:tagCategory name="SWE" lacv="752">  
  <spif:markingData phrase="Sweden">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:markingData xml:lang="fr" phrase="Suède">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
</spif:tagCategory>
```

```
<spif:tagCategory name="CHE" lacv="756">  
  <spif:markingData phrase="Switzerland">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:markingData xml:lang="fr" phrase="Suisse">  
    <spif:code>documentStart</spif:code>  
  </spif:markingData>  
  <spif:excludedClass>TOP SECRET</spif:excludedClass>  
</spif:tagCategory>
```

```
<spif:tagCategory name="TJK" lacv="762">  
  <spif:markingData phrase="Tajikistan">
```

```
<spif:code>documentStart</spif:code>
</spif:markingData>
<spif:markingData xml:lang="fr" phrase="Tadjikistan">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FYR" lacv="807">
  <spif:markingData phrase=" the former Yugoslav Republic of Macedonia">
    <!--Turkey recognises the Republic of Macedonia with its constitutional name-->
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr"
    phrase=" l'ex-République yougoslave de Macédoine">
    <!-- La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.-->
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="TUN" lacv="788">
  <spif:markingData phrase="Tunisia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tunisie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TUR" lacv="792">
  <spif:markingData phrase="Turkey">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Turquie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TKM" lacv="795">
  <spif:markingData phrase="Turkmenistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Turkménistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UKR" lacv="804">
  <spif:markingData phrase="Ukraine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Ukraine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ARE" lacv="784">
  <spif:markingData phrase="United Arab Emirates">
    <spif:code>documentStart</spif:code>
```



```
</spif:markingData>
<spif:markingData xml:lang="fr" phrase="Émirats Arabes Unis">
  <spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GBR" lacv="826">
  <spif:markingData phrase="United Kingdom">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Royaume-Uni">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="USA" lacv="840">
  <spif:markingData phrase="United States of America">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="États-Unis">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UZB" lacv="860">
  <spif:markingData phrase="Uzbekistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Ouzbékistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NATO" lacv="1001">
  <spif:markingData phrase="NATO">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="EAPC" lacv="1101">
  <spif:markingData phrase="NATO">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISAF" lacv="1201">
  <spif:markingData phrase="ISAF">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="IP" lacv="1301">
  <spif:markingData phrase="IP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
```

```
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ICI" lacv="1401">
  <spif:markingData phrase="ICI">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KFOR" lacv="1501">
  <spif:markingData phrase="KFOR">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MD" lacv="1601">
  <spif:markingData phrase="MD">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PATG" lacv="1701">
  <spif:markingData phrase="PATG">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PFP" lacv="1801">
  <spif:markingData phrase="PFP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RESOLUTE SUPPORT" lacv="1901">
  <spif:markingData phrase="RESOLUTE SUPPORT">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PARP" lacv="2001">
  <spif:markingData phrase="PARP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NGC" lacv="2101">
  <spif:markingData phrase="NGC">
```

```
<spif:code>documentStart</spif:code>
</spif:markingData>
<spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NUC" lacv="2201">
  <spif:markingData phrase="NUC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NRC" lacv="2301">
  <spif:markingData phrase="NRC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:markingQualifier markingCode="pageTop">
  <spif:qualifier markingQualifier=" ONLY" qualifierCode="suffix"/>
  <spif:qualifier xml:lang="fr" markingQualifier=" SEULEMENT"
    qualifierCode="suffix"/>
  <spif:qualifier markingQualifier="," qualifierCode="separator"/>
</spif:markingQualifier>
</spif:securityCategoryTag>
</spif:securityCategoryTagSet>
<spif:securityCategoryTagSet name="Administrative" id="1.3.26.1.4.3">
  <spif:securityCategoryTag name="Administrative" tagType="tagType7"
    tag7Encoding="bitSetAttributes" singleSelection="false">
    <spif:tagCategory name="MANAGEMENT" lacv="1"/>
    <spif:tagCategory name="STAFF" lacv="2"/>
    <spif:tagCategory name="PERSONAL" lacv="3"/>
    <spif:tagCategory name="MEDICAL" lacv="4"/>
    <spif:tagCategory name="COMMERCIAL" lacv="5"/>
    <spif:markingQualifier markingCode="pageTop">
      <spif:qualifier markingQualifier=" " qualifierCode="separator"/>
    </spif:markingQualifier>
  </spif:securityCategoryTag>
</spif:securityCategoryTagSet>
<spif:securityCategoryTagSet name="Context" id="1.3.26.1.4.4">
  <spif:securityCategoryTag name="Context" tagType="permissive" >
    <spif:tagCategory name="NATO" lacv="1001">
      <spif:markingData phrase="NATO">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
    </spif:tagCategory>
    <spif:tagCategory name="EAPC" lacv="1002">
      <spif:markingData phrase="NATO/EAPC">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
    <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="GEORGIA" lacv="1003">
    <!-- NATO + Georgia -->
    <spif:markingData phrase="NATO/GEORGIA">
      <spif:code>noNameDisplay</spif:code>
      <spif:code>replacePolicy</spif:code>
    </spif:markingData>
    <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>

```

```
</spif:tagCategory>
<spif:tagCategory name="ISAF" lacv="1004">
  <spif:markingData phrase="NATO/ISAF">
    <spif:code>noNameDisplay</spif:code>
    <spif:code>replacePolicy</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KFOR" lacv="1005">
  <spif:markingData phrase="NATO/KFOR">
    <spif:code>noNameDisplay</spif:code>
    <spif:code>replacePolicy</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PFP" lacv="1006">
  <spif:markingData phrase="NATO/PFP">
    <spif:code>noNameDisplay</spif:code>
    <spif:code>replacePolicy</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RUSSIA" lacv="1007">
  <spif:markingData phrase="NATO/RUSSIA">
    <spif:code>noNameDisplay</spif:code>
    <spif:code>replacePolicy</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UKRAINE" lacv="1008">
  <spif:markingData phrase="NATO/UKRAINE">
    <spif:code>noNameDisplay</spif:code>
    <spif:code>replacePolicy</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="IP" lacv="1009">
  <spif:markingData phrase="NATO/IP">
    <spif:code>noNameDisplay</spif:code>
    <spif:code>replacePolicy</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RESOLUTE SUPPORT" lacv="1010">
  <spif:markingData phrase="NATO/RESOLUTE SUPPORT">
    <spif:code>noNameDisplay</spif:code>
    <spif:code>replacePolicy</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="Releasable" lacv="10000">
  <spif:markingData>
    <spif:code>noNameDisplay</spif:code>
  </spif:markingData>
  <!-- Required when Releasable To category is used -->
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
</spif:securityCategoryTag>
</spif:securityCategoryTagSet>
```

</spif:securityCategoryTagSets>
</spif:SPIF>

INTENTIONALLY BLANK

ANNEX C: PUBLIC Security Policy Confidentiality Labels

Introduction

The confidentiality label schema defined in Annex A of Appendix 1 specifies the syntax for confidentiality labels and provides the semantics for the values a confidentiality label may contain. In other words, the confidentiality label schema is a generic framework for storing any confidentiality label values that supports multiple different security policies.

However, the confidentiality label schema itself does not define the semantics of the values a confidentiality label can contain for a given specific security policy.

Ingest

NATO may ingest information from the public domain that does not contain a confidentiality label.

In order to support the information lifecycle within NATO, an originator confidentiality label SHOULD be bound with the information on ingest to order to record the original confidentiality label associated with the information⁵.

In order to support the binding of an originator confidentiality label or information ingested from the public domain, a distinct security policy must be defined⁶ which can be used with the confidentiality label syntax.

Release

In addition, NATO may release NATO information into the public domain and consequently relinquish ownership of that information.

During the lifecycle of that NATO information, it may be required to indicate that the information will be released into the public domain at a certain date (e.g. using the SuccessionHandling element to embargo a press release), or propose an alternative confidentiality label to be used as and when the NATO information enters the public domain.

In order for confidentiality labels to be used effectively and consistently within an enterprise environment, there must be a well-defined mapping of the security policy onto the appropriate confidentiality label elements in order to ensure that the appropriate semantics (according to the security policy) are observed and applied.

⁵ In addition, on ingest, an alternative confidentiality label in the NATO security policy (see Appendix 2) should also be bound to the information to specify how the information should be handled within the NATO domain.

⁶ Note, it is not acceptable to use the NATO security policy (for example NATO UNCLASSIFIED) in the originator confidentiality label as this infers NATO ownership of the information. The NATO security policy can however be used in the alternative confidentiality label.

This annex describes the *ConfidentialityInformation* and its child elements in order to support effective and consistent application of the PUBLIC security policy within the NATO environment in accordance with:

- Technical and Implementation Directive for Confidentiality Labelling of NATO Information (Reference 2)

Note that all confidentiality labels with the PUBLIC security policy have a corresponding blank/empty security marking.

ConfidentialityInformation

The following table specifies the Value Domain for each of the *ConfidentialityInformation* elements and the defined *Category* elements, in support of the PUBLIC security policy.

All values within the ConfidentialityInformation element are treated as case insensitive during processing.

For example, “Unmarked” and “UNMARKED” are equivalent.

All values used in the ConfidentialityInformation element use the English terms.

Each of the Value Domains for the ConfidentialityInformation elements are described in further detail below.

PolicyIdentifier

The *PolicyIdentifier* element indicates the security policy authority and the semantics of the values of the other *ConfidentialityInformation* elements.

A single policy is used across NATO and all NAC-approved activities for unlabelled information from the public domain, and has the value “PUBLIC”.

The corresponding attributes for Policy element are:

Table 19: Attributes for Policy Element

Attribute	Value
URI	“urn:oid:1.3.6.1.4.1.31778.12.2.1”

For example,

<PolicyIdentifier>**PUBLIC**</PolicyIdentifier>

Classification

The Classification element indicates the sensitivity of the content of the data object to which the confidentiality label is bound.

The Value Domain for Classification element within the PUBLIC security policy are:

Table 20: Value Domain for Classification Element

Value	Definition
"UNMARKED"	

For example,

<Classification>**UNMARKED**</Classification>

PrivacyMark

The privacy mark is not used within the PUBLIC security policy.

Categories

Introduction

The PUBLIC security policy defines a single security category:

Table 21: Security Categories for the PUBLIC Security Policy

Value	Definition
"In Confidence"	Informative guidance on how the information should be handled.

The "In Confidence" category is described in the following section.

In Confidence

The corresponding attributes for the "In Confidence" category element are:

Table 22: Attributes for the Context Category Element

Attribute	Value
tagName	"In Confidence"
type	"INFORMATIVE"
URI	"urn:oid:1.3.6.1.4.1.31778.13.2.1"

The Value Domain of the "In Confidence" Category within the PUBLIC security policy is defined in Reference 1.

For example,

```
<ConfidentialityInformation>
  <PolicyIdentifier>PUBLIC</PolicyIdentifier>
  <Classification>UNMARKED</Classification>
  <Category   tagName="In   Confidence"   type="PERMISSIVE">
    <GenericValue>LEGAL</GenericValue>
  </ConfidentialityInformation>
```

Examples

The following table shows some example confidentiality labels in the PUBLIC security policy.

Table 23: Example - Confidentiality Labels

Confidentiality Label
<pre><ConfidentialityInformation> <PolicyIdentifier>PUBLIC</PolicyIdentifier> <Classification>UNMARKED</Classification> </ConfidentialityInformation></pre>
<pre><ConfidentialityInformation> <PolicyIdentifier>PUBLIC</PolicyIdentifier> <Classification>UNMARKED</Classification> <Category tagName="In Confidence" type="INFORMATIVE"> <GenericValue>MEDICAL</GenericValue> </Category> </ConfidentialityInformation></pre>
<pre><ConfidentialityInformation> <PolicyIdentifier>PUBLIC</PolicyIdentifier> <Classification>UNMARKED</Classification> <Category tagName="In Confidence" type="INFORMATIVE"> <GenericValue>COMMERCIAL</GenericValue> <GenericValue>LEGAL</GenericValue> </Category> </ConfidentialityInformation></pre>

ANNEX D: PUBLIC Security Policy Information File

Introduction

A Security Policy Information File (SPIF) describes all of the allowable values within a security policy and the relationships between them.

The SPIF can also include information that defines how the allowable values should be rendered as a security marking.

The SPIF can include information for rendering in different languages.

An XML schema for representing a SPIF is defined at www.xmlspif.org.

The following SPIF uses this XMLSPIF schema to encapsulate the PUBLIC security policy described in Appendix 2 Annex C.

Public SPIF

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- $Id: PUBLIC Security Policy.xml 58 2014-09-16 09:14:24Z g.lunt $ -->
<spif:SPIF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:spif="http://www.xmlspif.org/spif"
  xsi:schemaLocation="http://www.xmlspif.org/spif ../Schemas/spif.xsd"
  schemaVersion="1.0" version="1" creationDate="20140916090512Z"
  originatorDN="CN=Graeme Lunt,O=SMHS Ltd,C=GB"
  keyIdentifier="6AA4BA9F66BFCD44" privilegelid="2.16.840.1.101.2.1.8.3"
  rbaclid="2.16.840.1.101.2.1.8.3">
  <spif:securityPolicyId name="PUBLIC" id="1.3.6.1.4.1.31778.12.2.1"/>
  <spif:securityClassifications>
    <spif:securityClassification name="UNMARKED" lacv="0" hierarchy="0">
      <spif:markingData>
        <spif:code>noMarkingDisplay</spif:code>
      </spif:markingData>
    </spif:securityClassification>
  </spif:securityClassifications>
  <spif:securityCategoryTagSets>
    <spif:securityCategoryTagSet name="In Confidence"
      id="1.3.6.1.4.1.31778.13.2.1">
      <spif:securityCategoryTag name="In Confidence" tagType="tagType7"
        tag7Encoding="bitSetAttributes" singleSelection="false">
        <spif:tagCategory name="COMMERCIAL" lacv="1">
          <spif:markingData>
            <spif:code>noMarkingDisplay</spif:code>
          </spif:markingData>
        </spif:tagCategory>
        <spif:tagCategory name="INTELLECTUAL PROPERTY" lacv="2">
          <spif:markingData>
            <spif:code>noMarkingDisplay</spif:code>
          </spif:markingData>
        </spif:tagCategory>
        <spif:tagCategory name="JUSTICE" lacv="3">
          <spif:markingData>
            <spif:code>noMarkingDisplay</spif:code>
          </spif:markingData>
        </spif:tagCategory>
      </spif:securityCategoryTagSet>
    </spif:securityCategoryTagSets>
  </spif:SPIF>
```

```
<spif:tagCategory name="LEGAL" lacv="4">  
  <spif:markingData>  
    <spif:code>noMarkingDisplay</spif:code>  
  </spif:markingData>  
</spif:tagCategory>  
<spif:tagCategory name="MANAGEMENT" lacv="5">  
  <spif:markingData>  
    <spif:code>noMarkingDisplay</spif:code>  
  </spif:markingData>  
</spif:tagCategory>  
<spif:tagCategory name="MEDICAL" lacv="6">  
  <spif:markingData>  
    <spif:code>noMarkingDisplay</spif:code>  
  </spif:markingData>  
</spif:tagCategory>  
<spif:tagCategory name="PERSONAL" lacv="7">  
  <spif:markingData>  
    <spif:code>noMarkingDisplay</spif:code>  
  </spif:markingData>  
</spif:tagCategory>  
<spif:tagCategory name="SECURITY" lacv="8">  
  <spif:markingData>  
    <spif:code>noMarkingDisplay</spif:code>  
  </spif:markingData>  
</spif:tagCategory>  
<spif:tagCategory name="STAFF" lacv="9">  
  <spif:markingData>  
    <spif:code>noMarkingDisplay</spif:code>  
  </spif:markingData>  
</spif:tagCategory>  
</spif:securityCategoryTag>  
</spif:securityCategoryTagSet>  
</spif:securityCategoryTagSets>  
</spif:SPIF>
```

INTENTIONALLY BLANK

ADatP-4774(A)(1)

STANDARDS RELATED DOCUMENT

ADatP-4778.2

PROFILES FOR BINDING METADATA TO A DATA OBJECT

Edition A Version 1

DECEMBER 2020



NORTH ATLANTIC TREATY ORGANIZATION

**Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN**

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

2 December 2020

1. The enclosed Standards Related Document, ADatP-4778.2, Edition A, Version 1, PROFILES FOR BINDING METADATA TO A DATA OBJECT, which has been approved in conjunction with ADatP-4778 by the nations in the CONSULTATION, COMMAND AND CONTROL Board (C3B), is promulgated herewith.
2. ADatP-4778.2, Edition A, Version 1 is effective upon receipt.
3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (<https://nso.nato.int/nso/>) or through your national standardization authorities.
4. This publication shall be handled in accordance with C-M(2002)60.



Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1	Introduction.....	1-1
1.1.	Background.....	1-1
1.2.	Objective.....	1-1
1.3.	Scope.....	1-1
1.4.	NATO Metadata Regulatory Standards.....	1-1
1.5.	Summary.....	1-2
1.6.	Overview.....	1-3
1.7.	Conformance And Interoperability.....	1-5
1.8	Configuration Management And Governance.....	1-6
CHAPTER 2	Cryptographic Artefact Binding Profiles.....	2-1
2.1.	Introduction.....	2-1
2.2.	Identification.....	2-2
2.3.	Standards (Reference).....	2-2
ANNEX A	Generic XML Signature Cryptographic Artefact Profile.....	A-1
A.1.	Introduction.....	A-1
A.2.	General XMLDSIG Requirements.....	A-2
	Signature Types.....	A-2
	Same-Document URI-References.....	A-3
	XML Security Uniform Resource Identifiers (URIs).....	A-3
	XML Normalization.....	A-4
	URI Schemes.....	A-5
	Core Signature Syntax.....	A-5
ANNEX B	XML Signature: Digital Signature Cryptographic Artefact.....	B-1
ANNEX C	XML Signature: Keyed-Hash Message Authentication Code Cryptographic Artefact.....	C-1
ANNEX D	Example XML Signature Cryptographic Bindings.....	D-1
ANNEX E	Generic CMS Cryptographic Artefact Profile.....	E-1
E.1.	Introduction.....	E-1
E.2.	General Requirements.....	E-1
E.3.	CMS Profile.....	E-2
	General Syntax.....	E-2
E.4.	Binding Information.....	E-6
	Generate bindingData.....	E-7
	Processing bindingData.....	E-8
E.5.	Signature Generation.....	E-9
E.6.	Signature Verification.....	E-9
CHAPTER 3	Simple Mail Transfer Protocol Binding Profile.....	3-1
3.1.	Introduction.....	3-1
3.2.	Identification.....	3-1
3.3.	Standards (Reference).....	3-2
3.4.	Notational Conventions.....	3-2
3.5.	Internet Email Structure.....	3-2
3.6.	Cryptographic Artefacts Profile.....	3-6
3.7.	SignatureReference Schema.....	3-7

Figure 3-2 SignatureReference Schema	3-7
CHAPTER 4 Extensible Message And Presence Protocol Binding Profile.....	4-1
4.1. Introduction	4-1
4.2. Identification	4-1
4.3. Standards (Reference).....	4-2
4.4. Notational Conventions	4-2
4.5. Message Stanza Structure	4-2
4.6. IQ Stanza Structure.....	4-5
4.7. BindingData Schema.....	4-9
4.8. Cryptographic Artefacts Profile.....	4-10
CHAPTER 5 Office Open XML Formats Binding Profile.....	5-1
5.1. Introduction	5-1
5.2. Identification	5-1
5.3. Standards (Reference).....	5-2
5.4. Notational Conventions	5-2
5.5. Structure.....	5-2
5.6. Custom XML	5-3
Microsoft Office File Types	5-3
5.7. Cryptographic Artefacts Profile.....	5-5
CHAPTER 6 Simple Object Access Protocol Binding Profile	6-1
6.1. Introduction	6-1
6.2. Identification	6-1
6.3. Standards (Reference).....	6-2
6.4. Namespace Constraints	6-2
6.5. Notational Conventions	6-2
6.6. SOAP Message Structure	6-2
6.7. Cryptographic Artefacts Profile.....	6-5
CHAPTER 7 Representational State Transfer (REST) Binding Profile.....	7-1
7.1. Introduction	7-1
7.2. Identification	7-1
7.3. Standards (Reference).....	7-2
7.4. Notational Conventions	7-2
7.5. HTTP Request/Response for RESTful Web Services	7-2
7.6. Cryptographic Artefacts Profile.....	7-4
CHAPTER 8 Generic Open Packaging Convention Binding Profile	8-1
8.1. Introduction	8-1
8.2. Identification	8-1
8.3. Standards (Reference).....	8-1
8.4. Notational Conventions	8-2
8.5. File Package	8-2
8.6. Cryptographic Artefacts Profile.....	8-4
CHAPTER 9 Sidecar Files Binding Profile.....	9-1
9.1. Introduction	9-1
9.2. Identification	9-1
9.3. Standards (Reference).....	9-1
9.4. Notational Conventions	9-2

9.5.	File Package	9-2
9.6.	Cryptographic Artefacts Profile.....	9-3
CHAPTER 10	Extensible Metadata Platform Binding Profile.....	10-1
10.1.	Introduction	10-1
10.2.	Identification	10-1
10.3.	Standards (Reference).....	10-2
10.4.	Notational Conventions	10-2
10.5.	Structure.....	10-2
10.6.	XMP Sidecar File.....	10-6
10.7.	Cryptographic Artefacts Profile.....	10-8
CHAPTER 11	Web Service Messaging Profile Binding Profile.....	11-1
11.1.	Introduction	11-1
11.2.	Identification	11-1
11.3.	Standards (Reference).....	11-2
11.3.	Namespace Constraints	11-2
11.4.	Notational Conventions	11-2
11.5.	WSMP Message Structure	11-2
11.6.	Cryptographic Artefacts Profile.....	11-6
CHAPTER 12	Common XML Artefacts Binding Profile	12-1
12.1.	Introduction	12-1
12.2.	Identification	12-1
12.3.	Standards (Reference).....	12-2
12.4.	Namespace Constraints	12-3
12.5.	Notational Conventions	12-3
12.6.	XML Schema Structure	12-3
12.7.	Schematron Structure	12-5
12.8.	XML Stylesheet Structure.....	12-6
12.9.	Generic Codelist Structure	12-7
12.10.	Context/Value Association Structure.....	12-9
12.11.	Security Policy Information File Structure.....	12-11
12.12.	Cryptographic Artefacts Profile.....	12-13

INTENTIONALLY BLANK

CHAPTER 1 Introduction

1.1. Background

The Primary Directive on Information Management (PDIM) prescribes the application of metadata and markings in accordance with NATO policies and directives to facilitate sharing and control of NATO information.

The PDIM defines metadata as structured information that describes, explains, locates, and otherwise makes it easier to retrieve and use an information resource. The structure consists of 'elements', each of which will contain 'values'. The values relate to the resource itself, there may be controls over what the actual values can be.

Metadata is a key enabler for the effective and efficient management of information. Modern automated information systems require information resources to be labelled with metadata.

1.2. Objective

The NATO Core Metadata Specification defines a set of core metadata elements to support information management in the Alliance.

This document recognizes the existence of communities of interest's specific metadata standards and aims at steering their evolution in the mid to long term and at providing a single mediation standard in the short term to achieve sharing of information among different communities of interest.

1.3. Scope

NCMS applies to all NATO information and to any information resource handled or processed by NATO's communications and information systems. NCMS describes information resource and supports its consistent and appropriate handling.

All NATO civil and military bodies are mandated to use NCMS.

Allies and Partners must also use NCMS when handling NATO information.

1.4. NATO Metadata Regulatory Standards

NATO has the following metadata standards:

- **ADatP-5636** NATO Core Metadata Specification defines the core set of metadata elements that must be used to support interoperable information exchange

- **ADatP-4774** Confidentiality Metadata Label Syntax provides support for the Security Layer metadata elements
- **ADatP-4778** Metadata Binding Mechanism describes how to consistently bind metadata (of any sort) to a finite data object

Standards-related Documents (SRDs) complement those three standards by providing implementation and other guidance.

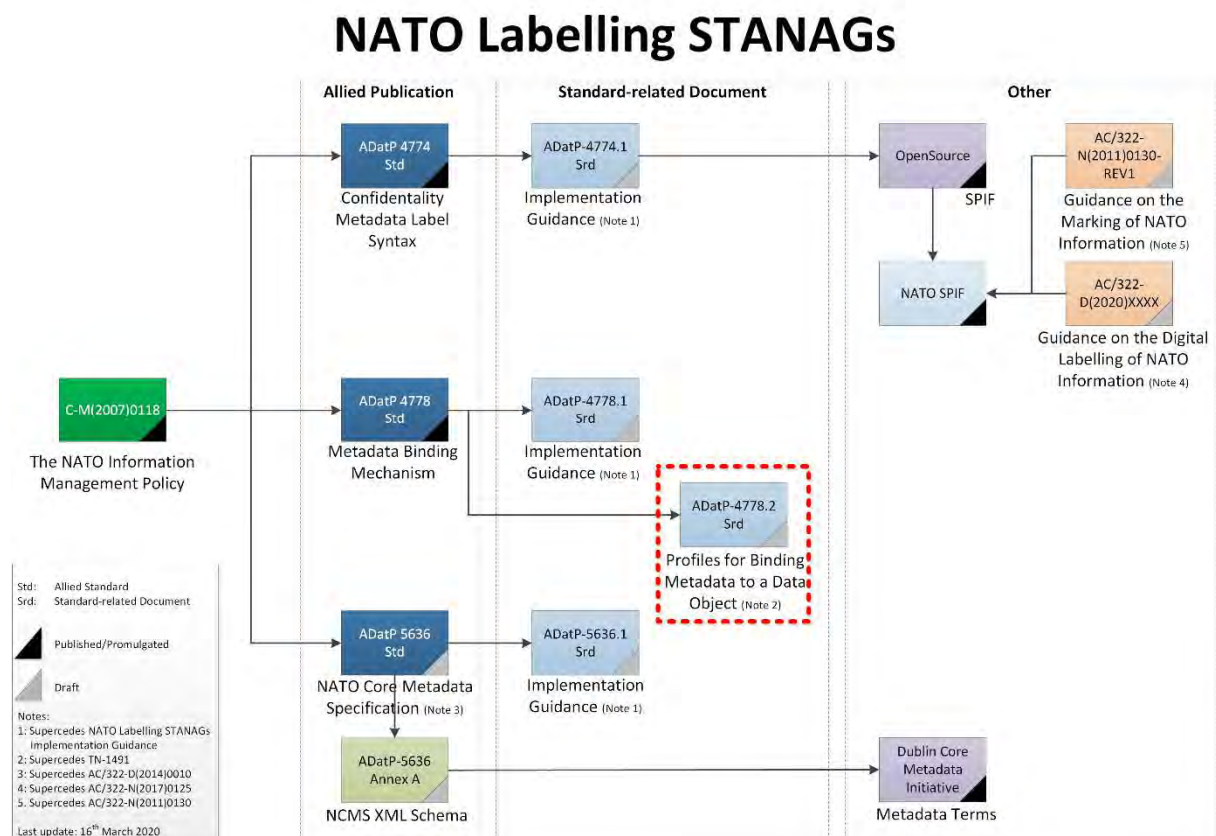


Figure 1 NATO Labelling STANAGs

This document (SRD) is Profiles for Binding Metadata to a Data Object for the Metadata Binding Mechanism (highlighted in a red, dashed box in Figure 1).

1.5. Summary

ADatP-4778 - Metadata Binding Mechanism specifies a method for binding metadata information (including confidentiality metadata labels) to finite data objects.

There is a need for complementary Binding Profiles that define how metadata should be bound to specific data object types and where the resulting binding should be located with respect to the data object.

These Binding Profiles reduce the risks to capability procurement for common funded programmes in the NATO Enterprise by ensuring that all data objects of a given type and labelled in a consistent manner and that the metadata binding can be located.

This Standards related document captures a number of Binding Profiles that use the mechanism defined in STANAG 4778 to allow the binding of the metadata to a selected data object.

These Binding Profiles have been under continual validation since the XML Labelling Guard deployment to the NATO missions in 2011. This continued during CWIX where successful validation efforts have been executed using newly defined profiles.

Additional Binding Profiles may be developed and supplement in future Editions and Versions of this Standards related document.

1.6. Overview

The term labelling is the process of determining the appropriate metadata for a given data object, creating the metadata label and binding the metadata label to the data object. A binding is a relationship between the data object(s) and the metadata label(s). A binding is realized by applying a binding mechanism. If a metadata label must be bound to a data object, both the metadata label and the data object are input to the binding mechanism. The output of the binding mechanism is the binding of a data object and metadata label (see Figure 2) which says that the data object and the metadata label belong together. The binding can be recorded as a structured data object, known as a Binding Data Object (BDO).

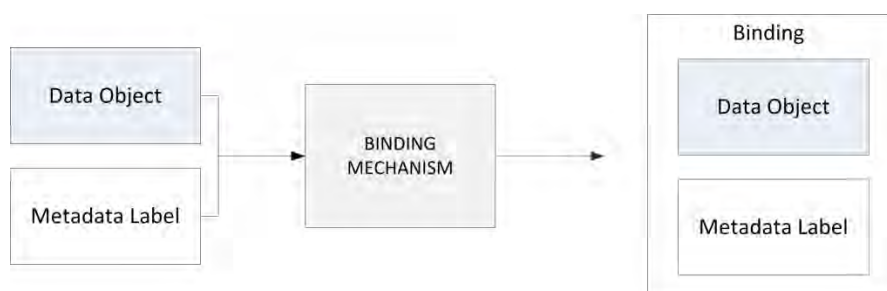


Figure 2 Creation of a binding

ADatP-4778 standardizes the binding of a data object and metadata label by specifying a common binding mechanism and a syntax for representing the BDO. However, to support information management and information sharing requirements it is necessary to further profile the application of ADatP-4778 to facilitate locating a BDO in higher level protocols, such as SMTP and HTTP, and embedding a BDO in data objects.

This document describes the application of the ADatP-4778 Metadata Binding Mechanism to specific data formats and protocols. It provides distinct binding profiles for the following protocols and data formats:

- Web Services (SOAP-based and REST-based web services);
- SMTP/MIME internet email messaging;
- Common XML Artefacts (e.g. XML schemas, stylesheets);
- Collaboration (Text-based instant messaging);
- Document management (including Office Tools);
- Extensible Metadata Platform (XMP); and
- Arbitrary Files.

Additionally, distinct profiles are provided to guide the application of strong bindings to any of the protocols and data formats indicated. A strong binding uses cryptographic techniques and mechanisms such as cryptographic digests, message authentication codes or digital signatures in order to protect the binding. Two distinct cryptographic bindings are provided:

- XML Signature cryptographic protocol using digital signatures; and
- XML Signature cryptographic protocol using Key-Hashed Message Authentication Code (HMAC).

This list of Binding Profiles is not exhaustive and new profiles may be added through the updates to this SRD, in accordance with AAP-03 (Reference [17]). In addition, it is quite possible that more than one Binding Profile will be defined for a particular protocol or data format.

Standards are aggregated in profiles. A standards profile is a set of standards for a particular purpose, covering certain services in the C3 taxonomy, with a guidance on implementation when and where needed. As profiles serve a particular purpose, they can be used in different environments, and therefore, they are not specific to a single overarching operational or technical concept. Profiles for Binding Metadata to a Data Object may and will be reused in other profiles.

In these profiles, interoperability standards fall into four obligation categories:

- **Mandatory** - Mandatory interoperability standards must be met to enable cross-domain information sharing
- **Conditional** - Conditional interoperability standards must be present under certain specific circumstances
- **Recommended** - Recommended interoperability standards may be excluded for valid reasons in particular circumstances, but the full implications must be understood and carefully weighed
- **Optional** - Optional interoperability standards are truly optional

The Binding Profiles, where applicable, use only recognized international and industry standards. The standards used are consistent with the use already declared by other services.

The Binding Profiles employ modular techniques and are extensible to provide agility in adapting to new use cases or scenarios. In other words, these profiles are designed to support the binding of any metadata to any type of finite data object.

These profiles support improved interoperability by providing a standard method to bind metadata to data objects. The examples provided to illustrate the semantics specified for each binding profile use Confidentiality Metadata Labels (Reference [1]) as example metadata with confidentiality metadata values specified for the AMOCO policy (Reference [22]).

1.7. Conformance And Interoperability

The profiles referenced in this document are methods of applying the binding mechanism stipulated in ADatP-4778. Conformance to these profiles would determine whether an implementation adheres to the features and framework of the STANAGs and the Binding Profiles. Traditionally implementers wishing to submit an implementation to conformance testing would be responsible for:

- Preparation of a Protocol Implementation Conformance Statement (PICS) against ADatP-4778;
- Preparation of the Protocol Implementation eXtra Information for Testing (PIXIT);
- Provide input to Test Plans and Procedures;
- Approve Test Cases;
- Provide input to and approve Test Scripts; and
- Provide the Implementation Under Test (IUT).

Conformance testing of these Binding Profiles may be performed by any authorized laboratory which provides a reference implementation of the Binding Profiles. For example, the NATO C&I Agency has several reference implementations for various standards and services where the Independent Verification and Validation (IV&V) team can perform such testing. Although a formal Reference facility for testing of external implementations of ADatP-4778 and these Binding Profiles is not yet established, a reference implementation for ADatP-4778 has been developed and the STANAG testing capability is currently under investigation.

The outcome of formal testing ensures that the exclusive requirements of the Binding Profile under test have been properly provided and that no optional requirement impacts the expected operation nor generates an error if received by a consumer that does not implement the optional requirement.

The Interoperability Capability Team (IP Cat) will oversee the approval of test plans and procedures to be followed for the testing of these Binding Profiles.

In development of test plans, consideration will be given to assure that the implementation under test is protected, and that representatives of the originating

and/or the sponsoring nation may be present while the implementation is being tested. Consideration will also be given in the test plans and procedures to protect any national or other proprietary techniques or information that may be present in an implementation submitted for compliancy or interoperability testing.

1.8 Configuration Management And Governance

Binding Profiles describe how to apply the binding mechanism specified in ADatP-4778 to specific data formats and protocols. The purpose of the Binding Profiles is to determine which of the three binding approaches (Embedded, Encapsulated, and Detached) shall be best used. They specify how the BDO will be stored and transmitted for a specific data format or protocol leveraging native support, if available and they specify the semantics required to further interpret the relationship between the data object and the metadata label.

As technology evolves new data formats and protocols emerge whilst others are deprecated. Therefore, Binding Profiles may also need to evolve. It is recommended that Binding Profiles are regularly reviewed for applicability and new Binding Profiles are specified to support evolving technologies.

These Binding Profiles will be stipulated for use with both common-funded and federated systems. They will be used to promote interoperability and thus governed by the NATO and/or national authorities for interoperability.

CHAPTER 2 Cryptographic Artefact Binding Profiles

2.1. Introduction

A metadata binding provides additional information specifying which metadata belongs to which data object(s) and provides a verifiable reference between metadata and data. A non-cryptographic binding provides a reference between the metadata and the data. This reference can be structurally verified to be correct. However, no assumptions besides this can be made. In contrast, cryptographic bindings are used to provide a certain level of integrity protection, and authenticity and non-repudiation of the entity that generated the metadata binding.

A cryptographic binding (that includes cryptographic artefacts) uses cryptographic techniques and mechanisms like cryptographic digests, message authentication codes or digital signatures in order to protect the integrity of the binding. Such cryptographic techniques and mechanisms are subject to the level of assurance required for protecting the integrity of the binding and for establishing confidence for the authenticity of the entity creating the binding. The level of assurance required for protecting the integrity of the binding and for establishing confidence for the authenticity of the entity creating the binding is a matter for organizational, national or federation security policies. As such, these profiles do not mandate cryptographic techniques or mechanisms for generating a cryptographic artefact. However, the intention is to profile the use of cryptographic protocols, which can be used to implement support for different cryptographic techniques and mechanisms, for generating cryptographic artefacts to be stored in a cryptographic binding.

The subprofiles here profile the XML Signature (XMLDSIG, Reference [3]) and Cryptographic Message Syntax (CMS, Reference [18]) cryptographic protocols for generating a cryptographic artefact using digital signatures and / or key-hashed message authentication code (HMAC, Reference [7]) as the cryptographic techniques and mechanisms.

Table 2-1 below lists the supported cryptographic protocols and cryptographic mechanisms that are profiled for generating cryptographic artefacts.

Cryptographic Protocol	Cryptographic Mechanism	Reference
XML Signature (Reference [3])	Digital Signature	ANNEX A and ANNEX B
	Keyed-Hash Message Authentication Code	ANNEX A and ANNEX C
CMS (Reference [18])	Digital Signature	ANNEX E

Table 2-1 Supported Cryptographic Protocols and Mechanisms Profiles

Further revisions to this profile may be required to add subprofiles (annexes) for other cryptographic protocols such as JSON Web Signature (JWS, Reference [9]), for

example, or to update supported cryptographic algorithms by either introducing new algorithms or deprecating existing algorithms.

2.2. Identification

The profile for cryptographic artefact binding is uniquely identified by the Canonical Identifier shown in Table 2-2.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:cryptoartefact
Version Identifier	urn:nato:stanag:4778:profile:cryptoartefact:1:2

Table 2-2 Profile Identifiers

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base standards
- support for additional algorithms
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 2-2.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:cryptographic:1:1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

2.3. Standards (Reference)

Reference [1] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [2] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

Reference [3] W3C XMLSIG-CORE, 2008, "XML- Signature Syntax and Processing (Second Edition)", at <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/>, W3C Recommendation, W3C, 10 June 2008

Reference [4] Web Services Security (WS-Security), SOAP Message Security 1 (WS-Security 2004), OASIS Standard Specification, 1 February 2006

Reference [5] W3C XPath 1.0, 1999, "XML Path Language (XPath) – Version 1.0", at <http://www.w3.org/TR/xpath/>, W3C Recommendation, W3C, 16 November 1999

Reference [6] W3C XPointer, 2002, "XML Pointer Language (XPointer)", at <http://www.w3.org/TR/xptr/>, W3C Working Draft, W3C, 16 August 2002

Reference [7] IETF RFC 2104, "HMAC: Keyed-Hashing for Message Authentication", at <http://tools.ietf.org/html/rfc2104>, February 1997

- Reference [8] IETF RFC 8551, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", at <http://tools.ietf.org/html/rfc8551>, April 2019
- Reference [9] IETF RFC 7515, "JSON Web Signature (JWS)", at <http://tools.ietf.org/html/rfc7515>, May 2015
- Reference [10] IETF RFC 6931, "Additional XML Security Uniform Resource Identifiers (URIs)", at <http://tools.ietf.org/html/rfc6931>, April 2013
- Reference [11] W3C XMLDSIG-2nd-Ed Errata, 2014, "Errata for XML Signature 2nd Edition", at <http://www.w3.org/2008/06/xmlsigcore-errata.html>, W3C Recommendation, W3C, 01 October 2014
- Reference [12] W3C XMLSEC, 2013, "XML Security Algorithm Cross-Reference", at <http://www.w3.org/TR/xmlsec-algorithms>, W3C Working Group Note, W3C, 11 April 2013.
- Reference [13] W3C XMLDSIG-CORE1, 2013, "XML Signature Syntax and Processing Version 1.1", at <http://www.w3.org/TR/2013/REC-xmlsig-core1-20130411/>, W3C Recommendation, W3C, 11 April 2013
- Reference [14] W3C XMLENC-CORE, 2002, "XML Encryption Syntax and Processing", at <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>, W3C Recommendation, W3C, 10 December 2002.
- Reference [15] W3C XMLENC-CORE1, 2013, "XML Encryption Syntax and Processing Version 1.1", at <http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/>, W3C Recommendation, W3C, 11 April 2013.
- Reference [16] IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", at <http://tools.ietf.org/html/rfc5280>, May 2008
- Reference [17] AAP-03 "Directive for the Production, Maintenance and Management of NATO Standardization Documents", Edition K, Version 1, February 2018.
- Reference [18] IETF RFC 5652, "Cryptographic Message Syntax (CMS)", at <http://tools.ietf.org/html/rfc5652>, September 2009
- Reference [19] IETF RFC 8550, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling", at <http://tools.ietf.org/html/rfc8550>, April 2019
- Reference [20] IETF RFC 2634, "Enhanced Security Services for S/MIME", at <http://tools.ietf.org/html/rfc2634>, June 1999
- Reference [21] IETF RFC 3629, "UTF-8, a transformation format of ISO 10646", at <http://tools.ietf.org/html/rfc3629>, November 2003
- Reference [22] IETF RFC 3114, "Implementing Company Classification Policy with the S/MIME Security Label", at <http://tools.ietf.org/html/rfc3114>, May 2002

ANNEX A Generic XML Signature Cryptographic Artefact Profile
--

A.1. Introduction

XML Signature (XMLDSIG, Reference [3]) offers powerful and flexible mechanisms that can support a wide variety of cryptographic requirements. XMLDSIG provides integrity, authentication and non-repudiation services for data (including metadata) of any type. XMLDSIG is applied to arbitrary data whereby a data object is digested with the resulting value stored in an element which is then digested and cryptographically signed. XMLDSIG indicates the location of the data object either by reference (in the case of an enveloped or detached signature) or by value (in the case of an enveloping signature whereby the signature contains the data object that is to be signed).

In order to highlight the differences and avoid duplication of text from XMLDSIG, a delta specification approach has been taken. This Appendix will refer to the relevant sections of XMLDSIG and will identify any necessary clarifications and/or amendments to these sections. This approach provides traceability and puts the delta text in context. It is required that this Annex is read together with XMLDSIG.

Figure A-1 illustrates the structure of an XML Signature element including the primary sibling elements: SignedInfo; SignatureValue; KeyInfo; and, Object.

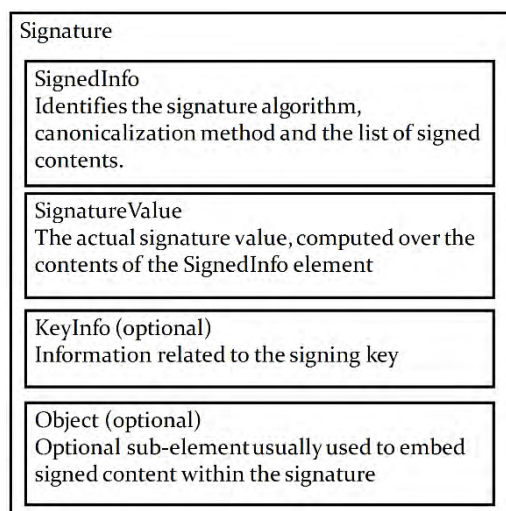


Figure A-1 XML Signature Structure

This Annex will use the same structure as illustrated in *Figure A-1* to profile those requirements that are generic for XML Signature based cryptographic artefacts and to further refine those requirements for cryptographic artefacts generated with the use of digital signatures or keyed-hash message authentication codes. In particular, this Annex will be divided into the following sub sections:

- General requirements for XMLDSIG including SignedInfo, SignatureValue and Object elements (refer to ANNEX A);
- Specific requirements for XMLDSIG SignedInfo and KeyInfo elements related to digital signatures (refer to ANNEX B); and,
- Specific requirements for XMLDSIG SignedInfo and KeyInfo elements related to keyed-hashed message authentication codes (refer to ANNEX C).

Example Binding Data Objects containing cryptographic artefacts conformant with this profile are illustrated in ANNEX D.

The notational conventions used for this Annex are as follows:

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [2].
- *Courier font* indicates syntax derived from various W3C XML Signature (Reference [3]) standard referenced in this Appendix.
- *Courier font* indicates syntax derived from Web Services Security (WSS) (Reference [4]) standard Section 10 referenced in this Appendix.

A.2. General XMLDSIG Requirements

Unless otherwise stated, all statements that apply to XMLDSIG also apply to this profile.

An entity that creates XML Signatures conformant with this profile (known as Originator) is REQUIRED to perform the processing rules for Core Generation as specified in XMLDSIG Section 3.1.

An entity that interprets and processes XML Signatures conformant with this profile (known as Recipient) is REQUIRED to perform the processing rules for Core Validation as specified in XMLDSIG Section 3.2.

Signature Types

Three types of signatures exist in XMLDSIG:

- enveloping signatures whereby the signature envelopes the data object to be signed; enveloped signatures whereby the signature is embedded within the data object; and,
- detached signatures whereby the signature and the data object reside independently.

Enveloping, Enveloped and Detached signature types are supported in this profile.

Same-Document URI-References

This section refers to XMLDSIG Section 4.4.3.1, 4.4.3.2 and 4.4.3.3

The significance of the URI fragment identifier for dereferencing subsets of data objects is a function of the type (media type) of the data object. Identification for the media type of a data object is supported in the general binding mechanism with the use of the *xmime:contentType* attribute. The *xmime:contentType* attribute for non-XML is a required attribute of the *DataReference* and *MetadataReference* elements.

In the case where the *xmime:contentType* attribute is present in the *DataReference* or *MetadataReference* element, the *xmime:contentType* attribute value specifies a non-XML data object type and the URI attribute value of the *DataReference* or *MetadataReference* element is deemed to be a 'same-document' reference (as specified in XMLDSIG Section 4.4.3.3) the following requirements are REQUIRED to be followed:

- Originator MUST create a *Manifest* element for each *DataReference* or *MetadataReference* elements (that conforms to this use case) contained in the *bindingInformation* that includes a *Reference* element (as specified in *Manifest* section of ANNEX A);
- The *Manifest* element that the Originator creates MUST be stored as a child element of an *Object* element;
- Recipient MUST perform the following additional Core Validation processing rules:
 - For each *Reference* in the *Manifest*:
 - Obtain the data object to be digested located by the URI attribute in the *Reference* element (According to the semantics specified for the URI fragment identifier defined by the media type);
 - Digest the resulting data object using the *DigestMethod* (as specified in the *Reference* section in ANNEX A).
 - Compare the generated digest value against *DigestValue* in the *Manifest Reference*; if there is any mismatch, validation fails.

XML Security Uniform Resource Identifiers (URIs)

XML security algorithm identifiers have been defined in a number of different specifications such as XML Signature, XML Encryption and RFCs. XML Security Algorithm Cross-Reference (Reference [12]) provides a non-normative list of identifiers that have been defined by XML Signature (References [3] and [13]), XML Encryption (References [14] and [15]) and Additional XML Security Uniform Resource Identifiers (URIs, Reference [10]).

This Appendix profiles the use of those algorithm identifiers listed in Reference [12] specifying whether support for that algorithm is mandatory, optional or prohibited for signature generation.

Mandatory and optional algorithms on signature generation **MUST** be supported on signature validation.

Prohibited algorithms on signature generation **MAY** be supported on signature validation.

XML Normalization

XML (de)serialization may result in a namespace prefix to be redefined within the XML document. XML documents that are provided as input to XML Signature Core Signature Generation and Verification may have differing information content, however, they are logically equivalent within a given application context. As a result the signature verification of the logically equivalent XML document will fail.

It is therefore **RECOMMENDED** that all XML documents prior to being provided as input to a XML Signature library for Core Signature Generation and Verification are passed through an XML normalization process that:

- Removes all namespace prefixes except “xml”;
- Visits each Element node in XML Document order;
- At each Element node all visibly utilised namespace URIs are considered;
- At each Element node duplicate namespace URIs are removed;
- At each Element node namespace URIs that have already been assigned are removed;
- At each Element node if an Attribute node of that Element node has a qualified name that is assigned a different namespace than the namespace of the Element node assign a prefix definition to the namespace of the Attribute node;
- Namespace declarations **SHALL** appear before attribute declarations;
- Attribute declarations are sorted lexicographically by namespaceURI as primary key and localName as secondary key;
- Attribute prefix definitions **SHALL** be written as “n0”, “n1”, “n2”etc. and,
- Preserve whitespace.

An XML Stylesheet (XSLT) 1.0 transform that performs XML normalization as described above is published in the NATO Metadata Registry and Repository (NMRR) at:

- https://nmrr.ncia.nato.int/rest/doc/NATO/Information%20Assurance/OLP/XML_Normalisation_1.0.xsl

It is RECOMMENDED that the XML Signature library when performing Core Signature Generation does not use a namespace prefix for the `<Signature/>` element and preserves whitespace when creating the XML Document containing the `<Signature/>` element.

URI Schemes

XML Signature Core Signature Generation and Verification may have differing levels of support to dereference specified URIs based on the URI scheme contained within a `Reference` element URI attribute value. In the use case whereby a URI scheme is used within a `Reference` element URI attribute value that may not be supported by XML Signature Core Signature Generation and Verification implementations the following requirements are REQUIRED to be followed:

- Originator MUST create a `Manifest` element for each `DataReference` or `MetadataReference` elements (that conforms to this use case) contained in the `bindingInformation` that includes a `Reference` element (as specified in `Manifest` section of ANNEX A);
- The `Manifest` element that the Originator creates MUST be stored as a child element of an `Object` element;
- Recipient MUST perform the following additional Core Validation processing rules:
 - For each `Reference` in the `Manifest`:
 - Obtain the data object to be digested located by the URI attribute in the `Reference` element (According to the semantics specified for the URI scheme);
 - Digest the resulting data object using the `DigestMethod` (as specified in the `Reference` section in ANNEX A).
 - Compare the generated digest value against `DigestValue` in the `Manifest Reference`; if there is any mismatch, validation fails.

Core Signature Syntax

This section refers to XMLDSIG Section 4.

Signature

This section refers to XMLDSIG Section 4.2.

In the case where a cryptographic binding is required the `bindingInformation` element (specified in Reference [2]) MUST contain at least one `Signature` element.

SignatureValue

This section refers to XMLDSIG Section 4.3.

SignedInfo

This section refers to XMLDSIG Section 4.4.

CanonicalizationMethod

This section refers to XMLDSIG Section 4.4.1.

The CanonicalizationMethod Algorithm attribute MUST be one of the following:

- <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>
- <http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>
- <http://www.w3.org/2006/12/xml-c14n11>
- <http://www.w3.org/2006/12/xml-c14n11#WithComments>
- <http://www.w3.org/2001/10/xml-exc-c14n#>
- <http://www.w3.org/2001/10/xml-exc-c14n#WithComments>
- <http://www.w3.org/2010/10/xml-c14n2>.

SignatureMethod

This section refers to XMLDSIG Section 4.4.2.

The SignatureMethod Algorithm attribute is REQUIRED.

The value of the SignatureMethod Algorithm is further specified depending on the cryptographic technique and mechanism being used (refer to ANNEX B for Digital Signatures or ANNEX C for HMAC).

Reference

This section refers to XMLDSIG Section 4.4.3.

For each *DataReference* or *MetadataReference* element included in a *bindingInformation* element there MUST be a Reference element

In the use case identified in Same-Document URI-References there MUST be a Reference element that identifies the Manifest element.

For each *MetadataBinding* element included in the *bindingInformation* element there MUST be a Reference element that identifies each *MetadataBinding* element.

URI

This section refers to XMLDSIG Section 4.4.3.1.

For each *DataReference* or *MetadataReference* element included in a *bindingInformation* element that contains a URI attribute with a value there MUST be a *Reference* element with the same URI attribute value, except in the case identified in Same-Document URI-References.

In the case identified in Same-Document URI-References there MUST be a URI attribute present with the value referencing the *Manifest* element.

For each *MetadataBinding* element included in the *bindingInformation* element there MUST be a *Reference* URI attribute with a shortname XPointer (Reference [6]) as the attribute value that identifies each *MetadataBinding* element.

Transforms

This section refers to XMLDSIG Section 4.4.3.4.

For Embedded BDOs in an XML data object an Enveloped Binding Data Object transform MUST first be applied to remove the *BindingInformation* element from the digest calculation of the *Reference* element containing the *BindingInformation* element.

The Enveloped Binding Data Object transform element MUST have *Transform Algorithm* attribute value of <http://www.w3.org/TR/1999/REC-xpath-19991116> and MUST contain the following XPath element:

```
<XPath>
  not(ancestor-or-self::*[local-name() = 'BindingInformation' and
    namespace-uri() = 'urn:nato:stanag:4778:bindinginformation:1:0'])
</XPath>
```

For Embedded BDOs where the *xmime:contentType* attribute is present in the *DataReference* element and the *xmime:contentType* attribute value specifies a non-XML data object type the use of the Enveloped Binding Data Object does not apply. In this use case the signature generation and signature validation process SHALL first exclude the Embedded Binding Data Object (the *BindingInformation* element) from the digest calculation of the *Reference* element containing the *BindingInformation* element.

For each *DataReference* or *MetadataReference* element included in a *bindingInformation* element that contains a *Transforms* element the first (or next in the case of Embedded BDOs) *Transform* element of the *Reference* *Transforms* element MUST be the *Transform* element from the *DataReference* or *MetadataReference* element.

For each *MetadataBinding* element included in the *bindingInformation* element there MAY be a *Transform* element (child of the *Transforms* element) that includes an XPath (Reference [5]) expression to identify *MetadataBinding* element.

For each *MetadataBinding*, *DataReference*, and *MetadataReference* that is identified by an XPath expression the *Transform* element MUST have an *Algorithm* attribute with the value 'http://www.w3.org/TR/1999/REC-xpath-19991116'.

Other *Transform* elements MAY be present.

For other *Transform* elements the *Transform Algorithm* attribute MUST have one of the following values:

- <http://www.w3.org/2000/09/xmlsig#base64>
- <http://www.w3.org/TR/1999/REC-xpath-19991116>
- <http://www.w3.org/2002/06/xmlsig-filter2>
- <http://www.w3.org/2000/09/xmlsig#enveloped-signature>
- <http://www.w3.org/TR/1999/REC-xslt-19991116>
- <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>
- <http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>
- <http://www.w3.org/2006/12/xml-c14n1>
- <http://www.w3.org/2006/12/xml-c14n11#WithComments>
- <http://www.w3.org/2001/10/xml-exc-c14n#>
- <http://www.w3.org/2001/10/xml-exc-c14n#WithComments>
- <http://www.w3.org/2010/10/xml-c14n2>

DigestMethod

This section refers to XMLDSIG Section 4.4.3.5.

The *DigestMethod Algorithm* attribute MUST conform to the specifications detailed in Table 2-3.

Algorithm Identifier	Mandatory/Optional/ Prohibited
http://www.w3.org/2001/04/xmlsig-more#md5	Prohibited
http://www.w3.org/2000/09/xmlsig#sha1	Prohibited
http://www.w3.org/2001/04/xmlsig-more#sha224	Prohibited
http://www.w3.org/2001/04/xmlenc#sha256	Optional
http://www.w3.org/2001/04/xmlsig-more#sha384	Mandatory
http://www.w3.org/2001/04/xmlenc#sha512	Optional
http://www.w3.org/2001/04/xmlenc#ripemd160	Optional

Table 2-3 DigestMethod Algorithm Identifiers

DigestValue

This section refers to XMLDSIG Section 4.4.3.6.

KeyInfo

This section refers to XMLDSIG Section 4.5.

The `KeyInfo` element is REQUIRED.

Refer to the relevant section, dependent upon the cryptographic technique and mechanism being used (refer to ANNEX B for Digital Signatures or ANNEX C for HMAC), for further profiling of the `KeyInfo` element.

Object

This section refers to XMLDSIG Section 4.6.

The `Object` element is REQUIRED.

Additional Signature Syntax

This section refers to XMLDSIG Section 5.

Manifest

This section refers to XMLDSIG Section 5.1.

The `Manifest` element is REQUIRED to support the use case for: Same-Document URI-References; and, URI Schemes not supported by XML Signature Core Signature Generation and Verification implementations.

The Originator MUST obtain the data object to be digested by dereferencing the URI attribute value in the *MetadataReference* or *DataReference* element in accordance to the semantics specified for: the URI fragment identifier defined by the media type (identified in the *MetadataReference contentType* or *DataReference contentType* attribute value); or, the URI scheme.

The Originator MUST perform the processing rules for Reference Generation as specified in XMLDSIG Section 3.1.1 with the following constraint:

The `Reference` element URI attribute value MUST be the same value as the *DataReference* (or *MetadataReference*) URI attribute value.

In other cases the use of the `Manifest` element is NOT REQUIRED.

In the case where the use of the `Manifest` element is required the originator MUST create a `Reference` element, including the identification of the `Manifest` element,

any `transform` elements, the digest algorithm and the `DigestValue` in order to be included in the signature

SignatureProperties

This section refers to XMLDSIG Section 5.2.

TimeStamp

This section refers to Web Services Security (WSS) (Reference [4]) Section 10.

The *TimeStamp* element MUST be present indicating the time that the cryptographic binding was created as a value of the *Created* element.

The *ValueType* attribute of the *Created* element MUST be *xsd:dateTime*.

The *Expires* element (child element of the *TimeStamp* element) is NOT REQUIRED.

The inclusion of an indication when the cryptographic binding was created supports the following two use cases:

1. Detection of replay attacks; and,
2. A valid cryptographic binding at time of signing, however, the key material used for creating the signature may have expired, been revoked or other.

It is RECOMMENDED that the originator create a *Reference* element, including the identification of the *TimeStamp* element in order to be included in the signature.

ANNEX B XML Signature: Digital Signature Cryptographic Artefact

Implementations that use digital signatures as the cryptographic mechanism for producing cryptographic artefacts are REQUIRED to be conformant with ANNEX A and this Annex.

SignedInfo

This section refers to XMLDSIG Section 4.4.

SignatureMethod

This section refers to XMLDSIG Section 4.4.2.

The `SignatureMethod` Algorithm attribute MUST conform to the specifications detailed in Table 2-4.

Algorithm Identifier	Mandatory/Optional/ Prohibited
http://www.w3.org/2000/09/xmlsig#dsa-sha1	Prohibited
http://www.w3.org/2009/xmlsig11#dsa-sha256	Optional
http://www.w3.org/2001/04/xmlsig-more#rsa-md5	Prohibited
http://www.w3.org/2000/09/xmlsig#rsa-sha1	Prohibited
http://www.w3.org/2001/04/xmlsig-more#rsa-sha224	Optional
http://www.w3.org/2001/04/xmlsig-more#rsa-sha256	Mandatory
http://www.w3.org/2001/04/xmlsig-more#rsa-sha384	Optional
http://www.w3.org/2001/04/xmlsig-more#rsa-sha512	Optional
http://www.w3.org/2001/04/xmlsig-more#rsa-ripemd160	Optional
http://www.w3.org/2001/04/xmlsig-more#ecdsa-sha1	Prohibited
http://www.w3.org/2001/04/xmlsig-more#ecdsa-sha224	Optional
http://www.w3.org/2001/04/xmlsig-more#ecdsa-sha256	Mandatory
http://www.w3.org/2001/04/xmlsig-more#ecdsa-sha384	Optional
http://www.w3.org/2001/04/xmlsig-more#ecdsa-sha512	Optional

Table 2-4 SignatureMethod (PKI) Algorithm Identifiers

KeyInfo

This section refers to XMLDSIG Section 4.5.

The `KeyInfo` element is REQUIRED.

KeyName

This section refers to XMLDSIG Section 4.5.1.

The `KeyName` element SHALL NOT be present.

KeyValue

This section refers to XMLDSIG Section 4.5.2.

The `KeyValue` MAY be present.

RetrievalMethod

This section refers to XMLDSIG Section 4.5.3.

The `RetrievalMethod` SHALL NOT be present.

X509Data

This section refers to XMLDSIG Section 4.5.4.

The `X509Data` element is REQUIRED.

In strategic systems with high throughput, certificates MUST be included. X.509 version 3 certificates (Reference [16]) MUST be supported.

The certificate profile specified in Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Reference [16]) MUST be supported.

The Originator SHOULD include at least one chain of certificates up to, but not including, a Certificate Authority (CA) that it believes that the Recipient may trust as authoritative.

Each certificate MUST be included in an `X509Certificate` element.

The Recipient SHOULD be able to handle an arbitrarily large number of certificates and chains.

In those cases where certificates may not be transmitted one of the `X509IssuerSerial`, `X509SKI` and `X509SubjectName` elements MUST be present.

The `X509CRL` element is NOT REQUIRED.

The CRL SHOULD be looked up based on the CRL Distribution Point (CDP) contained in the certificate.

The CRL profile specified in Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Reference [16]) MUST be supported.

PGPData

This section refers to XMLDSIG Section 4.5.5.

The PGPData element SHALL NOT be present.

SPKIData

This section refers to XMLDSIG Section 4.5.6.

The SPKIData element SHALL NOT be present.

MgmtData

This section refers to XMLDSIG Section 4.5.7.

The MgmtData element SHALL NOT be present.

ANNEX C XML Signature: Keyed-Hash Message Authentication Code Cryptographic Artefact
--

Implementations that use keyed-hash message authentication codes (Reference [7]) as the cryptographic mechanism for producing cryptographic artefacts are **REQUIRED** to be conformant with ANNEX A and this Annex.

SignedInfo

This section refers to XMLDSIG Section 4.4.

SignatureMethod

This section refers to XMLDSIG Section 4.4.2.

The `SignatureMethod` Algorithm attribute **MUST** conform to the specifications detailed in Table 2-5.

Algorithm Identifier	Mandatory/Optional/ Prohibited
http://www.w3.org/2000/09/xmlsig#hmac-sha1	Prohibited
http://www.w3.org/2001/04/xmlsig-more#hmac-sha224	Optional
http://www.w3.org/2001/04/xmlsig-more#hmac-sha256	Mandatory
http://www.w3.org/2001/04/xmlsig-more#hmac-sha384	Optional
http://www.w3.org/2001/04/xmlsig-more#hmac-sha512	Optional
http://www.w3.org/2001/04/xmlsig-more#hmac-ripemd160	Optional

Table 2-5 SignatureMethod (HMAC) Algorithm Identifiers

In the case whereby the `HMACOutputLength` is used for HMAC algorithms the errata to XMLDSIG (Reference [11]) **MUST** be followed.

KeyInfo

This section refers to XMLDSIG Section 4.5.

The `KeyInfo` element is **REQUIRED**.

KeyName

This section refers to XMLDSIG Section 4.5.1.

The `KeyName` element **MAY** be present.

KeyValue

This section refers to XMLDSIG Section 4.5.2.

The `KeyValue` SHALL NOT be present.

RetrievalMethod

This section refers to XMLDSIG Section 4.5.3.

The `RetrievalMethod` SHALL NOT be present.

X509Data

This section refers to XMLDSIG Section 4.5.4.

The `X509Data` SHALL NOT be present.

PGPData

This section refers to XMLDSIG Section 4.5.5.

The `PGPData` element SHALL NOT be present.

SPKIData

This section refers to XMLDSIG Section 4.5.6.

The `SPKIData` element SHALL NOT be present.

MgmtData

This section refers to XMLDSIG Section 4.5.7.

The `MgmtData` element SHALL NOT be present.

ANNEX D Example XML Signature Cryptographic Bindings

This Annex contains fictitious examples that illustrate cryptographic Binding Data Objects (BDOs) that contain cryptographic artefacts conformant with this appendix. All examples given in this appendix use Confidentiality Metadata Labels (Reference [1]) as example metadata.

The examples are provided as self-explanatory representations of BDOs.

```

<mb:BindingInformation xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
  <Signature Id="id-a99fac99-513d-4b08-8158-ef862e4d9f80"
xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#hmac-sha256" />
      <Reference URI="#id-66bb29e1-9696-4ea0-be3c-f7d0096a0d81">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      </Reference>
      <Reference URI="#id-d55d0123-babc-467f-b309-62e95291a9e4">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      </Reference>
      <Reference URI="#id-b3eaf318-700f-4740-b43e-2def8d98db81">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      </Reference>
      <Reference URI="#id-b3eaf318-700f-4740-b43e-2def8d98db81">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      </Reference>
      <Reference URI="#id-b3eaf318-700f-4740-b43e-2def8d98db81">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      </Reference>
    </SignedInfo>
    <SignatureValue>g3nzbBiu7msmVHfCjmVqqSiimlASoBSM/hxqFN7YxH0=</SignatureValue>
    <KeyInfo Id="id-b3eaf318-700f-4740-b43e-2def8d98db81">
      <KeyName>HMAC_SECRET_KEY</KeyName>
    </KeyInfo>
  </Signature>
</mb:BindingInformation>

```

```

</KeyInfo>
<Object Id="id-17250b2d-f0f5-4457-9e21-23db31e3460d">
  <SignatureProperties Id="id-d55d0123-babc-467f-b309-62e95291a9e4">
    <SignatureProperty>
      <wsu:TimeStamp xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <wsu:Created>2015-11-13T15:58:44Z</wsu:Created>
      </wsu:TimeStamp>
    </SignatureProperty>
  </SignatureProperties>
</Object>
</Signature>
<mb:MetadataBindingContainer>
  <mb:MetadataBinding mb:Id="#id-66bb29e1-9696-4ea0-be3c-f7d0096a0d81">
    <mb:Metadata>
      <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
        <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
          <slab:Classification>GENERAL</slab:Classification>
        </slab:ConfidentialityInformation>
        <slab:CreationDateTime>
          2015-09-30T12:30:00Z
        </slab:CreationDateTime>
      </slab:originatorConfidentialityLabel>
    </mb:Metadata>
    <mb:Data>
      <Document xmlns="">
        <Title>BDO Examples</Title>
        <Author>alan.ross@reach.nato.int</Author>
        <Abstract>
          Example XML File to support illustration of different types of BDO
and cryptographic artefacts
        </Abstract>
        <Introduction>...</Introduction>
        <Chapter Id="chapter-1">
          <Paragraph Id="para-1-1" />
          <Paragraph Id="para-1-2" />
        </Chapter>
        <Chapter Id="chapter-2">
          <Paragraph Id="para-2-1" />
          <Paragraph Id="para-2-2" />
        </Chapter>
      </Document>
    </mb:Data>
  </mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>

```

Figure 2-2 Encapsulating Cryptographic BDO Containing an Enveloped Signature with a Keyed-Hash Message Authentication Code Cryptographic Artefact


```

<mb:BindingInformation xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
  <Signature Id="id-fb00da79-4b32-4fcc-a302-4dbf789212e3"
xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
      <Reference URI="#id-20c07ca8-6960-4a36-bdd1-e3cb299f82c3">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<DigestValue>fAXcjRa4z1LyB+lchyBK/9Jz1soZSbxNCmr/27nA9aI=</DigestValue>
      </Reference>
      <Reference URI="#id-82744679-a547-40aa-a683-cf97619054fe">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<DigestValue>j5AgAamc6cv54VDz10kDlQ4wYZLLAU3761eFOUWvtX0=</DigestValue>
      </Reference>
      <Reference URI="#id-9920a48c-c3a1-45d0-a81c-1ce04d1d8de6">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<DigestValue>hWUoi0gFxnFsGnHJO/V2eNg/silda814PSP2/WlsqtU=</DigestValue>
      </Reference>
    </SignedInfo>

    <SignatureValue>gItAuwdeYkw5xDht50T0ei1xfT0q7KLaUXm4w/2rnpTjoxi0DTI3Wr8D4fmx/
404bVrX23StY6HHT/dxDPcg0Da+K9YL/p13y8RvIrfWghizReY5AUj1EF3mxI22ari/ao0shKe18a
PJ0J2RmGH3t30qrHfvUXcIcREIOT1S6GajpNCOJJPYoa9yb400M0x0oRHXkFegnQ5eXeSBih2u4Dhw
L0I4GSeuYA9Fvt8qyv1a9EnTTS6fG2+gLjd6YEQzfIBvVtrY5b9WnhqqiHy5tyepZgVtMSEXrukWr
NELpvwC467KR+MincgUA9RlsAEvCBaR4oQKTU0xBQ5tD+N/FzQ==</SignatureValue>
      <KeyInfo Id="id-9920a48c-c3a1-45d0-a81c-1ce04d1d8de6">
        <X509Data>

<X509Certificate>MIIDM.....wIBAgIJAI29/+A/MN7RPax5eOKQg==</X509Certificate>
      </X509Data>
      </KeyInfo>
      <Object Id="id-63fc02c0-10b6-49fd-9759-7bfb1d52ecf7">
        <SignatureProperties Id="id-82744679-a547-40aa-a683-cf97619054fe">
          <SignatureProperty>
            <wsu:TimeStamp xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
              <wsu:Created>2015-11-13T16:01:38Z</wsu:Created>
            </wsu:TimeStamp>
          </SignatureProperty>

```

```

    </SignatureProperties>
  </Object>
</Signature>
<mb:MetadataBindingContainer>
  <mb:MetadataBinding mb:Id="#id-20c07ca8-6960-4a36-bdd1-e3cb299f82c3">
    <mb:Metadata>
      <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
        <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
          <slab:Classification>GENERAL</slab:Classification>
        </slab:ConfidentialityInformation>
        <slab:CreationDateTime>
          2015-09-30T12:30:00Z
        </slab:CreationDateTime>
      </slab:originatorConfidentialityLabel>
    </mb:Metadata>
    <mb>Data>
      <Document xmlns="">
        <Title>BDO Examples</Title>
        <Author>alan.ross@reach.nato.int</Author>
        <Abstract>
          Example XML File to support illustration of different types of BDO
and cryptographic artefacts
        </Abstract>
        <Introduction>...</Introduction>
        <Chapter Id="chapter-1">
          <Paragraph Id="para-1-1" />
          <Paragraph Id="para-1-2" />
        </Chapter>
        <Chapter Id="chapter-2">
          <Paragraph Id="para-2-1" />
          <Paragraph Id="para-2-2" />
        </Chapter>
      </Document>
    </mb>Data>
  </mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>

```

Figure 2-3 Encapsulating Cryptographic BDO Containing an Enveloped Signature with a Digital Signature Cryptographic Artefact

```

<Document xmlns="http://example.com/doc">
  <Title>BDO Examples</Title>
  <Author>alan.ross@reach.nato.int</Author>
  <Abstract>
    Example XML File to support illustration of different types of BDO and
cryptographic artefacts
  </Abstract>
  <Introduction>...</Introduction>
  <Chapter Id="chapter-1">
    <Paragraph Id="para-1-1" />
  </Chapter>

```

```

    <Paragraph Id="para-1-2" />
  </Chapter>
  <Chapter Id="chapter-2">
    <Paragraph Id="para-2-1" />
    <Paragraph Id="para-2-2" />
  </Chapter>
  <mb:BindingInformation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
  <Signature Id="id-134ce280-1682-4963-b868-6621b480ce26"
xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#hmac-sha256" />
    <Reference URI="">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116">
          <XPath>not(ancestor-or-self::*[local-name() =
'BindingInformation' and namespace-uri() =
'http://www.nato.int/2014/06/n1/mb'])</XPath>
        </Transform>
      </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<DigestValue>RYxJZ8BN/MR2D0BDxiCxGSDaQvGFKQ86udb00v5A2s4=</DigestValue>
  </Reference>
  <Reference URI="#id-c9e4f1c8-ad34-4d4d-9909-827570de41a2">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<DigestValue>WKOwdda84YLuSqbaZsS8LQ6kqF6HR0dfC+iz/e+KPf0=</DigestValue>
  </Reference>
  <Reference URI="#id-1bd95780-277f-44b3-99fd-b2b69505ae5a">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<DigestValue>UbMTebL9lKFARnG1qWOpQ1DiuCFPzs6W1hse9gPOxUk=</DigestValue>
  </Reference>
  <Reference URI="#id-001c1a07-74c4-4815-aecd-dd1bcba8bc9c">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

```

```

<DigestValue>z7+6QZiSTqYMHCIy9o3uxGfA8q5ScEeH1HZs3w9+8S4=</DigestValue>
  </Reference>
</SignedInfo>

<SignatureValue>dk7Ds4Atik6yF/wKZj0IDVGGyv1rigTDLj6gRsQCTHY=</SignatureValue>
  <KeyInfo Id="id-001c1a07-74c4-4815-aecd-dd1bcba8bc9c">
    <KeyName>HMAC_SECRET_KEY</KeyName>
  </KeyInfo>
  <Object Id="id-4dcc6c48-6ed0-4cf0-b386-b85f7ee0c826">
    <SignatureProperties Id="id-1bd95780-277f-44b3-99fd-b2b69505ae5a">
      <SignatureProperty>
        <wsu:TimeStamp xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
          <wsu:Created>2015-11-13T16:07:37Z</wsu:Created>
        </wsu:TimeStamp>
      </SignatureProperty>
    </SignatureProperties>
  </Object>
</Signature>
<mb:MetadataBindingContainer>
  <mb:MetadataBinding mb:Id="#id-c9e4f1c8-ad34-4d4d-9909-827570de41a2">
    <mb:Metadata>
      <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
        <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
          <slab:Classification>GENERAL</slab:Classification>
        </slab:ConfidentialityInformation>
        <slab:CreationDateTime>
          2015-09-30T12:30:00Z
        </slab:CreationDateTime>
      </slab:originatorConfidentialityLabel>
      <slab:alternateConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
        <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
          <slab:Classification>GENERAL</slab:Classification>
        </slab:ConfidentialityInformation>
        <slab:CreationDateTime>
          2015-09-30T12:30:00Z
        </slab:CreationDateTime>
      </slab:alternateConfidentialityLabel>
    </mb:Metadata>
    <mb:DataReference mb:URI="" />
  </mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>
</Document>

```

Figure 2-4 Embedded Cryptographic BDO Containing an Enveloped Signature with a Keyed-Hash Message Authentication Code Cryptographic Artefact

```

<Document xmlns="http://example.com/doc">
  <Title>BDO Examples</Title>
  <Author>alan.ross@reach.nato.int</Author>
  <Abstract>
    Example XML File to support illustration of different types of BDO and
    cryptographic artefacts
  </Abstract>
  <Introduction>...</Introduction>
  <Chapter Id="chapter-1">
    <Paragraph Id="para-1-1" />
    <Paragraph Id="para-1-2" />
  </Chapter>
  <Chapter Id="chapter-2">
    <Paragraph Id="para-2-1" />
    <Paragraph Id="para-2-2" />
  </Chapter>
  <mb:BindingInformation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
  <Signature Id="id-3a7079e1-adeb-47b0-a4df-86a5f2962f57"
xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
      <Reference URI="#para-2-2">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<DigestValue>0JsT5SNKuCYoe91tl8n590Hcy/UivrId3Zf6kJy7pdg=</DigestValue>
      </Reference>
      <Reference URI="#id-b073db91-a8b3-4905-809d-82e92b0d0ecc">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<DigestValue>a3yUgG8j0eIPI6ZSw7aw4JPH01SBglS0+Fb7lwVmMeo=</DigestValue>
      </Reference>
      <Reference URI="#id-7d5d0648-59c1-48a9-a3bc-a07a24f0a67b">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<DigestValue>zMHgHTwG+0tqPY8+T4cwYGby2UoSv71QJ2eU0peB5ds=</DigestValue>
      </Reference>
      <Reference URI="#id-45f67abd-5803-4933-acb8-5061adde54f4">
        <Transforms>

```

```

        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<DigestValue>g8jESHigXr4bGZFwOzh204r8Vv0y6jfH7qKgQTGV9ww=</DigestValue>
    </Reference>
    </SignedInfo>

<SignatureValue>C1yPwzpU/ng042sXo2HHZTtbXNTE2FAXf2RivMy5u6z/xoNlmi/mHm5ejZPFW
koGaUmWDadREcc51I6XBYXeks2YVyMh05uDRCLPYNkIAx3BpUFH7y9Juk1j4Wv1DBeZ2GwNhp463
QMvn8pF35cXw1f86Vc0M3CtAm5MNbnS6BqqswdygCF/HivjHcQSnYGRhI4vegelwfYyhFRHQ10E3
ytUDR8VLKZfgyK3M6mcQjv1HtL2qjRxMhrkQQtt8oBQk6iAwYgbqeIzqw3cIYL5jb/ML2U0ycGgw
UIqGFx95EouKuOMZSN8e2dnaVaHp26X1zpdJkyTkVr5/T7v3hA==</SignatureValue>
    <KeyInfo Id="id-45f67abd-5803-4933-acb8-5061adde54f4">
        <X509Data>
            <X509Certificate>
MIIDM.....wIBAgIJAI29/+A/MN7RPax5eOKQg==</X509Certificate>
            </X509Data>
        </KeyInfo>
        <Object Id="id-221fefa8-fd81-4f98-8784-ac4a08e4eece">
            <SignatureProperties Id="id-7d5d0648-59c1-48a9-a3bc-a07a24f0a67b">
                <SignatureProperty>
                    <wsu:TimeStamp xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
                        <wsu:Created>2015-11-13T16:04:59Z</wsu:Created>
                    </wsu:TimeStamp>
                </SignatureProperty>
            </SignatureProperties>
        </Object>
    </Signature>
    <mb:MetadataBindingContainer>
        <mb:MetadataBinding mb:Id="#id-b073db91-a8b3-4905-809d-82e92b0d0ecc">
            <mb:Metadata>
                <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                    <slab:ConfidentialityInformation>
                        <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                        <slab:Classification>GENERAL</slab:Classification>
                    </slab:ConfidentialityInformation>
                    <slab:CreationDateTime>
                        2015-09-30T12:30:00Z
                    </slab:CreationDateTime>
                </slab:originatorConfidentialityLabel>
            </mb:Metadata>
            <mb:DataReference URI="" />
        </mb:MetadataBinding>
        <mb:MetadataBinding>
            <mb:Metadata>
                <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                    <slab:ConfidentialityInformation>
                        <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                        <slab:Classification>GENERAL</slab:Classification>
                    </slab:ConfidentialityInformation>

```

```
    <slab:CreationDateTime>
      2015-09-30T12:30:00Z
    </slab:CreationDateTime>
  </slab:originatorConfidentialityLabel>
</mb:Metadata>
  <mb:DataReference mb:URI="#para-2-1" />
</mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>
</Document>
```

Figure 2-5 : Embedded Cryptographic BDO Containing a Detached Signature with a Digital Signature Cryptographic Artefact

ANNEX E Generic CMS Cryptographic Artefact Profile
--

E.1. Introduction

The S/MIME protocol Cryptographic Message Syntax (CMS) (Reference [18]) leaves the implementers with a number of options that need to be agreed on in order to achieve interoperability. This Annex is a profile for the use of the CMS to facilitate the cryptographic protection of the integrity and authentication of a metadata binding, and describes which of the different elements of service that need to be present on origination and reception, in order to claim conformance to this profile.

In order to highlight the differences and avoid duplication of text from CMS, a delta specification approach has been taken. This Annex will refer to the relevant sections of CMS and will identify any necessary clarifications and/or amendments to these sections. This approach provides traceability and puts the delta text in context. It is required that this Annex is read together with CMS.

Additional CMS elements of service may be required to support security services, such as message authentication, confidentiality, integrity and non-repudiation. This Annex does not profile the additional security services. Unless exceptions are noted, all statements that apply to CMS and additional security services profiles (that are required to be supported) also apply to this profile.

The notational conventions used for this Annex are as follows:

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from STANAG 4778 (Reference [2]) referenced in this profile.
- `Courier font` indicates syntax derived from the CMS and S/MIME Specifications (References [8], [16], [18], [19] and [20]) referenced in this profile.

E.2. General Requirements

Unless otherwise stated, all statements that apply to Cryptographic Message Syntax (CMS, Reference [3]) also apply to this profile.

All of the mandatory elements of service (NOT explicitly marked as OPTIONAL), SHALL be supported by implementations which claim conformance to this profile. All of the elements of service that are mandatory to be generated on origination are also mandatory to be processed on reception.

An entity that creates CMS metadata bindings conformant with this profile (known as Originator) is REQUIRED to perform the rules for Message Digest Calculation Process and Signature Generation Process as specified in CMS Section 5.4 and 5.5. An entity that interprets and processes CMS metadata bindings conformant with this profile (known as Recipient) is REQUIRED to perform the rules for Message Digest Calculation Process and Signature Verification Process as specified in CMS Section 5.4 and 5.6.

E.3. CMS Profile

This section refers to section 5 in CMS.

General Syntax

`ContentInfo` SHALL be supported to encapsulate the `SignedData` in accordance with CMS. Conventions for inner wrappers SHALL comply with either Secure/Multipurpose Internet Mail Extensions (S/MIME, Reference [8]) depending on the type of content conveyed.

The `contentType` field SHALL be supported.

The `content` field SHALL be supported.

Data Content Type

This section refers to section 4 in CMS.

Conventions for inner wrappers SHALL comply with S/MIME depending on the type of content conveyed.

Signed-data Content Type

This section refers to section 5 in CMS.

Conventions for inner wrappers SHALL comply with S/MIME depending on the type of content conveyed.

SignedData Type

This section refers to section 5.1 in CMS.

In strategic systems with high throughput, the certificates field SHALL be included. X.509 version 3 certificates SHALL be supported.

The certificate profile specified in Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Reference [16]) SHALL be supported.

The Originator SHOULD include at least one chain of certificates up to, but not including, a Certificate Authority (CA) that it believes that the Recipient may trust as authoritative.

The Recipient SHOULD be able to handle an arbitrarily large number of certificates and chains.

There may be circumstances when the certificates SHOULD NOT be included, e.g. in tactical systems with low bandwidth.

The crls field is NOT REQUIRED.

The CRL profile specified in Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Reference [16]) SHALL be supported.

The digestAlgorithms field SHALL contain DigestAlgorithmIdentifiers that conform to the specifications detailed in Table 2-6.

Algorithm Identifier	Mandatory/Optional/ Prohibited
id-sha224 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 4 }	Prohibited
id-sha256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }	Mandatory
id-sha384 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 }	Optional
id-sha512 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }	Optional
id-shake256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 2 12 }	Optional

Table 2-6: CMS Message Digest Algorithms

The use of the mandatory and optional DigestAlgorithmIdentifiers specified in this profile MAY be further specified dependent upon national or organizational policy and agreed between implementation communities.

EncapsulatedContentInfo Type

This section refers to section 5.2 in CMS.

The `eContentType` field SHALL be supported.

The `eContentType` SHALL be set to the object identifier of the object to be signed: `id-data`.

The use of the `eContent` field SHALL be supported depending upon the signed-only format as specified in S/MIME.

SignerInfo Type

This section refers to section 5.3 in CMS.

Originators and the Recipients SHOULD be able to handle multiple instances of `SignerInfo`.

The `SignerIdentifier issuerAndSerialNumber` field SHALL be supported.

The `SignerIdentifier subjectKeyIdentifier` field SHALL be supported.

The `digestAlgorithm` SHALL be supported as specified in Table 2-6.

The `digestAlgorithm` SHALL be among those listed in the `digestAlgorithms` field of the associated `SignedData`.

The `signatureAlgorithm` field SHALL conform to the specifications detailed in Table 2-7.

Algorithm Identifier	Mandatory/Optional/ Prohibited
<code>id-dsa-with-sha224 OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) id-dsa-with-sha2(3) 1 }</code>	Optional
<code>id-dsa-with-sha256 OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) id-dsa-with-sha2(3) 2 }</code>	Mandatory
<code>sha224WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 14 }</code>	Optional
<code>sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }</code>	Mandatory
<code>sha384WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }</code>	Optional
<code>sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1)</code>	Optional

member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }	
ecdsa-with-SHA224 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }	Optional
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }	Optional
ecdsa-with-SHA384 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }	Optional
ecdsa-with-SHA512 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }	Optional
id-RSASSA-PSS-SHAKE256 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) 31 }	Optional
id-ecdsa-with-shake256 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) 33 }	Optional

Table 2-7: CMS Signature Algorithms

The use of the mandatory and optional `signatureAlgorithm` specified in this profile MAY be further specified dependent upon national or organizational policy and agreed between implementation communities.

The `signedAttrs` field SHALL be supported (see Section **Signed Attributes**).

Signed Attributes

The `SignerInfo` type allows unsigned and signed attributes to be included along with a signature.

A Recipient is REQUIRED to support all signed attributes on reception for the purpose of validating the signature value.

Requirements for processing of the attributes specified in this profile SHALL be adhered to.

No processing of the internal structure or semantics of any other attribute (not specified in this profile), or any of its sub-elements is required unless a specific claim of conformance is made to support the attribute type.

Additional attributes and values for these attributes may be defined in the future. A Recipient SHOULD handle attributes or values that it does not recognise in a graceful manner.

The `contentType` attribute SHALL be supported, as specified in CMS. Its value specifies the content type of the `contentInfo` being signed.

The `messageDigest` attribute SHALL be supported, as specified in CMS. The hash value received in this attribute SHALL NOT be used for signature validation (i.e. it SHALL be recalculated).

The `signingTime` attribute SHALL be supported.

The `eSSSecurityLabel` attribute, specified in Enhanced Security Services for S/MIME (ESS, Reference [20]), SHALL NOT be supported.

The `equivalentLabels` attribute, specified in ESS SHALL NOT be supported.

The `bindingData` attribute, specified in this profile, SHALL be supported (see Section Binding Information below).

E.4. Binding Information

The `bindingData` attribute type specifies the information required from the Binding Data Object that is required to be cryptographically protected.

The `bindingData` attribute type SHALL be present in `signed-data`.

The `bindingData` attribute SHALL be a signed attribute; it SHALL NOT be an unsigned attribute.

The following object identifier identifies the `bindingData` attribute:

```
id-bindingData OBJECT IDENTIFIER ::= { iso(1)
    identified-organization(3) nato(26) stanags(0)
    Generic Binding Mechanism(4778) infosec(1) 1 }
```

`bindingData` attribute values have ASN.1 type `BindingData`:

```
BindingData ::= SET {
    bindingType BindingType,
    bindingId BindingIdentifier,
    bindingDataInfos BindingDataInfos }
```

```
BindingType ::= UTF8String
```

```
-- The value from the Binding-Data header field binding-type parameter.
```

BindingIdentifier ::= UTF8String
 -- The identifier value from the *BindingInformation SignatureReference @URI* attribute.

BindingDataInfos ::= SEQUENCE SIZE (1..MAX) OF BindingDataInfo

BindingDataInfo ::= SEQUENCE {
 -- Per-*MetadataBinding* information is represented in this type.
 mbId MetadataBindingIdentifier,
 algId DigestAlgorithmIdentifier,
 -- Import DigestAlgorithmIdentifier from Reference [18]
 -- algId identifies the digest algorithm, and any associated parameters, under which the *MetadataBinding* is digested. The algId SHALL match the digest algorithm for the *SignerInfo* in which this bindingData attribute value is placed.
 metadataBindingDigest MetadataBindingDigest }

MetadataBindingIdentifier ::= UTF8String
 -- The value from the *@Id* attribute of the *MetadataBinding*.

MetadataBindingDigest ::= OCTET STRING
 -- The result of digesting the *MetadataBinding* associated with the *MetadataBindingIdentifier*.

UTF8String ::= [UNIVERSAL 12] IMPLICIT OCTET STRING
 -- The content of this type conforms to Reference [21].

A *bindingData* attribute SHALL have a single attribute value, even though the syntax is defined as a SET OF *AttributeValue*. There SHALL NOT be zero or multiple instances of *AttributeValue* present.

The *SignedAttributes* syntax is defined as a SET OF *Attributes*. The *SignedAttributes* in a *signerInfo* SHALL include only one instance of the *bindingData* attribute.

Generate bindingData

For each *MetadataBinding* element included in the *bindingInformation* element there SHALL be a *URI* attribute with a shortname *XPointer* as the attribute value that identifies each *MetadataBinding* element.

The *bindingType* SHALL be *urn:nato:stanag:4778:bindinginformation:1:0*.

The *bindingId* SHALL be the identifier of the *@URI* attribute value of the *SignatureReference* element contained in the BDO.

For each *MetadataBinding* element from the *bindingInformation*:

- 1) Create a BindingDataInfo;
- 2) Record the *@Id* attribute value in the MetadataBindingIdentifier;
- 3) Record the *SignerInfo* digestAlgorithm in the algId.
- 4) Normalise the *MetadataBinding* element conformant with the XML Normalization process specified in Annex A of this document;
- 5) The output from the normalised *MetadataBinding* element SHALL be passed into the digest calculation along with the algId digest algorithm, and any associated parameters; and,
- 6) Record the result of the digest calculation in the metadataBindingDigest.

Figure 2-6 bellows illustrates the relationship between the *bindingInformation* and the *BindingData* signed attribute.

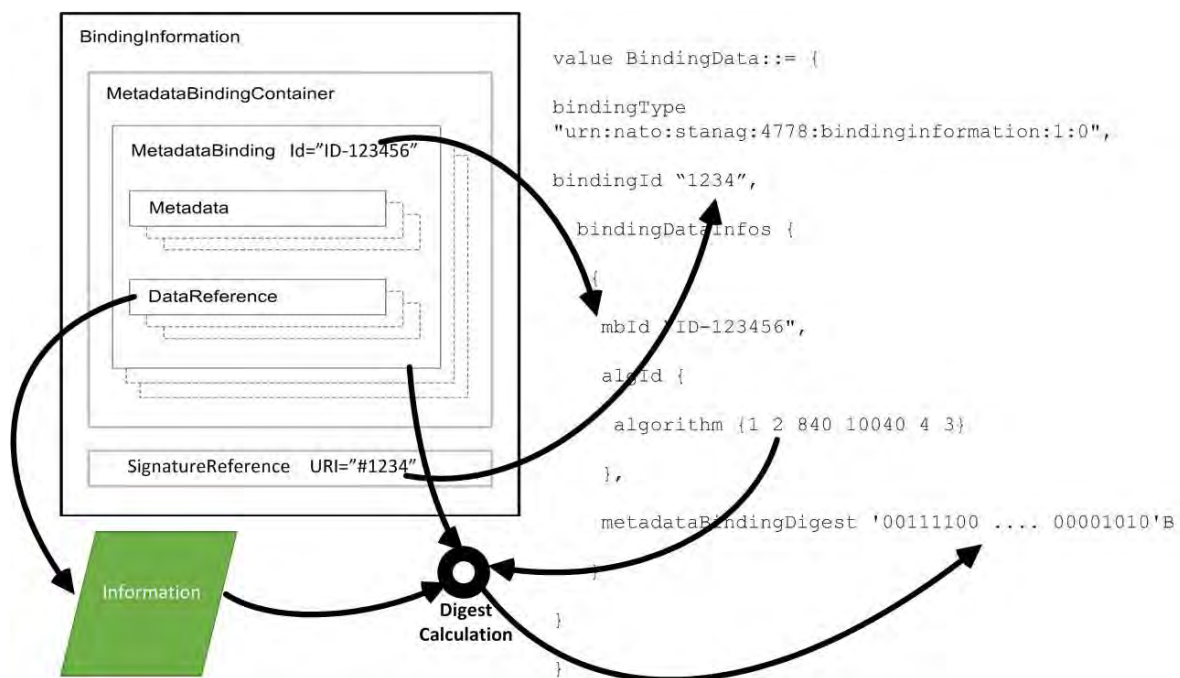


Figure 2-6: Relationship between the Binding Information and the BindingData signed attribute

Processing bindingData

The value from the *Binding-Data* header field *binding-type* parameter SHALL be compared with the value from the id-bindingData bindingType field.

The identifier value from the *@URI* attribute of the *SignatureReference* element SHALL be compared with the id-bindingData bindingId field.

If the *binding-type* parameter and *bindingType* field both match with *urn:nato:stanag:4778:bindinginformation:1:0* and the *bindingId* and *@URI* values match the following process for each *BindingDataInfo* SHALL be performed:

- 1) Locate the *MetadataBinding* element from the *bindingInformation* stored in the *Binding-Data* header field *binding-data-object* parameter that contains the *@id* attribute value in the *MetadataBindingIdentifier*;
- 2) Normalise the *MetadataBinding* element conformant with Annex A XML Normalization process specified in this profile.
- 3) The output from the normalised *MetadataBinding* element SHALL be passed into the digest calculation along with the *algId* digest algorithm, and any associated parameters; and,
- 4) Compare the result of the digest calculation with the *metadataBindingDigest*.

For each *MetadataBinding* element from the *bindingInformation* there SHALL be a matching *BindingDataInfo*.

E.5. Signature Generation

The *MetadataBinding DataReference @URI* attribute value SHALL be used to dereference the MIME entity that is to be prepared for signing dependent upon the signed-only format (specified in Section 3.5 of SMIME) required.

In addition to the CMS profile specified in this document, the following procedures SHALL be adhered to:

- The procedures for generating the *bindingData* signed attribute are specified in Section Generating *bindingData* above.
- The procedures for message digest calculation are specified in Section 5.4 of CMS.
- The procedures for signature generation are as specified in Section 5.5 of CMS.

E.6. Signature Verification

In addition to the CMS profile specified in this document, the following procedures SHALL be adhered to:

- The procedures for signature verification are as specified in Section 5.6 of CMS.
- For the cryptographic protection for the integrity of the binding to be valid the procedures for processing the *bindingData* signed attribute specified in Section Processing *bindingData* above SHALL be adhered to and the comparisons of digests SHALL match.

CHAPTER 3 Simple Mail Transfer Protocol Binding Profile
--

3.1. Introduction

This profile specifies the mechanism for binding metadata to MIME entities, such as internet mail messages. A MIME entity can be a sub-part, sub-parts of a message or the message with all its sub-parts. A MIME entity that is the message includes only the MIME message headers (Reference [6]) and MIME body (Reference [6]), and does not include the internet email headers (Reference [3]).

This profile supports binding metadata to a MIME entity that is a message including only the MIME message headers (Reference [6]) and MIME body (Reference [6]).

This profile does not support the capability for referencing internet email headers (or subsets thereof). A separate profile will specify how to bind metadata to internet email headers.

This profile does not support the capability for referencing a sub-part or sub-parts of a message. A separate profile will specify how to bind metadata to a sub-part or sub-parts of a message.

3.2. Identification

The profile for SMTP is uniquely identified by the Canonical Identifier shown in Table 3-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:smtp
Version Identifier	urn:nato:stanag:4778:profile:smtp:1:2

Table 3-1 Profile Identifiers

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base SMTP standards
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 3-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:smtp:1:1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

3.3. Standards (Reference)

Reference [1] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [2] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

Reference [3] IETF RFC 5322, "Internet Message Format", at <http://tools.ietf.org/html/rfc5322>, October 2008.

Reference [4] IETF RFC 7444, "Security Labels in Internet Email", K. Zeilenga and A. Melnikov, at <http://tools.ietf.org/html/rfc7444>, February 2015.

Reference [5] IETF RFC 2392, "Content-ID and Message-ID Uniform Resource Locators", at <http://tools.ietf.org/html/rfc2392>, August 1998.

Reference [6] IETF RFC 2045, "Multipurpose Internet Mail Extensions(MIME) Part One: Format of Internet Message Bodies", at <http://tools.ietf.org/html/rfc2045>, November 1996

Reference [7] IETF RFC 2231, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", at <http://tools.ietf.org/html/rfc2231>, November 1997.

Reference [8] IETF RFC 5751, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", at <http://tools.ietf.org/html/rfc5751>, January 2010

Reference [9] IETF RFC 5234, "Augmented BNF for Syntax Specifications: ABNF", at <http://tools.ietf.org/html/rfc5234>, January 2008

Reference [10] IETF RFC 822, "STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES", at <http://tools.ietf.org/html/rfc822>, August 1982

Reference [11] IETF RFC 3986, "Uniform Resource Identifier (URI): Generic Syntax", at <http://tools.ietf.org/html/rfc3986>, January 2005

Reference [12] IETF RFC 5646, "Tags for Identifying Languages", at <http://tools.ietf.org/html/rfc5646>, September 2009

3.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [2].
- `Courier font` indicates syntax derived from SIO -Label (Reference [4]), Message-ID ((Reference [5])) and Content-ID (Reference [5]) URI schemes and MIME Entities (Reference [6]).

3.5. Internet Email Structure

The BDO is a detached BDO that MUST contain at least one *MetadataBinding* that contains a null *DataReference URI* attribute value. By conforming to this profile to

syntactically and semantically interpret the *DataReference URI* attribute allows for the metadata to be bound to the entire message. For the purposes of this profile the entire message is a MIME Entity that consists of the MIME message headers and the MIME body as described at Reference [6].

The *DataReference xmime:contentType* attribute value is REQUIRED.

The *DataReference xmime:contentType* attribute value SHALL be `message/rfc822`.

This profile requires the use of a new header field that is based upon the protocol of the `SIO-Label` header field, as specified in (Reference [4]). The reason for a new header field is predicated upon the implied semantics of the `SIO-Label` header field for conveying the confidentiality of an electronic mail message as a whole (Reference [3]). This profile implies that any type of metadata (including confidentiality metadata) can be bound to any MIME entity.

The new header field name SHALL be "Binding-Data", and its content consists of a set of key/value pairs.

Each key/value pair SHALL be referred to as a parameter.

Implementations conformant with this profile SHALL comply with the following formal header field syntax:

```
binding-data = "Binding-Data:" [FWS] binding-data-param-seq [FWS] CRLF
binding-data-param-seq = binding-data-param
                        [ [FWS] ";" [FWS] binding-data-param-seq ]
binding-data-param = parameter
```

Parameter production SHALL conform to Reference [7].

As specified in Reference [7] parameter production permits white space immediately before and after the "=".

FWS production SHALL conform to Reference [3].

CRLF production SHALL conform to Reference [9].

The Binding-Data header field SHALL be used to embed the BDO within the internet mail message.

The BDO SHALL be included in the Binding-Data header field "binding-data-object" parameter.

The Binding-Data “binding-data-object” parameter value SHALL be a quoted string that contains the base64 encoding of the BDO.

The Binding-Data “binding-data-object” parameter value SHALL always be present. It is noted that the Binding-Data “binding-data-object” parameter SHALL conform to Reference [7] specifically in relation to parameter value continuation.

Depending upon the line length limit (recommended to be 78 characters or less and not more than 998 characters – see Reference [3]) the Binding-Data “binding-data-object” parameter SHALL be split into multiple Binding-Data “binding-data-object” parameters, as illustrated below¹.

```
binding-data-object*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
binding-data-object*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
binding-data-object*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
binding-data-object*2="ZGVudG1maWVyIFVSS0idXJu0m9pZDoxLjEiLz";
binding-data-object*4="YXRpb24+PC9TZWNMYWJlbD4=";
```

It is noted that Binding-Data “binding-data-object” parameter value production implicitly allows for white space as Reference [7] relies on the Augmented Backus–Naur form (ABNF) as specified in Reference [10]. However, implementations SHALL be able to process Binding-Data “binding-data-object” parameter values that contain white space as illustrated below:

```
binding-data-object*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbXBsZS5jb20vc2VjLW
xhYmVsLzAiPjxQb2xpY3lJ";
binding-data-object*1="ZGVudG1maWVyIFVSS0idXJu0m9pZDoxLjEiLz48Q2xhc3NpZmlj
YXRpb24+MzwvQ2xhc3NpZmlj";
binding-data-object*2="YXRpb24+PC9TZWNMYWJlbD4=";
```

It is also noted that Reference [7] allows for quoted-string values (for parameter production). As such, implementations SHALL be able to process Binding-Data “binding-data-object” parameter values that contain quoted-string values.

The Binding-Data “binding-type” parameter SHALL be a quoted string.

The Binding-Data “binding-type” parameter value SHALL be a Uniform Resource Identifier (URI, Reference [11]) that denotes the type, syntax and semantics for the binding mechanism represented by the Binding-Data “binding-data-object” parameter.

The Binding-Data “binding-type” SHALL always be present.

Implementations conformant with this profile SHALL contain a Binding-Data “binding-type” parameter with the value urn:nato:stanag:4778:bindinginformation:1:0.

¹ Note, as specified in Reference [7], the ordering of parameters can not be relied upon, therefore, the original parameter value is recovered by concatenating the multiple parameters, in order as specified in Reference [7].

Not all consumers may be metadata-aware and as such are not capable of processing the Binding-Data-Object “binding-data” parameter for the purposes of rendering a human-readable representation of the metadata bound to the MIME entity(or entities). To support consumers that are not metadata-aware the Binding-Data “marking” parameter MAY be used.

The Binding-Data “marking” parameter is a string that represents the human-readable representation of the metadata that is bound to the MIME entity (or entities) in the language indicated by the language field within the parameter value (if present, default language assumed if not present).

The Binding-Data “marking” parameter language field, if present, MUST have a value set to a language identifier specified in Tags for Identifying Languages (Reference [12]).

In the case a Binding-Data “marking” parameter is present with no language field within the parameter value, a default value of “en” SHALL be assumed to identify the language of the Binding-Data “marking” parameter.

Additional specifications for the production and semantics intended for the use of the Binding-Data “marking” MAY be provided in accompanying organizational, national or Community-Of-Interest implementation guidance documents.

An example of an Embedded BDO contained in the Binding-Data header field of an internet mail message that illustrates the binding of Confidentiality Metadata Labels (Reference [1]) as example metadata to the message is provided in Figure 3-1.

From: alan.ross@smhs.co.uk
 To: alan.ross@reach.nato.int
 Binding-Data: binding-type="urn:nato:stanag:4778:bindinginformation:1:0";
 binding-data-object=<base64 BDO>
 Message-Id: <unique-msg-id@smhs.co.uk>

This is a simple informal message



```
<mb:BindingInformation
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xmime="http://www.w3.org/2005/05/xmlmime">
  <mb:MetadataBindingContainer>
    <mb:MetadataBinding>
      <mb:Metadata>
        <slab:originatorConfidentialityLabel
          xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
            <slab:Classification>GENERAL</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>
            2015-09-30T12:30:00Z
          </slab:CreationDateTime>
        </slab:originatorConfidentialityLabel>
      </mb:Metadata>
      <mb:DataReference
        URI=""
        xmime:contentType="message/rfc822"/>
      </mb:MetadataBinding>
    </mb:MetadataBindingContainer>
  </mb:BindingInformation>
```

Figure 3-1 Example of Binding Confidentiality Metadata Label to Email

3.6. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annex E CMS Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts CMS Binding Profile (Chapter 2 Annex E) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the Originator generate S/MIME multipart/signed format.

The Recipient SHALL support both the S/MIME multipart/signed and application/pkcs7-mime formats.

In addition to the Signature Generation Section of the CMS Binding Profile the following requirements SHALL be adhered to:

- The binding information SHALL contain a new signature reference element, SignatureReference as specified in Section 4 of this profile that is a child element of the binding information.
- The URI attribute of the SignatureReference element SHALL contain a fragment identifier (indicated by the presence of a “#” character and a substring to the right of the “#” in the URI) used to uniquely identify the S/MIME entity (as specified in the CMS Binding Profile).
- The MIME Content-Type header field value, that indicates the S/MIME entity, MAY be used as the SignatureReference xmime:contentType attribute value.

3.7. SignatureReference Schema

```

<?xml version='1.0' encoding='UTF-8'?>
<!--
*****
NATO UNCLASSIFIED
XML Schema To support dereferencing Cryptographic Artefacts.
I
/ \
-< + >-
\ /
I NCI AGENCY
## # ### # P.O. box 174
## # # # 2501 CD The Hague
# # # # #
# # # # # Core Enterprise Services
# ## ##### #
A G E N C Y
*****
-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="urn:nato:stanag:4778:profile:cryptoartefact:1:0"
  xmlns:xml="http://www.w3.org/XML/1998/namespace" xmlns="urn:nato:stanag:4778:profile:cryptoartefact:1:0"
  xmlns:xmime="http://www.w3.org/2005/05/xmime"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0" xml:lang="en">

  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>urn:nato:stanag:4778:profile:cryptoartefact:1:0</UniqueIdentifier>
      <Name>Dereference Cryptographic Artefact Schema</Name>
      <Definition>Schema To support dereferencing Cryptographic Artefacts</Definition>
      <VersionIndicator>1.0</VersionIndicator>
      <UsageGuidance>Used within NATO to Schema To support dereferencing Cryptographic Artefacts</UsageGuidance>
      <RestrictionType/>
      <RestrictionValue/>
    </xs:appinfo>
    <xs:documentation>
      The schema can be used to support dereferencing Cryptographic Artefacts.
    </xs:documentation>
  </xs:annotation>

  <xs:element name="SignatureReference">
    <xs:complexType>
      <xs:attribute name="URI" type="xs:anyURI" use="required"/>
      <xs:attribute ref="xmime:contentType"/>
      <xs:anyAttribute processContents="lax"/>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

Figure 3-2 SignatureReference Schema

CHAPTER 4 Extensible Message And Presence Protocol Binding Profile

4.1. Introduction

Confidentiality metadata labels can be supported in XMPP stanzas as indicated by XEP-0258 (Reference [4]) whereby a mechanism for carrying Enhanced Security Services (ESS) Security labels (Reference [1]) is standardized. This profile is based upon the XEP-0258 (Reference [4]) specification to support carrying any type of metadata (including confidentiality metadata) contained in Embedded or Detached BDO for Message stanzas. As such, this profile supports the XMPP use cases for one-to-one instant messaging, multi-user chat and publish-subscribe notifications.

While XMPP-Core (Reference [7]) offers flexible extensibility for Message and Presence stanzas it is not the case for IQ stanzas. This profile specifies support for carrying a Detached BDO for IQ stanzas that contain item elements, such as XEP-0060 Publish-Subscribe (Reference [5]).

This profile does not support labelling Presence Stanzas.

4.2. Identification

The profile for XMPP is uniquely identified by the Canonical Identifier shown in Table 4-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:xmpp
Version Identifier	urn:nato:stanag:4778:profile:xmpp:1:3

Table 4-1 Profile Identifiers

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base XMPP standard
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 4-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:xmpp:1:2.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

4.3. Standards (Reference)

Reference [1] IETF RFC 2634, “Enhanced Security Services for S/MIME”, at <http://tools.ietf.org/html/rfc2634>, June 1999.

Reference [2] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [3] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

Reference [4] XEP-0258, “Security Labels in XMPP”, version 1.1, at <http://www.xmpp.org/extensions/xep-0258.html>, April 2013

Reference [5] XEP-0060, “Publish-Subscribe”, version 1.3, at <http://www.xmpp.org/extensions/xep-0060.html>, July 2010

Reference [6] IETF RFC 6122, “Extensible Messaging and Presence Protocol (XMPP): Address Format”, at <http://tools.ietf.org/html/rfc6122>, March 2011

Reference [7] IETF RFC 6120, “Extensible Messaging and Presence Protocol (XMPP): Core”, at <http://tools.ietf.org/html/rfc6120>, March 2011

Reference [8] IETF RFC 6121, “Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence”, at <http://tools.ietf.org/html/rfc6121>, March 2011

Reference [9] XEP-0030, “Service Discovery”, version 2.5rc3, at <http://www.xmpp.org/extensions/xep-0030.html>, October 2017

4.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [3] and this profile.
- Courier font indicates syntax derived from XMPP (References [8] and [6]) and XEP-0258 (Reference [4]).

4.5. Message Stanza Structure

The `Message` stanza structure is specified in (Reference [8]). Dependent upon system information exchange requirements it may be necessary that the `Message` stanza is bound to the metadata or subsets of the `Message` stanza are bound to the metadata. As such, Binding Information SHALL be represented either as: an Embedded BDO; or, a Detached BDO.

This profile specifies a new XML element, `<BindingData/>`, that SHALL be used to carry the BDO (refer to Section 8).

The `<BindingData/>` element SHALL contain one `<BindingDataObject/>` element, and an OPTIONAL `<Marking/>` element.

The Embedded or Detached BDO SHALL be contained as a child element of the `<BindingDataObject/>` element.

The <BindingDataObject/> element SHALL contain one or more BDOs. Not all consumers may be metadata-aware and as such are not capable of processing the <BindingDataObject/> element for the purposes of rendering a human-readable representation of the metadata bound to the XMPP Message stanza (or subparts thereof). To support consumers that are not metadata-aware the <Marking/> element MAY be used.

The <Marking/> element, if present, SHALL contain a 'xml:lang' attribute to identify the language used to represent the human-readable rendering of the metadata.

Additional specifications for the production and semantics intended for the use of the <Marking/> element MAY be provided in accompanying organizational, national or Community-Of-Interest implementation guidance documents.

Figure 4-1 illustrates the high-level structure of a Message stanza that contains an Embedded BDO contained within a <BindingData/> element (as specified in this profile).

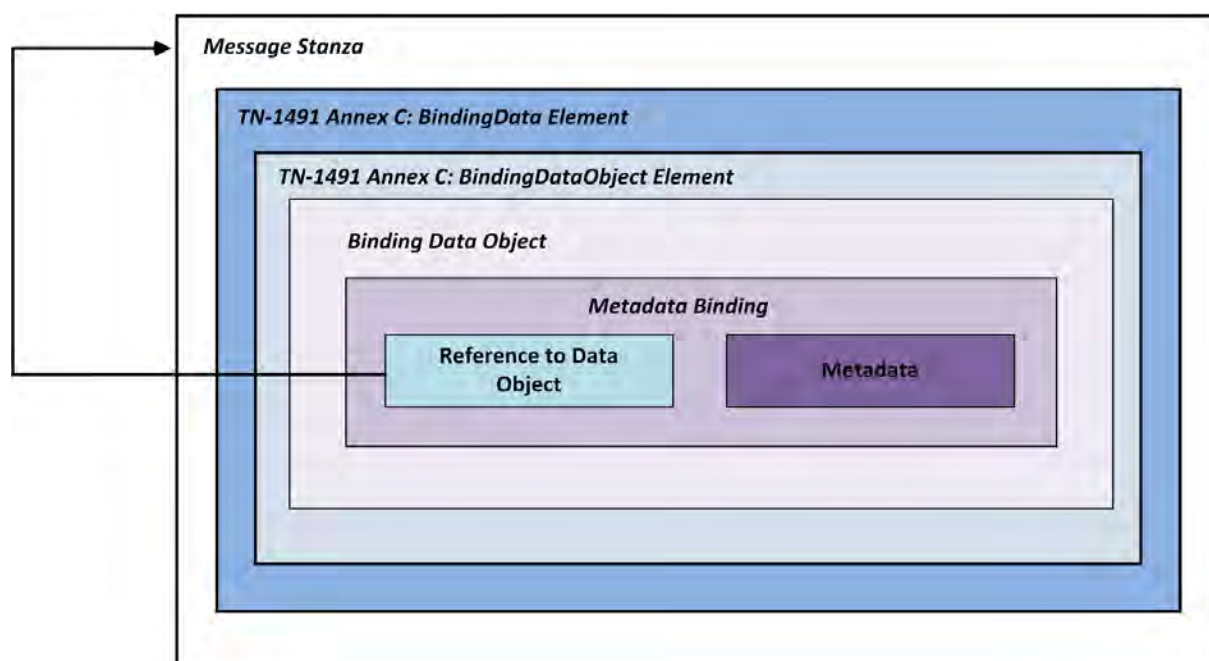


Figure 4-1 Structure of Message Stanza Containing Embedded BDO

An Embedded BDO MUST contain at least one *MetadataBinding* that contains a null *DataReference URI* attribute value only.

It is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

An example of a BDO embedded in a `Message` stanza that illustrates the binding of the entire `Message` stanza to metadata is provided in Figure 4-2. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```
<message to="alan.ross@smhs.co.uk" from="alan.ross@reach.nato.int">
  <body>This is a labelled XMPP message</body>
  <BindingData xmlns=`urn:nato:stanag:4778:profile:xmpp:1:0`>
    <BindingDataObject>
      <BindingInformation
        xmlns="urn:nato:stanag:4778:bindinginformation:1:0">
        <MetadataBindingContainer>
          <MetadataBinding>
            <Metadata>
              <originatorConfidentialityLabel
                xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                <ConfidentialityInformation>
                  <PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                  <Classification>General</slab:Classification>
                </ConfidentialityInformation>
                <CreationDateTime>
                  2018-10-30T12:00:00Z
                </CreationDateTime>
              </originatorConfidentialityLabel>
            </Metadata>
            <DataReference URI=""/>
          </MetadataBinding>
        </MetadataBindingContainer>
      </BindingInformation>
    </BindingDataObject>
  </BindingData>
</message>
```



Figure 4-2 Example Embedded Binding Data Object for Message Stanza (XMPP)

An example of a detached BDO contained in a `Message` stanza that illustrates the binding of the `item` element (descendant of the `Message` stanza) to metadata is provided in Figure 4-3 below. This example illustrates the use of XPath for referencing the `item` element. This example uses Confidentiality Metadata Labels (Reference [2]) as example metadata.

```

<message from="pubsub.smhs.co.uk" to="alan.ross@reach.nato.int">
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
    <items node='princely_musings'>
      <item id='ae890ac52d0df67ed7cfd51b644e901'>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>Soliloquy</title>
          <summary>
To be, or not to be: that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them?
          </summary>
          <link rel='alternate' type='text/html'
            href='http://denmark.lit/2003/12/13/atom03'/>
          <id>tag:denmark.lit,2003:entry-32397</id>
          <published>2003-12-13T18:30:02Z</published>
          <updated>2003-12-13T18:30:02Z</updated>
        </entry>
      </item>
    </items>
  </event>
  <BindingData xmlns='urn:nato:stanag:4778:profile:xmpp:1:0'>
    <BindingDataObject>
      <mb:BindingInformation
        xmlns:mb='urn:nato:stanag:4778:bindinginformation:1:0'
        xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <slab:originatorConfidentialityLabel
                xmlns:slab='urn:nato:stanag:4774:confidentialitymetadatalabel:1:0'>
              <slab:ConfidentialityInformation>
                <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                <slab:Classification>GENERAL</slab:Classification>
              </slab:ConfidentialityInformation>
              <slab:CreationDateTime>
                2015-09-30T12:30:00Z
              </slab:CreationDateTime>
            </mb:Metadata>
          </mb:MetadataBinding>
          <mb>DataReference URI="">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
                <ds:XPath>
                  ancestor-or-self::*[local-name()='item' and namespace-uri()='http://jabber.org/protocol/pubsub#event'
and @id='ae890ac52d0df67ed7cfd51b644e901']/[local-name()='event' and namespace-uri()='http://www.w3.org/2005/Atom']
                </ds:XPath>
              </ds:Transform>
            </ds:Transforms>
          </mb>DataReference>
        </mb:MetadataBindingContainer>
      </mb:BindingInformation>
    </BindingDataObject>
  </BindingData>
</message>

```

Figure 4-3 Example Detached Binding Data Object Contained in Message Stanza (XMPP)

4.6. IQ Stanza Structure

The IQ stanza structure is specified in (Reference [8]) and can only have a single unique child element. Other specifications define the elements to be used as the child of the IQ stanza. This profile specifies how to label IQ stanzas that contain `item` sub-elements exchanged between XMPP entities, such as XEP-0060 Publish-Subscribe (Reference [5]). Dependent upon system information exchange requirements it may be necessary that the child element (payload) of the item is bound to the metadata or subsets thereof are bound to the metadata. As such, Binding Information SHALL be represented as a Detached BDO.

This profile overrides the XMPP Publish-Subscribe specifications to support binding of metadata to the child element, and subsets thereof, for `item` elements within the IQ stanzas.

Figure C 4 illustrates the high-level structure of a IQ stanza that contains an `item` element which, in its turn, contains the detached BDO included within the `<BindingData/>` element.

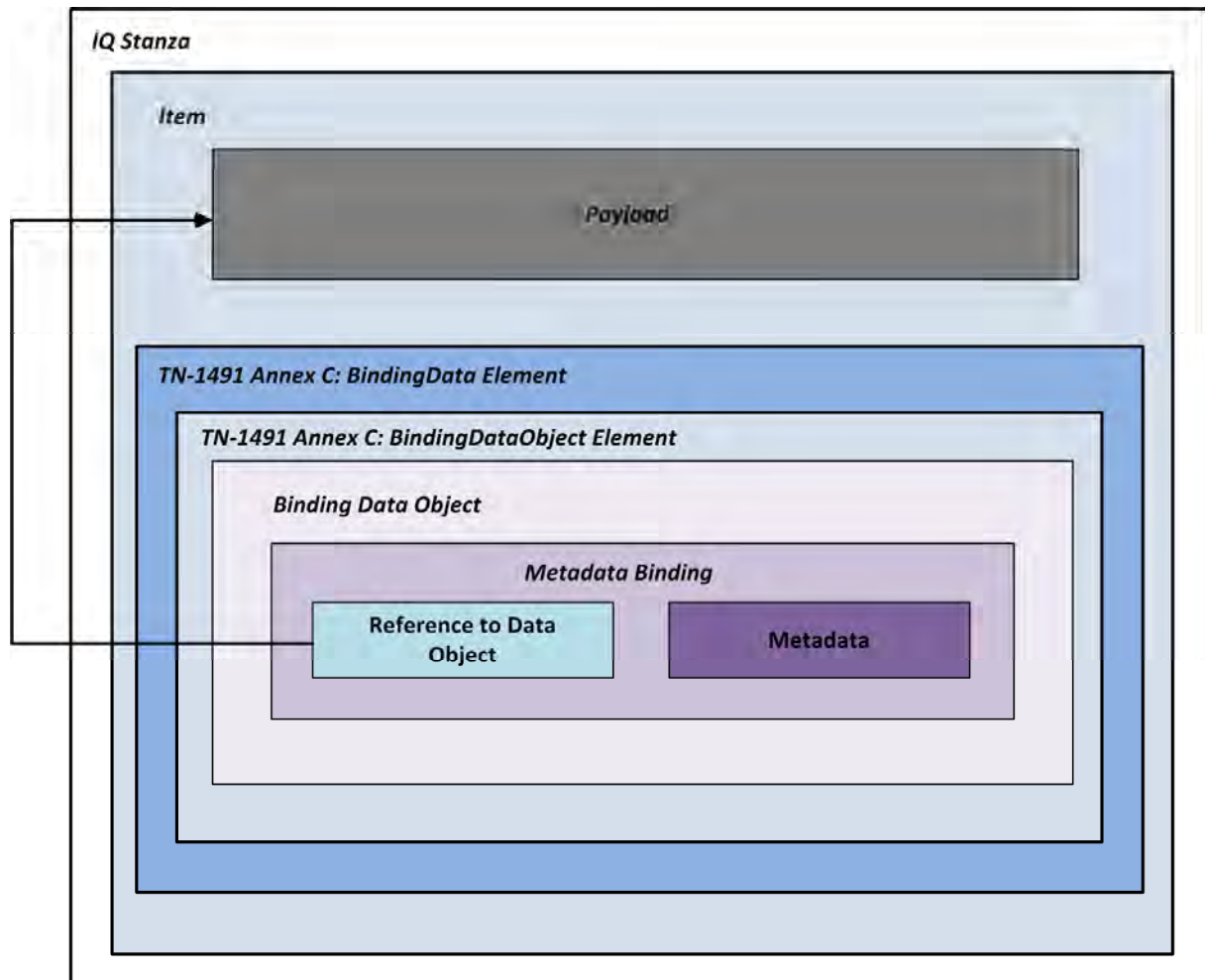


Figure 4-4 Structure of IQ Stanza containing a Detached BDO

The `<BindingData/>` element SHALL be the second child element of the `item` element.

When the `item` element contains the `<BindingData/>` child element, it SHALL have an `id` attribute with a value that uniquely identifies that item element.

The Detached BDO SHALL dereference the root node of the item element by containing one *DataReference URI* attribute value with a value that contains the

value of the `item id` attribute value, along with a *Transforms* element containing a single *Transform* element that contains a *Transform Algorithm* attribute value of <http://www.w3.org/TR/1999/REC-xpath-19991116> and a child XPath element that dereferences the child element (payload) of the item element.

It is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

An example of a detached BDO contained in a `IQ` stanza that illustrates the binding of the payload (first child of the `IQ` stanza) to metadata is provided in Figure 4-5. This example illustrates the use of XPath for referencing the payload (first child of the `IQ` stanza) element. This example uses Confidentiality Metadata Labels (Reference [2]) as example metadata.

```

<iq type='set' from='pubsub.smhs.co.uk' to='alan.ross@reach.nato.int' id='publish1'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <publish node='princely_musings'>
      <item id='bnd81g37d61f49fgn581'>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>Soliloquy</title>
          <summary>
To be, or not to be: that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them?
          </summary>
          <link rel='alternate' type='text/html'
            href='http://denmark.lit/2003/12/13/atom03'/>
          <id>tag:denmark.lit,2003:entry-32397</id>
          <published>2003-12-13T18:30:02Z</published>
          <updated>2003-12-13T18:30:02Z</updated>
        </entry>
        <BindingData xmlns='urn:nato:stanag:4778:profile:xmpp:1:0'>
          <BindingDataObject>
            <mb:BindingInformation
              xmlns:mb='urn:nato:stanag:4778:bindinginformation:1:0'
              xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
              <mb:MetadataBindingContainer>
                <mb:MetadataBinding>
                  <mb:Metadata>
                    <slab:originatorConfidentialityLabel
                      xmlns:slab='urn:nato:stanag:4774:confidentialitymetadatalabel:1:0'>
                      <slab:ConfidentialityInformation>
                        <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                        <slab:Classification>GENERAL</slab:Classification>
                      </slab:ConfidentialityInformation>
                      <slab:CreationDateTime>
                        2015-09-30T12:30:00Z
                      </slab:CreationDateTime>
                    </slab:originatorConfidentialityLabel>
                  </mb:Metadata>
                  <mb>DataReference URI=''>
                    <ds:Transforms>
                      <ds:Transform Algorithm='http://www.w3.org/TR/1999/REC-xpath-19991116'>
                        <ds:XPath>
                          ancestor-or-self::*[local-name()='item' and namespace-uri()='http://jabber.org/protocol/pubsub'
and @id='ae890ac52d0df67ed7cfd51b644e901']/[local-name()='event' and namespace-uri()='http://www.w3.org/2005/Atom']
                        </ds:XPath>
                      </ds:Transform>
                    </ds:Transforms>
                  </mb>DataReference>
                </mb:MetadataBinding>
              </mb:MetadataBindingContainer>
            </mb:BindingInformation>
          </BindingDataObject>
        </BindingData>
      </item>
    </publish>
  </pubsub>
</iq>

```



Figure 4-5 Example Detached BDO contained in IQ Stanza

4.7. BindingData Schema

```

<?xml version='1.0' encoding='UTF-8'?>
<!--
*****
NATO UNCLASSIFIED
XML Schema for carrying STANAG 4778 Binding Information
in XMPP stanzas.
I
/ \
-< + >-
\ /
I NCI AGENCY
## # ### # P.O. box 174
## # # # 2501 CD The Hague
# # # #
# # # # # Core Enterprise Services
# ## #####
A G E N C Y
*****
-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="urn:nato:stanag:4778:profile:xmpp:1:0"
  xmlns:xml="http://www.w3.org/XML/1998/namespace" xmlns="urn:nato:stanag:4778:profile:xmpp:1:0"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0" xml:lang="en">

  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>urn:nato:stanag:4778:profile:xmpp:1:0</UniqueIdentifier>
      <Name>XMPP Binding Information Wrapper Schema</Name>
      <Definition>Schema for carrying STANAG 4778 Binding Information in XMPP Stanzas</Definition>
      <VersionIndicator>1.4</VersionIndicator>
      <UsageGuidance>Used within NATO to carry STANAG 4778 Binding Information in XMPP Stanzas</UsageGuidance>
      <RestrictionType/>
      <RestrictionValue/>
    </xs:appinfo>
    <xs:documentation>
      The schema can be used to carry STANAG 4778 Binding Information in XMPP Stanzas as specified in TN-1491 Edition 3.
    </xs:documentation>
  </xs:annotation>

  <xs:import namespace="http://www.w3.org/XML/1998/namespace" schemaLocation="xml.xsd"/>

  <xs:complexType name="markingType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>urn:nato:stanag:4778:profile:xmpp:1:0:appinfo:markingType</UniqueIdentifier>
        <Name>Marking Type</Name>
        <Definition>Human-readable string.</Definition>
        <VersionIndicator>1.0</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>Human-readable representation of metadata bound to XMPP stanzas (or subsets thereof).</xs:documentation>
      <xs:documentation>String which may be used depending on organizational, national or Community-of-Interest policy</xs:documentation>
    </xs:annotation>
    <xs:attribute ref="xml:lang" use="required"/>
    <xs:anyAttribute processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="bindingDataObjectType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>urn:nato:stanag:4778:profile:xmpp:1:0:appinfo:bindingDataObjectType</UniqueIdentifier>
        <Name>BDO Type</Name>
        <Definition>An object to carry binding information for associating metadata to XMPP data objects.</Definition>
        <VersionIndicator>1.0</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>
        </xs:documentation>
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:anyAttribute processContents="lax"/>
  </xs:complexType>

  <xs:element name="BindingData">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Marking" type="markingType" minOccurs="0"/>
        <xs:element name="BindingDataObject" type="bindingDataObjectType"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:anyAttribute processContents="lax"/>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

Figure 4-6 BindingData Schema

4.8. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

With XMPP, stanzas may belong to different XMPP content namespaces i.e. `jabber:client` and `jabber:server` depending on whether the XMPP stream is negotiated between an XMPP client and XMPP server or an XMPP server and a peer XMPP server, respectively. The only difference between the two is that the `to` and `from` attributes are optional on stanzas qualified by the `jabber:client` namespace and required on stanzas qualified by the `jabber:server` namespace. To accommodate the re-scoping of XMPP content namespaces as described above the following rules apply for XML Signature Core Signature Generation and Verification:

- 1) If the XMPP Binding Profile is supported between XMPP entities (an originating entity and a recipient entity) without re-scoping of the originating `Message` stanza:
 - a. The Binding Information MAY be represented either as an Embedded BDO (the metadata SHALL be bound to the entire `Message` stanza) or a Detached BDO (the metadata SHALL be bound to a subset of the `Message` stanza); and,
 - b. The content namespace SHALL be `jabber:client`.
- 2) Otherwise:
 - a. The Binding Information SHALL be represented as a Detached BDO (the metadata SHALL be bound to a subset of the stanza); and,
 - b. The content namespace SHALL be `jabber:client`.

CHAPTER 5 Office Open XML Formats Binding Profile

5.1. Introduction

The Office Open XML Formats (OOXML) are defined ISO/IEC 29500 (Reference [1]) and offer standards for representing office documents, including spreadsheets, presentations and word processing documents.

OOXML adopts a structured format which consists of a number of XML-based files packaged into an archive file according to the Open Packaging Conventions (OPC), which is defined in Part 2 of ISO/IEC 29500 (Reference [1]).

OOXML allows for custom XML files to be included within the package without impacting the underlying application. This provides a mechanism for a metadata to be bound to the OOXML document and maintained within the package.

This profile for the OOXML describes how metadata can be maintained.

5.2. Identification

The profile for OOXML is uniquely identified by the Canonical Identifier shown in Table 5-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:ooxml
Version Identifier	urn:nato:stanag:4778:profile:ooxml:1:2

Table 5-1 Profile Identifiers

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base OOXML standard e.g.
 - introduction of new package parts
- additional profiles for OOXML e.g.
 - different combinations of package parts
 - bindings to elements within a package part (e.g. binding metadata to paragraphs within a document)
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 5-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:ooxml:1:1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

5.3. Standards (Reference)

Reference [1] ISO/IEC 29500-2 “Office Open XML File Formats - Part 2: Open Packaging Conventions”, at http://standards.iso.org/ittf/PubliclyAvailableStandards/c061796_ISO_IEC_29500-2_2012.zip, August 2012

Reference [2] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [3] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

5.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [3].

5.5. Structure

The structure of an OOXML package consists of a number of folders which contain different components of the document.

Name	Type	Modified	Size	Ratio	Packed
_rels	Folder	01/01/1980 00:...			
item1.xml	XML Docum...	01/01/1980 00:...	2,080	72%	573
itemProps1.xml	XML Docum...	01/01/1980 00:...	376	36%	242

Figure 5-1 General Structure of an OPC Package

The structure, as shown in Figure 5-1, generally consists of:

- An application specific folder, for example “word”, “ppt” or “xl”.
- A “customXml” folder in which arbitrary XML files can be stored.
- A “docProps” folder in which core and custom document properties are held.
- Multiple “_rels” folder which contains details of the parts within a folder.

This structure is then packaged into an archive file with an application specific extension (for example, .docx).

The document that is displayed to a user is generally split over a number of different XML files contained with the package. This does not present a problem when applying granular metadata to different parts of the document.

However care must be taken when the intention is to bind metadata to the complete document (refer to Microsoft Office File Types section below for normative text related to binding metadata to a whole document). For example, the XML file /word/document.xml within a Microsoft Word OPC package does not contain the headers or footers of the document (these are contained in the separate files /word/header1.xml and /word/footer1.xml.)

5.6. Custom XML

In order to support metadata binding within an OPC package, a single CustomXML file SHALL be maintained within the OPC package with the Metadata Binding Container namespace, “*urn:nato:stanag:4778:bindinginformation:1:0*”.

DataReference elements SHALL be used to reference the files within the OPC package.

Data elements SHALL NOT be used.

DataReference elements used to reference the files within the OPC package will use the Pack URI scheme ‘pack’ as specified in Reference [1] Annex B.

The authority component of the Pack URI scheme SHALL be empty that denotes the package root.

When referring to files, or portions of files, within the OPC package, absolute URIs from the package root SHALL be used with the *DataReference* element. For example,

```
<DataReference URI="pack:///word/document.xml"/>
```

Microsoft Office File Types

Microsoft Office has used the OOXML standard, since Microsoft Office 2007, for a number of its document types, including Microsoft Word, Microsoft Excel and Microsoft PowerPoint.

When binding metadata to a complete document (as opposed to a specific part of a document), all of the files (when they are present within the package) listed in the

“Package File” for the particular document type SHALL be referenced in the binding (see in Table 5-2).

Application	Package File	Description
Microsoft Word	/word/document.xml	The document.
	/word/styles.xml	The styles within the document.
	/word/header<N>.xml	The headers for sections within the document.
	/word/footer<N>.xml	The footers for sections within the document.
	/word/media/*	The media (e.g. pictures) embedded in the document.
	/word/footnotes.xml	The footnotes.
	/word/endnotes.xml	The endnotes.
	/word/comments.xml	The review comments.
	/word/commentsExtended.xml	The review comments.
Microsoft Excel	/xl/workbook.xml	The workbook.
	/xl/styles.xml	The styles within the workbook.
	/xl/sharedStrings.xml	The strings shared between worksheets.
	/xl/worksheets/sheet<N>.xml	The worksheets within the workbook.
	/xl/charts/chart<N>.xml	The charts on a worksheet.
	/xl/charts/colors<N>.xml	The colors of a chart on a worksheet.
	/xl/charts/styles<N>.xml	The style of a chart on a worksheet.
	/xl/pivotTables/pivotTable<N>.xml	The pivotTables on a worksheet.
	/xl/comments<N>.xml	The comments on a worksheet.
/xl/media/*	The media (e.g.) pictures embedded on the worksheets.	
Microsoft PowerPoint	/ppt/presentation.xml	The presentation.
	/ppt/slides/slide<N>.xml	The slides within the presentation.
	/ppt/slideLayouts/slideLayout<N>.xml	The slide layouts.
	/ppt/slideMaster/slideMaster<N>.xml	The slide masters.
	/ppt/comments/comment<N>.xml	The comments on a slide.
	/ppt/media/*	The media (e.g. pictures) embedded on the slides.
	/ppt/presProps.xml	The additional presentation-wide properties.
	/ppt/viewProps.xml	The additional presentation-wide properties.

Table 5-2 Packages Files to be Referenced in a Binding to a Complete Document²

The common document properties package files (where they are present within the package) SHALL also be referenced in the binding (see Table 5-2).

Additional package files, beyond those listed in Table 5-2 and Table 5-3, MAY be referenced in the binding (e.g. packages files created by COI-specific Office Add-Ins).

² The notation “<N>” in the “Package File” column indicate an increasing integer. For example, “/word/header<N>.xml” would indicate the package files “/word/header1.xml” and “/word/header2.xml” in a document with two headers.

Package File	Description
/docProps/core.xml	The common document properties.
/docProps/app.xml	The application-specific document properties.
/docProps/custom.xml	The custom (e.g. user defined) document properties.

Table 5-3 Common Packages Files to be Referenced in a Binding to a Complete Document

Figure 5-2 shows the contents of a CustomXML file, stored in /customXml/item1.xml, for a simple Microsoft Word document containing an embedded image. Its uses Confidentiality Metadata Labels (Reference [2]) as example metadata.

```

<mb:BindingInformation
  xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:xmime="http://www.w3.org/2005/05/xmlmime">
  <mb:MetadataBindingContainer>
    <mb:MetadataBinding>
      <mb:Metadata>
        <slab:originatorConfidentialityLabel
          xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
            <slab:Classification>GENERAL</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>2016-11-10T12:30:00Z</slab:CreationDateTime>
        </slab:originatorConfidentialityLabel>
      </mb:Metadata>
      <mb:DataReference URI="pack:///word/document.xml"/>
      <mb:DataReference URI="pack:///word/styles.xml"/>
      <mb:DataReference URI="pack:///word/header1.xml"/>
      <mb:DataReference URI="pack:///word/footer1.xml"/>
      <mb:DataReference URI="pack:///word/media/image.jpeg"
xmime:contentType="image/jpeg"/>
      <mb:DataReference URI="pack:///word/footnotes.xml"/>
      <mb:DataReference URI="pack:///word/endnotes.xml"/>
      <mb:DataReference URI="pack:///docProps/app.xml"/>
      <mb:DataReference URI="pack:///docProps/core.xml"/>
      <mb:DataReference URI="pack:///docProps/custom.xml"/>
    </mb:MetadataBinding>
  </mb:MetadataBindingContainer>
</mb:BindingInformation>

```

Figure 5-2 CustomXML file

5.7. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

CHAPTER 6 Simple Object Access Protocol Binding Profile
--

6.1. Introduction

It is recognized that service providers and service consumers implementing web services based on SOAP operate under different frameworks and application contexts. As such, this profile includes support for both SOAP 1.1 (Reference [3]) and SOAP 1.2 (Reference [4]). To support information sharing between partners it may be necessary to locate a Binding Data Object (BDO) in the SOAP protocol layer. Metadata may be bound to the whole data object (SOAP message) or may be bound to subsets of the SOAP message (data object(s) in the SOAP body). Where there is a requirement to bind metadata to a SOAP message or data object (s) within the SOAP body that is exchanged between a service consumer and a service provider, the SOAP Binding Profile specified must be adhered to.

6.2. Identification

The profile for SOAP is uniquely identified by the Canonical Identifier shown in Table 6-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:soap
Version Identifier	urn:nato:stanag:4778:profile:soap:1:1

Table 6-1 Profile Identifiers

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base SOAP standard
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 6-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:soap:1:0.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

6.3. Standards (Reference)

Reference [1] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [2] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

Reference [3] W3C SOAP Version 1.1, 2000, "Simple Object Access Protocol (SOAP 1.1)", at <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>, W3C Recommendation, W3C, 8 May 2000.

Reference [4] W3C SOAP Version 1.2, 2007, "SOAP Version 1.2", at <http://www.w3.org/TR/soap12-part1/>, W3C Recommendation, W3C, 27 April 2007.

Reference [5] W3C XMLSIG-CORE, 2008, "XML- Signature Syntax and Processing (Second Edition)", at <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/>, W3C Recommendation, W3C, 10 June 2008

6.4. Namespace Constraints

Table 6-2 summarises the XML namespaces and corresponding prefixes used throughout for the binding of metadata to SOAP data objects and portions thereof.

Prefix	Namespace
mb	urn:nato:stanag:4778:bindinginformation:1:0
soap	http://schemas.xmlsoap.org/soap/envelope/ or http://www.w3.org/2003/05/soap-envelope
soap11	http://schemas.xmlsoap.org/soap/envelope/
soap12	http://www.w3.org/2003/05/soap-envelope
wsa	http://www.w3.org/2005/08/addressing
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsse11	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www/w3.org/2001/XMLSchema-instance

Table 6-2 XML Namespaces and Prefixes

6.5. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [3].
- `Courier font` indicates syntax derived from various W3C XML Signature (Reference [5]) and SOAP (References [3], [4]) standards.

6.6. SOAP Message Structure

The SOAP message structure is specified in (References [3], [4]). Dependent upon system information exchange requirements it may be necessary that the whole SOAP message is bound to the metadata or subsets of the SOAP message are

bound to the metadata. As such, Binding Information SHALL be represented either as: an Embedded BDO; or, a Detached BDO.

The BDO is contained in a `Security` header that SHALL include the `BindingInformation` element only (as a child element of the `Security` element). If the SOAP message is SOAP 1.1 the `Security @actor` attribute SHALL be included with a value of `urn:nato:stanag:4778:bindinginformation:1:0:role:bindingInformationReceiver`.

If the SOAP message is SOAP 1.2 the `Security @role` attribute SHALL be included with a value of `urn:nato:stanag:4778:bindinginformation:1:0:role:bindingInformationReceiver`.

It is RECOMMENDED that metadata is contained within the `Metadata` child element of the `MetadataBinding` element; not referenced with the use of the `MetadataReference` element.

An example of a BDO embedded in a SOAP 1.1 message that illustrates the binding of the SOAP message to metadata is provided in Figure 6-1. Also illustrated is the use of the `actor` attribute to support multiple `Security` elements. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
  <soap11:Header>
    <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
      soap11:actor="
urn:nato:stanag:4778:bindinginformation:1:0:role:bindingInformationReceiver">
      <mb:BindingInformation
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <slab:originatorConfidentialityLabel
                xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                <slab:ConfidentialityInformation>
                  <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                  <slab:Classification>GENERAL</slab:Classification>
                </slab:ConfidentialityInformation>
                <slab:CreationDateTime>
                  2015-09-30T12:30:00Z
                </slab:CreationDateTime>
              </slab:originatorConfidentialityLabel>
            </mb:Metadata>
            <mb:DataReference URI="" />
          </mb:MetadataBinding>
        </mb:MetadataBindingContainer>
      </mb:BindingInformation>
    </wsse:Security>
  </soap11:Header>
</soap11:Envelope>
```

```

    </mb:MetadataBindingContainer>
  </mb:BindingInformation>
</wsse:Security>
</soap11:Header>
<soap11:Body>
  <Track xmlns="http://example.com/trackInformation">
    ....
  </Track>
</soap11:Body>
</soap11:Envelope>

```

Figure 6-1 Example Embedded BDO for SOAP

An example of a detached BDO contained in a SOAP 1.1 message that illustrates the binding of an external data object in the SOAP body to metadata is provided in Figure 6-2. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

Figure 6-2 illustrates the use of XPointer and XPath to reference the data object. Also illustrated is the use of the `actor` attribute to support multiple `Security` elements.

```

<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
  <soap11:Header>
    <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
      soap11:actor="
urn:nato:stanag:4778:bindinginformation:1:0:role:bindingInformationReceiver
">
      <mb:BindingInformation
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <slab:originatorConfidentialityLabel
                xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                <slab:ConfidentialityInformation>
                  <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                  <slab:Classification>GENERAL</slab:Classification>
                </slab:ConfidentialityInformation>
                <slab:CreationDateTime>
                  2015-09-30T12:30:00Z
                </slab:CreationDateTime>
              </slab:originatorConfidentialityLabel>
            </mb:Metadata>
            <mb:DataReference URI="">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116">
                  <ds:XPath>

```

```

        ancestor-or-self::*[local-name()='Track' and namespace-
uri()='http://example.com/trackInformation']
    </ds:XPath>
    </ds:Transform>
</ds:Transforms>
    </mb:DataReference>
</mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>
</wsse:Security>
</soap11:Header>
<soap11:Body>
    <Track xmlns="http://example.com/trackInformation">
        ....
    </Track>
</soap11:Body>
</soap11:Envelope>

```

Figure 6-2 Example Detached BDO for SOAP

6.7. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

CHAPTER 7 Representational State Transfer (REST) Binding Profile
--

7.1. Introduction

REST is an architectural style defined as a set of constraints on a distributed hypermedia system and implemented by a set of standard protocols that adhere to these constraints. The REST architectural style can be employed for implementing web services which are known as RESTful web services. RESTful web services rely upon the Hypertext Transport Protocol (HTTP) (Reference [4]) as the standard interface between service providers and service consumers utilizing the HTTP verbs GET, PUT, POST, DELETE, etc. in their specified manner. Resources that are exposed through RESTful web services are identified by URIs and are represented to service consumers in any (mutually agreed) media type format. In other words, a URI identifies a resource, rather than a representation, and when a service consumer asks a service provider for a resource, the service provider will respond with the best possible representation for that resource, given the service consumer's preferences. In an environment where data objects must have bound metadata, the resource identified in the URI will already contain a BDO (detached, encapsulating or embedded). As such, there is no requirement for metadata binding that is specific for REST. However, to support information sharing between partners it may be necessary to locate a Binding Data Object (BDO) in the HTTP protocol layer.

This profile specifies the mechanism for binding metadata to the HTTP Entity message body (Reference [4] Section 3.3).

This profile does not support the capability for referencing HTTP Entity message start line (Reference [4] Section 3.1) or HTTP Entity message headers (Reference [4] Section 3.2). A separate profile will specify how to bind metadata to HTTP Entity message start line and headers.

7.2. Identification

The profile for REST is uniquely identified by the Canonical Identifier shown in Table 7-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:rest
Version Identifier	urn:nato:stanag:4778:profile:rest:1:2

Table 7-1 Profiles Identifier

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base RESTful standard
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 7-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:http:1:1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

7.3. Standards (Reference)

Reference [1] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [2] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

Reference [3] IETF RFC 7444, "Security Labels in Internet Email", K. Zeilenga and A. Melnikov, at <http://tools.ietf.org/html/rfc7444>, February 2015.

Reference [4] IETF RFC 7230, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", at <http://tools.ietf.org/html/rfc7230>, June 2014.

Reference [5] IETF RFC 2231, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", at <http://tools.ietf.org/html/rfc2231>, November 1997.

Reference [6] ITU-T X.841, "Information Technology – Security Techniques – Security information objects for access control", at <https://www.itu.int/rec/T-REC-X.841/en>, October 2000

Reference [7] IETF RFC 5751, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", at <http://tools.ietf.org/html/rfc5751>, January 2010

7.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [4]
- `Courier font` indicates syntax derived from SIO -Label (Reference [3]) and HTTP (Reference [4]) referenced in this Annex.

7.5. HTTP Request/Response for RESTful Web Services

In the cases where there is a requirement for BDOs to be located in the HTTP protocol layer it is RECOMMENDED to use the Binding-Data header field (refer to

Chapter 3:, based on the SIO-Label Reference [4]) as a HTTP Entity message header for HTTP Entity requests and responses for storing the BDO.

The BDO is a detached BDO that MUST contain at least one *MetadataBinding* that contains a null *DataReference URI* attribute value (refer to Same-Document References Section of Reference [2]) that semantically indicates a binding relationship to the HTTP Entity message body request or response.

The *DataReference xmime:contentType* attribute MUST be present with a value of `message/http`.

The Binding-Data header field SHALL be used to embed the BDO within the HTTP Entity message.

The BDO SHALL be included in the Binding-Data header field “binding-data-object” parameter.

The Binding-Data “binding-data-object” parameter value SHALL be the base64 encoding of the BDO.

The Binding-Data “binding-data-object” parameter value SHALL always be present. HTTP (Reference [4]) does not specify a line length limit for HTTP header field values and does not support parameter value continuation as specified in Reference [7]. Therefore, the Binding-Data “binding-data-object” parameter MUST not support Reference [7] for parameter value continuation.

The Binding-Data “binding-type” parameter SHALL be present with the value `urn:nato:stanag:4778:bindinginformation:1:0`.

Figure 7-1 illustrates an HTTP POST request with the Binding-Data HTTP header field with the header field value as specified in this Binding Profile. Figure 7-2 illustrates the base64 decoded value of the Binding-Data “binding-data-object” value parameter. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```

POST /token HTTP/1.1
Host: server.example.com
Binding-Data: binding-type="urn:nato:stanag:4778:bindinginformation:1:0"
binding-data-object="<base64 encoded BDO>"
Content-Type: text/xml

<Document>
...
</Document>

```

Figure 7-1 An example HTTP POST Request which includes an Embedded BDO

```

<mb:BindingInformation
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <mb:MetadataBindingContainer>
    <mb:MetadataBinding>
      <mb:Metadata>
        <slab:originatorConfidentialityLabel
          xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
            <slab:Classification>GENERAL</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>
            2015-09-30T12:30:00Z
          </slab:CreationDateTime>
        </slab:originatorConfidentialityLabel>
      </mb:Metadata>
      <mb:DataReference URI="" mimeType="message/http"/>
    </mb:MetadataBinding>
  </mb:MetadataBindingContainer>
</mb:BindingInformation>

```

Figure 7-2 Base64 Decoded Embedded BDO illustrating the binding of the HTTP POST REQUEST

7.6. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

In addition, the creation of the DigestValue specific to this profile SHALL conform to the following rules for XML Signature Core Generation:

- The HTTP Entity message body SHALL be canonicalised according to Reference [8] Section 3.1.1.

- The canonicalised HTTP Entity message body SHALL be input to the DigestMethod Algorithm.

The creation of the DigestValue specific to this profile SHALL conform to the following rules for XML Signature Core Validation:

- For each Reference in the Manifest that dereferences the HTTP Entity message body SHALL be canonicalised according to Reference [8] Section 3.1.1.
- The canonicalised HTTP Entity message body SHALL be input to the DigestMethod Algorithm.

CHAPTER 8 Generic Open Packaging Convention Binding Profile

8.1. Introduction

This profile defines a generic packaging mechanism, based upon the Open Packaging Container (OPC) defined in ISO/IEC 29500-2:2008 (Reference [1]), to associate any arbitrary file that do not use the Office Open XML (OOXML) format (Reference [1]) or have no specific profile for supporting the BindingInformation with their own file format.

In OPC terminology, the term *package* corresponds to a ZIP archive and the term *part* corresponds to a file stored within the ZIP. Every part in a package has a unique URI-compliant part name along with a specified content-type expressed in the form of a MIME media type. A part's content-type explicitly defines the type of data stored in the part, and reduces duplication and ambiguity issues inherent with file extensions.

8.2. Identification

The profile for generic OPC is uniquely identified by the Canonical Identifier shown in Table 8-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:gopc
Version Identifier	urn:nato:stanag:4778:profile:gopc:1:2

Table 8-1 Profiles Identifier

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base OPC standard
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 8-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:gopc:1:1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

8.3. Standards (Reference)

Reference [1] ISO/IEC 29500-2 “Office Open XML File Formats - Part 2: Open Packaging Conventions”, at

http://standards.iso.org/ittf/PubliclyAvailableStandards/c061796_ISO_IEC_29500-2_2012.zip, August 2012

Reference [2] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [3] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

8.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [3].

8.5. File Package

One of the common ways to package a number of files together is to use the archive file format. An archive file may contain a number of different files and an associated folder structure.

This profile adopts the Open Packaging Conventions (OPC) as defined as Part 2 of the Office Open XML specification (Reference [1]).

By adopting OPC this profile provides a structured and consistent mechanism for associating *BindingInformation* with a data object within an archive file.

This profile uses the same customXml files and relationships within the archive file as those defined in the OOXML Binding Profile, as shown in Figure 8-1.

Specifically:

- A top-level relationship within the package SHALL be defined which identifies the file with which the *BindingInformation* will be associated.
- The file SHALL be held in a folder called "files"
- The *BindingInformation* SHALL be held within a file called "customXml".
- *DataReference* elements SHALL be used to reference the files within the OPC package.
- *Data* elements SHALL NOT be used.
- *DataReference* elements used to reference the files within the OPC package will use the Pack URI scheme 'pack' as specified in Reference [1] Annex B.
- The authority component of the Pack URI scheme SHALL be empty that denotes the package root.
- When referring to files, or portions of files, within the OPC package, absolute URIs from the package root SHALL be used with the *DataReference* element.
- As such, a relationship is defined between the file and the *BindingInformation*.

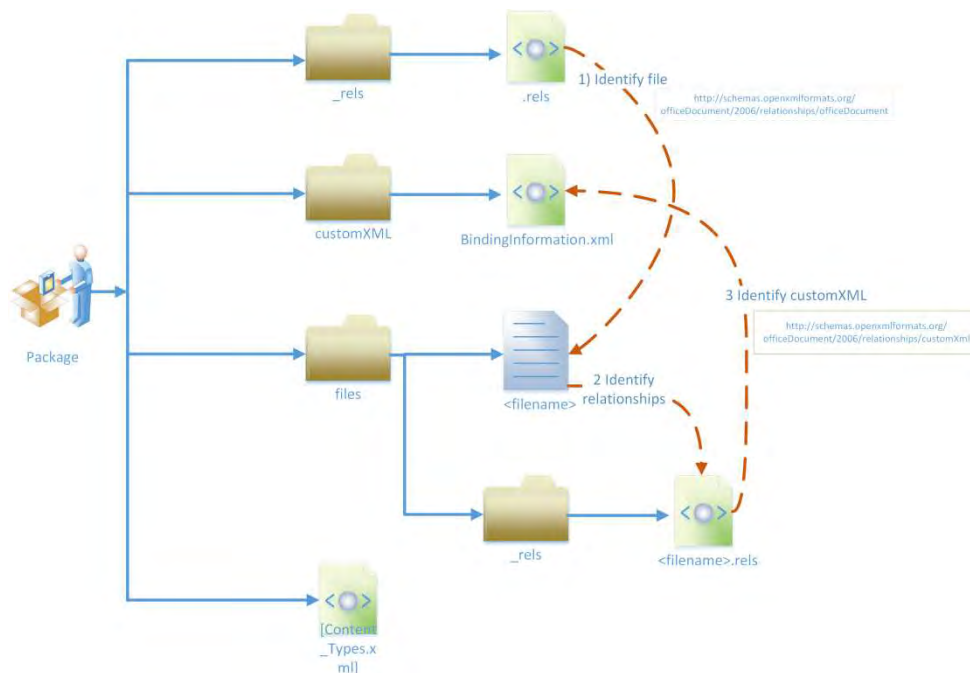


Figure 8-1 OPC Structure for packaging BindingInformation with an arbitrary file

This approach allows multiple files, of different types, to be held within the same package and be bound to distinct metadata. Figure 8-2 shows an example customXML file for a package containing the file “image1.jpeg”. This example uses Confidentiality Metadata Labels (Reference [2]) as example metadata.

```

<mb:BindingInformation
  xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:xmime="http://www.w3.org/2005/05/xmlmime">
  <mb:MetadataBindingContainer>
    <mb:MetadataBinding>
      <mb:Metadata>
        <slab:originatorConfidentialityLabel
          xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
            <slab:Classification>GENERAL</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>
            2016-11-10T12:30:00Z
          </slab:CreationDateTime>
        </slab:originatorConfidentialityLabel>
      </mb:Metadata>
      <mb:DataReference URI="pack://files/image1.jpeg"
        xmime:contentType="image/jpeg" />
    </mb:MetadataBinding>
  </mb:MetadataBindingContainer>
</mb:BindingInformation>

```

Figure 8-2 Example Packaged CustomXML file

8.6. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

CHAPTER 9 Sidecar Files Binding Profile

9.1. Introduction

If a file cannot be packaged (for example, if it is a file on a file share which needs to be accessed using the original applications), a simple naming convention to relate the BDO with the data object is proposed.

Sidecar files allow the association of metadata with a data object for which there is no profile.

This approach is well known and understood for associating data (typically metadata) with other data of a different format.

9.2. Identification

The profile for sidecar files is uniquely identified by the Canonical Identifier shown in Table 9-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:sidecar
Version Identifier	urn:nato:stanag:4778:profile:sidecar:1:2

Table 9-1 Profiles Identifier

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- support for specific file types
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 9-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:sidecar:1:1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

9.3. Standards (Reference)

Reference [1] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [2] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

9.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [2].

9.5. File Package

A simple naming convention is defined that allows the Binding Data Object to be maintained in a separate, but identifiable, file to the data object file, as shown in Figure 9-1.

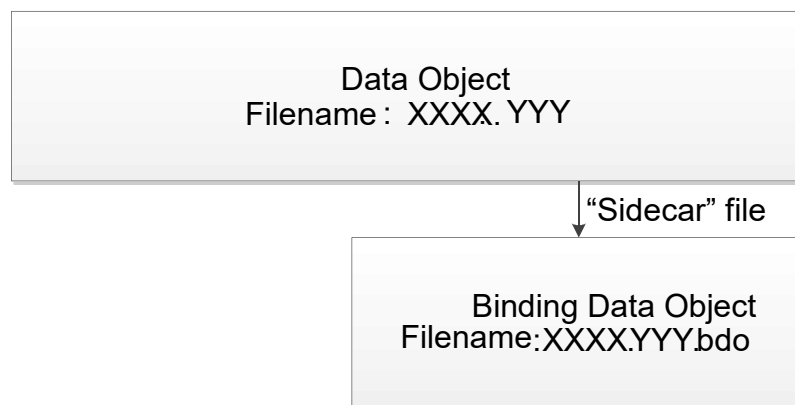


Figure 9-1 BDO as a Sidecar File

The name of the Binding Data Object file SHALL be the same as the data object file, with a further ".bdo" suffix.

Values used in *DataReference URI* with the BDO SHALL use relative paths and assume that the data object resides at the same location as the BDO.

For example, distinct metadata may be associated with an image file, "image1.jpeg", by creating a *BindingInformation* element and storing it as "image1.jpeg.bdo" in the same folder as the original file.

Figure 9-2 shows an example sidecar file for "image1.jpeg". This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```

<mb:BindingInformation
  xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:xmime="http://www.w3.org/2005/05/xmlmime">
  <mb:MetadataBindingContainer>
  
```

```

<mb:MetadataBinding>
  <mb:Metadata>
    <slab:originatorConfidentialityLabel
      xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
      <slab:ConfidentialityInformation>
        <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
        <slab:Classification>GENERAL</slab:Classification>
      </slab:ConfidentialityInformation>
      <slab:CreationDateTime>
        2016-11-10T12:30:00Z
      </slab:CreationDateTime>
    </slab:originatorConfidentialityLabel>
  </mb:Metadata>
  <mb:DataReference URI="./image1.jpeg" mimeType="image/jpeg" />
</mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>

```

Figure 9-2 Example Sidecar file

9.6. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

CHAPTER 10 Extensible Metadata Platform Binding Profile

10.1. Introduction

The Extensible Metadata Platform (XMP) specifications are defined in ISO 16684-1:2012 (Reference [1]) and offer standards for the creation, processing and interchange of standardized and custom metadata for specific finite data formats.

XMP is an XML-based format modelled after the World Wide Web Consortium (W3C) Resource Description Framework (RDF) (Reference [2]) that standardizes a data model, serialization of the data model in XML, core metadata properties, definition and processing of customized metadata and a mechanism for embedding XMP information into documents, such as JPEG and PDF.

XMP offers an alternative for storing metadata in side car files whereby the XMP metadata is associated with a file format by embedding the metadata in that file format. The file formats that are supported by XMP and the locations for embedding the XMP metadata within those file formats is documented in XMP Part 3, Storage in Files (Reference [3]).

An instance of the XMP data model is called an XMP packet. An XMP packet is a set of XMP metadata properties each of which has a name and value. A value can take the form of a simple value, a structured value or an array value. This Binding Profile for XMP describes how metadata should be incorporated within an XMP packet as a simple value.

10.2. Identification

The profile for XMP is uniquely identified by the Canonical Identifier shown in Table 10-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:xmp
Version Identifier	urn:nato:stanag:4778:profile:xmp:1:1

Table 10-1 Profiles Identifier

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base XMP standard
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 10-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:xmp:1:0.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

10.3. Standards (Reference)

Reference [1] Adobe XMP, “XMP Specification Part 1, Data Model, Serialization and Core Properties”, at

<http://www.images.adobe.com/content/dam/Adobe/en/devnet/xmp/pdfs/XMP%20SDK%20Release%20cc-2016-08/XMPSpecificationPart1.pdf>, August 2016.

Reference [2] W3C Recommendation, “RDF Primer”, at

<https://www.w3.org/TR/2004/REC-rdf-primer-20040210/>, February 2004.

Reference [3] Adobe XMP, “XMP Specification Part 3, Storage in Files”, at

<http://www.images.adobe.com/content/dam/Adobe/en/devnet/xmp/pdfs/XMP%20SDK%20Release%20cc-2016-08/XMPSpecificationPart3.pdf>, August 2016.

Reference [4] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [5] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

Reference [6] W3C Recommendation, “RDF 1.1 Concepts and Abstract Syntax”, at <https://www.w3.org/TR/rdf11-concepts/>, February 2014.

Reference [7] W3C Recommendation, “Extensible Markup Language (XML) 1.0 (Fifth Edition)”, November 2008.

10.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Reference [3].
- `Courier` font indicates syntax derived from XMP (Reference [6]), RDF (Reference [2]) and XML (Reference [7]).

10.5. Structure

An XMP packet contains a set of XMP metadata properties, with each property having a unique name and a value. Each unique name needs to be an XML expanded name.

Values have one of three forms (Section 3 of Reference [1]):

- simple – a string of Unicode text – see Figure 10-1:

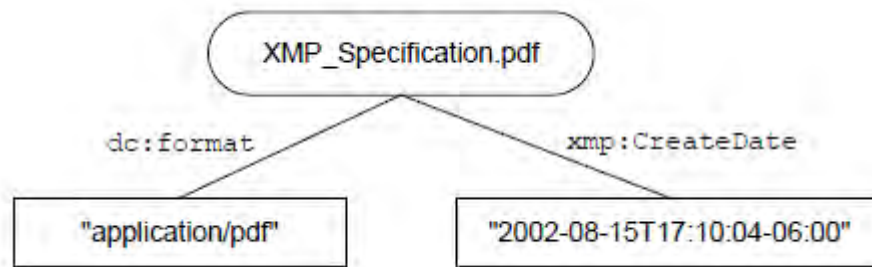


Figure 10-1 Two Simple XMP Properties, dc:format and xmp:CreateDate

- structure – a container for zero or more named fields – see Figure 10-2; and

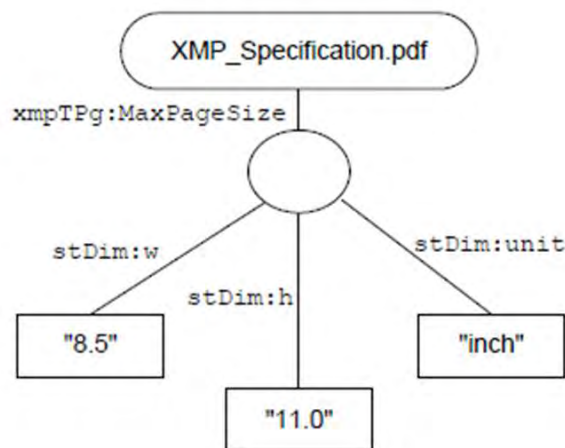


Figure 10-2 An XMP Structured Property, xmpTPg:MaxPageSize containing 3 fields

- array – a container for zero or more items e.g. to support multi-valued properties – see Figure 10-3:

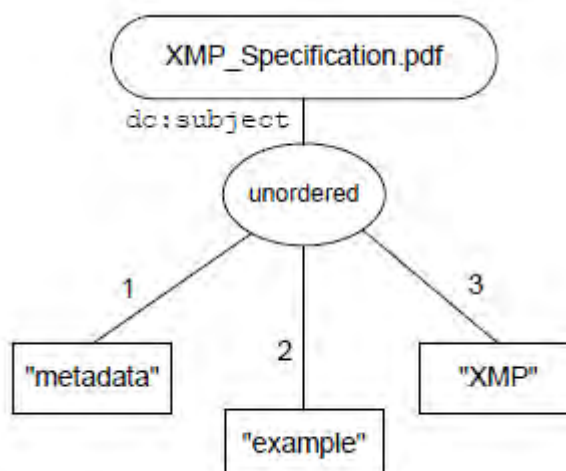


Figure 10-3 An XMP Array Property, dc:subject containing 3 items

This profile defines a single metadata property with a simple form value which contains the XML markup of the *BindingInformation*, represented as an embedded Binding Data Object (BDO).

Specifically:

- RDF provides for XML content as a literal value. Therefore, the *BindingInformation* SHALL be escaped as Character Data (see Reference [6] Section 2.4) and converted to an XML literal string value compliant with Section 5.3 Reference [6].
- The *BindingInformation* SHALL be stored as a value within a 'bindingInformation' XML element or attribute qualified by the namespace: *urn:nato:stanag:4778:bindinginformation:1:0:xmp#*.
- The 'bindingInformation' XML (containing the *BindingInformation*) SHALL be stored as either
 - a child XML element of the `rdf:Description` element (canonical form – see Section 7.5 of Reference [1]); or
 - an XML attribute of `rdf:Description` element (equivalent form – see Section 7.9.2.2 of Reference [1])
- The serialized `rdf:RDF` XML element (containing the *BindingInformation*) is known as the XMP Binding Packet.
- The *BindingInformation* MUST contain at least one *MetadataBinding* that contains a null *DataReference URI* attribute value (refer to Same-Document References Section of Reference [3]) that semantically indicates a binding relationship of the metadata to the data object.
- The *DataReference xmime:contentType* attribute is REQUIRED when the data reference is to a non-XML entity.
- A relationship is defined between the data object and the *BindingInformation* by embedding the XMP Binding Packet in the data object (of a supported XMP file format).
- The supported XMP file formats are listed in Reference [3].
- Depending on the file format, the XMP Binding Packet SHALL be embedded in the data object, or held as a separate sidecar file (refer to XMP Sidecar Files Section of this profile), as specified in Reference [3].

Figure 10-4 shows the structure of an XMP Binding Packet using the canonical form of the 'bindingInformation' property. This *BindingInformation* uses Confidentiality Metadata Labels (Reference [2]) as example metadata, bound to an XML entity.

```

<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:mbxmp="urn:nato:stanag:4778:bindinginformation:1:0:xmp#" >
  <rdf:Description rdf:about="" >
    <mbxmp:bindingInformation>
      <mb:BindingInformation

xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0";
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance";
xmlns:xsd="http://www.w3.org/2001/XMLSchema";
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0";
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xmime="http://www.w3.org/2005/05/xmlmime";
<mb:MetadataBindingContainer>
  <mb:MetadataBinding>
    <mb:Metadata>
      <slab:originatorConfidentialityLabel

xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0";
      <slab:ConfidentialityInformation>
        <slab:PolicyIdentifier>TEST
Amoco</slab:PolicyIdentifier>
        <slab:Classification>
GENERAL</slab:Classification>
        </slab:ConfidentialityInformation>
        <slab:CreationDateTime>
          2015-09-30T12:30:00Z
        </slab:CreationDateTime>
        </slab:originatorConfidentialityLabel>
      </mb:Metadata>
      <mb:DataReference URI=""; />
      </mb:MetadataBinding>
    </mb:MetadataBindingContainer>
  </mb:BindingInformation>
</mbxmp:bindingInformation>
</rdf:Description>
</rdf:RDF>

```

Figure 10-4 Example XMP Binding Packet (Canonical form)

Figure 10-5 shows the structure of an XMP Binding Packet using the equivalent form of the 'bindingInformation' property. This *BindingInformation* uses Confidentiality Metadata Labels (Reference [2]) as example metadata, bound to an XML entity.

```

<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:mbxmp="urn:nato:stanag:4778:bindinginformation:1:0:xmp#" >
  <rdf:Description rdf:about=""
    xmlns:mbxmp="urn:nato:stanag:4778:bindinginformation:1:0:xmp#"
    mbxmp:bindingInformation="&lt;mb:BindingInformation
      xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0&quot;";
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance&quot;";
      xmlns:xsd="http://www.w3.org/2001/XMLSchema&quot;";
      xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0&quot;";
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#&quot;";
      xmlns:xmime="http://www.w3.org/2005/05/xmlmime&quot;";&gt;
      &lt;mb:MetadataBindingContainer&gt;
        &lt;mb:MetadataBinding&gt;
          &lt;mb:Metadata&gt;
            &lt;slab:originatorConfidentialityLabel
              xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0&quot;";
            &gt;
              &lt;slab:ConfidentialityInformation&gt;
                &lt;slab:PolicyIdentifier&gt;TEST
                Amoco&lt;/slab:PolicyIdentifier&gt;
                &lt;slab:Classification&gt;
                GENERAL&lt;/slab:Classification&gt;
                &lt;/slab:ConfidentialityInformation&gt;
                &lt;slab:CreationDateTime&gt;
                2015-09-30T12:30:00Z
                &lt;/slab:CreationDateTime&gt;
                &lt;/slab:originatorConfidentialityLabel&gt;
              &lt;/mb:Metadata&gt;
              &lt;mb:DataReference URI="&quot;&quot; /&gt;
              &lt;/mb:MetadataBinding&gt;
            &lt;/mb:MetadataBindingContainer&gt;
          &lt;/mb:BindingInformation&gt;"
    </rdf:Description>
  </rdf:RDF>

```

Figure 10-5 Example XMP Binding Packet (Equivalent form)

10.6. XMP Sidecar File

If a data object file format is not supported by XMP (refer to Reference [3] to determine XMP supported file formats), XMP offers a simple naming convention to relate the XMP Binding Packet with the data object. As the XMP Binding Packet is stored separately from the data object, there is a risk that the association between the metadata and the data object may get lost. XMP-aware applications that support this profile are REQUIRED to conform with the following rules:

- 1) The XMP Binding Packet SHALL be written as a complete and well-formed XML document, including the leading XML declaration.
- 2) The base name for the XMP Binding Packet file SHALL be the same as the file to which it relates.

- 3) The file extension for the XMP Binding Packet file SHALL be '.xmp'.
- 4) The XMP Binding Packet file name SHALL include the base name of the file that the XMP Binding Packet relates to appended with the file extension '.xmp'. For example, the XMP Binding Packet file name for a file named 'example.txt' SHALL be 'example.txt.xmp'.
- 5) If a MIME type is required 'application/rdf+xml' SHALL be used.
- 6) The *BindingInformation* SHALL be represented as a detached BDO. The 'External Storage of Media' Section of Reference [3] states "Write external metadata as though it were embedded and then had the XMP packets extracted and catenated by a postprocessor." However, this approach does not match the semantics for a detached BDO as described in Reference [3].
- 7) The *BindingInformation* MUST contain at least one *MetadataBinding*.
- 8) The value used in the *DataReference URI* attribute SHALL use relative paths and assume that the data object resides at the same location as the XMP Binding packet. As such, the data object file and the XMP Binding Packet file (that relates to the data object file) SHALL reside at the same location.
- 9) The *DataReference xmime:contentType* attribute is REQUIRED when the data reference is to a non-XML entity.

As an example, distinct metadata may be associated with an MPEG file, "example.mpg", by creating an XMP Binding Packet containing a *bindingInformation* element and storing it as "example.mpg.xmp" in the same folder as the original file. Figure 10-6 shows an example XMP sidecar file for "example.mpg". This example uses Confidentiality Metadata Labels (Reference [2]) as example metadata, bound to a non-XML entity.

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:mbxmp="urn:nato:stanag:4778:bindinginformation:1:0:xmp#" >
  <rdf:Description rdf:about="" >
    <mbxmp:bindingInformation>
      &lt;mb:BindingInformation

xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0";
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance";
xmlns:xsd="http://www.w3.org/2001/XMLSchema";
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0";
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xmime="http://www.w3.org/2005/05/xmlmime">&gt;
      &lt;mb:MetadataBinding>
        &lt;mb:Metadata>
          &lt;slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">&
          &gt;
            &lt;slab:ConfidentialityInformation>
              &lt;slab:PolicyIdentifier>TEST
Amoco&lt;/slab:PolicyIdentifier>
              &lt;slab:Classification>
GENERAL&lt;/slab:Classification>
              &lt;/slab:ConfidentialityInformation>
              &lt;slab:CreationDateTime>
                2015-09-30T12:30:00Z
              &lt;/slab:CreationDateTime>
              &lt;/slab:originatorConfidentialityLabel>
            &lt;/mb:Metadata>
            &lt;mb:DataReference URI="example.mpg">
xmime:contentType="audio/mpeg" /&gt;
            &lt;/mb:MetadataBinding>
          &lt;/mb:MetadataBindingContainer>
          &lt;/mb:BindingInformation>
        </mbxmp:bindingInformation>
      </rdf:Description>
    </rdf:RDF>
  
```

Figure 10-6 Example XMP Sidecar file (example.mpg.xmp)

10.7. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

For an embedded BDO the use of the Enveloped Binding Data Object transform element (see ANNEX A Transforms Section) SHALL NOT apply.

For this use case where an embedded BDO (specified in Structure) references a non-XML data object (indicated by the *xmime:contentType* attribute value) the XML Signature Core Generation and XML Signature Core Validation processes SHALL first exclude the embedded BDO (the *BindingInformation* element) from the digest calculation of the Reference element that contains the *BindingInformation* element. The *BindingInformation* element SHALL be excluded by removing the XMP Binding Packet (the serialized `rdf:RDF` XML element containing the *BindingInformation* element) from the cryptographic digest calculation.

For this use case where an embedded BDO (specified in Structure) references a XML data object the XML Signature Core Generation and XML Signature Core Validation processes SHALL exclude the embedded BDO (the *BindingInformation* element) from the digest calculation of the Reference element that contains the *BindingInformation* element. The *BindingInformation* element SHALL be excluded by removing the XMP Binding Packet (the serialized `rdf:RDF` XML element containing the *BindingInformation* element) from the cryptographic digest calculation. As such, the Enveloped Binding Data Object transform (as specified in ANNEX A) SHALL be replaced by an Enveloped XMP Binding Packet transform.

The Enveloped XMP Binding Packet transform element MUST have *Transform* Algorithm attribute value of `http://www.w3.org/TR/1999/REC-xpath-19991116` and MUST contain the following XPath element:

```
<XPath>
  not(ancestor-or-self::*[local-name() = 'RDF' and
    namespace-uri() = 'http://www.w3.org/1999/02/22-rdf-syntax-ns#'])
</XPath>
```

CHAPTER 11 Web Service Messaging Profile Binding Profile

11.1. Introduction

The Web Service Messaging Profile (WSMP) defines a set of service profiles to exchange arbitrary XML-based messages. WSMP is extensible and may be used by any Community of Interest (COI). It is based on publicly available standards,

WSMP profiles a standardised messaging infrastructure able to reduce the interoperability shortfall by adopting a clear and well defined protocol and rule set. This to support the data exchange via a generic and reusable interface with the following main characteristics:

- Support of Push and Pull operations
- Usable on different communication protocols like SOAP, REST, JMS, AMQP, WEBSocket.
- Configurable for the use of different COI.

With these characteristics, WSMP is intended to be a framework for the definition of a standardised way to exchange messages.

The base of the WSMP specification are the concepts of data and metadata. Typically, the relationship between the metadata and data is implicitly realized by simply including the metadata with the data in the same parent XML element.

This profile supports the requirement to explicitly bind metadata to data (or subsets thereof) whereby the data is XML-based and exchanged between service consumers and service providers using the WSMP message wrapper mechanism.

11.2. Identification

The profile for WSMP is uniquely identified by the Canonical Identifier shown in Table 11-1.

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:wsmpp
Version Identifier	urn:nato:stanag:4778:profile:wsmpp:1:1

Table 11-1 Profiles Identifier

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base WSMP standard
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 11-1.

This document deprecates the previous version identified by Version Identifier urn:nato:stanag:4778:profile:wsmp:1:0.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

11.3. Standards (Reference)

Reference [1] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium

Reference [2] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium

Reference [3] NCB011784-2.7-D01 v1.1, "WEB SERVICE MESSAGING PROFILE (WSMP) TECHNICAL SPECIFICATIONS (DRAFT 1.2)"

11.3. Namespace Constraints

Table 11-2 below summarises the XML namespaces and corresponding prefixes used throughout for the binding of metadata to WSMP data objects and portions thereof.

Prefix	Namespace
mb	urn:nato:stanag:4778:bindinginformation:1:0
wsmp-m	urn:nato:wsmp:1:2

Table 11-2 XML Namespaces and Prefixes

11.4. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from STANAG 4778 (Reference [1]) referenced in this profile.
- *Courier font* indicates syntax derived from the WSMP Specification (Reference [3]) referenced in this profile.

11.5. WSMP Message Structure

The WSMP message that encapsulates the COI-specific data is specified in the WSMP specification (Reference [3]). A WSMP message may consist of:

- a) a WSMP message wrapper with one or more WSMP data wrappers; or,

- b) one or more WSMP data wrappers.

WSMP COI Profiles may specify that the data carried in the WSMP message (or subsets thereof) is bound to the metadata compliant with STANAG 4778 (Reference [1]). As such, STANAG 4778 Binding Information can be represented as follows:

- a) an Embedded Binding Data Object (BDO) that binds metadata to the WSMP message wrapper `WSMPMsg`; and/or,
- b) a Detached BDO for each of the following WSMP data wrapper elements `Create`, `Read`, `Update`, `Delete` that binds metadata to the `Data` child element (or subsets thereof) of these elements.

An Embedded BDO MUST be present in a WSMP message that uses the WSMP message wrapper contained in the `WSMPMsg/MetadataBinding` element that SHALL include the *BindingInformation* element (as a child element of the `WSMPMsg/MetadataBinding` element).

An Embedded BDO SHALL dereference the root node of the WSMP message (`WSMPMsg`) by containing one null *DataReference URI* attribute value (`URI=""`) and, where applicable, a *Transforms* element containing a single *Transform* element that contains a *Transform Algorithm* attribute value of `http://www.w3.org/TR/1999/REC-xpath-19991116` and the following child XPath element:

```

<XPath>
  ancestor-or-self::*[local-name() = 'WSMPMsg' and
    namespace-uri() = 'urn:nato:wsm:1:1'
</XPath>
```

Figure 11-1 XPath element

An Embedded BDO MAY contain one or more *DataReference* elements present in a *MetadataBinding* element containing a *URI* attribute (with optional *Transform* elements) in order to locate the data (and subsets thereof) that is contained in the WSMP Message (`WSMPMsg`).

For a WSMP message that consists of a WSMP message wrapper and one or more WSMP data wrapper elements (`Create`, `Read`, `Update` and `Delete`) a Detached BDO MAY be present.

For a WSMP message that consists of one or more WSMP data wrapper elements (`Create`, `Read`, `Update` and `Delete`) a Detached BDO SHALL be present.

A Detached BDO for a `Create` data wrapper SHALL be contained in the `Create/MetadataBinding` element that SHALL include the *BindingInformation* element (as a child element of the `Create/MetadataBinding` element).

A Detached BDO for a Read data wrapper SHALL be contained in the Read/MetadataBinding element that SHALL include the *BindingInformation* element (as a child element of the Read/MetadataBinding element).

A Detached BDO for an Update data wrapper SHALL be contained in the Update/MetadataBinding element that SHALL include the *BindingInformation* element (as a child element of the Update/MetadataBinding element).

A Detached BDO for a Delete data wrapper SHALL be contained in the Delete/MetadataBinding element that SHALL include the *BindingInformation* element (as a child element of the Delete/MetadataBinding element).

For the remainder of this normative section WSMP data wrapper elements Create, Read, Update and Delete SHALL be referred to as <data wrapper element>.

A Detached BDO SHALL contain one or more *DataReference* elements present in a *MetadataBinding* element containing a *URI* attribute in order to locate the data (and subsets thereof) that is contained in the WSMP message <data wrapper element>/Data element. A null *DataReference URI* attribute value (URI="") for a Detached BDO SHALL dereference the root node of the WSMP message <data wrapper element> element.

For each BDO contained in a WSMP message the parent *MetadataBinding* element SHALL contain a *Dialect* attribute with the value *urn:nato:stanag:4778:bindinginformation:1:0*.

For each BDO contained in a WSMP message it is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

An example of a WSMP message (consisting of a WSMP message wrapper and an Update WSMP data wrapper element) that illustrates the binding of the data, contained in the WSMP message wrapper *WSMPMsg* and the WSMP data wrapper *WSMPMsg/Update/Data* element, to metadata is provided in Figure 11-2. This example uses Confidentiality Metadata Labels (Reference [2]), referenced in this profile, as example metadata.

```
<wsmp-m:WSMPMsg
  xmlns:wsmp-m="urn:nato:wsmp:1:2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <wsmp-m:MetadataBinding Dialect="urn:nato:stanag:4778:bindinginformation:1:0">
    <mb:BindingInformation
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <mb:MetadataBindingContainer>
        <mb:MetadataBinding>
```

```

<mb:Metadata>
  <slab:originatorConfidentialityLabel
    xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
    <slab:ConfidentialityInformation>
      <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
      <slab:Classification>GENERAL</slab:Classification>
    </slab:ConfidentialityInformation>
    <slab:CreationDateTime>
      2016-11-20T12:30:00Z
    </slab:CreationDateTime>
  </slab:originatorConfidentialityLabel>
</mb:Metadata>
<mb:DataReference URI=""/>
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
      <ds:XPath>
        ancestor-or-self::*[local-name()='WSMPMsg' and namespace-uri()='
urn:nato:wsm:1:1']
      </ds:XPath>
    </ds:Transform>
  </ds:Transforms>
</mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>
</wsm-m:MetadataBinding>
<wsm-m:Update>
  <wsm-m:Data Dialect=" http://example.com/trackInformation ">
    <ns1:Track xmlns:ns1="http://example.com/trackInformation">
      . . . .
    </ns1:Track>
  </wsm-m:Data>
<wsm-m:MetadataBinding Dialect="urn:nato:stanag:4778:bindinginformation:1:0">
  <mb:BindingInformation
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <mb:MetadataBindingContainer>
  <mb:MetadataBinding>
  <mb:Metadata>
    <slab:originatorConfidentialityLabel
      xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
      <slab:ConfidentialityInformation>
        <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
        <slab:Classification>GENERAL</slab:Classification>
      </slab:ConfidentialityInformation>
      <slab:CreationDateTime>
        2016-11-20T12:30:00Z
      </slab:CreationDateTime>
    </slab:originatorConfidentialityLabel>
  </mb:Metadata>
  <mb:DataReference URI="">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
        <ds:XPath>

```

```

        ancestor-or-self::*[local-name()='Data' and namespace-uri()='
urn:nato:wsm:1:1']
    </ds:XPath>
    </ds:Transform>
</ds:Transforms>
    </mb:DataReference>
</mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>
</wsm-m:MetadataBinding>
</wsm-m:Update>
</wsm-m:WSMPMsg>

```

Figure 11-2 Example WSMP Metadata Binding

11.6. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

CHAPTER 12 Common XML Artefacts Binding Profile

12.1. Introduction

When defining the syntax, semantics and transformation of XML-encoded data objects, a number of standard XML-encoded artefacts may typically be employed. For example, a Community of Interest (COI) may produce a schema definition that describes the syntax of their COI-specific data objects, and a transformation that renders the data object as human-readable text.

This profile supports the requirement to bind metadata to data (or subsets thereof) whereby the data is XML-encoded in one of the following schemas:

- XML Schema – to define the syntactic structure/validation of XML-encoded data objects (Reference [3])
- ISO Schematron – to define semantic validation (e.g. business rules) of XML-encoded data objects (Reference [4])
- XML Stylesheet – to define the transformation XML-encoded data objects (Reference [5])
- Genericcode Code List – to represent lists in a tabular form (Reference [6])
- Context/Value Association – to associate code lists with elements within XML-encoded data objects (Reference [7])
- Security Policy Information File (SPIF) – to define the value domain, equivalencies and markings instructions for a security policy used, for example, with confidentiality metadata labels (Reference [9]).

12.2. Identification

The profiles for XML Artefacts are uniquely identified by the Canonical Identifiers shown in Table 12-1.

XML Artefact	Type	Identifier
XML Schema	Canonical Identifier	urn:nato:stanag:4778:profile.xml:schema
	Version Identifier	urn:nato:stanag:4778:profile.xml:schema:1:0
ISO Schematron	Canonical Identifier	urn:nato:stanag:4778:profile.xml:schematron
	Version Identifier	urn:nato:stanag:4778:profile.xml:schematron:1:0
XML Stylesheet	Canonical Identifier	urn:nato:stanag:4778:profile.xml:stylesheet
	Version Identifier	urn:nato:stanag:4778:profile.xml:stylesheet:1:0
Genericcode List	Canonical Identifier	urn:nato:stanag:4778:profile.xml:codelist
	Version Identifier	urn:nato:stanag:4778:profile.xml:codelist:1:0
Context/Value Association	Canonical Identifier	urn:nato:stanag:4778:profile.xml:cva
	Version Identifier	urn:nato:stanag:4778:profile.xml:cva:1:0
Security Policy Information File	Canonical Identifier	urn:nato:stanag:4778:profile.xml:spif
	Version Identifier	urn:nato:stanag:4778:profile.xml:spif:1:0

Table 12-1 XML Artefact Profile Identifiers

It is recognized that these profiles may evolve during their review cycle. For example, a review might identify:

- changes to the base standards
- improvements to the existing profiles based upon operational feedback

Therefore these versions of the profiles are uniquely identified by the Version Identifier shown in Table 12-1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

12.3. Standards (Reference)

Reference [1] NATO Standardization Agency (NSA) STANAG 4774, “Confidentiality Metadata Label Syntax”, MCMSB, NATO Headquarters, Brussels, Belgium, 14 April 2016.

Reference [2] NATO Standardization Agency (NSA) STANAG 4778, “Metadata Binding Mechanism”, MCMSB, NATO Headquarters, Brussels, Belgium

Reference [3] World Wide Web Consortium (W3C) Web Standard W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures, “W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures”, M. Maloney, N. Mendelsohn, H. Thompson, D. Beech, S. Gao, M. Sperberg-McQueen, at <http://www.w3.org/TR/2012/REC-xmlschema11-1-20120405/>, 5 April 2012.

Reference [4] ISO/IEC 19757-3 Second Edition 2016-01-15 – Information Technology – Document Schema Definition Languages (DSDL) – Part 3: Rules-based validation – Schematron Second Edition at http://standards.iso.org/ittf/PubliclyAvailableStandards/c055982_ISO_IEC_19757-3_2016.zip, 15 January 2016.

Reference [5] World Wide Web Consortium (W3C) Web Standard XSL Transformations (XSLT) Version 1.0, “XSL Transformations (XSLT) Version 1.0”, J. Clark, at <http://www.w3.org/TR/1999/REC-xslt-19991116>, 16 November 1999.

Reference [6] Organization for the Advancement of Structured Information Standards (OASIS) “Code List Representation (Genericcode)”, Version 1.0 , at <https://docs.oasis-open.org/codelist/cs-genericcode-1.0/doc/oasis-code-list-representation-genericcode.pdf>, 28 December 2007.

Reference [7] Organization for the Advancement of Structured Information Standards (OASIS) “Context/value Association using genericcode 1.0”, at <http://docs.oasis-open.org/codelist/ns/ContextValueAssociation/1.0/doc/context-value-association.pdf>, 15 April 2010.

Reference [8] Internet Engineering Task Force (IETF) Request for Comment 2119, “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, at <http://tools.ietf.org/html/rfc2119>, Sterling, Virginia, US, March 1997.

Reference [9] Security Policy Information File (SPIF) at <http://www.xmlspif.org/>

Reference [10] <http://docs.oasis-open.org/codelist/cs01-ContextValueAssociation-1.0/xsd/ContextValueAssociation.xsd>

12.4. Namespace Constraints

Table 12-2 below summarises the XML namespaces and corresponding prefixes used throughout for the binding of metadata to Common XML Artefact data objects and portions thereof.

Prefix	Namespace
mb	urn:nato:stanag:4778:bindinginformation:1:0
slab	urn:nato:stanag:4774:confidentialitymetadatalabel:1:0
xsd	http://www.w3.org/2001/XMLSchema
sch	http://purl.oclc.org/dsdl/schematron
xsl	http://www.w3.org/1999/XSL/Transform
gc	http://docs.oasis-open.org/codelist/ns/genericcode/1.0/
cva	http://docs.oasis-open.org/codelist/ns/ContextValueAssociation/1.0/
spif	http://www.xmlspif.org/spif

Table 12-2 XML Namespaces and Prefixes

12.5. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in Reference [8].
- Words in *italics* indicate terms defined in Appendix 1 of Reference [2].
- Courier font indicates syntax derived from the Specifications referenced in this Profile.

12.6. XML Schema Structure

The XML Schema contains an `xsd:annotation` element which allows for both human readable and machine-processible, inline documentation to be provided for any element within the schema. The `xsd:annotation` element has a child element, `xsd:appinfo`, which allows any well-formed XML content to be included within the annotation. The Binding Information can thus be included within the `xsd:appinfo` element.

As such, the Binding Information SHALL be represented as an Embedded BDO. A BDO SHALL be embedded within the XML Schema as a child *mb:BindingInformation* of the `xsd:appinfo` element of the `xsd:annotation` element(s) of the top-level `xsd:schema` element.

(XPath:

`/xsd:schema/xsd:annotation/xsd:appinfo/mb:BindingInformation`).

A BDO SHALL NOT be embedded in any other location within the XML Schema.

Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of a single `xsd:appinfo` element.

Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of distinct `xsd:appinfo` elements.

It is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

One or more *DataReference* elements SHALL be present in a *MetadataBinding* element containing a *URI* attribute in order to locate the data (and subsets thereof) that is contained in the `xsd:schema` top-level element.

An example of an BDO embedded in a XML Schema that illustrates the binding of the data, contained in the parent `xsd:schema` element, to metadata is provided in Figure 12-1. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```
<xsd:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://example.com/simpleSchema"
  xmlns:tns="http://example.com/simpleSchema" version="1.0">
  <xsd:annotation>
    <xsd:appinfo>
      <mb:BindingInformation
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                <slab:ConfidentialityInformation>
                  <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                  <slab:Classification>GENERAL</slab:Classification>
                </slab:ConfidentialityInformation>
                <slab:CreationDateTime>2016-11-
20T12:30:00Z</slab:CreationDateTime>
              </slab:originatorConfidentialityLabel>
            </mb:Metadata>
            <mb>DataReference URI=""/>
          </mb:MetadataBinding>
        </mb:MetadataBindingContainer>
      </mb:BindingInformation>
    </xsd:appinfo>
  </xsd:annotation>
  <xsd:simpleType name="exampleType">
    <xsd:restriction base="xsd:string">
```

```

<xsd:minLength value="1"/>
</xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Figure 12-1 Example XML Schema Metadata Binding

12.7. Schematron Structure

The Schematron (<https://www.w3.org/2007/schema-for-xslt20> xsd) allows any element from a different schema to be included within the top-level element of the schematron. The Binding Information can thus be included within the `sch:schema` element.

As such, the Binding Information SHALL be represented as an Embedded BDO. A BDO SHALL be embedded within the Schematron as a child `mb:BindingInformation` element of the top-level `sch:schema` element. (XPath: `/sch:schema/mb:BindingInformation`).

A BDO SHALL NOT be embedded in any other location within the Schematron. Multiple BDOs MAY be embedded as child `mb:BindingInformation` elements of the top level `sch:schema` element.

It is RECOMMENDED that the `mb:BindingInformation` elements be placed at the start of the stylesheet, as the first child element of the `sch:schema` element.

It is RECOMMENDED that metadata is contained within the `Metadata` child element of the `MetadataBinding` element; not referenced with the use of the `MetadataReference` element.

One or more `DataReference` elements SHALL be present in a `MetadataBinding` element containing a `URI` attribute in order to locate the data (and subsets thereof) that is contained in the `sch:schema` top-level element.

An example of an BDO embedded in an Schematron that illustrates the binding of the data, contained in the parent `sch:schema` element, to metadata is provided in Figure 12-2. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```

<sch:schema xmlns:sch="http://purl.oclc.org/dsdl/schematron">
  <mb:BindingInformation xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
    <mb:MetadataBindingContainer>
      <mb:MetadataBinding>
        <mb:Metadata>
          <slab:originatorConfidentialityLabel
            xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">

```

```

    <slab:ConfidentialityInformation>
      <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
      <slab:Classification>GENERAL</slab:Classification>
    </slab:ConfidentialityInformation>
    <slab:CreationDateTime>2016-11-20T12:30:00Z</slab:CreationDateTime>
  </slab:originatorConfidentialityLabel>
</mb:Metadata>
  <mb:DataReference URI=""/>
</mb:MetadataBinding>
</mb:MetadataBindingContainer>
</mb:BindingInformation>
<sch:title>Example Schematron</sch:title>
<sch:rule context="example">
  <sch:assert test="@example">Example</sch:assert>
</sch:rule>
</sch:schema>

```

Figure 12-2 Example XML Schematron Metadata Binding

12.8. XML Stylesheet Structure

The XML Stylesheet (https://www.w3.org/2007/schema-for-xslt20_xsd) allows any element from a different schema to be included within the top-level element of the XML stylesheet, after any `xsl:import` elements. The Binding Information can thus be included within the `xsl:stylesheet` element.

As such, the Binding Information SHALL be represented as an Embedded BDO. A BDO SHALL be embedded within the XML Stylesheet as a child *mb:BindingInformation* element of the top-level `xsl:stylesheet` element. (XPath: `/xsl:stylesheet/mb:BindingInformation`).

A BDO SHALL NOT be embedded in any other location within the XML Stylesheet. Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of the top level `xsl:stylesheet` element.

It is RECOMMENDED that the *mb:BindingInformation* elements be placed at the start of the stylesheet, immediately after the `xsl:import` elements, if present.

It is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

One or more *DataReference* elements SHALL be present in a *MetadataBinding* element containing a *URI* attribute in order to locate the data (and subsets thereof) that is contained in the `xsl:stylesheet` top-level element.

An example of an BDO embedded in an XML Stylesheet that illustrates the binding of the data, contained in the parent `xsl:stylesheet` element, to metadata is provided in Figure 12-3. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:import href="example.xsl"/>
  <mb:BindingInformation xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
    <mb:MetadataBindingContainer>
      <mb:MetadataBinding>
        <mb:Metadata>
          <slab:originatorConfidentialityLabel
            xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
            <slab:ConfidentialityInformation>
              <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
              <slab:Classification>GENERAL</slab:Classification>
            </slab:ConfidentialityInformation>
            <slab:CreationDateTime>2016-11-20T12:30:00Z</slab:CreationDateTime>
          </slab:originatorConfidentialityLabel>
        </mb:Metadata>
        <mb:DataReference URI=""/>
      </mb:MetadataBinding>
    </mb:MetadataBindingContainer>
  </mb:BindingInformation>
  <xsl:output method="text"/>
  <xsl:template match="/">
    <xsl:text>Example</xsl:text>
  </xsl:template>
</xsl:stylesheet>
```

Figure 12-3 Example XML Stylesheet Metadata Binding

12.9. Generic Codelist Structure

The Generic Code List (<https://docs.oasis-open.org/codelist/cs-genericcode-1.0/xsd/genericcode.xsd>) contains an `Annotation` element which allows for both human readable and machine-processible, inline, documentation to be provided for any element within the schema. The `Annotation` element has a child element, `AppInfo`, which allows any well-formed XML content to be included within the annotation. The Binding Information can thus be included within the `AppInfo` element. As such, the Binding Information SHALL be represented as an Embedded BDO.

A BDO SHALL be embedded within the `GenericCodeCodeList` as a child `mb:BindingInformation` of the `AppInfo` element of the `Annotation` element(s) of the top-level `gc:CodeList` element.

(XPath: /gc:CodeList /Annotation/AppInfo/mb:BindingInformation). A BDO SHALL NOT be embedded in any other location within the Genericcode Code List.

Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of a single *AppInfo* element.

Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of distinct *AppInfo* elements.

It is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

One or more *DataReference* elements SHALL be present in a *MetadataBinding* element containing a *URI* attribute in order to locate the data (and subsets thereof) that is contained in the *gc:CodeList* top-level element.

An example of an BDO embedded in a Genericcode CodeList that illustrates the binding of the data, contained in the parent *gc:CodeList* element, to metadata is provided in Figure 12-4. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```
<gc:CodeList xmlns:gc=" http://docs.oasis-open.org/codelist/ns/genericcode/1.0/"
  <Annotation>
    <AppInfo>
      <mb:BindingInformation
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                <slab:ConfidentialityInformation>
                  <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                  <slab:Classification>GENERAL</slab:Classification>
                </slab:ConfidentialityInformation>
                <slab:CreationDateTime>2016-11-
20T12:30:00Z</slab:CreationDateTime>
              </slab:originatorConfidentialityLabel>
            </mb:Metadata>
            <mb:DataReference URI=""/>
          </mb:MetadataBinding>
        </mb:MetadataBindingContainer>
      </mb:BindingInformation>
    </AppInfo>
```

```

</Annotation>
<Identification>
  <ShortName>example</ShortName>
</Identification>
<ColumnSet>
  <Column id="id">
    <ShortName>ID</ShortName>
    <Data Type="xsd:string"/>
  </Column>
  <Column id="price">
    <ShortName>Price</ShortName>
    <Data Type="xsd:string"/>
  </Column>
</ColumnSet>
<SimpleCodeList>
  <Row>
    <Value ColumnRef="id"><SimpleValue>1</SimpleValue></Value>
    <Value ColumnRef="price"><SimpleValue>100</SimpleValue></Value>
  </Row>
</SimpleCodeList>
</gc:CodeList>

```

Figure 12-4 Example XML Genericcode Metadata Binding

12.10. Context/Value Association Structure

The Context/Value Association (Reference [10]) contains an `cva:Annotation` element which allows for both human readable and machine-processible, inline, documentation to be provided for any element within the schema. The `cva:Annotation` element has a child element, `cva:AppInfo`, which allows any well-formed XML content to be included within the annotation. The Binding Information can thus be included within the `cva:AppInfo` element. As such, the Binding Information SHALL be represented as an Embedded BDO.

A BDO SHALL be embedded within the Context/Value Association as a child *mb:BindingInformation* of the `cva:AppInfo` element of the `cva:Annotation` element(s) of the top-level `cva:ContextValueAssociation` element.

(XPath: `/cva:ContextValueAssociation/cva:Annotation/cva:AppInfo/mb:BindingInformation`).

A BDO SHALL NOT be embedded in any other location within the Context/Value Association.

Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of a single `cva:AppInfo` element.

Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of distinct *cva:AppInfo* elements.

It is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

One or more *DataReference* elements SHALL be present in a *MetadataBinding* element containing a *URI* attribute in order to locate the data (and subsets thereof) that is contained in the *cva:ContextValueAssociation* top-level element.

An example of an BDO embedded in a Context/Value Association that illustrates the binding of the data, contained in the parent *cva:ContextValueAssociation* element, to metadata is provided in Figure 12-5. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```
<cva:ContextValueAssociation
  xmlns:cva="http://docs.oasis-
open.org/codelist/ns/ContextValueAssociation/1.0/"
  name="exampleCVA" version="1.0">
  <cva:Annotation>
    <cva:AppInfo>
      <mb:BindingInformation
xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0">
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
                <slab:ConfidentialityInformation>
                  <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
                  <slab:Classification>GENERAL</slab:Classification>
                </slab:ConfidentialityInformation>
                <slab:CreationDateTime>2016-11-
20T12:30:00Z</slab:CreationDateTime>
              </slab:originatorConfidentialityLabel>
            </mb:Metadata>
            <mb>DataReference URI=""/>
          </mb:MetadataBinding>
        </mb:MetadataBindingContainer>
      </mb:BindingInformation>
    </cva:AppInfo>
  </cva:Annotation>
  <cva:Title>Example CVA</cva:Title>
  <cva:ValueLists>
```

```

    <cva:ValueList xml:id="exampleCodes-v1" uri="CodeLists/exampleCode-
v1.gc"/>
  </cva:ValueLists>
  <cva:Contexts>
    <cva:Context address="example" values="exampleCode-v1" />
  </cva:Contexts>
</cva:ContextValueAssociation>

```

Figure 12-5 Example XML Context/Value Association Metadata Binding

12.11. Security Policy Information File Structure

The Security Policy Information File

(<http://www.xmlspif.org/schema/xmlspif.xsd>) contains an `spif:extensions` element which allows for arbitrary extensions to be included within the SPIF.

The Binding Information can thus be included within the `spif:extensions` element. As such, the Binding Information SHALL be represented as an Embedded BDO.

A BDO SHALL be embedded within the SPIF as a child *mb:BindingInformation* of the `spif:extensions` element of the top-level `spif:SPIF` element.

(XPath: `/spif:SPIF/spif:extensions/mb:BindingInformation`).

A BDO SHALL NOT be embedded in any other location within the SPIF.

Multiple BDOs MAY be embedded as child *mb:BindingInformation* elements of a single `spif:extensions` element.

It is RECOMMENDED that metadata is contained within the *Metadata* child element of the *MetadataBinding* element; not referenced with the use of the *MetadataReference* element.

One or more *DataReference* elements SHALL be present in a *MetadataBinding* element containing a *URI* attribute in order to locate the data (and subsets thereof) that is contained in the `spif:SPIF` top-level element.

An example of an BDO embedded in a SPIF that illustrates the binding of the data, contained in the parent `spif:SPIF` element, to metadata is provided in Figure 12-6. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```

<spif:SPIF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:spif="http://www.xmlspif.org/spif"
  schemaVersion="1.0" version="1" creationDate="20170330150423Z"
  originatorDN="CN=SPIF ADMIN,O=SMHS Ltd,C=GB"
  keyIdentifier="6AA4BA9F66BFCD44"

```

```

privilegeId="1.3.6.1.4.1.31778.110.110"
rbacId="1.3.6.1.4.1.31778.110.110">
<spif:securityPolicyId name="TEST Amoco" id="1.2.840.113549.1.9.16.7.1" />
<spif:securityClassifications>
  <spif:securityClassification name="GENERAL" lacv="6" hierarchy="6">
    <spif:markingData xml:lang="fr" phrase="GÉNÉRAL">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="CONFIDENTIAL" lacv="7" hierarchy="7">
    <spif:markingData xml:lang="fr" phrase="CONFIDENTIEL">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="HIGHLY CONFIDENTIAL" lacv="8"
hierarchy="10">
    <spif:markingData xml:lang="fr" phrase="TRÈS CONFIDENTIEL">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
</spif:securityClassifications>
<spif:extensions>
  <BindingInformation xmlns="urn:nato:stanag:4778:bindinginformation:1:0">
    <MetadataBindingContainer>
      <MetadataBinding xml:id="id-4ec8e07f-2336-4ee0-af34-1e7f15f946ea">
        <Metadata xml:id="id-d3e4fa3b-4318-4a65-9eba-53341c3fb92d">
          <slab:originatorConfidentialityLabel
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
xmlns:slab-ext="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:ext">
            <slab:ConfidentialityInformation>
              <slab:PolicyIdentifier>TEST Amoco</slab:PolicyIdentifier>
              <slab:Classification>GENERAL</slab:Classification>
              <slab-ext:Marking xml:lang="en">TEST Amoco GENERAL</slab-
ext:Marking>
            </slab:ConfidentialityInformation>
            <slab:CreationDateTime>2015-09-
30T12:30:00Z</slab:CreationDateTime>
          </slab:originatorConfidentialityLabel>
        </Metadata>
        <DataReference URI="" />
      </MetadataBinding>
    </MetadataBindingContainer>
  </BindingInformation>
</spif:extensions>
</spif:SPIF>

```

Figure 12-6 Example XML SPIF Metadata Binding

12.12. Cryptographic Artefacts Profile

The Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) SHALL be adhered to for the use cases that cryptographic bindings are required to provide a higher level of integrity protection, authenticity and non-repudiation of the binding specified in this profile.

Unless otherwise stated, all statements that apply to the Cryptographic Artefacts binding profile (Chapter 2 Annexes A, B and C XML Signature Binding Profile) also apply to this profile for generating and validating cryptographic bindings.

It is RECOMMENDED that the requirements specified in Cryptographic Artefacts binding profile (Chapter 2 Annex A) URI Schemes are adhered to.

INTENTIONALLY BLANK

ADatP-4778.2(A)(1)



**LOGFAS INTERFACE CONTROL DOCUMENT
ANNEX - A**

Effective date: 1-Apr-23
Version No: 8.0.0
Issued by: APP041 - Logistics Functional Area Services (LOGFAS) Application Services

1 Contents

1 Contents..... 2













2 Item List of Referenced ICD Materials 3

3 LOGFAS Interface Overview 5




2 Item List of Referenced ICD Materials

This list contains embedded documents referenced in the main Interface Control Document to use as reference or as example for LOGFAS related functions. The .zip files contain many files pertaining to a central topic. Use of this table is best when referred to side-by-side with the main document. The items are not listed in order of reference.

In Word, double-click on the file icon to open the material. You may have to choose 'Enable Content' to allow the content to open.

Item	Link	Topic/Description	ICD Section
1.	 ModificationFile_v2.xsd	Reference Data	4.1.1
2.	 2018_03 Schema and Examples.zip	FAS Interoperability XML Interface Version 2018/03 Schema and Examples	6.1.1.3
3.	 FASInterop 2022_07.zip	FAS Interoperability XML Interface Version 2022/07 Schema and examples	6.1.1.3
4.	 LOGFAS7_NativeXML.zip	LOGFAS 7 Native XML Interface Schemas & Examples	6.1.3.3
5.	 LOGFAS8_NativeXML.zip	LOGFAS 8 Native XML Interface schemas and examples	6.1.4
6.	 NVG.zip	NVG 1.4, 1.5, and 2.0 WSDL reference, schemas and examples	6.1.5.3-4
7.	 MRFSservice.zip	Mission Request Form (MRF) Service web service WSDL reference, schemas and examples	6.1.6.3-5
8.	 MissionSummary.zip	Mission Summary web service WSDL reference, schema and examples	6.1.7.3-4
9.	 LDM_Excel_Interfaces.zip	MS Excel interface template and example for LDM	6.1.8.4
10.	 EVE_Excel_Interfaces.zip	MS Excel interface template and example for EVE	6.1.9.4
11.	 HNS_CAPCAT_Template.xlsx	HNS CAPCAT Template	6.1.10.3
12.	 HNSCor_Bel_DNK.zip	HNS COR non-schema based example	6.1.11.3

LOGFAS Interface Control Document Annex A

13.	 ICC.zip	LOGFAS/ICC Interoperability example	6.2.4.4
14.	 TOPFAS JTAL.txt	LOGFAS/TOPFAS Interoperability in TFE example	6.2.10.4
15.	 USSMS.zip	LOGFAS/USSMS Interoperability example	6.2.11.4

LOGFAS Interface Control Document Annex A

3 LOGFAS Interface Overview

8 Sep 2021 v1.4

