    - The rules for data sanitization based on the use of a granular binding;
    - Whether or not a confidentiality metadata label and associated binding information for *DO* shall be removed before release of *DO*.
    - Whether or not a confidentiality metadata label and associated binding information for *DO* shall be regenerated based on the sanitization of *DO*.
- Whether or not the WG shall sign the released content.
- The text string 'SANITIZED_STRING' which will be added to the filename of sanitized files.
- The format of the date variable 'TIMESTAMP' based on RFC 3339 [IETF RFC 3339, 2002].

Requirement ID: [SRS-6-501]

The policy WG_CIP_LH_MD SHALL specify the actions ACTIONS-LH_MD that need to be performed by WG_CIS_MD.

Requirement ID: [SRS-6-502]

ACTIONS-LH_MD SHALL include the following actions based on RULESET_WG_CIS_MD:

- Identify;
- Verify;
- Transform;
- Block;
- Quarantine,

as specified in the NATO CIPE functional specification in [NC3A TN-1486, 2012].

Requirement ID: [SRS-6-503]

ACTIONS-LH_MD SHALL include the action to exclude an HTTP Message from policy enforcement by WG_CIS_MD based on RULESET_WG_CIS_MD.

Requirement ID: [SRS-6-504]

WG_CIP_LH_MD SHALL specify RULESET_WG_CIS_MD.

Requirement ID: [SRS-6-505]

RULESET_WG_CIS_MD SHALL be configurable.

Requirement ID: [SRS-6-506]

RULESET_WG_CIS_MD SHALL specify:

- A default scan rule that ensures all HTTP Messages are scanned for known malware;

- Whitelist of values for the information attributes in [SRS-6-510] for which an HTTP Message can be excluded from malware scanning;
- Whitelist of information flow characteristics for which HTTP Messages belonging to that information flow can be excluded from malware scanning. These characteristics SHALL include:
    - Source and destination IP-address of the information flow.

6.6 Protection Services

6.6.1 Content Inspection Services

Requirement ID: [SRS-6-190]

The WG MUST provide a content inspection services (CIS) capability WG_CIS that enables WG_CIPE to identify, verify and transform content based on the content inspection policy WG_CIP.

Requirement ID: [SRS-6-191]

For the identification, verification and transformation of content based on WG_CIP, WG_CIS SHALL provide a content-filter capability as specified in the NATO CIPE functional specification in [NC3A TN-1486, 2012].

Requirement ID: [SRS-6-192]

WG_CIS SHALL support the message syntax of HTTP messages as defined in Hypertext Transfer Protocol - HTTP/1.1 [IETF RFC 7230, 2014].

Requirement ID: [SRS-6-507]

WG_CIS SHALL support the message syntax of HTTP messages as defined in Hypertext Transfer Protocol - HTTP/2 [IETF RFC 7540, 2014].

Requirement ID: [SRS-6-193]

WG_CIS SHALL support XML 1.0 [W3C XML, 2006].

Requirement ID: [SRS-6-194]

WG_CIS SHALL support the XML Schema Language 1.0 [W3C XML Schema 1, 2004], [W3C XML Schema 2, 2004].

Requirement ID: [SRS-6-195]

WG_CIS SHALL support Canonical XML Version 1.1 [W3X Canonical XML 1.1, 2008].

Requirement ID: [SRS-6-196]

WG_CIS SHALL support XML Path Language (XPath) Version 1.0 [W3C XML Path Language 1.0, 1999].

Requirement ID: [SRS-6-197]

WG_CIS SHALL support XML Pointer Language (XPointer) [W3C XPointer, 2002].

Requirement ID: [SRS-6-198]

WG_CIS MUST offer an interface 'Content Inspection Services' that serves as a communication mechanism between the content filters and WG_CIPE.

Requirement ID: [SRS-6-199]

The interface 'Content Inspection Services' MUST support an operation 'Initialize' that initializes a content filter.

Requirement ID: [SRS-6-200]

The operation 'Initialize' MUST support the identification of a content filter based on a content filter identifier CIPE_CF_ID.

Requirement ID: [SRS-6-201]

The interface 'Content Inspection Services' MUST support an operation 'Filter' that executes a content filter.

Requirement ID: [SRS-6-202]

The operation 'Filter' SHALL accept as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA.

Requirement ID: [SRS-6-203]

The interface 'Content Inspection Services' MUST support an operation 'Halt' that halts a content filter.

Requirement ID: [SRS-6-204]

The operation 'Halt' MUST support the identification of a content filter based on a content filter identifier CIPE_CF_ID.

Requirement ID: [SRS-6-205]

WG_CIS SHALL inform WG_CIPE of the outcome O_WG_CIS of the execution of an action in ACTIONS ([SRS-6-158]).

Requirement ID: [SRS-6-206]

If the outcome O_WG_CIS is negative (e.g. verification or validation fails), WG_CIS SHALL interpret O_WG_CIS as a policy violation and inform WG_CIPE according to WG_CIP ([SRS-6-163]).

Requirement ID: [SRS-6-207]

WG_CIS SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_CIS ([SRS-6-115]).

Requirement ID: [SRS-6-508]

WG_CIS SHALL provide a malware detection capability WG_CIS_MD that comprises the content filters that are executed in order to enforce the policy WG_CIP_LH_MD.

Requirement ID: [SRS-6-509]

WG_CIS_MD SHALL be able to identify known malware in the contents of an HTTP Message (headers and body) and enforce WG_CIP_LH_MD on the HTTP Message.

Requirement ID: [SRS-6-510]

WG_CIS_MD SHALL enforce WG_CIP_LH_MD based on the following types of information attributes in the HTTP message header:

- Start-line:
  - Method;
  - Request-URI;
  - HTTP-version;
  - Status-code.
- Message-header:
  - Field-name;
  - Field-value.

Requirement ID: [SRS-6-511]

WG_CIS_MD SHALL be able to verify the information attributes in [SRS-6-510] against the rulesets RULESET_WG_CIS_MD.

Requirement ID: [SRS-6-512]

WG_CIS_MD SHALL use a malware/virus scanner which is approved for use in the NATO Enterprise.

Requirement ID: [SRS-6-513]

The management of WG_CIS_MD, including the process of updating malware signatures, SHALL integrate with the NCI Agency management solution of existing malware detection solutions in the NATO Enterprise.

Requirement ID: [SRS-6-514]

WG_CIS_MD SHALL support the migration of the configuration of existing malware detection solutions in the NATO Enterprise, to the WG.

Requirement ID: [SRS-6-208]

WG_CIS SHALL provide an XML schema validation capability WG_CIS_SV that comprises the content filters that are executed in order to enforce the policy WG_CIP_LH_SV.

Requirement ID: [SRS-6-209]

WG_CIS_SV SHALL enforce WG_CIP_LH_SV based on the contents of the HTTP Message body.

Requirement ID: [SRS-6-210]

WG_CIS_SV SHALL be able to check the body of an HTTP message for XML well-formedness.

Requirement ID: [SRS-6-211]

WG_CIS_SV SHALL be able to validate the body of an HTTP message against a list LIST_WG_CIS_SV-XS of W3C XML Schemas (defined in the policy WG_CIP_LH_SV).

Requirement ID: [SRS-6-212]

WG_CIS_SV SHALL be able to check that the namespace of the root node in the HTTP message body belongs to a list of namespaces LIST_WG_CIS_SV-NS (defined in the policy WG_CIP_LH_SV).

Requirement ID: [SRS-6-213]

WG_CIS SHALL provide an HTTP header vetting capability WG_CIS_HV that comprises the filters that are executed in order to enforce the policies WG_CIP_HL_HV and WG_CIP_LH_HV.

Requirement ID: [SRS-6-214]

WG_CIS_HV SHALL enforce WG_CIP_LH_HV and WG_CIP_HL_HV based on the following types of information attributes in the HTTP message header:

- Start-line:
  - Method;
  - Request-URI;
  - HTTP-version;
  - Status-code.
- Message-header:
  - Field-name;
  - Field-value.

Requirement ID: [SRS-6-215]

WG_CIS_HV SHALL be able to verify the information attributes in [SRS-6-214] against the rulesets RULESET_WG_CIS_HV-HL and RULESET_WG_CIS_HV-LH (specified in the policies WG_CIP_HL_HV and WG_CIP_LH_HV respectively).

Requirement ID: [SRS-6-216]

WG_CIS_HV SHALL be able to add, remove or rewrite entire header lines of an HTTP message.

Requirement ID: [SRS-6-217]

WG_CIS_HV SHALL be able to add, remove or rewrite values of the information attributes in [SRS-6-214].

Requirement ID: [SRS-6-218]

WG_CIS_HV SHALL be able to normalize URIs in header lines of an HTTP message (i.e. remove all unneeded or escaped characters from a URI and ensure sure all characters that require escaping are escaped).

Requirement ID: [SRS-6-219]

WG_CIS MUST provide a label validation capability WG_CIS_LV that comprises the content filters that are executed in order to enforce the policy WG_CIP_HL_LV.

Requirement ID: [SRS-6-220]

WG_CIS_LV MUST support the NATO standard ADatP-4774 "Confidentiality Metadata Label Syntax" [STANAG 4774].

Requirement ID: [SRS-6-221]

WG_CIS_LV MUST support the NATO standard and ADatP-4778 "Metadata Binding Mechanism" [STANAG 4778].

Requirement ID: [SRS-6-222]

WG_CIS_LV MUST support the binding approaches 'encapsulating' and 'embedded' as defined in [STANAG 4778].

Requirement ID: [SRS-6-223]

WG_CIS_LV MAY support the binding approach 'detached' as defined in [STANAG 4778].

Requirement ID: [SRS-6-224]

WG_CIS_LV MUST support the binding profile "Simple Object Access Protocol (SOAP) Binding Profile" in [STANAG 4778 SRD.2].

Requirement ID: [SRS-6-225]

WG_CIS_LV MUST support the binding profile "Representational State Transfer (REST) Profile" in [STANAG 4778 SRD.2].

Requirement ID: [SRS-6-226]

WG_CIS_LV MUST support the binding profile "XML Signature Cryptographic Artefact Profile" in [STANAG 4778 SRD.2].

Requirement ID: [SRS-6-227]

WG_CIS_LV MUST support the binding profile "Digital Signature Cryptographic Artefact Profile" in [STANAG 4778 SRD.2].

Requirement ID: [SRS-6-228]

WG_CIS_LV MUST support the binding profile "Keyed-Hash Message Authentication Code Cryptographic Artefact Profile" in [STANAG 4778 SRD.2].

Requirement ID: [SRS-6-229]

WG_CIS_LV SHALL be able to validate a digital signature by invoking the operation 'Verify' (6.6.2.2.3) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-230]

WG_CIS_LV SHALL be able to perform the validation of XML against a list LIST_WG_CIS_LV-XS of W3C XML Schemas (defined in the policy WG_CIP_HL_LV).

Requirement ID: [SRS-6-231]

For a given child element *CE*, CIS_LV SHALL be able to match the value of *CE* and the values of attributes of *CE* against a list of values.

Requirement ID: [SRS-6-232]

For a given HTTP message, WG_CIS_LV SHALL be able to evaluate the bindings in the HTTP message body *HB* and identify the set of data objects *S* in *HB* (or referenced in *HB*) that are labelled (i.e. for each data object *DO* in *S* there is a confidentiality metadata label *CL* that is bound to *DO*).

Requirement ID: [SRS-6-233]

For a confidentiality metadata label *CL* that is bound to a data object *DO*, WG_CIS_LV SHALL be able to associate the following information attributes in *CL* (see [STANAG 4774]) with *DO*:

- Policy identifier;
- Classification;
- Categories.

Requirement ID: [SRS-6-234]

WG_CIS_LV SHALL be able to verify the values of the information attributes in ([SRS-6-233]) against a metadata policy information file MPIF_NATO.

Requirement ID: [SRS-6-235]

WG_CIS_LV SHALL enforce the ruleset RULESET_WG_CIS_LV (specified in the policy WG_CIP_HL_LV) based on the information attributes in ([SRS-6-233]).

Requirement ID: [SRS-6-236]

WG_CIS_LV MAY support the sanitization of data based on RULESET_WG_CIS_LV.

Requirement ID: [SRS-6-237]

WG_CIS_LV SHALL be able to apply XML canonicalization to a data object.

Requirement ID: [SRS-6-238]

WG_CIS_LV SHALL be able to generate a digital signature by invoking the operation 'Sign' (6.6.2.2.2) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

6.6.2 Public Key Cryptographic Services

6.6.2.1 WG_PKCS

Requirement ID: [SRS-6-239]

WG MUST provide a capability WG_PKCS that enables the WG to perform cryptographic operations and key management.

Requirement ID: [SRS-6-240]

WG_PKCS SHALL conform to the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms [NAC AC/322-D/0047-REV2 (INV), 2009].

Requirement ID: [SRS-6-241]

The cryptographic mechanisms implemented by WG_PKCS SHALL be based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].

Requirement ID: [SRS-6-372]

WG_PKCS SHALL support the use Simple Certificate Enrolment Protocol (SCEP) [IETF RFC 8894, 2020] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.

Requirement ID: [SRS-6-373]

WG_PKCS SHOULD support the use of Enrolment over Secure Transport (EST) [IETF RFC 7030, 2013] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.

6.6.2.2 Public Key Cryptographic Services

Requirement ID: [SRS-6-242]

WG_PKCS MUST offer an interface 'Public Key Cryptographic Services' that supports the following cryptographic operations:

- Sign (6.6.2.2.2);
- Verify (6.6.2.2.3);
- Encrypt (6.6.2.2.4);
- Decrypt (6.6.2.2.5).

Requirement ID: [SRS-6-243]

For every action taken, the operations 'Sign', 'Verify', 'Encrypt' and 'Decrypt' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log both the action and the result of the action.

6.6.2.2.1 Sign

Requirement ID: [SRS-6-244]

The operation 'Sign' MUST support:

- The generation of cryptographic bindings according to ‘Cryptographic Artefact Binding Profiles’ [STANAG 4778 SRD.2].
- The generation of XML digital signatures based on XMLDSIG Core Generation [W3C XMLDSIG-CORE, 2008];
- The generation of key-hashed message authentication code (HMAC, [IETF RFC 2104, 1997]) conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]);
- The generation of cryptographic digest values in accordance with a specified cryptographic algorithm: the Secure Hash Algorithm (SHA) [NIST FIPS-180-3, 2008] and lengths of cryptographic digest values of 160 bits, 256 bits, or 384 bits that meet the following:
  - Requirements defined in the “CIS Security Technical And Implementation Directive On The NATO PKI Certificate Policy” [NAC AC/322-D(2004)0024-REV3-COR1, 2018] and [NAC AC/322-D(2007)0002-REV1, 2015]
  - The XML Signature Syntax and Processing standard (Second Edition) [W3C XMLDSIG-CORE, 2008].

6.6.2.2.2 Verify

Requirement ID: [SRS-6-245]

The operation 'Verify':

- MUST support the validation of XML digital signatures based on XMLDSIG Core Validation [W3C XMLDSIG-CORE, 2008];
- MUST support validation of XML digital signatures in accordance with a specified cryptographic algorithm: the Rivest Shamir Adleman (RSA) algorithm [RSA PKCS#1, 2002] and cryptographic key sizes of 2048 bits that meet the following:
  - Requirements defined in the CIS Security Technical And Implementation Directive On The NATO PKI Certificate Policy [NAC AC/322-D(2004)0024-REV3-COR1, 2018] and [NAC AC/322-D(2007)0002-REV1, 2015]
  - The XML Signature Syntax and Processing standard (Second Edition) [W3C XMLDsig-2nd-Ed, 2008].
- MUST support signatures of the types XMLDSIG ‘enveloping’ and ‘enveloped’.

- MAY support signatures of the type XMLDSIG ‘detached’.
- MUST support the validation and of cryptographic bindings according to ‘Cryptographic Artefact Binding Profiles’ [STANAG 4778 SRD.2].

6.6.2.2.3 Encrypt

Requirement ID: [SRS-6-246]

The operation 'Encrypt' MUST support encryption of data conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

6.6.2.2.4 Decrypt

Requirement ID: [SRS-6-247]

The operation 'Decrypt' MUST support decryption of data conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

6.7 Element Management Services

6.7.1 WG_MGMT

Requirement ID: [SRS-6-248]

The WG MUST provide a management capability WG_MGMT that supports local and remote management of the WG.

6.7.2 WG_IF_LOCAL_MGMT

Requirement ID: [SRS-6-249]

For local management, WG_MGMT MUST offer an interface WG_IF_LOCAL_MGMT consisting of a directly attached keyboard and display console.

Requirement ID: [SRS-6-250]

WG_IF_LOCAL_MGMT SHALL support the invocation of the operations at the interfaces 'CIS Security' ([SRS-6-270]), 'SMC Configuration Management' ([SRS-6-288]) and 'Cyber Defence' (6.7.6.2).

6.7.3 WG_MGMT_AM

Requirement ID: [SRS-6-251]

WG_MGMT MUST provide a capability WG_MGMT_AM that allows Audit Administrators to fulfil their role.

Requirement ID: [SRS-6-252]

WG_MGMT_AM MUST be interoperable with NATO auditing and system management tools.

Requirement ID: [SRS-6-253]

WG_MGMT_AM SHALL provide the capability to detect and create records of security-relevant events associated with users.

Requirement ID: [SRS-6-254]

WG_MGMT_AM SHALL provide the capability to detect and create records of security-relevant events associated with end users requests for accessing information cross domain.

Requirement ID: [SRS-6-255]

WG_MGMT_AM SHALL provide the capability to appropriately classify and protect audit information in accordance with NATO security policy.

Requirement ID: [SRS-6-256]

WG_MGMT_AM SHALL provide mechanisms to protect audit logs from unauthorised access, modification and deletion.

Requirement ID: [SRS-6-257]

WG_MGMT_AM SHALL provide the capability to selectively view audit information, and alert the Audit Administrator of identified potential security violations.

Requirement ID: [SRS-6-258]

WG_MGMT_AM SHALL provide reliable time stamps and the capability for the Audit Administrator to set the time used for these time stamps.

Requirement ID: [SRS-6-259]

WG_MGMT_AM SHALL support the generation of an audit log for each of the following general auditable events:

- WG start-up and shutdown;
- WG Users logon and logoff;
- Creation, modification (i.e. changes to permissions) or deletion of user accounts;
- Changes to security related system management functions;
- Audit log access;
- Invocation of privileged operations;
- Modification to WG access rights;
- Unauthorised attempts to access WG system files;
- All modified objects are recorded with date, time, details of change and user.

Requirement ID: [SRS-6-260]

WG_MGMT_AM SHALL support the generation of an audit log for each of the following Data Exchange Services auditable events:

- Data Exchange Services start-up and shutdown;

- Unauthorised attempts to request access to information cross domain;
- Unauthorised attempts to modify Data Exchange Services configuration;
- Failed Data Exchange Services operations.

Requirement ID: [SRS-6-261]

WG_MGMT_AM SHALL support the generation of an audit log for each of the following Protection Services auditable events:

- Protection Services start-up and shutdown;
- Failed Protection Services operations;
- Unauthorised attempts to modify Protection Services configuration;
- Creation, modification and deletion of Public Key Cryptographic Services keying material;
- Updates of Content Inspection Services content filters;
- Failed certificate path validation and revocation.

Requirement ID: [SRS-6-262]

WG_MGMT_AM SHALL support the generation of an audit log for each of the following Protection Policy Enforcement Services auditable events:

- Protection Policy Enforcement Services start-up and shutdown;
- Failed Protection Policy Enforcement Services operations;
- Unauthorised attempts to create, modify or delete Information Flow Control policies;
- Unauthorised attempts to create, modify or delete Content Inspection policies.

Requirement ID: [SRS-6-263]

WG_MGMT_AM SHALL support the archiving of the audit log after a period of time as configured by the Audit Administrator.

Requirement ID: [SRS-6-264]

WG_MGMT_AM SHALL by default archive the audit log daily.

Requirement ID: [SRS-6-265]

WG_MGMT_AM SHALL automatically back up audit logs at configurable intervals.

Requirement ID: [SRS-6-266]

WG_MGMT_AM SHALL provide the capability, including integrity checking, to verify that the audit log has been archived correctly.

Requirement ID: [SRS-6-267]

WG_MGMT_AM SHALL provide the capability to alert the Audit Administrator when the audit log exceeds a configurable percentage of the configurable maximum permitted size.

Requirement ID: [SRS-6-268]

WG_MGMT_AM SHALL by default set the configurable percentage to 90% of the configurable maximum permitted size.

6.7.4 WG_MGMT_CS

Requirement ID: [SRS-6-269]

WG_MGMT MUST provide a capability WG_MGMT_CS that allows for the management of CIS Security information specific to the WG.

Requirement ID: [SRS-6-270]

WG_MGMT_CS MUST support the retrieval of key material, certificates and CRLs from locations external to the WG.

Requirement ID: [SRS-6-271]

WG_MGMT_CS MUST support one or more of the following protocols and associated CIS Security Messages for the retrieval of key material, certificates and CRLs:

- Secure LDAP (LDAPS) [IETF RFC 4510 – 4519, 2006];
- HTTP(S) ([IETF RFC 7230, 2014], [IETF RFC 7540, 2015]. [IETF RFC 8446, 2018], [IETF RFC 2818, 2000];
- SOAP ([W3C SOAP 1.1, 2000] and [W3C SOAP 1.2, 2007]).

Requirement ID: [SRS-6-272]

WG_MGMT_CS SHALL check the status or certificates against CRLs in accordance with the NPKI Certificate Policy [NAC AC/322-D(2004)0024-REV3-COR1, 2018].

Requirement ID: [SRS-6-273]

WG_MGMT_CS MAY support remote checking of the status of certificates using the Online Certificate Status protocol (OCSP) [IETF RFC 6960, 2013].

Requirement ID: [SRS-6-274]

WG_MGMT_CS MUST support automated execution of the following actions:

- Updating of certificates;
- Updating of CRLs;

Requirement ID: [SRS-6-275]

WG_MGMT_CS MUST support scheduling of each operation in [SRS-6-274] such that:

- The operation will be executed at a configurable date and time, with:

    - date expressed in years, month and day;
    - time expressed in hours and minutes.
- When starting at a configurable date and time, the operation will be executed at a configurable regular time interval expressed in days, weeks or months.

Requirement ID: [SRS-6-276]

WG_MGMT_CS SHALL pass outgoing CIS Security Messages to the interface 'Core Services Management' (6.4.5.1) for further processing.

6.7.4.1 CIS Security

Requirement ID: [SRS-6-277]

WG_MGMT_CS MUST offer an interface 'CIS Security' that accepts an incoming 'CIS Security Message' for further processing.

6.7.4.1.1 Manage Protection Policies

Requirement ID: [SRS-6-278]

The interface 'CIS Security' MUST support an operation 'Manage Protection Policies' that provides the capability to manage the lifecycle of the IFPs and CIPs in support of WG_IFCPE ([SRS-6-70]) and WG_CIPE (6.5.3.1) respectively.

Requirement ID: [SRS-6-279]

The operation 'Manage Protection Policies' SHALL support the following actions:

- Create policy;
- Read policy;
- Update policy;
- Delete policy;
- Activate policy;
- De-activate policy;
- Backup policy;
- Restore policy.

Requirement ID: [SRS-6-280]

WG_MGMT_CS MUST support the automated execution of those operations in [SRS-6-279] that comprise a policy update.

Requirement ID: [SRS-6-281]

WG_MGMT_CS MUST support the automated execution of the operation 'Backup policy' in [SRS-6-279].

Requirement ID: [SRS-6-282]

WG_MGMT_CS MUST support scheduling of policy updates such that:

- The policy update will be executed at a configurable date and time, with:

    - date expressed in years, month and day;
    - time expressed in hours and minutes.
- When starting at a configurable date and time, the policy update will be executed at a configurable regular time interval expressed in days, weeks or months.

6.7.4.1.2 Review

Requirement ID: [SRS-6-283]

The interface 'CIS Security' MUST support an operation 'Review' that provides the capability to review audit logs.

6.7.4.1.3 Manage Public Key Material

Requirement ID: [SRS-6-284]

The interface 'CIS Security' MUST support an operation 'Manage Public Key Material' that provides the capability to manage key material to support WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-285]

The operation 'Manage Public Key Material' SHALL be compliant with CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Artefacts [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-6-286]

The operation 'Manage Public Key Material' MUST provide the capability to:

- Import and store key material;
- Install and de-install certificates;
- Update certificates;
- Import and update CRLs.

6.7.5 WG_MGMT_CM

Requirement ID: [SRS-6-287]

WG_MGMT MUST provide a management capability WG_MGMT_CM that enables the configuration and management of the WG.

Requirement ID: [SRS-6-288]

WG_MGMT_CM MUST provide the capability to change, capture, duplicate, backup or restore the configuration of the WG.

Requirement ID: [SRS-6-289]

WG_MGMT_CM MUST provide the capability to remotely prepare a WG configuration WG_CONFIG and deploy WG_CONFIG onto multiple instances of the WG.

Requirement ID: [SRS-6-290]

WG_MGMT_CM MUST offer a graphical user interface for all configuration and installation options, including the updating of XML artefacts (6.7.5).

Requirement ID: [SRS-6-291]

WG_MGMT_CM MUST support configuration of the WG based on a customizable (pre-loaded) configuration templates (e.g. XML schemas are pre-installed) in support of common information exchange scenarios.

Requirement ID: [SRS-6-292]

WG_MGMT_CM MUST support the creation and installation (pre-loading) of the configuration templates as described in [SRS-6-291].

Requirement ID: [SRS-6-293]

WG_MGMT_CM MUST support the retrieval of XML artefacts from locations external to the WG.

Requirement ID: [SRS-6-294]

WG_MGMT_CM MUST support one or more of the following management protocols and associated SMC Messages for the retrieval of XML artefacts:

- Secure LDAP (LDAPS) [IETF RFC 4510 – 4519, 2006];
- HTTP(S) ([IETF RFC 7230, 2014], [IETF RFC 7540, 2015] [IETF RFC 8446, 2008], [IETF RFC 2818, 2000];
- SOAP ([W3C SOAP 1.1, 2000] and [W3C SOAP 1.2, 2007]).

Requirement ID: [SRS-6-295]

WG_MGMT_CM MUST support automated execution of the following action:

- Updating of XML artefacts including XML Schemas and MPIFs.

Requirement ID: [SRS-6-296]

WG_MGMT_CM MUST support scheduling of the operation in [SRS-6-291] such that:

- The operation will be executed at a configurable date and time, with:
  - date expressed in years, month and day;
  - time expressed in hours and minutes.
- When starting at a configurable date and time, the operation will be executed at a configurable regular time interval expressed in days, weeks or months.

Requirement ID: [SRS-6-297]

To track WG configuration information, WG_MGMT_CM SHALL interface to the enterprise configuration management database (BMC ITSM Atrium CMDB) via the interface 'SMC Configuration Management' in order to support the enterprise configuration management.

Requirement ID: [SRS-6-298]

WG_MGMT_CM SHALL pass outgoing SMC Messages to the interface 'Core Services Management' (6.4.5.1) for further processing.

6.7.5.1 SMC Configuration Management

Requirement ID: [SRS-6-299]

WG_MGMT_CM MUST offer an interface 'SMC Configuration Management' that accepts an incoming 'SMC Message' for further processing.

6.7.5.1.1 Configure OS

Requirement ID: [SRS-6-300]

The interface 'SMC Configuration Management' MUST support an operation 'Configure OS' that provides the ability to configure and manage the operating system(s) and platform(s) the WG is running on, and the applications running on the operating system.

Requirement ID: [SRS-6-301]

The operation 'Configure OS' SHALL support SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Network Time Protocol (NTP, [IETF RFC 5905, 2010]);
- Intelligent Platform Management Interface (IPMI, [IPMI V2.0, 2013]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

6.7.5.1.2 Configure Protection Policy Enforcement Services

Requirement ID: [SRS-6-302]

The interface 'SMC Configuration Management' MUST support an operation 'Configure Protection Policy Enforcement Services' that provides the capability to configure and manage WG_IFCPE ([SRS-6-70]) and WG_CIPE (6.5.3.1).

Requirement ID: [SRS-6-303]

The operation 'Configure Protection Policy Enforcement Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of WG_IFCPE and WG_CIPE.

Requirement ID: [SRS-6-304]

The operation 'Configure Protection Policy Enforcement Services' SHALL support one or more SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Remote Desktop Protocol (RDP);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

6.7.5.1.3 Configure Data Exchange Services

Requirement ID: [SRS-6-305]

The interface 'SMC Configuration Management' MUST support an operation 'Configure Data Exchange Services' that provides the capability to configure and manage WG_DEX ([SRS-6-1]).

Requirement ID: [SRS-6-306]

The operation 'Configure Data Exchange Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of WG_DEX.

Requirement ID: [SRS-6-307]

The operation 'Configure Data Exchange Services' SHALL support SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Remote Desktop Protocol (RDP);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

6.7.5.1.4 Configure Protection Services

Requirement ID: [SRS-6-308]

The interface 'SMC Configuration Management' MUST support an operation 'Configure Protection Services' that provides the capability to configure and manage WG_CIS ([SRS-6-190]) and WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-309]

The operation 'Configure Protection Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of WG_CIS and WG_PKCS.

Requirement ID: [SRS-6-310]

The operation 'Configure Protection Services' SHALL support SMC Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Remote Desktop Protocol (RDP);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

Requirement ID: [SRS-6-311]

The operation 'Configure Protection Services' MUST provide the capability to manage filters for WG_CIS.

Requirement ID: [SRS-6-312]

The management of filters for WG_CIS SHALL include:

- Installation and de-installation of content filters;
- Updating of content filters.

Requirement ID: [SRS-6-313]

The operation 'Configure Protection Services' MUST provide the capability to manage XML artefacts for WG_CIS.

Requirement ID: [SRS-6-314]

The management of XML artefacts for WG_CIS SHALL include:

- Loading and removal of XML artefacts (including XML Schemas and MPIFs);
- Updating of XML artefacts.

6.7.6 WG_MGMT_CD

Requirement ID: [SRS-6-315]

WG_MGMT MUST provide a management capability WG_MGMT_CD that provides the capability to manage and respond to cyber-related attacks on the WG.

Requirement ID: [SRS-6-316]

WG_MGMT_CD SHALL pass outgoing Cyber Defence Messages to interface 'Core Services Management' (6.4.5.1) for further processing.

6.7.6.1 Cyber Defence

Requirement ID: [SRS-6-317]

WG_MGMT_CD MUST offer an interface 'Cyber Defence' that accepts an incoming 'Cyber Defence Message' for further processing.

6.7.6.1.1 Assess

Requirement ID: [SRS-6-318]

The interface 'Cyber Defence' MUST support an operation 'Assess' that provides the capability to assess damage and attacks/faults of WG components that have been affected by attacks and faults.

Requirement ID: [SRS-6-319]

The operation 'Assess' SHALL be able to support analysis and evaluation of an attack.

Requirement ID: [SRS-6-515]

The operation 'Assess' SHALL be able to support the collection of cybersecurity-related log, alert, and event data in accordance with the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017] and the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-6-320]

The operation 'Assess' SHALL be able to support the aggregation of cybersecurity-related log, alert, and event data to a central repository or log aggregator as provided by the monitoring infrastructure in use by NCSC.

Requirement ID: [SRS-6-516]

The operation 'Assess' SHALL be able to support the ingestion of cybersecurity-related log, alert, and event data in the SIEM solution that is operated by NCSC.

Requirement ID: [SRS-6-517]

The operation 'Assess' SHALL ensure that all cyber-related log, alert, and event data can be parsed correctly by the SIEM solution that is operated by NCSC.

6.7.6.1.2 Respond

Requirement ID: [SRS-6-321]

The interface 'Cyber Defence' MUST support an operation 'Respond' that provides the capability to dynamically mitigate the risk identified by a suspected attack/fault.

Requirement ID: [SRS-6-322]

The operation 'Respond' SHALL be able to support the controlling of traffic flows for the purpose of stopping or mitigating an attack or fault.

Requirement ID: [SRS-6-323]

The controlling of traffic flow by WG_MGMT_CD SHALL include:

- Termination;
- Throttling to a certain level of bandwidth or with a certain delay;
- Redirection.

6.7.6.1.3 Recover

Requirement ID: [SRS-6-324]

The interface 'Cyber Defence' MUST support an operation 'Recover' that provides the capability to take the required action to recover from an attack/fault and restore the components of the WG that were affected by the attack/fault.

6.7.7 WG_MGMT_EM

Requirement ID: [SRS-6-325]

WG_MGMT MUST provide a management capability WG_MGMT_EM that enables the management of events.

Requirement ID: [SRS-6-327]

WG_MGMT_EM SHALL collect events and support the forwarding of events to the event management system (EMS).

Requirement ID: [SRS-6-328]

WG_MGMT_EM SHOULD support monitoring based on the Microsoft System Center Operations Manager (SCOM).

Requirement ID: [SRS-6-329]

WG_MGMT_EM SHALL support SNMP v3 [IETF RFC 3412, 2002] with appropriate Management Information Bases (MIBs).

Requirement ID: [SRS-6-330]

WG_MGMT_EM SHALL provide a toolset which allows WG Administrators to define, filter, correlate and group events according to their context, criticality, source and impacts.

Requirement ID: [SRS-6-331]

WG_MGMT_EM SHALL provide an event correlation toolset that can be either customizable or adaptive to detect normal and abnormal behaviour patterns.

Requirement ID: [SRS-6-332]

WG_MGMT_EM SHALL provide the capability to examine recorded historical logs and archives.

Requirement ID: [SRS-6-333]

WG_MGMT_EM SHALL support the correlation of requests and responses in order to track all responses (or faults) with the correct request for information access.

Requirement ID: [SRS-6-335]

WG_MGMT_EM SHALL provide an event management toolset which allows WG Administrators to customize the building and saving of reports.

Requirement ID: [SRS-6-336]

The event management toolset SHALL support the provision of visibility on usage patterns over daily, monthly and variable periods.

Requirement ID: [SRS-6-337]

The event management toolset SHALL support trend and abnormal behaviour analysis.

Requirement ID: [SRS-6-338]

WG_MGMT_EM SHALL be able to generate reports of the following types:

- Service Level Agreement (SLA) compliance reports;

- Error/exception reports;
- Service usage reports;
- Other customizable reports based on captured metrics which can be filtered and sorted based on various criteria.

Requirement ID: [SRS-6-339]

WG_MGMT_EM SHALL pass outgoing SMC Messages to interface 'Core Services Management' (6.4.5.1) for further processing.

6.7.7.1 Event Management

Requirement ID: [SRS-6-340]

WG_MGMT_EM MUST offer an interface 'Event Management' that generates and forwards 'SMC Messages' in support of the operations 'Log' (6.7.7.1.1), 'Alert' (6.7.7.1.2) and 'Report' (6.7.7.1.3).

6.7.7.1.1 Log

Requirement ID: [SRS-6-341]

The interface 'Event Management' MUST support an operation 'Log' that provides the capability to record events that occur in software, or messages between components.

Requirement ID: [SRS-6-342]

The operation 'Log' SHALL support writing log messages to a log file.

Requirement ID: [SRS-6-343]

The operation 'Log' MUST provide the capability to log request and response attributes. These include:

- Time-stamp;
- Source and target address(es);
- URL;
- Operation;
- Size;
- Unique request id (extracted from the request/response or automatically generated by WG_MGMT_EM).

Requirement ID: [SRS-6-344]

The operation 'Log' MUST provide the capability to log attributes extracted from the HTTP headers and HTTP body.

Requirement ID: [SRS-6-345]

The operation 'Log' MUST provide the capability to selectively log whole messages based on pre-configured criteria or filter (e.g. policy based).

Requirement ID: [SRS-6-346]

The operation 'Log' SHALL support SMC Messages of the following types:

- Syslog [IETF RFC 5424, 2009];
- HTTP Message [IETF RFC 7230, 2014].

6.7.7.1.2 Alert

Requirement ID: [SRS-6-347]

The interface 'Event Management' MUST support an operation 'Alert' that provides the capability to generate an alert event when the acceptable threshold for a service has been reached, or is approached within a certain range.

Requirement ID: [SRS-6-348]

The operation 'Alert' SHALL be able to support the generation of an alert of type 'Warning' that indicates it is necessary to take action in order to prevent an exception occurring.

Requirement ID: [SRS-6-349]

The operation 'Alert' SHALL be able to support the generation of an alert of type 'Exception' that indicates that a given service is operating below the normal predefined parameters/indicators.

Requirement ID: [SRS-6-350]

The operation 'Alert' SHALL support SMC Messages of the type SNMP v3 [IETF RFC, 3412, 2002].

6.7.7.1.3 Report

Requirement ID: [SRS-6-351]

The interface 'Event Management' MUST support an operation 'Report' that provides the capability to generate reports in support of compliance, auditing, billing and service value determination.

Requirement ID: [SRS-6-352]

The operation 'Report' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

6.7.8 WG_MGMT_PM

Requirement ID: [SRS-6-353]

WG_MGMT MUST provide a management capability WG_MGMT_PM that enables the management of the performance and capacity of the WG.

Requirement ID: [SRS-6-354]

WG_MGMT_PM MUST SHALL provide customizable dashboards for monitoring selected statistics and metrics for WG services.

Requirement ID: [SRS-6-355]

WG_MGMT_PM SHALL pass outgoing SMC Messages to interface 'Core Services Management' (6.4.5.1) for further processing.

6.7.8.1 Performance Management

Requirement ID: [SRS-6-356]

WG_MGMT_PM MUST offer an interface 'Performance Management' that generates and forwards 'SMC Messages' in support of the operations 'Monitor'(6.7.8.2.2), 'Meter' (6.7.8.2.3) and 'Track Messages' (6.7.8.2.4).

6.7.8.1.1 Monitor

Requirement ID: [SRS-6-357]

The interface 'Performance Management' MUST support an operation 'Monitor' that provides the capability to observe and track the operations and activities of end users (services) on the WG.

Requirement ID: [SRS-6-358]

The operation 'Monitor' SHALL support the real-time monitoring of WG services against expected Key Performance Indicators (KPI), SLA or other metric thresholds as configured.

Requirement ID: [SRS-6-359]

The operation 'Monitor' SHALL support the monitoring service faults and exceptions.

Requirement ID: [SRS-6-360]

The operation 'Monitor' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

6.7.8.1.2 Meter

Requirement ID: [SRS-6-361]

The interface 'Performance Management' MUST support an operation 'Meter' that provides the capability to measure levels of resource utilization consumed by service subscribers.

Requirement ID: [SRS-6-362]

The operation 'Meter' SHALL support the storing of measured data for the purpose of summarizing and analysis.

Requirement ID: [SRS-6-363]

The operation 'Meter' SHALL provide the capability to collect and present the statistics on service utilisation broken down by end user or system.

Requirement ID: [SRS-6-364]

The operation 'Meter' SHALL support the collection of statistics for a given end user or system or group of end user or system over specified periods of time.

Requirement ID: [SRS-6-365]

The operation 'Meter' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

6.7.8.1.3 Track Messages

Requirement ID: [SRS-6-366]

The interface 'Performance Management' MUST support an operation 'Track Messages' that provides the capability to track, monitor and log all message routing and service invocation activities.

Requirement ID: [SRS-6-367]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all access requests for information from the high domain to the low domain.

Requirement ID: [SRS-6-368]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all responses to access requests for information from the high domain to the low domain.

Requirement ID: [SRS-6-369]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all access requests for information from the low domain to the high domain.

Requirement ID: [SRS-6-370]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all responses to access requests for information from the low domain to the high domain.

Requirement ID: [SRS-6-371]

The operation 'Track Messages' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].

6.8 Security Functional Requirements

6.8.1 Introduction

6.8.1.1 Relationship with MAXLG PP

The security requirements that apply to the WG are based on the Common Criteria (CC) Protection Profile (PP) for a Medium Assurance NATO XML-Labelling Guard [NCI Agency TN 1485 v1.1, 2012] developed by NCIA. The PP was developed in order to support industry in developing a commercial alternative for the NC3A MAXLG ([NC3A RD-3381, 2012].The main purpose of the PP is to formalize the security functional requirements (SFRs) and security assurance requirements (SARs) for medium-assurance XML-Labelling Guard solutions to be used within NATO.

The PP can be used as a target specification for the implementation and CC Evaluation Assurance Level (EAL) 4+ evaluation of commercial products that provide a WG in an IEG-C. It must be noted that for the purpose of the development of a WG based on this SRS, the contents of the PP [NCIA TN-1485 v1.1, 2012] that are included in this section must be interpreted within the context of the applicable NATO policy [AC/322-D/0030-REV5].

6.8.1.2 Applicability of MAXLG PP when developing a WG

The SFRs that are defined in [NCIA TN-1485 v1.1, 2012] have not been transferred to this section one-to-one. The reason for this is that the PP was written with the NC3A MAXLG in mind, meaning that:

- Some SFRs in the PP are too implementation-specific or are based on versions of standards that have been revised in the meantime. Where needed, the SFRs included in this section have been updated accordingly.
- SFRs that did not need revision, are referenced and not included. Instead the higher level objectives (that are implemented by the SFRs) are included.
- The definitions of Target of Evaluation (TOE) and TOE Security Functionality (TSF) are influenced by the system architecture of the NC3A MAXLG and the assumptions that were made for the IT operational environment. For a WG to be developed based on this SRS, some of the SFRs that depend on the definitions of TOE, TSF and said assumptions must be generalized. Section 6.8.1.3 shows the correspondence between the TOE and IT operational environment assumed in the PP, and the WG.

Note that some SFRs have been integrated in the WG functional requirements in previous sections.

6.8.1.3 Interpretation of TOE, TSF and IT operational environment

The formulation of SFRs in [NCIA TN-1485 v1.1, 2012] is based on the definitions of TOE, TSF and IT operational environment in [NCIA TN-1485 v1.1, 2012] as illustrated in Figure 19.

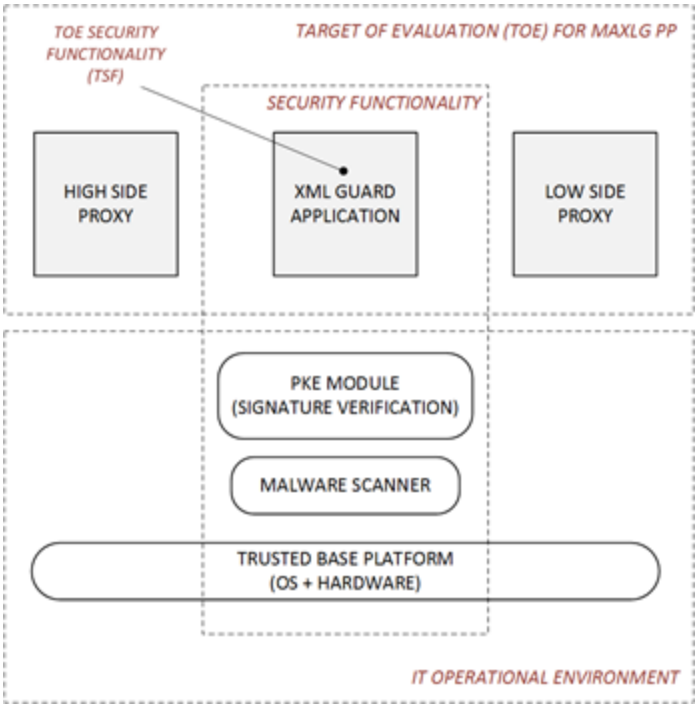

Figure 19 TOE, TSF and IT operational environment defined in [NCIA TN-1485 v1.1, 2012]

In support of the development of a WG based on this SRS, Figure 19 must be interpreted as shown in Figure 20 given the below:

- NC3A MAXLG implements two HTTP proxies; in the WG this is generalized to client/proxy HTTP connectivity;
- NC3A MAXLG assumes an XML Guard application; in the WG this is generalized to a component called ‘WG security policy enforcement’ that implements the ABBs ‘Protection Services’ and ‘Protection Policy Enforcement Services’;
- The PKE module is included as part of the WG. It is kept in Figure 20 in the form of a module to show the correspondence, however it is part of the ABB ‘Protection Services’ (‘Public Key Cryptography Services’);
- The Trusted Base Platform is part of the WG. The NC3A MAXLG assumes one physical platform, however the WG may be built using multiple platforms.
- For the purpose of interpretation of the SFRs, the malware scanner is assumed to be implemented in the IEG-C (but outside the WG).
- Instead of TOE Security Functionality, Figure 20 defines the ‘WG – Security Functionality (WG-SF)’ that excludes the malware scanner.

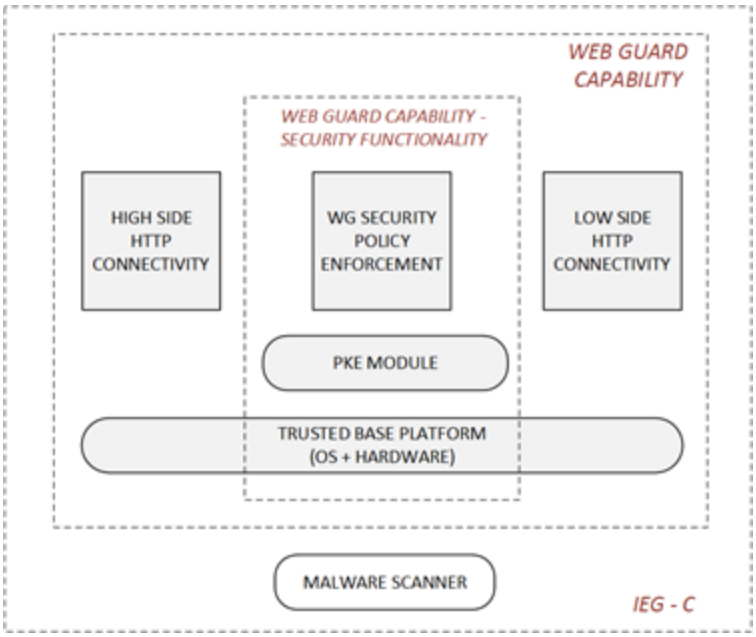

Figure 20 Interpretation of TOE, TSF and IT operational environment for the WG

The WG Trusted Base Platform (TBP) implements part of the ABBs 'Data Exchange Services' (TCP/IP connectivity). Figure 21 shows the overall correspondence between the WG components in Figure 20 and the IEG-C ABBs.

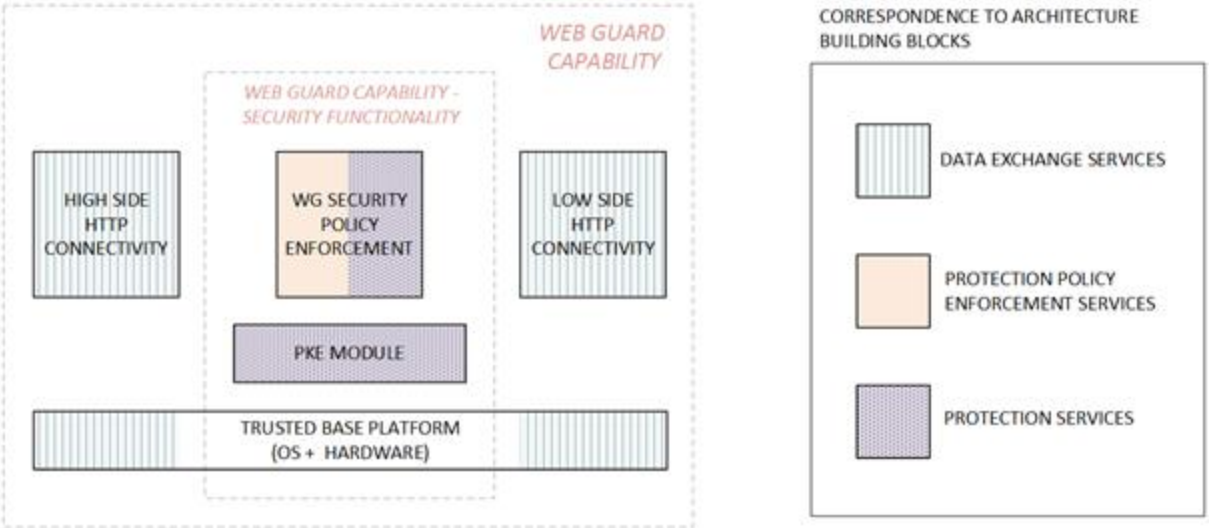

Figure 21 Correspondence between the WG components in Figure 20 and the IEG-C ABBs

6.8.1.4 PP objectives and assumptions

Instead of including SFRs that do not need revision, this section includes the higher level requirement that the SFRs implement (called 'objectives' in the PP). Similarly, the PP includes requirements in the form of assumptions (met by the IT operational environment). Given that for the WG these assumptions cannot be made (see Figure 21), such requirements are included in this SRS.

6.8.1.5 SARs

SARs are not included for the WG in this SRS. The applicability of the SARs documented in [NCIA TN-1485 v1.1, 2012] must be interpreted within the context of the NATO policy that applies to the WG [NAC AC/322-D/0030-REV5, 2011].

6.8.1.6 SFR categories

The next sections contain the WG SFRs. If applicable, for each requirement the source in [NCIA TN-1485 v1.1, 2012] is identified, and the associated SFRs are referenced. The requirements are grouped per the following categories (the grouping only serves to facilitate ordering of the requirements):

- PKE module (Section 6.8.2);
- Trusted Base Platform (Section 6.8.3);
- System administration (Section 6.8.4);
- System audit (Section 6.8.5);
- Self-protection (Section 6.8.6).

6.8.2 PKE Module

It is assumed that an implementation of the ABB 'Public Key Cryptography Services' will rely on a cryptographic module. This module is referred to as the 'PKE module'.

Table 13 PKE Module: requirements and sources

Requirement	**Source in [NCIA TN-1485 v1.1, 2012]**
Requirement ID: [SRS-6-374] The PKE module SHALL be validated according to the Smart Card Protection Profile [SCSUG-SCPP, 2001] or validated to at least FIPS 140-2 Level 2 [NIST FIPS 1402, 2001], or otherwise verified to an equivalent level of functionality and assurance by a NATO nation COMSEC authority. Ref.: [NAC AC/322-D(2004)0024-REV3-COR1, 2018].	A.CRYPTOGRAPHY_MODULE_VALIDATED OE.CRYPTOGRAPHY_MODULE_VALIDATED
Requirement ID: [SRS-6-375] The PKE module used by the WG SHALL be a NATO-approved cryptographic module with NATO-approved methods for key management (i.e. generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e. encryption, decryption, signature, hashing, key exchange, and random-number-generation services) as described in [NAC AC/322-D(2007)0002-REV1, 2015].	A.CRYPTOGRAPHY_NATO_APPROVED OE.CRYPTOGRAPHY_NATO_APPROVED

Requirement	Source in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-376] The PKE module SHALL be evaluated according to the US Government Basic Robustness PKE PP with CPV - Basic Package, CPV - Basic Policy Package, CPV - Policy Mapping Package, CPV - Name Constraints Package, PKI Signature Verification Package, Online Certificate Status Protocol Client Package and Audit Package at EAL 4.	A.PKI_MODULE_EVALUATED OE.PKI_MODULE_EVALUATED

6.8.3 Trusted Base Platform

Table 14 Trusted Base Platform: requirements, sources and supporting SFRs

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-377] Any operating system of the WG is a trusted and securely configured operating system. The operating system is evaluated according to [OSPP, 2010] extended with [OSPP EP-IV, 2010] and [OSPP EP-TB, 2010] (or equivalent) and configured according to relevant NATO guidance and directives. Ref.: [AC AC/322-D/0048-REV3, 2019]	A.OS_TRUSTED OE.OS_TRUSTED	
Requirement ID: [SRS-6-378] If the WG is a distributed system *S* (consisting of one or more hardware platforms or operating systems) it SHALL implement measures that prevent eavesdropping on communication channels between the systems (hardware platforms or operating systems) that comprise *S*.		

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-379] The operating system depends on the underlying platform, which consists of hardware (processors, memory, and devices) and firmware. The underlying platform MUST provide functions that allow the operating system to:	Section 2.2.2 'TOE Model'	
(i) Protect devices and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.		
(ii) Protect any other function of the underlying platform from being used by untrusted subjects in a way that would violate the security policy of the operating system.		
(iii) Ensure that any information contained in a protected resource is not released when the resource is reallocated; this includes ensuring that no residual information from a previously relayed message is transmitted.		FDP_RIP.2
(iv) Enable enforcement of direction of information flow between the WG components 'WG security policy enforcement', 'high side http connectivity' and 'low side http connectivity' in Figure 20.		
Requirement ID: [SRS-6-380] The WG hardware and firmware MUST be selected such that requirement [SRS-6-371] is met[6].		

[6] *An OS is CC evaluated given a choice of hardware and firmware.*

6.8.4 System Administration

Table 15 System administration: requirements, sources and supporting SFRs

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-381] The WG SHALL provide well specified administrator roles in order to isolate administrative actions, and to make the administrative functions available locally and remotely.	O.ADMIN_ROLE	FMT_SMR.2
Requirement ID: [SRS-6-382] The WG SHALL display an advisory warning regarding use of the WG.	O.DISPLAY_BANNER	FTA_TAB.1
Requirement ID: [SRS-6-383] The WG SHALL provide a mode from which recovery or initial start-up procedures can be performed.	O.MAINT_MODE	FMT_SMF.1 FPT_RCV.2

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-384] The WG SHALL provide all the functions and facilities necessary to support the WG Administrators in their management of the security of the WG, and restrict these functions and facilities from unauthorized use.	O.MANAGE	FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_SEL.1 FAU_STG.1 FAU_STG.3 FAU_STG.4(1) FAU_STG.4(2) FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MOF.1(4) FMT_MOF.1(5) FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MTD.2(1) FMT_MTD.2(2) FMT_MTD.2(3) FMT_SMF.1
Requirement ID: [SRS-6-385] The WG SHALL provide a means to ensure that WG Administrators are not communicating with some other entity pretending to be the WG when supplying identification and authentication data.	O.TRUSTED_PATH	FTP_ITC.1(1) FTP_ITC.1(2) FTP_TRP.1(1) FTP_TRP.1(2)
Requirement ID: [SRS-6-386] The WG SHALL provide the ability for a CIS Security Administrator to revoke the user's access through the TOE and TOE's ability to mediate data traffic: if the CIS Security Administrator revokes a user's access (e.g. by revoking an administrative role from a user) or modifies an information flow policy, the TOE SHALL immediately enforce the new CIS-Security-Administrator-defined policy.	FMT_REV.1(1) FMT_REV.1(2)	

6.8.5 System Audit

Table 16 System audit: requirements, sources and supporting SFRs

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-387] The WG SHALL provide the capability to detect and create records of security-relevant events associated with users.	O.AUDIT_GENERATION	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1 FAU_STG.3 FAU_STG.4(1) FAU_STG.4(2) FIA_USB.1

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-388] The WG SHALL provide the capability to protect audit information.	O.AUDIT_PROTECTION	FAU_SAR.2 FAU_STG.1 FAU_STG.3 FAU_STG.4(1) FAU_STG.4(2) FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MOF.1(4) FMT_MOF.1(5)
Requirement ID: [SRS-6-389] The WG SHALL provide the capability to selectively view audit information, and alert the Audit Administrator of identified potential security violations.	O.AUDIT_REVIEW	FAU_ARP.1 FAU_ARP.2 FAU_SAA.1 FAU_SAR.1 FAU_SAR.3 FMT_MOF.1(3) FMT_MOF.1(4) FMT_MOF.1(5) FMT_SMF.1
Requirement ID: [SRS-6-390] The WG SHALL provide reliable time stamps and the capability for a WG Administrator to set the time used for these time stamps.	TIME_STAMPS	FMT_MTD.1 FMT_SMF.1 FPT_STM.1

6.8.6 Self-Protection

Table 17 Self-protection: requirements, sources and supporting SFRs

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-391] The WG SHALL provide a means to detect and reject the replay of authentication data as well as other data and security attributes used by the WG-SF.	O.REPLAY_DETECTION	FPT_RPL.1

Requirement	Source in [NCIA TN-1485 v1.1, 2012]	Supporting SFRs in [NCIA TN-1485 v1.1, 2012]
Requirement ID: [SRS-6-392] The WG SHALL provide mechanisms that mitigate attempts to exhaust resources provided by the WG and thus protect availability of high side resources.	O.RESOURCE_SHARING	FMT_MOF.1(5) FMT_MTD.2(2) FMT_MTD.2(3) FRU_RSA.1(1) FRU_RSA.1(2)
Requirement ID: [SRS-6-393] The WG SHALL provide mechanisms that control a user's logical access to the WG and to explicitly deny access to specific users when appropriate.	O.ROBUST_TOE_ACCESS	FIA_AFL.1 FIA_ATD.1 FIA_UAU.2 FIA_UID.2 FMT_SAE.1 FTA_SSL.1 FTA_SSL.2 FTA_SSL.3 FTA_TSE.1
Requirement ID: [SRS-6-394] The WG-SF SHALL maintain a domain for its own execution that protects itself and its resources from external interference, tampering and unauthorized disclosure.	O.SELF_PROTECTION	FMT_SAE.1 FTP_ITC.1(1) FTP_ITC.1(2) FTP_TRP.1(1) FTP_TRP.1(2)

7 Mail Guard Functional Requirements

7.1 Background

7.1.1 Introduction

This chapter describes the functional requirements for a 'Mail Guard Capability' (MG). The functional requirements are described in terms of interfaces and operations that have been defined for the IEG-C ABBs (see [NCIA TR/2016/NSE010871/01, 2017]). The ABBs, interfaces and operations that together comprise a Mail Guard capability are captured in MG patterns. The patterns are described in Section 7.3. In each pattern the MG enforces a number of policies. An overview of the policies is provided in Section 7.2.

Due to the choice for an IEG-C architecture based on a DMZ, and the MG being part of that DMZ, the operations at the external interfaces of the MG are not identical to those at the external interfaces of the IEG-C. This distinction is important to note in order to correctly interpret the MG patterns. The next section explains the use of the interfaces and operations for the MG and IEG-C.

7.1.2 Domains, Interfaces and Operations

The IEG-C TA [NCIA TR/2016/NSE010871/01, 2017] assumes a DMZ architecture. Figure 22 shows the logical placement of the MG in the DMZ, the interfaces of IEG and MG, and the domains to which the IEG-C and MG interface. The MG interfaces to the high side of the DMZ at MG_IF_NET_HIGH, and to the low side of the DMZ at MG_IF_NET_LOW.

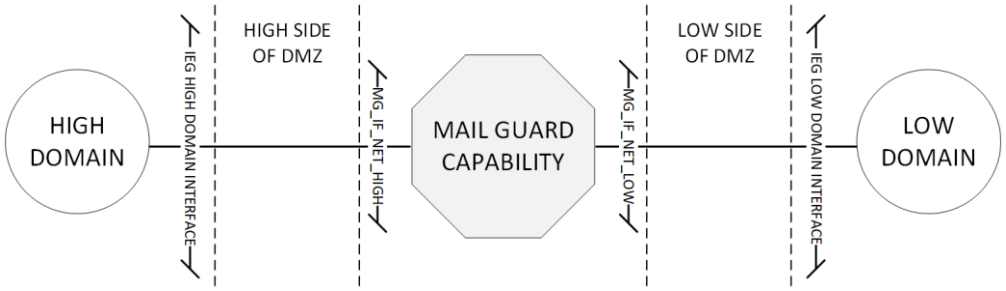

Figure 22: MG in DMZ Architecture: Domains and Interfaces

Note that the MG is not aware of the DMZ configuration; a release of information to the low side of the DMZ is considered a release to the low domain, and an import from the high side of the DMZ is considered an import from the high domain.

The interfaces MG_IF_NET_HIGH and MG_IF_NET_LOW offer TCP/IP over Ethernet network connectivity. Both interfaces support a subset of the logical interfaces offered by the IEG-C ABB 'Data Exchange Services'. Table 18 provides an overview.

Table 18: Subset of logical IEG-C ABB Interfaces Supported by MG Interfaces

MG interfaces (Section 7.4)	**Supported subset of logical interfaces from IEG-C ABB 'Data Exchange Services'**	**Note on security domains**
MG_IF_NET_HIGH	Communications Access Services HL Interface Communications Access Services LH Interface Business Support Services HL Interface Business Support Services LH Interface	From the point of view of the MG, the high side DMZ and the high domain are the same security domain referred to as 'high domain'.
MG_IF_NET_LOW	Communications Access Services HL Interface Communications Access Services LH Interface Business Support Services HL Interface Business Support Services LH Interface.	From the point of view of the MG, the low side DMZ and the low domain are the same security domain referred to as 'low domain'.
MG_IF_MGMT (Not shown in Figure 22)	Management interface	The management interface can be implemented as a logical interface on top of MG_IF_NET_HIGH in which case – from the point of view of the MG - the management domain is equal to the high domain. If the management interface is implemented as a separate physical interface, then – from the point of view of the MG – the management domain is considered a separate security domain referred to as 'management domain'.

In the DMZ architecture in Figure 22, the external networks are those represented by the low and high domains; the internal networks are those represented by the high side and low side of the DMZ. From the point of view of the MG however, both sides of the DMZ are external domains. This point of view has no consequence on the selection of logical interfaces that apply to the MG as shown in Table 18. However, the operations that are defined for the logical interface 'Communications Access Services' do distinguish between internal and external networks, where the point of view taken is that of the IEG-C. These operations are 'ReceiveExternalNetwork', 'ReceiveInternalNetwork', 'ForwardInternalNetwork' and 'ForwardExternalNetwork' (see section A.3.3.1. "Communication Access Services Interfaces", of [NCIA TR/2016/NSE010871/01, 2017]). So even though both sides of the DMZ are external to the MG, the operations that apply to the MG are 'ReceiveInternalNetwork' and 'ForwardInternalNetwork'.

Figure 23 illustrates the logical interface 'Communications Access Services HL interface' and its operations supporting the traffic flow from the high domain to the low domain.

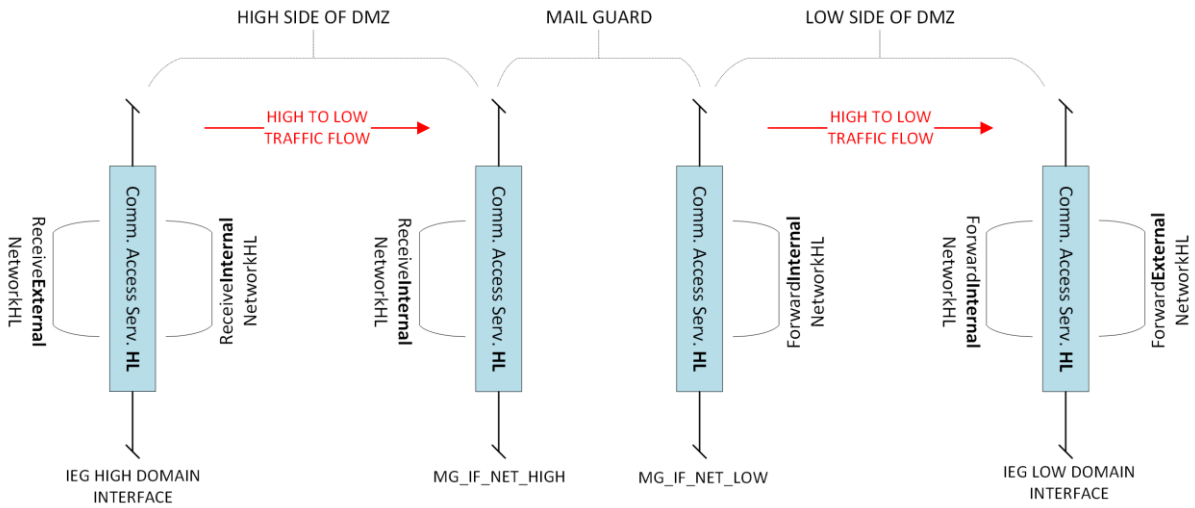

Figure 23: Operations at instances of the interface 'Communication Access Services HL' for traffic flowing from the high to the low domain

Figure 24 illustrates the logical interface 'Communications Access Services LH interface' and its operations supporting the traffic flow from the low domain to the high domain.

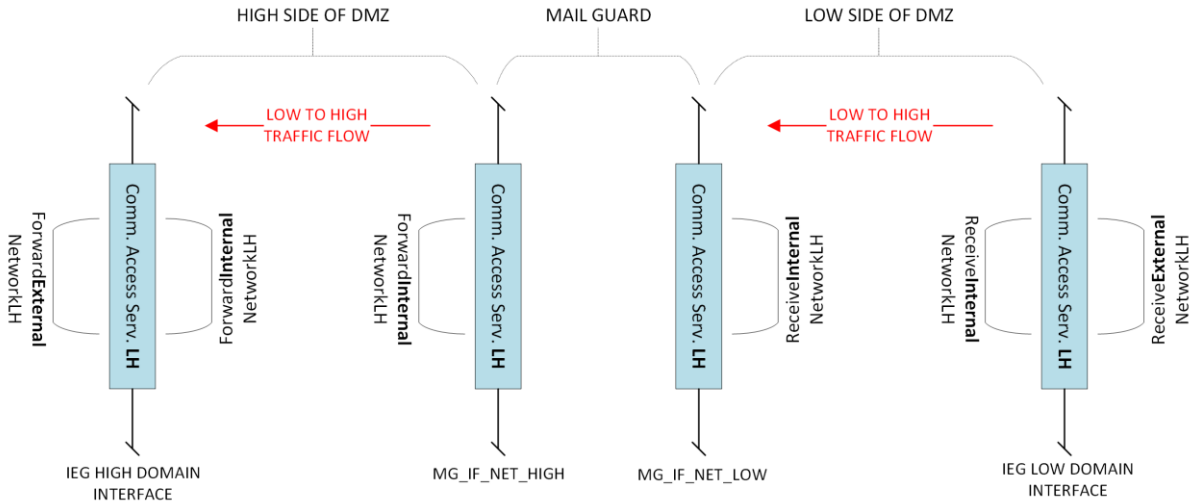

Figure 24: Operations at instances of the interface 'Communication Access Services LH' for traffic flowing from the low to the high domain

7.2 MG Policy Enforcement

7.2.1 MG Security Policy

The MG enforces a security policy. This policy is referred to as the 'MG security policy'. Regarding the enforcement of the MG security policy on low-to-high and high-to-low traffic[2], the MG security policy is composed of two types of policies:

- Information flow control policies (Section 7.2.2)

[2] Note that the MG also needs to enforce a security policy with respect to local access control (in support of system administration, system audit and self-protection (see Section 7.8)). The local access control policy is considered a part of the MG security policy, however it may be administered separately from the policies listed in Section 7.2.

- Content inspection policies (Section 7.2.3)

7.2.2 MG Information Flow Control Policies

The information flow control (IFP) policy that is enforced by the MG is referred to as 'MG_IFP'. The policy MG_IFP is the union of three sub-policies:

- The sub-policy that pertains to high-to-low traffic, referred to as 'MG_IFP_HL';
- The sub-policy that pertains to low-to-high traffic, referred to as 'MG_IFP_LH'; and
- The sub-policy that pertains to management traffic, referred to as 'MG_IFP_MGMT'.

All three policies can be broken down further into sub-polices. Table 19 provides an overview of all IFPs and their scope; each IFP is covered in Section 7.5.2.

Table 19: IFPs enforced by MG and their scope

Policy	**Union of sub-policies**	**Scope**
MG_IFP	MG_IFP_HL	High to low traffic
	MG_IFP_LH	Low to high traffic
	MG_IFP_MGMT	Management traffic (related to management of the MG itself).
MG_IFP_MGMT	MG_IFP_MGMT_IN	Management traffic destined for MG
	MG_IFP_MGMT_OUT	Management traffic leaving MG
MG_IFP_HL	MG_IFP_CA_HL	High to low SMTP traffic
	MG_IFP_BS_HL	SMTP messages transferred from high to low
MG_IFP_LH	MG_IFP_CA_LH	Low to high SMTP traffic
	MG_IFP_BS_LH	SMTP messages transferred from low to high

7.2.3 MG Content Inspection Policies

The content inspection policy (CIP) that is enforced by the MG is referred to as 'MG_CIP'. The policy MG_CIP is the union of the policies 'MG_CIP_HL' and 'MG_CIP_LH', see Table 20.

Table 20: CIPs enforced by MG and their scope

Policy	**Union of sub-policies**	**Scope**
MG_CIP	MG_CIP_HL	SMTP messages transferred from high to low
	MG_CIP_LH	SMTP messages transferred from low to high

Note that the outcome of the enforcement of IFPs MG_IFP_HL and MG_IFP_LH depends on the outcome of the enforcement of MG_CIP in the sense that MG_IFP_HL and MG_IFP_LH will not permit traffic flow when traffic violates MG_CIP (see requirements [SRS-7-142] and [SRS-7-143]).

Section 7.5.4 specifies the functional requirements of the MG for the ABB 'Content Inspection Services'. The enforcement functionality of the MG related to this ABB is label validation and message/attachment validation. The MG provides this

functionality through the application of content filters that enforce the content inspection policies MG_CIP_HL and MG_CIP_LH. In order to be able to group functional requirements per MG functionality, MG_CIP_HL and MG_CIP_LH are split into sub-policies as per Table 21; each CIP is described in Section 7.5.4. The selection and configuration of sub-policies for a given information flow depends on the information exchange scenario that will be supported.

Table 21: Further breakdown of MG content inspection policies in support of the common MG information exchange scenario.

Policy	**Union of sub-policies**	**Scope**	**MG functionality**
MG_CIP_HL	MG_CIP_EV	SMTP message envelope	SMTP envelope validation
	MG_CIP_LV	SMTP message headers/ IMF message body	Label validation
	MG_CIP_AV	IMF message body	IMF message body validation
MG_CIP_LH	MG_CIP_EV	SMTP message envelope	SMTP envelope validation
	MG_CIP_LV	SMTP message headers/ IMF message body	Label validation
	MG_CIP_AV	IMF message body	IMF message body validation

7.3 MG Patterns

7.3.1 Main Patterns

Three main patterns comprise the MG. Each pattern is a combination of two sub-patterns, see Table 22.

Table 22: Patterns that comprise the MG

Pattern	**Combination of sub-patterns**	**Depicted in**
MG High to Low Pattern	MG High to Low Node Self Protection Pattern	Figure 25
	MG High to Low Cross Domain Information Exchange Pattern	
MG Low to High Pattern	MG Low to High Node Self Protection Pattern	Figure 26
	MG Low to High Cross Domain Information Exchange Pattern	
MG Management pattern	MG Management Self Protection Pattern	Figure 27
	MG Element Management Services Pattern	Figure 28

The MG patterns enforce the information flow control and content inspection policies that are described in Sections 7.3.2 and 7.3.3. It should be noted that support for the enforcement of additional policies (Section 7.3.4) may require a modification to the patterns.

7.3.2 MG High to Low Pattern

Figure 25 provides an overview of Transfer Informal Email Services – High To Low, which is an example of the High to Low Cross Domain Information Exchange Pattern. It is

invoked by a Message Transfer Agent (MTA) in the High Domain in order to transfer an informal email to a recipient in the Low Domain, and determines the destination host for the Low Domain recipient is the Mail Guard residing within the IEG-C[3].

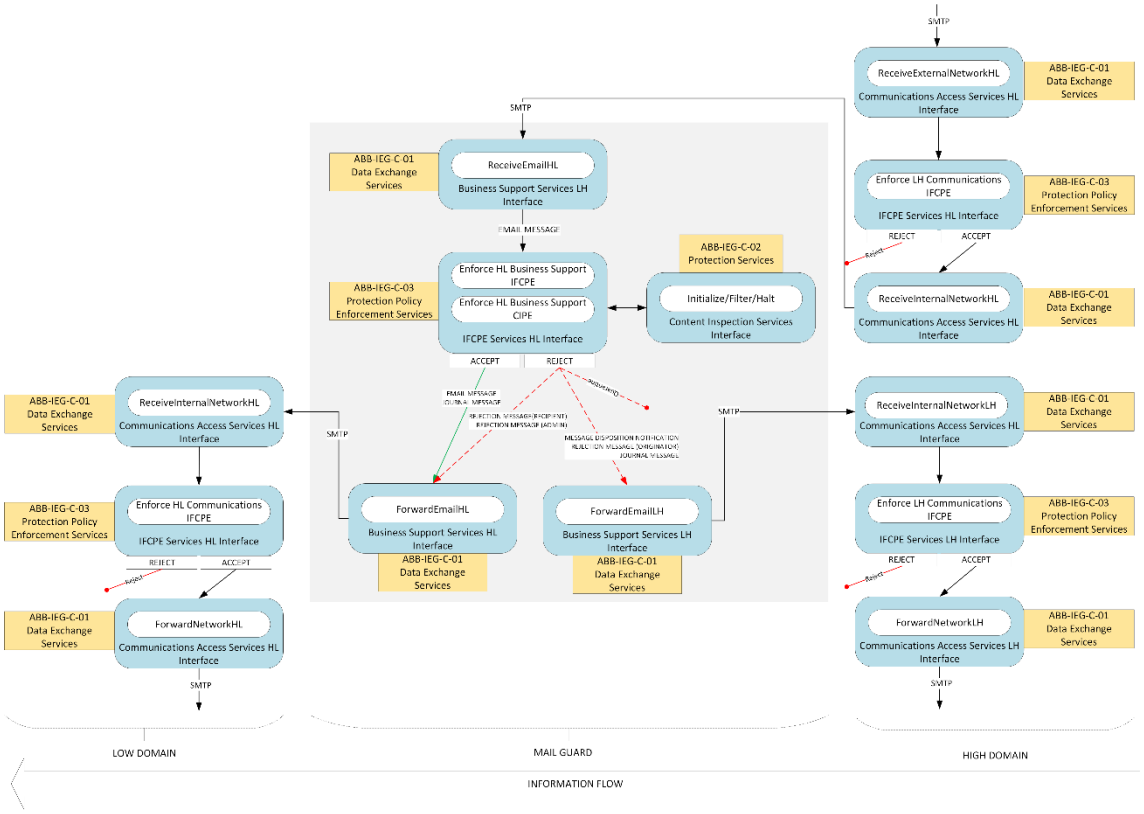

Figure 25: Transfer Informal Email Service High To Low

The Transfer Informal Email Services – High To Low consists of the following steps:

1. The Communication Access Services HL Interface of the Data Exchange Services receives the SMTP transfer operation from an MTA in the High Domain and invokes the ReceiveExternalNetworkHL operation.

The Enforce HL Communications IFCPE of the IFCPE Service HL Interface is invoked to determine whether the High Domain MTA is allowed to communicate with the Mail Guard.

If the High Domain MTA is not allowed to communicate with the Mail Guard, the connection attempt is rejected.

If the High Domain MTA is allowed to communicate with the Mail Guard, the connection attempt is passed on the Internal Network within the IEG-C using the ReceiveInternalNetworkHL operation of the Communication Access Service HL Interface.

The Mail Guard receives the email message on the Business Services HL Interface with the ReceiveEmailHL operation.

[3] This routing decision is performed in the High Domain and is not enforced by the Mail Guard.

The Policy Protection Enforcement Services applies the Enforce HL Business Services IFCPE of the Business Services HL Interface to determine if the email message is allowed to flow from the High Domain to the Low Domain.

In turn, the Enforce HL Business Services IFCPE operation calls the Enforce HL Business Services CIP to determine if the email message is compliant with the content inspection policy and is therefore allowed to flow from the High Domain to the Low Domain.

The Enforce HL Business Support CIP calls the Initialize/Filter/Halt operation of the Content Inspections Services to verify that the email messages:

1. contains only MIME types allowed by the CIP;
2. contains less than the maximum number of attachments allowed by the CIP;
3. does not contain any attachments that contain malware;
4. contains a valid sensitivity marking allowed by the CIP;
5. is from an originator allowed by the CIP;
6. is destined for a recipient allowed by the CIP;

If the email message is compliant with the content inspection policy, the Protection Policy Enforcement Services:

(i) pass the email to the ForwardEmailHL operation of the Business Support Service HL Interface; and

(ii) optionally sends a copy of the email message to a journal recipient.

(iii) optionally generates an SNMP trap

If the email message is not compliant with the content inspection policy, the Protection Policy Enforcement Services:

(i) does not pass the email to the ForwardEmailHL operation of the Business Support Service HL Interface;

(i) optionally generates a delivery status notification for the email message and passes it to the ForwardEmailLH operation of the Business Support Services LH Interface;

(ii) optionally generates a rejection message for the email message;

(iii) optionally sends the rejection message to the email message originator by passing it to the ForwardEmailLH operation of the Business Support Services HL Interfaces;

(iv) optionally sends the rejection message to the email message recipients by passing it to the ForwardEmailHL operation of the Business Support Services HL Interfaces;

(v) optionally sends the rejection message to the mail guard administrator by passing it to the ForwardEmailHL operation of the Business Support Services LH Interfaces;

(vi) optionally sends a copy of the non-compliant email message to a journal recipient;

(vii) optionally, quarantines the message (for later manual handling by an administrator); and

(viii) [optionally generates an SNMP trap?]

2. Note that an email message may contain multiple recipients and may therefore be compliant with the CIP for some recipients and non-compliant for other recipients. In this case, the MG may accept the message for some recipients and reject message for other recipients.
3. The ForwardEmailHL operation determines the Low Domain MTA that the email message, journal message and rejection message should be transferred to.
4. The ReceiveInternalNetworkHL operation of the Communications Access Services HL Interface receives the SMTP request from the Mail Guard to the Low Domain MTA.
5. The Enforce HL Communications IFCPE of the IFCPE Services HL Interface is invoked to determine whether the Mail Guard is allowed to communicate with the Low Domain MTA.
6. If the Mail Guard is not allowed to communicate with the Low Domain MTA, the connection attempt is rejected.
7. If the Mail Guard is allowed to communicate with the Low Domain MTA, the connection attempt is passed on the Network in the Low Domain using the ForwardNetworkHL operation of the Communication Access Service HL Interface.
8. The ForwardEmailLH operation determines the High Domain MTA that the delivery status notification, journal message and rejection message should be transferred to.
9. The ReceiveInternalNetworkLH operation of the Communications Access Services LH Interface receives the SMTP request from the Mail Guard to the High Domain MTA.
10. The Enforce LH Communications IFCPE of the IFCPE Services LH Interface is invoked to determine whether the Mail Guard is allowed to communicate with the Hugh Domain MTA.
11. If the Mail Guard is not allowed to communicate with the High Domain MTA, the connection attempt is rejected.
12. If the Mail Guard is allowed to communicate with the High Domain MTA, the connection attempt is passed on the Network in the High Domain using the ForwardNetworkLH operation of the Communication Access Service HL Interface.

7.3.3 MG Low to High Pattern

Figure 26 provides an overview of Transfer Informal Email Services – Low To High, which is an example of the Low to High Cross Domain Information Exchange Pattern. It is invoked by an MTA in the Low Domain that wishes to transfer an informal email to a recipient in the High Domain, and determines the destination host for the High Domain recipient is the Mail Guard residing within the IEG-C[4].

[4] This routing decision is performed in the Low Domain and is not enforced by the Mail Guard.

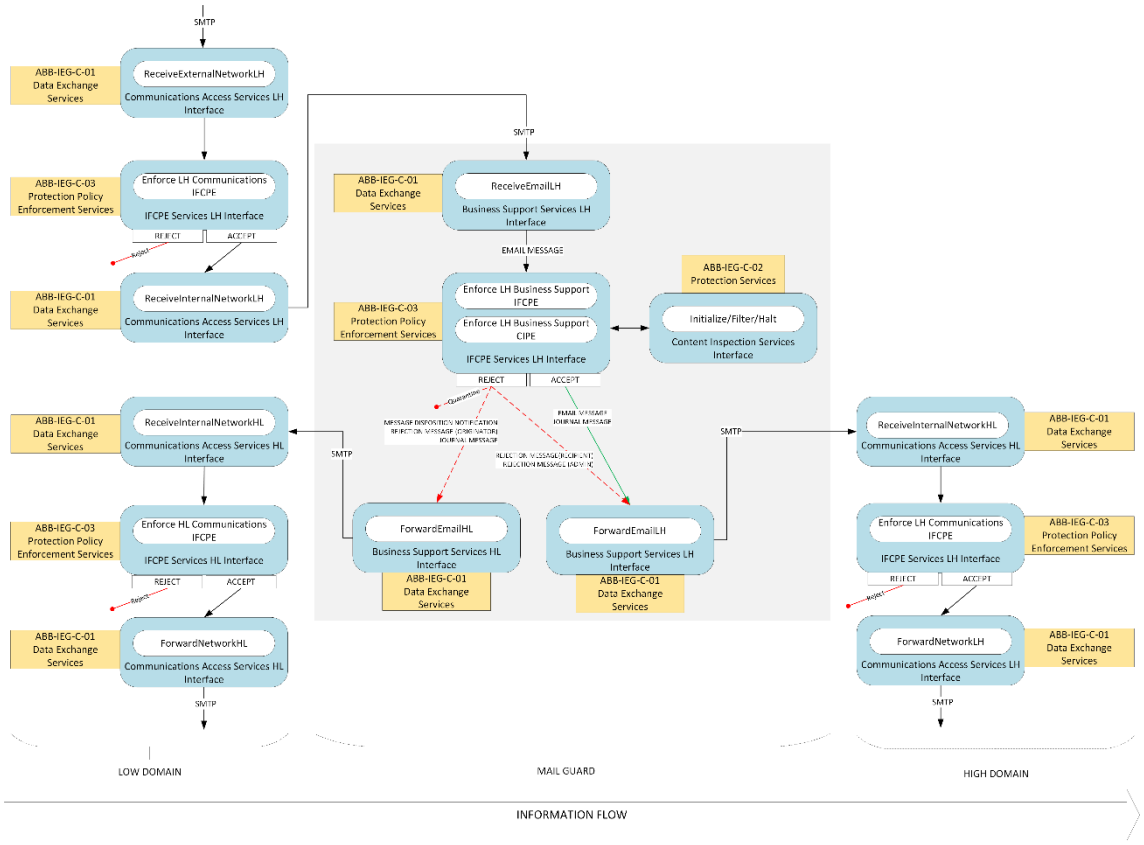

Figure 26: Transfer Informal Email Service Low To High

The Transfer Informal Email Services – Low To High consists of the following steps:

1. The Communication Access Services LH Interface of the Data Exchange Services receives the SMTP transfer operation from an MTA in the Low Domain and invokes the ReceiveExternalNetworkLH operation.

The Enforce LH Communications IFCPE of the IFCPE Service LH Interface is invoked to determine whether the Low Domain MTA is allowed to communicate with the Mail Guard.

If the Low Domain MTA is not allowed to communicate with the Mail Guard, the connection attempt is rejected.

If the Low Domain MTA is allowed to communicate with the Mail Guard, the connection attempt is passed on the Internal Network within the IEG-C using the ReceiveInternalNetworkLH operation of the Communication Access Service LH Interface.

The Mail Guard receives the email message on the Business Services LH Interface with the ReceiveEmailLH operation.

The Policy Protection Enforcement Services applies the Enforce LH Business Services IFCPE of the Business Services LH Interface to determine if the email message is allowed to flow from the Low Domain to the High Domain.

In turn, the Enforce LH Business Services IFCPE operation calls the Enforce LH Business Services CIP to determine if the email message is compliant with the content inspection policy and is therefore allowed to flow from the Low Domain to the High Domain.

The Enforce LH Business Support CIP calls the Initialize/Filter/Halt operation of the Content Inspections Services to verify that the email messages:

(i) contains only attachments allowed by the CIP;

(ii) contains less than the maximum number of attachments allowed by the CIP;

(iii) does not contain any attachments that contain malware;

(iv) contains a valid sensitivity marking allowed by the CIP;

(v) is from an originator allowed by the CIP;

(vi) is destined for a recipient allowed by the CIP;

If the email message is compliant with the content inspection policy, the Protection Policy Enforcement Services:

(i) pass the email to the ForwardEmailLH operation of the Business Support Service LH Interface; and

(ii) optionally sends a copy of the email message to a journal recipient.

(iii) optionally generates an SNMP trap.

If the email message is not compliant with the content inspection policy, the Protection Policy Enforcement Service:

(ix) does not pass the email to the ForwardEmailLH operation of the Business Support Service LH Interface;

(x) optionally generates a delivery status notification for the email message and passes it to the ForwardEmailHL operation of the Business Support Services HL Interfaces;

(xi) optionally generates a rejection message for the email message;

(xii) optionally sends the rejection message to the email message originator by passing it to the ForwardEmailHL operation of the Business Support Services HL Interfaces;

(xiii) optionally sends the rejection message to the email message recipients by passing it to the ForwardEmailLH operation of the Business Support Services LH Interfaces;

(xiv) optionally sends the rejection message to the mail guard administrator by passing it to the ForwardEmailLH operation of the Business Support Services LH Interfaces;

(xv) optionally sends a copy of the non-compliant email message to a journal recipient;

(xvi) optionally, quarantines the message (for later manual handling by an administrator); and

(xvii) optionally generates an SNMP trap.

2. Note that an email message may contain multiple recipients and may therefore be compliant with the CIP for some recipients and non-compliant for other recipients. . In this case, the MG may accept the message for some recipients and reject message for other recipients

3. The ForwardEmailLH operation determines the High Domain MTA that the email message, journal message and rejection message should be transferred to.

4. The ReceiveInternalNetworkLH operation of the Communications Access Services LH Interface receives the SMTP request from the Mail Guard to the High Domain MTA.
5. The Enforce LH Communications IFCPE of the IFCPE Services LH Interface is invoked to determine whether the Mail Guard is allowed to communicate with the High Domain MTA.
6. If the Mail Guard is not allowed to communicate with the High Domain MTA, the connection attempt is rejected.
7. If the Mail Guard is allowed to communicate with the High Domain MTA, the connection attempt is passed on the Network in the High Domain using the ForwardNetworkLH operation of the Communication Access Service LH Interface.
8. The ForwardEmailHL operation determines the Low Domain MTA that the delivery status notification, journal message and rejection message should be transferred to.
9. The ReceiveInternalNetworkHL operation of the Communications Access Services HL Interface receives the SMTP request from the Mail Guard to the Low Domain MTA.
10. The Enforce LH Communications IFCPE of the IFCPE Services LH Interface is invoked to determine whether the Mail Guard is allowed to communicate with the Low Domain MTA.
11. If the Mail Guard is not allowed to communicate with the Low Domain MTA, the connection attempt is rejected.
12. If the Mail Guard is allowed to communicate with the Low Domain MTA, the connection attempt is passed on the Network in the Low Domain using the ForwardNetworkHL operation of the Communication Access Service HL Interface.

7.3.4 MG Management Pattern

The MG Management Pattern is composed of the ‘MG Management Self Protection Pattern’ (Figure 27) and the ‘MG Element Management Services Pattern’ (Figure 28). The ‘MG Management Self Protection Pattern’ enforces the policy MG_IFP_MGMT, and the ‘MG Element Management Services Pattern’ enables management of the operating system and the MG ABBs. Management services at the MG are offered by the ABB ‘Element Management Services’ (see Section 7.7). The MG Management Pattern also applies to management traffic initiated at the MG with external destination (related to the operations described in Sections 7.7.7and 7.7.8).

7.3.4.1 MG Management Self Protection Pattern

Figure 27 shows the ‘MG Management Self Protection Pattern’. The pattern forwards incoming management traffic to the ‘MG Element Management Services Pattern’. Traffic that is output by the ‘MG Element Management Services Pattern’ is picked up again by the ‘MG Management Self Protection Pattern’. It is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

- [START]
- Data Exchange Services -> Communications Access Services Management -> ReceiveNetworkManagement

- Protection Policy Enforcement Services -> IFCPE Services Management -> EnforceManagemenCommunicationstIFCPE [IFP: MG_IFP_MGMT_IN] -> ‘MG Element Management Services Pattern’
- Processing by ‘MG Element Management Services Pattern’ (Figure 28)
- ‘MG Element Management Services Pattern’ -> Protection Policy Enforcement Services -> IFCPE Services Management -> EnforceManagementCommunicationsIFCPE [IFP: MG_IFP_MGMT_OUT]
- Data Exchange Services -> Communications Access Services Management -> ForwardNetworkManagement
- [END]

Traffic will follow the pattern from [START] to [END] if no policy violation occurs. If enforcement of MG_IFP_MGMT_IN or MG_IFP_MGMT_OUT results in a policy violation, traffic will be rejected and an action shall be executed as specified in [SRS-7-125].

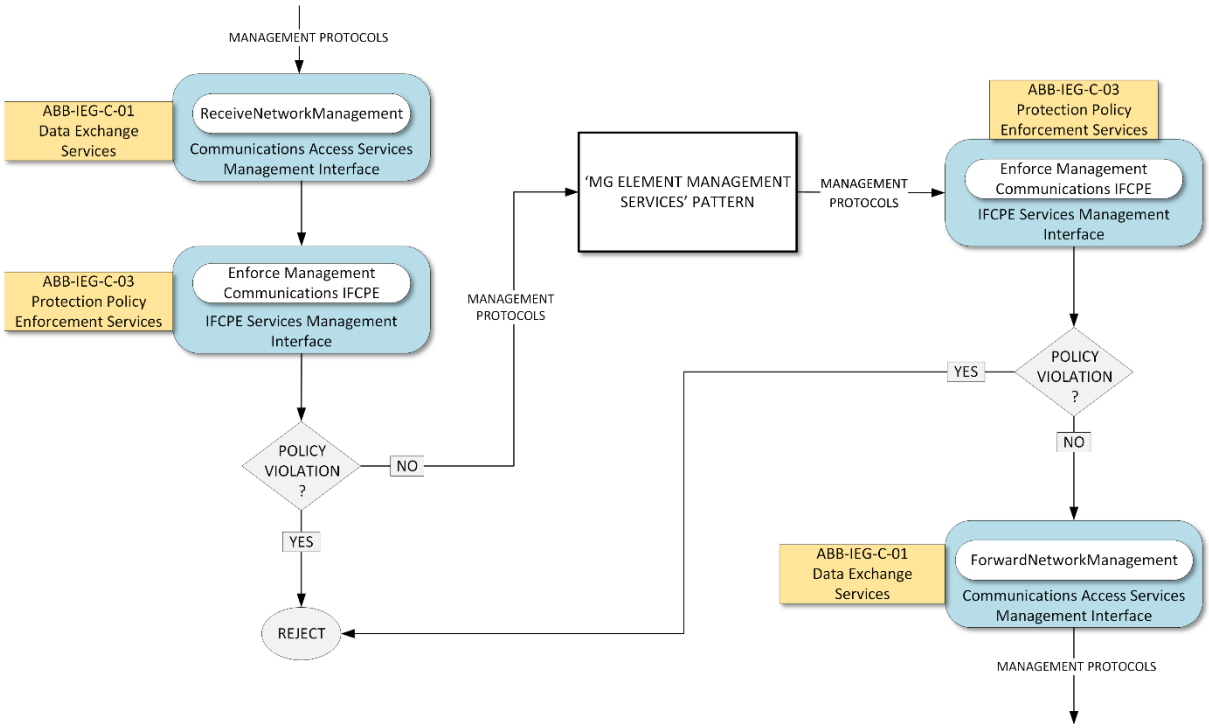

Figure 27: MG Management Self Protection Pattern; this pattern is connected to the pattern ‘MG Element Management Services’ and enforces an IFP on incoming and outgoing management traffic

7.3.4.2 MG Element Management Services Pattern

Figure 28 shows the ‘MG Element Management Services Pattern’. The pattern takes input from and outputs to the ‘MG Management Self Protection Pattern’. It is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

- ‘MG Management Self Protection Pattern’ - > [START] Data Exchange Services -> Core Services Management -> ReceiveManagementContent
- Element Management Services -> CIS Security -> Manage Protection Policies / Review / Manage Public Key Material

OR:

- Element Management Services -> SMC Configuration Management -> Configure OS / Configure Protection Policy Enforcement Services / Configure Data Exchange Services / Configure Protection Services
  OR:
- Element Management Services -> Event Management -> Log / Alert / Report
  OR:
- Element Management Services -> Cyber Defence -> Assess / Response / Recover
  OR:
- Element Management Services -> Performance Management -> Monitor / Meter / Track Messages
  OR:
- Data Exchange Services -> Core Services Management -> ForwardManagementContent
- Protection Services -> Public Key Cryptographic Services -> Encrypt (Required if TLS connection is used)
- [END] -> ‘MG Management Self Protection Pattern’

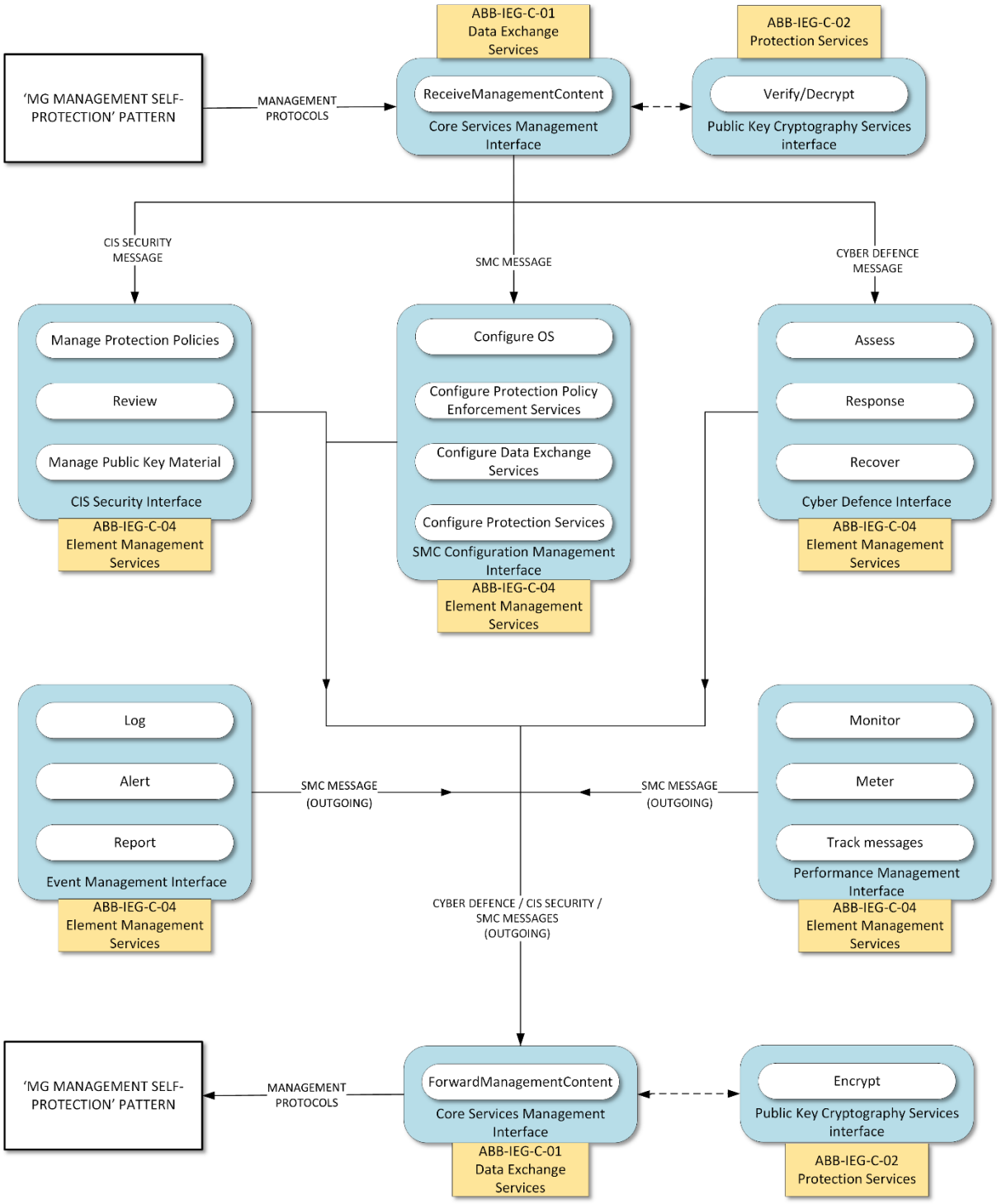

Figure 28: MG Element Management Services Pattern; this pattern takes input from and outputs to the 'MG Management Self Protection Pattern'

7.3.4.3 Types of Management Content

Note that the payload (i.e. the management content) of the management protocols that are processed at the interface 'Core Services Management' is referred to as a 'management message'. There are three types of management message:

- CIS Security message