- SMC message; or
- Cyber Defence message.

All the management messages that are delivered to one of the interfaces of 'Element Management Services' are referred to as 'incoming management messages'. The incoming management messages are processed by one of the operations of 'Element Management Services'. The result of the processing is a management message of the same type; these are referred to as 'outgoing management messages'. At the interface 'Core Services Management' the outgoing management messsages are forwarded as payload of the appropriate management protocol by the operation 'ForwardManagementContent'.

Note that operations of 'Element Management Services' can also generate outgoing management messages that have not been preceded by an incoming management messages.

The next sections group the functional requirements for the MG per IEG-C ABB and assume the MG patterns from Section 7.3.

7.4 Data Exchange Services

The terms 'high domain' and 'low domain' used in this section are to be interpreted according to Table 18.

7.4.1 Interfaces

7.4.1.1 MG_DEX

Requirement ID: [SRS-7-1]

The MG MUST provide a data exchange capability MG_DEX that facilitates the mediation of data between the high domain and the low domain.

7.4.1.2 MG_IF_NET_HIGH

Requirement ID: [SRS-7-2]

The MG SHALL offer a physical network interface MG_IF_NET_HIGH that provides Ethernet connectivity to the high domain.

Requirement ID: [SRS-7-3]

MG_IF_NET_HIGH SHALL support an operation 'ReceiveHigh' that receives (transfer-in) data from the high domain for processing by the MG.

Requirement ID: [SRS-7-4]

MG_IF_NET_HIGH SHALL support an operation 'ForwardHigh' that forwards (transfer-out) data that has been processed by the MG to the high domain.

7.4.1.3 MG_IF_NET_LOW

Requirement ID: [SRS-7-5]

The MG SHALL offer a physical network interface MG_IF_NET_LOW that provides Ethernet connectivity to the low domain.

Requirement ID: [SRS-7-6]

MG_IF_NET_LOW SHALL support an operation ‘ReceiveLow’ that receives (transfer-in) data from the low domain for processing by the MG.

Requirement ID: [SRS-7-7]

MG_IF_NET_LOW SHALL support an operation ‘ForwardLow’ that forwards (transfer-out) data that has been processed by the MG to the low domain.

7.4.1.4 MG_IF_MGMT

Requirement ID: [SRS-7-8]

The MG MAY offer a physical network interface MG_IF_MGMT that provides Ethernet connectivity to the management domain.

Requirement ID: [SRS-7-9]

If the MG does not offer a physical network interface MG_IF_MGMT, the MG SHALL offer a logical network interface MG_IF_MGMT on top of MG_IF_NET_HIGH.

Requirement ID: [SRS-7-10]

MG_IF_MGMT SHALL support an operation ‘ReceiveManagement’ that receives data from the management domain for processing by the MG.

Requirement ID: [SRS-7-11]

MG_IF_MGMT SHALL support an operation ‘ForwardManagement’ that forwards data that has been processed by the MG to the management domain.

7.4.2 Communication Access Services

7.4.2.1 Communications Access Services HL

Requirement ID: [SRS-7-12]

MG_DEX MUST offer a IPv4 and IPv6, [IETF RFC 791, 1981], and [IETF RFC 8200, 2017] over Ethernet interface ‘Communications Access Services HL’ on top of MG_IF_NET_HIGH and MG_IF_NET_LOW.

7.4.2.1.1 ReceiveInternalNetworkHL

Requirement ID: [SRS-7-13]

The interface ‘Communications Access Services HL’ MUST support an operation ‘ReceiveInternalNetworkHL’ on top of MG_IF_NET_HIGH that provides TCP/IP connectivity on the high domain by receiving IP traffic for processing by the MG.

Requirement ID: [SRS-7-14]

The operation ‘ReceiveInternalNetworkHL’ MUST support error handling as specified in [IETF RFC 7414, 2015].

7.4.2.1.2 ForwardInternalNetworkHL

Requirement ID: [SRS-7-15]

The interface ‘Communications Access Services HL’ MUST support an operation ‘ForwardInternalNetworkHL’ on top of MG_IF_NET_LOW that forwards IP traffic to the low domain.

Requirement ID: [SRS-7-16]

The operation ‘ForwardInternalNetworkHL’ MUST support error handling as specified in [IETF RFC 7414, 2015].

7.4.2.2 Communications Access Services LH

Requirement ID: [SRS-7-17]

MG_DEX MUST offer a IPv4 and IPv6, [IETF RFC 791, 1981], and [IETF RFC 8200, 2017], over Ethernet interface ‘Communications Access Services LH’ on top of MG_IF_NET_LOW and MG_IF_NET_HIGH.

7.4.2.2.1 ReceiveInternalNetworkLH

Requirement ID: [SRS-7-18]

The interface ‘Communications Access Services LH’ MUST support an operation ‘ReceiveInternalNetworkLH’ on top of MG_IF_NET_LOW that provides TCP/IP connectivity on the low domain by receiving IP traffic for processing by the MG.

Requirement ID: [SRS-7-19]

The operation ‘ReceiveInternalNetworkLH’ MUST support error handling as specified in [IETF RFC 7414, 2015].

7.4.2.2.2 ForwardInternalNetworkLH

Requirement ID: [SRS-7-20]

The interface ‘Communications Access Services LH’ MUST support an operation ‘ForwardInternalNetworkLH’ on top of MG_IF_NET_HIGH that forwards IP traffic to the high domain.

Requirement ID: [SRS-7-21]

The operation 'ForwardInternalNetworkLH' MUST support error handling as specified in [IETF RFC 7414, 2015].

7.4.3 Business Support Services

7.4.3.1 Business Support Service LH Interface

7.4.3.1.1 ReceiveEmailLH

Requirement ID: [SRS-7-22]

The Business Support Service LH Interface SHALL support an operation "ReceiveEmailLH" that supports the reception of an email message from the Low Domain.

Requirement ID: [SRS-7-23]

The "ReceiveEmailLH" operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].

Requirement ID: [SRS-7-24]

The "ReceiveEmailLH" operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].

Requirement ID: [SRS-7-25]

The "ReceiveEmailLH" operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].

Requirement ID: [SRS-7-26]

The "ReceiveEmailLH" operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].

Requirement ID: [SRS-7-27]

The "ReceiveEmailLH" operation SHALL audit the following information for each email received:

- received time;
- originator;
- recipients;
- subject; and
- message identifier.

7.4.3.2 ForwardEmailLH

Requirement ID: [SRS-7-28]

The Business Support Service LH Interface SHALL support an operation "ForwardEmailLH" that supports the transfer of an email message to the low domain.

Requirement ID: [SRS-7-29]

The “ForwardEmailLH” operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].

Requirement ID: [SRS-7-30]

The “ForwardEmailLH” operation SHALL be compliant with the Internet Message Format [IETF RFC 5322, 2008].

Requirement ID: [SRS-7-31]

The “ForwardEmailLH” operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].

Requirement ID: [SRS-7-32]

The “ForwardEmailLH” operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].

Requirement ID: [SRS-7-33]

The “ForwardEmailLH” operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].

Requirement ID: [SRS-7-34]

The ‘ForwardEmailLH” operation SHALL be configurable to determine the destination host of a recipient from either DNS MX records or local configuration.

Requirement ID: [SRS-7-35]

The local configuration of the destination hosts for the ‘ForwardEmailLH” operation SHALL allow the use of wildcards in the domain name.

Requirement ID: [SRS-7-36]

The “ForwardEmailLH” operation SHALL allow the use the best match when determining the destination host from local configuration.

Requirement ID: [SRS-7-37]

The “ForwardEmailLH” operation SHALL be able to rewrite the originator and recipient email addresses in both the Simple Mail Transfer Protocol and the Internet Message Format.

Requirement ID: [SRS-7-38]

The “ForwardEmailLH” address rewriting SHALL allow the rewriting of both the local-part and the domain components of the email address.

7.4.3.3 Business Support Services HL Interface

7.4.3.3.1 ReceiveEmailHL

Requirement ID: [SRS-7-39]

The Business Support Service LH Interface SHALL support an operation "ReceiveEmailHL" that supports the reception of an email message from the high domain.

Requirement ID: [SRS-7-40]

The "ReceiveEmailHL" operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].

Requirement ID: [SRS-7-41]

The "ReceiveEmailHL" operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].

Requirement ID: [SRS-7-42]

The "ReceiveEmailHL" operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].

Requirement ID: [SRS-7-43]

The "ReceiveEmailHL" operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].

7.4.3.3.2 ForwardEmailHL

Requirement ID: [SRS-7-44]

The Business Support Service HL Interface SHALL support an operation "ForwardEmailLH" that supports the transfer of an email message to the high domain.

Requirement ID: [SRS-7-45]

The "ForwardEmailHL" operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].

Requirement ID: [SRS-7-46]

The "ForwardEmailHL" operation SHALL be compliant with the Internet Message Format [IETF RFC 5322, 2008].

Requirement ID: [SRS-7-47]

The "ForwardEmailHL" operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].

Requirement ID: [SRS-7-48]

The “ForwardEmailHL” operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].

Requirement ID: [SRS-7-49]

The “FowardEmailHL” operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].

Requirement ID: [SRS-7-50]

The ‘ForwardEmailHL” operation SHALL be configurable to determine the destination host of a recipient from either DNS MX records or local configuration.

Requirement ID: [SRS-7-51]

The local configuration of the destination hosts for the ‘ForwardEmailLH” operation SHALL allow the use of wildcards in the domain name.

Requirement ID: [SRS-7-52]

The local configuration of the destination hosts for the ‘ForwardEmailHL” operation SHALL allow the use of wildcards in the domain name.

Requirement ID: [SRS-7-53]

The ‘ForwardEmailHL” operation SHALL allow the use the best match when determining the destination host from local configuration.

Requirement ID: [SRS-7-54]

The “ForwardEmailHL” operation SHALL be able to rewrite the originator and recipient email addresses in both the Simple Mail Transfer Protocol and the Internet Message Format.

Requirement ID: [SRS-7-55]

The “ForwardEmailHL” address rewriting SHALL allow the rewriting of both the local-part and the domain components of the email address.

7.4.4 Communication Access Management Services

7.4.4.1 Communications Access Services Management

Requirement ID: [SRS-7-56]

MG_DEX MUST offer a IPv4 and IPv6 [IETF RFC 791, 1981], and [IETF RFC 8200, 2017], over Ethernet interface ‘Communications Access Services Management’ on top of MG_IF_MGMT.

7.4.4.1.1 ReceiveNetworkManagement

Requirement ID: [SRS-7-57]

The interface ‘Communications Access Services Management’ MUST support an operation ‘ReceiveNetworkManagement’ that provides TCP/IP connectivity on the management domain by receiving IP traffic for processing by the MG.

Requirement ID: [SRS-7-58]

The operation ‘ReceiveNetworkManagement’ MUST support error handling as specified in [IETF RFC 7414, 2015].

7.4.4.1.2 ForwardNetworkManagement

Requirement ID: [SRS-7-59]

The interface ‘Communications Access Services Management’ MUST support an operation ‘ForwardNetworkManagement’ that forwards IP traffic to the management domain.

Requirement ID: [SRS-7-60]

The operation ‘ForwardNetworkManagement’ MUST support error handling as specified in [IETF RFC 7414, 2015].

7.4.5 Core Services Management

7.4.5.1 Core Services Management

Requirement ID: [SRS-7-61]

MG_DEX MUST offer an interface ‘Core Services Management’ on top of ‘Communications Access Services Management’.

Requirement ID: [SRS-7-70]

The interface ‘Core Services Management’ MUST support of the following management protocols:

- Simple Network Management Protocol (SNMP) Version 3 [IETF RFC 3410 - 3418, 2002];
- Syslog;
- Network Time Protocol;
- Intelligent Platform Management Interface (IPMI) [IPMI V2.0, 2013];
- Hyper-Text Transport Protocol (HTTP) Web interface [IETF RFC 7230, 2014] and [IETF RFC 7231, 2014];
- Remote Desktop (RDP).

Requirement ID: [SRS-7-71]

The interface ‘Core Services Management’ MAY support the following management protocols:

- Remote Procedure Call (RPC).
- Keyboard, video and mouse (KVM) over Ethernet;
- Command Line interface (CLI) via Secure Shell (SSH) Transport Layer protocol [IETF RFC 4251, 2006];

7.4.5.1.1 ReceiveManagementContent

Requirement ID: [SRS-7-72]

The interface ‘Core Services Management’ MUST support an operation ‘ReceiveManagementContent’ that receives external management traffic for further processing.

Requirement ID: [SRS-7-73]

The operation ‘ReceiveManagementContent’ MUST support Transport Layer Security (TLS), [IETF RFC 8446, 2018].

Requirement ID: [SRS-7-74]

The operation ‘ReceiveManagementContent’ MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].

Requirement ID: [SRS-7-75]

The operation ‘ReceiveManagementContent’ MUST support the invocation of the operations ‘Verify’ (7.6.2.2.1) and ‘Decrypt’ (7.6.2.2.4) at the interface ‘Public Key Cryptographic Services’ ([SRS-7-296]) provided by MG_PKCS ([SRS-7-294]).

Requirement ID: [SRS-7-76]

The operation ‘ReceiveManagementContent’ SHALL pass management content in the form of a management message to the appropriate interface offered by MG_MGMT ([SRS7-302]) for further processing.

7.4.5.1.2 ForwardManagementContent

Requirement ID: [SRS-7-77]

The interface ‘Core Services Management’ MUST support an operation ‘ForwardManagementContent’ that accepts outgoing management messages for further processing.

Requirement ID: [SRS-7-78]

After receiving a management message from one of the interfaces offered by MG_MGMT ([SRS-7-302]), the operation ‘ForwardManagementContent’ SHALL forward the management message, as payload of the appropriate management protocol, to the management domain.

Requirement ID: [SRS-7-79]

The operation ‘ForwardManagementContent’ MUST support Transport Layer Security (TLS), [IETF RFC 8446, 2018].

Requirement ID: [SRS-7-80]

The operation ‘ForwardManagementContent’ MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].

Requirement ID: [SRS-7-81]

The operation ‘ForwardManagementContent’ MUST support the invocation of the operation ‘Encrypt’ (7.6.2.2.3) at the interface ‘Public Key Cryptographic Services’ provided by MG_PKCS ([SRS-7-294]).

7.5 Protection Policy Enforcement Services

7.5.1 Information Flow Control Policy (IFP) Enforcement

7.5.1.1 MG_IFCPE

Requirement ID: [SRS-7-82]

The MG MUST provide an information flow control policy enforcement (IFCPE) capability MG_IFCPE that enables the MG to:

- Mediate the flow of information between MG_IF_NET_HIGH and MG_IF_NET_LOW in accordance with the MG information flow policy MG_IFP;
- Control incoming and outgoing management traffic at MG_IF_MGMT in accordance with the MG information flow policy MG_IFP.

Requirement ID: [SRS-7-83]

Mediate the flow of information between MG_IF_NET_HIGH and MG_IF_NET_LOW in accordance with the MG information flow policy MG_IFP;

Requirement ID: [SRS-7-84]

Control incoming and outgoing management traffic at MG_IF_MGMT in accordance with the MG information flow policy MG_IFP.

7.5.1.2 IFCPE Services High To Low

Requirement ID: [SRS-7-86]

For the flow of information from MG_IF_NET_HIGH to MG_IF_NET_LOW, MG_IFCPE MUST offer an interface ‘IFCPE Services High to Low’ that accepts information for further processing.

7.5.1.2.1 Enforce HL Communications IFCPE

Requirement ID: [SRS-7-87]

The interface ‘IFCPE Services High to Low’ MUST support an operation ‘Enforce HL Communications IFCPE’ that enforces the policy MG_IFP_CA_HL.

Requirement ID: [SRS-7-88]

The operation ‘Enforce HL Communications IFCPE’ SHOULD enforce the policy MG_IFP_CA_HL_IN on the following information flow:

- Source: Communications Access Services HL Interface -> ReceiveInternalNetworkHL;
- Destination: Business Support Services HL Interface -> ReceiveEmailHL;
- Information: SMTP(S) traffic;
- Operation: pass SMTP(S) traffic by ensuring the following conditions:
  - MG_IFP_CA_HL_IN permits information flow.

Requirement ID: [SRS-7-89]

The operation ‘Enforce HL Communications IFCPE’ SHALL enforce the policy MG_IFP_CA_HL_OUT on the following information flow:

- Source: SOA Platform HL Interface -> ForwardEmailHL;
- Destination: Communications Access Services HL Interface -> ForwardNetworkHL;
- Information: SMTP(S) traffic;
- Operation: pass SMTP(S) traffic by ensuring the following conditions:
  - MG_IFP_CA_HL_OUT permits information flow.

Requirement ID: [SRS-7-500]

If MG_IFP_CA_HL_IN or MG_IFP_CA_HL_OUT does not permit information flow, the MG SHALL execute the actions specified in MG_IFP_CA_HL.

Requirement ID: [SRS-7-90]

For every action taken, the operation ‘Enforce HL Communications IFCPE’ SHALL invoke the operation ‘Log’ at the interface ‘Event Management’ and log the action.

Requirement ID: [SRS-7-91]

If MG_IFP_CA_HL does not permit the release of information due to a policy violation, the MG SHALL invoke the operation ‘Log’ at the interface ‘Event Management’ and log the outcome O_MG_IFCPE.

Requirement ID: [SRS-7-92]

The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_IFP_CA_HL

7.5.1.2.2 Enforce HL Business Support IFCPE

Requirement ID: [SRS-7-93]

The interface ‘IFCPE Services High to Low’ MUST support an operation ‘Enforce HL Business Support IFCPE’ that enforces the policy MG_IFP_BS_HL.

Requirement ID: [SRS-7-94]

The operation ‘Enforce HL Business Support IFCPE’ SHALL enforce the policy MG_IFP_BS_HL on the following information flow:

- Source: Business Support Services HL Interface->ReceiveEmailHL;
- Destination: Business Support Services HL Interface >ForwardEmailHL;
- Information: SMTP Messages;
- Operation: pass SMTP Messages from source to destination ensuring the following conditions:
  - the SMTP Message has been processed by the MG content inspection policy enforcement capability MG_CIPE ([SRS-7-169]) based on the content inspection policy MG_CIP_HL (Table 19, 7.5.4.3 and 7.5.4.4);
  - Based on the outcome of processing by MG_CIPE, MG_IFP_BS_HL permits the release of the SMTP Message to the low domain.

Requirement ID: [SRS-7-95]

The operation ‘Enforce HL Business Support IFCPE’ MUST support the invocation of the operation ‘Enforce HL Business Support CIPE’ at the interface ‘CIPE Services High to Low’ ([SRS-7-173]). The operation ‘Enforce HL Business Support CIPE’ SHALL take as input:

- The SMTP message that is being processed;
- The policy MG_CIP_HL.

Requirement ID: [SRS-7-96]

If MG_IFP_BS_HL does not permit the release of information, the MG SHALL execute the actions specified in MG_IFP_BS_HL.

Requirement ID: [SRS-7-97]

For every action taken, the operation ‘Enforce HL Business Support IFCPE’ SHALL invoke the operation ‘Log’ (7.7.7.1.1) at the interface ‘Event Management’ ([SRS-7-392]) and log the action.

Requirement ID: [SRS-7-98]

If MG_IFP_SOA_HL does not permit the release of information due to a policy violation, the MG SHALL invoke the operation ‘Log’ 7.7.7.1.1) at the interface ‘Event Management’ ([SRS-7-392]) and log the outcome O_MG_IFCPE ([SRS-7-91]).

Requirement ID: [SRS-7-99]

The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_IFP_BS_HL.

7.5.1.3 IFPCPE Services Low To High

Requirement ID: [SRS-7-100]

For the flow of information from MG_IF_NET_LOW to MG_IF_NET_HIGH, MG_IFCPE MUST offer an interface ‘IFCPE Services Low to High’ that accepts information for further processing.

7.5.1.3.1 Enforce LH Communications IFCPE

Requirement ID: [SRS-7-101]

The interface ‘IFCPE Services Low to High’ MUST support an operation ‘Enforce LH Communications IFCPE’ that enforces the policy MG_IFP_CA_LH.

Requirement ID: [SRS-7-102]

The operation ‘Enforce LH Communications IFCPE’ SHOULD enforce the policy MG_IFP_CA_LH_IN on the following information flow:

- Source: Communications Access Services LH Interface -> ReceiveInternalNetworkLH;
- Destination: Business Support Services LH Interface -> ReceiveEmailLH;
- Information: SMTP(S) traffic;
- Operation: pass SMTP(S) traffic by ensuring the following conditions:
    - MG_IFP_CA_LH_IN permits information flow.

Requirement ID: [SRS-7-103]

The operation ‘Enforce LH Communications IFCPE’ SHOULD enforce the policy MG_IFP_CA_LH_OUT on the following information flow:

- Source: Business Support Services LH Interface -> ForwardEmailLH;
- Destination: Communications Access Services LH Interface -> ForwardEmailLH;
  Information: SMTP(S) traffic;
- Operation: pass SMTP(S) traffic by ensuring the following conditions:
    - MG_IFP_CA_LH_OUT permits information flow.

Requirement ID: [SRS-7-501]

If MG_IFP_CA_LH_IN or MG_IFP_CA_LH_OUT do not permit information flow, the MG SHALL execute the actions specified in MG_IFP_CA_LH.

Requirement ID: [SRS-7-104]

For every action taken, the operation ‘Enforce LH Communications IFCPE’ SHALL invoke the operation ‘Log’ (7.7.7.1.1) at the interface ‘Event Management’ ([SRS-7-392]) and log the action.

Requirement ID: [SRS-7-105]

If MG_IFP_CA_LH does not permit the release of information due to a policy violation, the MG SHALL invoke the operation 'Log' (7.7.7.1.1) at the interface 'Event Management' ([SRS-7-392]) and log the outcome O_MG_IFCPE ([SRS-7-91]).

Requirement ID: [SRS-7-106]

The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_IFP_CA_LH.

7.5.1.3.2 Enforce LH Business Support IFCPE

Requirement ID: [SRS-7-107]

The Business Support Services IFCPE SHALL enforce the information flow control policy to mediate the flow of email between the Low Domain and the High Domain.

Requirement ID: [SRS-7-108]

The Business Support Services IFCPE SHALL maintain a separate Business Support Services IFCP for the flow of information from the Low Domain to the High Domain (IEG-C_IFP_BS_EMAIL_LH).

Requirement ID: [SRS-7-109]

The Business Support Services IFCP from the Low Domain to the High Domain (IEG-C_IFP_BS_EMAIL_LH) shall identify a Business Support Service CIP (IEG-C_CIP_BS_EMAIL_LH) (see section 7.2.3).

Requirement ID: [SRS-7-110]

The Enforce LH Business Support IFCPE operation SHALL call the Enforce LH Business Support CIP operation to determine if the email message from the Low Domain is compliant with the CIP (see section 7.2.3).

7.5.1.4 IFCP Services Management

Requirement ID: [SRS-7-111]

For incoming and outgoing management traffic at MG_IF_MGMT, MG_IFCPE MUST offer an interface 'IFCPE Services Management' that accepts information for further processing.

7.5.1.4.1 Enforce Management Communication IFCPE

Requirement ID: [SRS-7-112]

The interface 'IFCPE Services Management' MUST support an operation 'Enforce Management Communications IFCPE' that enforces the policy MG_IFP_MGMT.

Requirement ID: [SRS-7-113]

The operation 'Enforce Management Communications IFCPE' SHALL enforce the policy MG_IFP_MGMT_IN on the following information flow:

- Source: Communications Access Services Management Interface -> ReceiveNetworkManagement
- Destination: Core Services Management Interface -> ReceiveManagementContent
- Information: Management traffic.
- Operation: pass management traffic by ensuring the following conditions:
    - Management traffic is filtered based on source IP addresses and ports, destination IP addresses, ports and protocol fields;
    - MG_IFP_MGMT_IN permits information flow.

Requirement ID: [SRS-7-114]

The operation ‘Enforce Management Communications IFCPE’ SHALL enforce the policy MG_IFP_MGMT_OUT on the following information flow:

- Source: Core Services Management Interface -> ForwardManagementContent
- Destination: Communications Access Services Management Interface -> ForwardNetworkManagement
- Information: Management traffic.
- Operation: pass management traffic by ensuring the following conditions:
    - Management traffic is filtered based on source IP addresses and ports, destination IP addresses, ports and protocol fields;
    - MG_IFP_MGMT_OUT permits information flow.

Requirement ID: [SRS-7-115]

If MG_IFP_MGMT_IN or MG_IFP_MGMT_OUT do not permit information flow, the MG SHALL execute the action specified in MG_IFP_MGMT.

Requirement ID: [SRS-7-116]

For every action taken, the operation ‘Enforce Management Communications IFCPE’ SHALL invoke the operation ‘Log’ (7.7.1.1) at the interface ‘Event Management’ ([SRS-7-392]) and log the action.

Requirement ID: [SRS-7-117]

If MG_IFP_MGMT does not permit the release of information due to a policy violation, the MG SHALL invoke the operation ‘Log’ 7.7.7.1.1) at the interface ‘Event Management’ ([SRS-7-392]) and log the outcome O_MG_IFCPE ([SRS-7-91]).

Requirement ID: [SRS-7-118]

The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_IFP_MGMT.

7.5.2 Information Flow Control Policies

Requirement ID: [SRS-7-119]

MG_IFP SHALL be configurable.

Requirement ID: [SRS-7-120]

MG_IFP SHALL specify the actions ACTIONS that need to be executed by MG_IFCPE.

Requirement ID: [SRS-7-121]

For each action in ACTIONS it SHALL be possible to:

- Enable or disable the action.
- Instruct MG_IFCPE to ignore the outcome of the execution of the action.
- If the outcome O_MG_IFCPE of the execution of the action is negative (e.g. verification or validation fails, or a policy violation was determined): instruct MG_IFCPE to continue the enforcement of MG_IFP, or to stop.

Requirement ID: [SRS-7-122]

It SHALL be possible to enable or disable the enforcement of each of the following sub-policies:

- MG_IFP_CA_LH_IN;
- MG_IFP_CA_LH_OUT;
- MG_IFP_CA_HL_IN;
- MG_IFP_CA_HL_OUT;
- MG_IFP_MGMT_IN;
- MG_IFP_MGMT_OUT;
- MG_IFP_BS_LH;
- MG_IFP_BS_HL.

Requirement ID: [SRS-7-123]

MG_IFP SHALL specify the level of granularity of the outcome O_MG_IFCPE.

Requirement ID: [SRS-7-124]

It SHALL be possible for MG_IFCPE to distinguish within O_MG_IFCPE:

- The sub-policy ([SRS-7-122]) that was enforced when a policy violation was determined;
- Identification of the action that led to the policy violation;
- Reason for policy violation.

Requirement ID: [SRS-7-125]

The policies MG_IFP_CA_HL, MG_IFP_CA_LH and MG_IFP_MGMT SHALL specify:

- That an information flow (as described in 7.5.1.2.2, 7.5.1.3.2 and 7.5.1.4.1 respectively) is not permitted if the outcome O_MG_IFCPE constitutes a policy violation;
- The action the MG shall take in case information flow is not permitted. The possible actions SHALL include:
  - Silently drop traffic;
  - Reset the TCP/IP connection.

Requirement ID: [SRS-7-126]

The policy MG_IFP_CA_HL_IN SHALL specify the actions ACTIONS_MG_CA_HL_IN that the operation ‘Enforce HL Communications IFCPE’ SHALL execute for the information flow described in ([SRS-7-86]).

Requirement ID: [SRS-7-127]

ACTIONS_MG_CA_HL_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_HL_IN.

Requirement ID: [SRS-7-450]

The policy MG_IFP_CA_HL_OUT SHALL specify the actions ACTIONS_MG_CA_HL_OUT that the operation ‘Enforce HL Communications IFCPE’ SHALL execute for the information flow described in ([SRS-7-89]).

Requirement ID: [SRS-7-451]

ACTIONS_MG_CA_HL_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_HL_OUT.

Requirement ID: [SRS-7-128]

The policy MG_IFP_CA_LH_IN SHALL specify the actions ACTIONS_MG_CA_LH_IN that the operation ‘Enforce LH Communications IFCPE’ SHALL execute for the information flow described in 7.5.1.2.4.2.

Requirement ID: [SRS-7-129]

ACTIONS_MG_CA_LH_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_LH_IN.

Requirement ID: [SRS-7-130]

The policy MG_IFP_CA_LH_OUT SHALL specify the actions ACTIONS_MG_CA_LH_OUT that the operation ‘Enforce LH Communications IFCPE’ SHALL execute for the information flow described in ([SRS-7-103]).

Requirement ID: [SRS-7-131]

ACTIONS_MG_CA_LH_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_LH_OUT.

Requirement ID: [SRS-7-132]

The policy MG_IFP_MGMT_IN SHALL specify the actions ACTIONS_MG_MGMT_IN that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in ([SRS-7-88]).

Requirement ID: [SRS-7-452]

ACTIONS_MG_MGMT_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_MG_IFCPE-MGT_IN.

Requirement ID: [SRS-7-133]

The policy MG_IFP_MGMT_OUT SHALL specify the actions ACTIONS_MG_MGMT_OUT that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in ([SRS-7-102]).

Requirement ID: [SRS-7-134]

ACTIONS_MG_MGMT_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_MG_IFCPE-MGT_OUT.

Requirement ID: [SRS-7-135]

The policy MG_IFP_CA_HL SHALL specify RULESET_MG_IFCPE-CA_HL_IN and RULESET_MG_IFCPE-CA_HL_OUT.

Requirement ID: [SRS-7-136]

RULESET_MG_IFCPE-CA_HL_IN and RULESET_MG_IFCPE-CA_HL_OUT SHALL be configurable.

Requirement ID: [SRS-7-137]

The policy MG_IFP_CA_LH SHALL specify RULESET_MG_IFCPE-CA_LH_IN and RULESET_MG_IFCPE-CA_LH_OUT.

Requirement ID: [SRS-7-138]

RULESET_MG_IFCPE-CA_LH_IN and RULESET_MG_IFCPE-CA_LH_OUT SHALL be configurable.

Requirement ID: [SRS-7-139]

The policy MG_IFP_MGMT SHALL specify RULESET_MG_IFCPE-MGT_IN and RULESET_MG_IFCPE-MGT_OUT.

Requirement ID: [SRS-7-140]

RULESET_MG_IFCPE-MGT_IN and RULESET_MG_IFCPE-MGT_OUT SHALL be configurable.

Requirement ID: [SRS-7-141]

Each of the rulesets RULESET_MG_IFCPE-CA_HL_IN, RULESET_MG_IFCPE-CA_HL_OUT, RULESET_MG_IFCPE-CA_LH_IN, RULESET_MG_IFCPE-CA_LH_OUT, RULESET_MG_IFCPE-MGT_IN, RULESET_MG_IFCPE-MGT_OUT SHALL include:

- Identification of traffic flow that is allowed or disallowed based on source and destination IP addresses;
- Identification of traffic that is allowed or disallowed based on protocols and ports;
- Identification of traffic that is allowed or disallowed based on values of protocol fields.

Requirement ID: [SRS-7-142]

The policy MG_IFP_BS_HL SHALL specify:

- That a release of information to the low domain is not permitted if O_MG_CIPE_HL ([SRS-7-178]) constitutes a policy violation;
- The action the MG shall take in case of a policy violation, see [SRS-7-144]

Requirement ID: [SRS-7-143]

The policy MG_IFP_BS_LH SHALL specify:

- That an import of information to the high domain is not permitted if O_MG_CIPE_LH ([SRS-7-184]) constitutes a policy violation;
- The action the MG shall take in case of a policy violation, see [SRS-7-144].

Requirement ID: [SRS-7-144]

The policies MG_IFP_BS_HL and MG_IFP_BS_LH SHALL specify a list of actions the MG shall take for non-compliant email messages.

Requirement ID: [SRS-7-145]

The possible actions for non-compliant email messages SHALL include:

- MG_IFP_ACTION_NONCOMPLIANT
- MG_IFP_ACTION_NOTIFY
- MG_IFP_ACTION_ALERT

Requirement ID: [SRS-7-146]

The policies MG_IFP_BS_HL and MG_IFP_BS_LH SHALL specify the actions the MG shall take for compliant email messages.

Requirement ID: [SRS-7-147]

The actions for compliant email messages SHALL include:

- MG_IFP_ACTION_COMPLIANT
- MG_IFP_ACTION _JOURNAL
- MG_IFP_ACTION_ALERT

7.5.2.1 Actions

7.5.2.1.1 MG_IFP_ACTION_NONCOMPLIANT

Requirement ID: [SRS-7-148]

The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_NONCOMPLIANT) which processes the non-compliant email message.

Requirement ID: [SRS-7-149]

MG_IFP_ACTION_NONCOMPLIANT action SHALL support an option (DROP) to silently drop the email message from the information flow (i.e. the email message is not transferred to the recipients and a delivery status notification is not returned to the originator).

Requirement ID: [SRS-7-150]

MG_IFP_ACTION_NONCOMPLIANT action SHALL support an option (NON-DELIVER) to non-deliver the non-compliant email message (i.e. the message is not transferred to the recipients and a delivery status notification is returned to the originator).

Requirement ID: [SRS-7-151]

MG_IFP_ACTION_NONCOMPLIANT action with the option NON-DELIVER SHALL generate a delivery status notification in accordance with [IETF RFC 3464, 2003].

Requirement ID: [SRS-7-152]

MG_IFP_ACTION_NONCOMPLIANT action SHALL support an option (QUARANTINE) to hold the email message in quarantine (i.e. the message is not transferred to the recipients and a delivery status notification is not returned to the originator).

Requirement ID: [SRS-7-153]

The email messages that are placed into quarantine SHALL be held in quarantine until either released (to the recipients) or deleted by an administrator.

Requirement ID: [SRS-7-154]

The BSS_IFCP_ACTION_NONCOMPLIANT action SHALL only be configured with one of the options (DROP, NON-DELIVER or QUARANTINE).

7.5.2.1.2 MG_IFP_ACTION_JOURNAL

Requirement ID: [SRS-7-155]

The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_JOURNAL) which processes a non-compliant email message.

Requirement ID: [SRS-7-156]

The MG_ICP_ACTION_JOURNAL action SHALL be capable of being either enabled or disabled with an IFCP.

Requirement ID: [SRS-7-157]

The MG_IFP_ACTION_JOURNAL action SHALL forward a copy of the non-compliant email message to a configurable email recipient.

7.5.2.1.3 MG_IFP_ACTION_NOTIFY

Requirement ID: [SRS-7-158]

The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_NOTIFY) which processes a non-compliant email message.

Requirement ID: [SRS-7-159]

MG_IFP_ACTION_NOTIFY action SHALL be capable of being either enabled or disabled with an IFCP.

Requirement ID: [SRS-7-160]

MG_IFP_ACTION_NOTIFY action SHALL support an option (ORIGINATOR) to send the notification message to the originator of the non-compliant email message.

Requirement ID: [SRS-7-161]

MG_IFP_ACTION_NOTIFY action SHALL support an option (RECIPIENTS) to send the notification message to the intended recipients of the non-compliant email message.

Requirement ID: [SRS-7-162]

MG_IFP_ACTION_NOTIFY action SHALL support an option (ADMINISTRATOR) to send the notification message to a configurable administrator recipient.

Requirement ID: [SRS-7-163]

MG_IFP_ACTION_NOTIFY action SHALL be configured with zero or more of the options (ORIGINATOR, RECIPIENTS and ADMINISTRATOR).

7.5.2.1.4 MG_IFP_ACTION_COMPLIANT

Requirement ID: [SRS-7-164]

The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_COMPLIANT) which processes the compliant email message.

Requirement ID: [SRS-7-165]

MG_IFP_ACTION_COMPLIANT action SHALL always being enabled within an IFCP.

Requirement ID: [SRS-7-166]

MG_IFP_ACTION_COMPLIANT action SHALL release the compliant message to the recipient domain.

7.5.2.1.5 _MG_IFP_ACTION_ALERT

Requirement ID: [SRS-7-167]

The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_JOURNAL) which processes the compliant email message.

Requirement ID: [SRS-7-168]

The MG_IFP_ACTION_JOURNAL action SHALL forward a copy of the compliant email message to a configurable email recipient.

7.5.3 Content Inspection Policy (CIP) Enforcement

7.5.3.1 MG_CIPE

Requirement ID: [SRS-7-169]

The MG SHALL provide a content inspection policy enforcement (CIPE) capability MG_CIPE that enables the MG to manage and schedule the routing of content through content filters (by MG_CIS ([SRS-7-196])) in accordance with the MG content inspection policy IEG-C_CIP_BS_EMAIL.

Requirement ID: [SRS-7-170]

The design and functionality of MG_CIPE SHALL conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012].

Requirement ID: [SRS-7-171]

MG_CIPE SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_CIP.

Requirement ID: [SRS-7-172]

MG_CIPE SHALL ensure that enforcement actions are executed in the order as specified in IEG-C_CIP_BS_EMAIL ([SRS-7-109])

7.5.3.2 High To Low

Requirement ID: [SRS-7-173]

For the flow of information from MG_IF_NET_HIGH to MG_IF_NET_LOW, MG_CIPE SHALL offer an interface ‘CIPE Services High to Low’ that accepts information for further processing.

Requirement ID: [SRS-7-174]

The interface ‘CIPE Services High to Low’ MUST support an operation ‘Enforce HL Business Support CIPE’ that enforces the policy IEG-C_CIP_BS_EMAIL_HL.

Requirement ID: [SRS-7-175]

The operation ‘Enforce HL Business Support CIPE’ MUST support the invocation of the following operations at the interface ‘Content Inspection Services’ ([SRS-7-204]) provided by MG_CIS ([SRS-7-196]):

- Operation ‘Initialize’ ([SRS-7-205]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in MG_CIS;
- Operation ‘Filter’ ([SRS-7-207]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA;
- Operation ‘Halt’ ([SRS-7-209]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in MG_CIS.

Requirement ID: [SRS-7-176]

MG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy IEG-C_CIP_BS_EMAIL_HL.

Requirement ID: [SRS-7-177]

The operation ‘Enforce HL Business Support CIPE’ SHALL log and report the actions taken.

Requirement ID: [SRS-7-178]

MG_CIPE SHALL inform MG_IFCPE of the outcome O_MG_CIPE_HL of the enforcement of IEG-C_CIP_BS_EMAIL_HL based on MG_CIP.

7.5.3.3 Low To High

Requirement ID: [SRS-7-179]

For the flow of information from MG_IF_NET_LOW to MG_IF_NET_HIGH, MG_CIPE MUST offer an interface ‘CIPE Services Low to High’ that accepts information for further processing.

Requirement ID: [SRS-7-180]

The interface ‘CIPE Services Low to High’ MUST support an operation ‘Enforce LH BS CIPE’ that enforces the policy IEG-C_CIP_BS_EMAIL_LH.

Requirement ID: [SRS-7-181]

The operation ‘Enforce LH Business Support CIPE’ MUST support the invocation of the following operations at the interface ‘Content Inspection Services’ ([SRS-7-204]) provided by MG_CIS ([SRS-7-196]):

- Operation ‘Initialize’ ([SRS-7-205]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in MG_CIS;
- Operation ‘Filter’ ([SRS-7-207]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA;
- Operation ‘Halt’ ([SRS-7-209]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in MG_CIS.

Requirement ID: [SRS-7-181]

MG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy IEG-C_CIP_BS_EMAIL_LH.

Requirement ID: [SRS-7-183]

The operation ‘Enforce LH Business Support CIPE’ SHALL log and report the actions taken.

Requirement ID: [SRS-7-184]

MG_CIPE SHALL inform MG_IFCPE of the outcome O_MG_CIPE_LH of the enforcement of MG_CIP_LH based on IEG-C_CIP_BS_EMAIL_LH ([SRS-7-109]).

7.5.4 Content Inspection Policies

Requirement ID: [SRS-7-185]

MG_CIP SHALL be configurable.

Requirement ID: [SRS-7-186]

MG_CIP SHALL specify the actions ACTIONS that need to be executed by MG_CIS.

Requirement ID: [SRS-7-187]

MG_CIP SHALL specify the order in which ACTIONS need to be executed.

Requirement ID: [SRS-7-188]

For each action in ACTIONS it SHALL be possible to:

- Enable or disable the action.

- Instruct MG_CIPE to ignore the outcome of the execution of the action by MG_CIS (as received from MG_CIS ([SRS-7-196])).
- If the outcome of the execution of the action by MG_CIS is a policy violation: instruct MG_CIPE to continue the enforcement of MG_CIP, or to stop.

Requirement ID: [SRS-7-189]

It SHALL be possible to group ACTIONS per the following sub-policies:

- MG_CIP_EV – SMTP Envelope Validation
- MG_CIP_AV – Attachment Validation
- MG_CIP_LV – Label Validation

Requirement ID: [SRS-7-453]

It SHALL be possible to enable or disable the enforcement of each sub-policy in ([SRS-7-189]).

Requirement ID: [SRS-7-454]

It SHALL be possible to apply each sub-policy to either information flow ('CIPE Services Low to High' and 'CIPE Services High to Low).

Requirement ID: [SRS-7-190]

MG_CIP SHALL specify the level of granularity of the outcomes O_MG_CIS ([SRS-7-205]), O_MG_CIPE_HL ([SRS-7-178]) and O_MG_CIPE_LH ([SRS-7-184]).

Requirement ID: [SRS-7-191]

It SHALL be possible for MG_CIS to distinguish within O_MG_CIS, O_MG_CIPE_HL and O_MG_CIPE_LH:

- The MG_CIS capability that determined a policy violation (MG_CIS_EV ([SRS-7-274]), MG_CIS_AV ([SRS-7-240]) and MG_CIS_LV ([SRS-7-214]));
- Identification CIPE_CF_ID of the content filter that determined the policy violation;
- Identification of the action that led to policy violation;
- Reason for policy violation.

7.5.4.1 MG_CIP_EV

Requirement ID: [SRS-7-192]

MG_CIP_EV SHALL specify the lists that are used by the Envelope Validation Content Inspection Service (MG_CIS_EV):

- LIST_MG_CIS_EV_ORIG – list of allowable SMTP originators;
- LIST_MG_CIS_EV_RECIPS – list of allowable SMTP recipients.

7.5.4.2 MG_CIP_AV

Requirement ID: [SRS-7-193]

MG_CIP_AV SHALL specify the lists that are used by the Attachment Validation Content Inspection Service (MG_CIS_AV):

- NUM_MG_CIS_AV_ATTACHMENTS – the maximum number of attachments;
- LIST_MG_CIS_AV_TYPES – list of allowable MIME attachment types.
- LIST_MG_CIS_AV_DIRTYWORDS – list of words or phrases not allowed in an email message.
- LIST_MG_CIS_AV_MALWARE_DEFINITIONS – list of definitions/signatures of currently known malware

7.5.4.3 MG_CIP_LV

Requirement ID: [SRS-7-194]

MG_CIP_LV SHALL specify the parameters for the Label Validation Content Inspection Service (MG_CIS_LV):

- LIST_MG_CIS_LV-SPIF – list of allowable security policies (including classifications and categories);
- LIST_MG_CIS_LV-DM – list of allowable digest method algorithms;
- LIST_MG_CIS_LV-SM – list of allowable signature method algorithms;
- LIST_MG_CIS_LV-CRL – list of certificate revocation lists
- LIST_MG_CIS_LV_TP – list of trust points (e.g. trusted root certificates).
- BOOL_MG_CIS_LV_CB – to indicate whether a Cryptographic Binding is required.
- STR_MG_CIS_LV_FLOT_PREFIX – prefix to identify a FLOT in a message;
- LIST_MG_CIS_LV_FLOT – list of valid FLOT markings;
- STR_MG_CIS_LV_KEYWORD_HEADER – SMTP header field which contains keywords;
- LIST_MG_CIS_LV_KEYWORDS – list of valid keywords.

7.6 Protection Services

7.6.1 Content Inspection Services

Requirement ID: [SRS-7-196]

The MG MUST provide a content inspection services (CIS) capability MG_CIS that enables MG_CIPE to identify and verify content based on the content inspection policy MG_CIP.

Requirement ID: [SRS-7-197]

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

Requirement ID: [SRS-7-198]

MG_CIS SHALL support the message syntax of SMTP messages as defined in Simple Mail

Requirement ID: [SRS-7-199]

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

Requirement ID: [SRS-7-200]

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

Requirement ID: [SRS-7-201]

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

Requirement ID: [SRS-7-202]

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

Requirement ID: [SRS-7-203]

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

Requirement ID: [SRS-7-204]

MG_CIS MUST offer an interface ‘Content Inspection Services’ that serves as a communication mechanism between the content filters and MG_CIPE.

Requirement ID: [SRS-7-205]

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

Requirement ID: [SRS-7-206]

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

Requirement ID: [SRS-7-207]

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

Requirement ID: [SRS-7-208]

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-7-209]

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

Requirement ID: [SRS-7-210]

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

Requirement ID: [SRS-7-211]

MG_CIS SHALL inform MG_CIPE of the outcome O_MG_CIS of the execution of an action in ACTIONS ([SRS-7-120]).

Requirement ID: [SRS-7-212]

If the outcome O_MG_CIS is negative (e.g. verification or validation fails), MG_CIS SHALL interpret O_MG_CIS as a policy violation and inform MG_CIPE according to MG_CIP ([SRS-7-185]).

Requirement ID: [SRS-7-213]

MG_CIS SHALL invoke the operation ‘Log’ (7.7.7.1.1) at the interface ‘Event Management’ ([SRS-6-328]) and log the outcome O_MG_CIS ([SRS-6-115]).

7.6.1.1 MG_CIS_LV

Requirement ID: [SRS-7-214]

MG_CIS SHALL provide a Label validation capability MG_CIS_LV.

Requirement ID: [SRS-7-215]

MG_CIS_LV SHALL act upon the contents of the SMTP Message body.

Requirement ID: [SRS-7-216]

MG_CIS_LV SHALL make use of the following subordinate Label validation capabilities:

- MG_CIS_LV_STANAG – validation of a STANAG 4774 confidentiality label
- MG_CIS_LV_FLOT – validation of a First Line of Text (FLOT) marking
- MG_CIS_LV_KEYWORDS – validation of keywords.

Requirement ID: [SRS-7-217]

MG_CIS_LV SHALL return a positive O_MG_CIS_LV if any of the subordinate Label validation capabilities (MG_CS_LV_STANAG, MG_CIS_LV_FLOT and MG_CIS_LV_KEYWORDS) returns a positive outcome.

7.6.1.1.1 MG_CIS_LV_STANAG

Requirement ID: [SRS-7-218]

The subordinate Label validation capability MG_CIS_LV_STANAG SHALL ensure that a valid and allowable STANAG 4774 confidentiality label is bound with a valid and allowable STANAG 4778 Metadata Binding to every email message.

Requirement ID: [SRS-7-219]

MG_CIS_LV_STANAG MUST support the NATO standard ADatP-4774 “Confidentiality Metadata Label Syntax” [STANAG 4774].

Requirement ID: [SRS-7-220]

MG_CIS_LV_STANAG MUST support the NATO standard ADatP-4778 “Metadata Binding Mechanism” [STANAG 4778].

Requirement ID: [SRS-7-221]

MG_CIS_LV_STANAG MUST support the binding profile “Simple Message Transport Protocol (SMTP) Binding Profile” in [STANAG 4778 SRD.2].

Requirement ID: [SRS-7-222]

MG_CIS_LV_STANAG MUST support the binding profile “Cryptographic Message Syntax (CMS) Cryptographic Artefact Binding Profile” in [STANAG 4778 SRD.2].

Requirement ID: [SRS-7-223]

MG_CIS_LV_STANAG SHALL be able to validate a digital signature by invoking the operation ‘VerifyCMS’ (7.6.2.2.1) at the interface ‘Public Key Cryptographic Services’ ([SRS-7-296]) provided by MG_PKCS ([SRS-7-294]).

Requirement ID: [SRS-7-224]

For the confidentiality metadata labels (originator or alternative) *CLs* that are bound to a data object *DO*, MG_CIS_LV_STANAG SHALL be able to verify at least one *CL* against a security policy information file (SPIF) contained in LIST_MG_CIS_LV-SPIF.

Requirement ID: [SRS-7-225]

MG_CIS_LV_STANAG SHALL be able to validate a digital signature on each SPIF contained in LIST_MG_CIS_LV-SPIF by invoking the operation 'VerifyXML' (7.6.2.2.2) at the interface 'Public Key Cryptographic Services' ([SRS7-296]) provided by MG_PKCS ([SRS-7-294]).

7.6.1.1.2 MG_CIS_LV_FLOT

Requirement ID: [SRS-7-226]

The subordinate Label validation capability MG_CIS_LV_FLOT SHALL ensure that a valid and allowable First Line Of Text marking is contained in every email message.

Requirement ID: [SRS-7-227]

MG_CIS_LV_FLOT SHALL identify the FLOT security marking of an email message as the text following the prefix STR_MG_CIS_LV_FLOT_PREFIX on the first line of the first text attachment in the message.

Requirement ID: [SRS-7-228]

The sub-policy IEG-C_CIP_BS_EMAIL_LV_FLOT SHALL determine that an email message that does not contain a FLOT security marking is non-compliant with the policy and return a negative outcome to MG_CIS_LV.

Requirement ID: [SRS-7-229]

MG_CIS_LV_FLOT SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when comparing the FLOT security marking with the allowable security markings in LIST_MG_CIS_LV_FLOT

Requirement ID: [SRS-7-230]

MG_CIS_LV_FLOT SHALL determine that an email message that contains a FLOT security marking that is not an allowable security marking is non-compliant with the policy and return a negative outcome to MG_CIS_LV.

Requirement ID: [SRS-7-231]

MG_CIS_LV_FLOT SHALL determine that an email message that contains a FLOT security marking that is an allowable security marking is compliant with the policy and return an positive outcome to MG_CIS_LV.

7.6.1.1.3 MG_CIS_LV_KEYWORDS

Requirement ID: [SRS-7-232]

The subordinate Label validation capability MG_CIS_LV_KEYWORDS SHALL ensure that at least one valid and allowable keyword is contained in every email message.

Requirement ID: [SRS-7-233]

MG_CIS_LV_KEYWORDS SHALL return a positive outcome if the list of keywords, LIST_MG_CIS_LV_KEYWORDS is empty, or the header field STR_MG_CIS_LV_KEYWORD_HEADER is empty.

Requirement ID: [SRS-7-234]

MG_CIS_LV_KEYWORDS SHALL identify the KEYWORDS security marking of an email message as the text of the header field, STR_MG_CIS_LV_KEYWORD_HEADER.

Requirement ID: [SRS-7-235]

The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL split the comma-separated KEYWORDS into a list of KEYWORDs.

Requirement ID: [SRS-7-236]

The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when comparing each of the KEYWORD security marking with the allowable security markings.

Requirement ID: [SRS-7-237]

The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL determine that an email message that does not contain a KEYWORDS header field is non-compliant with the policy.

Requirement ID: [SRS-7-238]

The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL determine that an email message that contains a KEYWORD security marking that is not an allowable security marking is non-compliant with the policy.

Requirement ID: [SRS-7-239]

The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL determine that an email message that contains a KEYWORD security marking that is an allowable security marking is compliant with the policy.

7.6.1.2 MG_CIS_AV

Requirement ID: [SRS-7-240]

MG_CIS SHALL provide an attachment validation capability MG_CIS_AV.

Requirement ID: [SRS-7-241]

MG_CIS_AV SHALL act upon on the contents of the SMTP Message body.

Requirement ID: [SRS-7-242]

MG_CIS_AV SHALL make use of the following subordinate Attachment validation capabilities:

- MG_CIS_AV_MAX – validation of the maximum number of attachments;
- MG_CIS_AV_TYPES – validation attachment types;
- MG_CIS_AV_DIRTY – detection of dirty words;
- MG_CIS_AV_MALWARE – detection of malware.

Requirement ID: [SRS-7-243]

MG_CIS_AV SHALL return a positive outcome O_MG_CIS_AV only if all of the subordinate Attachment validation capabilities (MG_CS_LV_STANAG, MG_CIS_LV_FLOT and MG_CIS_LV_KEYWORDS) returns a positive outcome.

7.6.1.2.1 MG_CIS_AV_MAX

Requirement ID: [SRS-7-244]

The subordinate Attachment validation capability MG_CIS_AV_MAX SHALL verify that an email message does not exceed a maximum number of attachments.

Requirement ID: [SRS-7-245]

MG_CIS_AV_MAX SHALL determine the number of attachments included within a message, recursively including attachments in attached messages.

Requirement ID: [SRS-7-246]

MG_CIS_AV_MAX SHALL determine that an email message that contains the configured maximum number of attachment, or less, is **compliant** with the policy.

Requirement ID: [SRS-7-247]

MG_CIS_AV_MAX SHALL determine that an email message that contains more than the configured maximum number of attachment is **non-compliant** with the policy and return a negative outcome to MG_CIS_AV;

7.6.1.2.2 MG_CIS_AV_TYPES

Requirement ID: [SRS-7-248]

The subordinate Attachment validation capability MG_CIS_AV_TYPES SHALL ensure that an email message only contains allowed attachment types.

Requirement ID: [SRS-7-249]

MG_CIS_AV_TYPES SHALL determine the *declared* media types as those contained in the Content-Type header fields, within the email message.

Requirement ID: [SRS-7-250]

MG_CIS_AV_TYPES SHALL determine the *disposition* media types, as derived[5] from the filename parameter in the Content-Disposition header fields, within the email message.

Requirement ID: [SRS-7-252]

MG_CIS_AV_TYPES SHALL return a positive outcome if the list of media types, LIST_MG_CIS_AV_TYPES, is empty.

Requirement ID: [SRS-7-253]

MG_CIS_AV_TYPES SHALL determine an email message is compliant with the policy, if all the *disposition* media types are present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.

Requirement ID: [SRS-7-254]

MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy, if one or more the *disposition* media types are not present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.

Requirement ID: [SRS-7-255]

MG_CIS_AV_TYPES SHALL determine the *analysed* media types from an analysis of the contents of the email attachments.

Requirement ID: [SRS-7-256]

MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy it is unable to determine an *analysed* media type for one or more attachments.

Requirement ID: [SRS-7-257]

MG_CIS_AV_TYPES SHALL determine an email message is compliant with the policy, if all the *analysed* media types are present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.

Requirement ID: [SRS-7-258]

MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy, if one or more the *analysed* media types are not present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.

Requirement ID: [SRS-7-259]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_TYPES SHALL determine the *container* media types (e.g. zip), as derived from the filenames and binary analysis of the files found within container email attachments.

Requirement ID: [SRS-7-260]

MG_CIS_AV_TYPES SHALL determine an email message is compliant with the policy, if all the *container* media types are present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.

Requirement ID: [SRS-7-261]

MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy, if one or more the *container* media types are not present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.

7.6.1.2.3 MG_CIS_AV_DIRTY

Requirement ID: [SRS-7-262]

The subordinate Label validation capability MG_CIS_AV_DIRTY SHALL ensure an email message does not contain any of a configured set of words or phrases (LIST_MG_CIS_AV_DIRTYWORDS).

Requirement ID: [SRS-7-263]

MG_CIS_AV_DIRTY SHALL return a positive outcome if the list of dirty words, LIST_MG_CIS_AV_DIRTYWORDS, is empty.

Requirement ID: [SRS-7-264]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL inspect each of the email attachments, including the message body, for occurrences of any of the dirty words/phrases (LIST_MG_CIS_AV_DIRTYWORDS).

Requirement ID: [SRS-7-265]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL recursively inspect each of the email message attachments for occurrences of any of the dirty words/phrases (LIST_MG_CIS_AV_DIRTYWORDS).

Requirement ID: [SRS-7-266]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when searching for each of the dirty words/phrases in the message body/attachment.

Requirement ID: [SRS-7-267]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL determine that an email message that contains at least one of the dirty word/phrases (LIST_MG_CIS_AV_DIRTYWORDS) is non-compliant with the policy.

Requirement ID: [SRS-7-268]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL determine that an email message that does not contains any of the dirty words/phrases in LIST_MG_CIS_AV_DIRTYWORDS is compliant with the policy.

7.6.1.2.4 MG_CIS_AV_MALWARE

Requirement ID: [SRS-7-269]

The subordinate Attachment validation capability MG_CIS_AV_MALWARE SHALL ensure an email message does not contain any known malware.

Requirement ID: [SRS-7-270]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_MALWARE SHALL scan each attachment within the email message for malware using the current set of malware definitions (LIST_MG_CIS_AV_MALWARE_DEFINTIONS).

Requirement ID: [SRS-7-272]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_MALWARE SHALL determine that an email message that contains at least one attachment that is reported to contain malware is non-compliant with the policy.

Requirement ID: [SRS-7-273]

The sub-policy IEG-C_CIP_BS_EMAIL_AV_MALWARE SHALL determine that an email message that does not contains any attachment that is reported to contain malware is compliant with the policy.

7.6.1.3 MG_CIS_EV

Requirement ID: [SRS-7-274]

MG_CIS SHALL provide an SMTP envelope validation capability MG_CIS_EV that comprises a set of content filters.

Requirement ID: [SRS-7-275]

MG_CIS_EV SHALL act upon on the contents of the SMTP message envelope.

Requirement ID: [SRS-7-276]

MG_CIS_EV SHALL make use of the following subordinate SMTP envelope validation capabilities:

- MG_CIS_EV_ORIG – validation of the SMTP originator;
- MG_CIS_EV_RECIP – validation of the SMTP recipients;

Requirement ID: [SRS-7-277]

MG_CIS_EV SHALL return a positive outcome OMG__CIS_EV only if all of the subordinate Envelope validation capabilities (MG_CS_EV_ORIG and MG_CIS_EV_RECIP) return a positive outcome.

7.6.1.3.1 MG_CIS_EV_ORIG

Requirement ID: [SRS-7-278]

The subordinate SMTP envelope validation capability, MG_CIS_EV_ORIG, SHALL allow the configuration of a set of allowable message originators, LIST_MG_CIS_EV_ORIG, one of which a compliant email message must contain.

Requirement ID: [SRS-7-279]

MG_CIS_EV_ORIG SHALL allow a configured message originator to contain wildcards in the local-part of the address.

Requirement ID: [SRS-7-280]

MG_CIS_EV_ORIG SHALL allow a configured message originator to contain wildcards in the domain components of the address.

Requirement ID: [SRS-7-281]

MG_CIS_EV_ORIG SHALL identify the email message originator as the MAIL FROM: field as defined in [IETF RFC 5321, 2008].

Requirement ID: [SRS-7-282]

MG_CIS_EV_ORIG SHALL perform case insensitive matching when comparing the email message originator with the allowable message originators.

Requirement ID: [SRS-7-283]

MG_CIS_EV_ORIG SHALL take into account the wildcards when comparing the email message originator with the allowable message originators.

Requirement ID: [SRS-7-284]

MG_CIS_EV_ORIG SHALL determine that an email message that contains an email message originator that is not an allowable message originator is **non-compliant** with the policy.

Requirement ID: [SRS-7-285]

MG_CIS_EV_ORIG SHALL determine that an email message that contains an originator that is an allowable message originator is **compliant** with the policy.

7.6.1.3.2 MG_CIS_EV_RECIP

Requirement ID: [SRS-7-286]

The subordinate SMTP envelope validation capability, MG_CIS_EV_RECIP, SHALL allow the configuration of a set of allowable message recipients that a compliant email message may contain.

Requirement ID: [SRS-7-287]

MG_CIS_EV_RECIP SHALL allow a message recipient to contain wildcards in the local-part of the address.

Requirement ID: [SRS-7-288]

MG_CIS_EV_RECIP SHALL allow a message recipient to contain wildcards in the domain components of the address.

Requirement ID: [SRS-7-289]

MG_CIS_EV_RECIP SHALL identify the email message originator as the RCPT TO: field as defined in [IETF RFC 5321, 2008].

Requirement ID: [SRS-7-290]

MG_CIS_EV_RECIP SHALL perform case insensitive matching when comparing the email message recipient with the allowable message recipients.

Requirement ID: [SRS-7-291]

MG_CIS_EV_RECIP SHALL take into the wildcards when comparing the email message originator with the allowable message originators.

Requirement ID: [SRS-7-292]

MG_CIS_EV_RECIP SHALL determine that an email message that contains an email message recipient that is not an allowable message recipient is **non-compliant** with the policy.

Requirement ID: [SRS-7-293]

MG_CIS_EV_RECIP SHALL determine that an email message that contains a recipient that is an allowable message recipient is **compliant** with the policy.

7.6.2 Public Key Cryptographic Services

7.6.2.1 MG_PKCS

Requirement ID: [SRS-7-294]

MG MUST provide a capability MG_PKCS that enables the MG to perform cryptographic operations and key management.

Requirement ID: [SRS-7-295]

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

Requirement ID: [SRS-7-455]

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

7.6.2.2 Public Key Cryptographic Services

Requirement ID: [SRS-7-296]

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

- VerifyCMS (7.6.2.2.1);
- VerifyXML (7.6.2.2.2);
- Encrypt (7.6.2.2.3);
- Decrypt (7.6.2.2.4).

Requirement ID: [SRS-7-297]

For every action taken, the operations 'VerifyCMS, 'VerifyXML', 'Encrypt' and 'Decrypt' SHALL invoke the operation 'Log' (6.7.7.2.2) at the interface 'Event Management' ([SRS-6-328]) and log both the action and the result of the action.

7.6.2.2.1 VerifyCMS

Requirement ID: [SRS-7-298]

The operation 'VerifyCMS':

- MUST support the validation of Cryptographic Message Syntax SignedData digital signatures based on the Cryptographic Message Syntax ([IETF RFC 5652, 2009]);
- MUST support validation of digital signatures in accordance with a specified cryptographic algorithm: the Rivest Shamir Adleman (RSA) algorithm [RSA PKCS#1, 2002] and cryptographic key sizes of 3072 bits that meet the following:
    - Requirements defined in the NPKI Certificate Policy [NAC AC/322-D(2004)0024 REV3-COR1, 2018] and [NAC AC/322-D(2007)0002-REV1, 2015]

7.6.2.2.2 VerifyXML

Requirement ID: [SRS-7-299]

The operation 'VerifyXML':

- 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 3072 bits that meet the following:

  - Requirements defined in the NPKI 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].

7.6.2.2.3 Encrypt

Requirement ID: [SRS-7-300]

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

7.6.2.2.4 Decrypt

Requirement ID: [SRS-7-301]

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

7.6.3 Management

7.7 Element Management Services

7.7.1 Management

Requirement ID: [SRS-7-302]

The MG MUST provide a management capability MG_MGMT that supports local and remote management of the MG.

Requirement ID: [SRS-7-502]

The MG management capability SHALL be installed on the management workstation.

7.7.2 Local Management

Requirement ID: [SRS-7-303]

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

Requirement ID: [SRS-7-304]

MG_IF_LOCAL_MGMT SHALL support the invocation of the operations at the interfaces 'CIS Security' ([SRS-7-331]), 'SMC Configuration Management' ([SRS-7-352]) and 'Cyber Defence' 7.7.6).

7.7.3 Audit Management

Requirement ID: [SRS-7-305]

MG_MGMT MUST provide a capability MG_MGMT_AM that allows Audit Administrators to fulfil their role.

Requirement ID: [SRS-7-306]

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

Requirement ID: [SRS-7-307]

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

Requirement ID: [SRS-7-308]

MG_MGMT_AM SHALL provide the capability to detect and create records of security-relevant events associated with end users transferring messages cross domain.

Requirement ID: [SRS-7-309]

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

Requirement ID: [SRS-7-310]

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

Requirement ID: [SRS-7-311

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

Requirement ID: [SRS-7-312]

MG_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-7-313]

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

- MG start-up and shutdown;
- Changes to security related system management functions;

- Audit log access;
- Creation, modification or deletion of audit log records;
- Invocation of privileged operations;
- Modification to MG access rights;
- Unauthorised attempts to access MG system files;
- All modified objects are recorded with date, time, details of change and user.

Requirement ID: [SRS-7-314]

MG_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-7-315]

MG_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-7-316]

MG_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-7-317]

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

Requirement ID: [SRS-7-318]

MG_MGMT_AM SHALL by default archive the audit log daily.

Requirement ID: [SRS-7-319]

MG_MGMT_AM SHALL automatically back up audit logs at configurable intervals.

Requirement ID: [SRS-7-320]

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

Requirement ID: [SRS-7-321]

MG_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-7-322]

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

7.7.4 CIS Security

Requirement ID: [SRS-7-323]

MG_MGMT SHALL provide a capability MG_MGMT_CS that allows for the management of CIS Security information specific to the MG.

Requirement ID: [SRS-7-503]

MG_MGMT SHALL generate private keys and corresponding Certificate Signing Requests (CSRs) for signing by the appropriate NATO Registration Authority (RA).

Requirement ID: [SRS-7-324]

MG_MGMT_CS SHALL support the retrieval of key material, certificates and CRLs from locations external to the MG.

Requirement ID: [SRS-7-325]

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

Requirement ID: [SRS-7-507]

MG_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-7-326]

MG_MGMT_CS SHALL only trust certificates that

- Are validated using OCSP
- Can be validated to an installed trusted certificate.

Requirement ID: [SRS-7-327]

MG_MGMT_CS SHALL allow the installation of multiple trusted certificates.

Requirement ID: [SRS-7-328]

MG_MGMT_CS SHALL support automated execution of the following actions:

- Updating of certificates;
- Updating of CRLs;

Requirement ID: [SRS-7-329]

MG_MGMT_CS MUST support scheduling of each operation in [SRS-7-328] 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-7-330]

MG_MGMT_CS SHALL pass outgoing CIS Security Messages to the interface 'Core Services Management' ([SRS-7-60]) for further processing.

Requirement ID: [SRS-7-504]

MG_MGMT_CS SHALL update the malware/virus signatures used by the MG malware/virus scanner on a daily basis.

7.7.4.1 Interfaces

Requirement ID: [SRS-7-331]

MG_MGMT_CS MUST offer an interface 'CIS Security' that accepts an incoming 'CIS Security Message' in support of the operations 'Manage Protection Policies' (7.7.4.1.1), 'Review' (7.7.4.1.2) and 'Manage Public Key Material' (7.7.4.1.3).

7.7.4.1.1 Manage Protection Policies

Requirement ID: [SRS-7-332]

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 MG_IFCPE ([SRS-7-82] and MG_CIPE ([SRS-7-169] respectively.

Requirement ID: [SRS-7-333]

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-7-334]

MG_MGMT_CS MUST support the automated execution of those operations in [SRS-7-333] that comprise a policy update.

Requirement ID: [SRS-7-335]

MG_MGMT_CS MUST support the automated execution of the operation ‘Backup policy’ in [SRS-7-333].

Requirement ID: [SRS-7-336]

MG_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.

7.7.4.1.2 Review

Requirement ID: [SRS-7-337]

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

7.7.4.1.3 Manage Public Key Material

Requirement ID: [SRS-7-338]

The interface ‘CIS Security’ MUST support an operation ‘Manage Public Key Material’ that provides the capability to manage key material to support MG_PKCS ([SRS-7-294]).

Requirement ID: [SRS-7-339]

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-7-340]

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.

7.7.5 SMC Configuration Management

Requirement ID: [SRS-7-341]

MG_MGMT MUST provide a management capability MG_MGMT_CM that enables the configuration and management of the MG.

Requirement ID: [SRS-7-342]

MG_MGMT_CM MUST provide the capability to change, capture, duplicate, backup or restore the configuration of the MG.

Requirement ID: [SRS-7-343]

MG_MGMT_CM MUST provide the capability to remotely prepare a MG configuration MG_CONFIG and deploy MG_CONFIG onto multiple instances of the MG.

Requirement ID: [SRS-7-344]

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

Requirement ID: [SRS-7-345]

MG_MGMT_CM MUST support configuration of the MG based on a customizable (pre-loaded) configuration templates (e.g. SPIFs are pre-installed) in support of common information exchange scenarios.

Requirement ID: [SRS-7-346]

MG_MGMT_CM MUST support the creation and installation (pre-loading) of the configuration templates.

Requirement ID: [SRS-7-347]

MG_MGMT_CM MUST support the retrieval of XML artefacts from locations external to the MG.

Requirement ID: [SRS-7-348]

MG_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-7-349]

MG_MGMT_CM MUST support automated execution of the following action:

- Updating of XML artefacts including SPIFs.

Requirement ID: [SRS-7-350]

MG_MGMT_CM MUST support scheduling of the operation in [SRS-7-349] 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-7-351]

MG_MGMT_CM SHALL pass outgoing SMC Messages to the interface ‘Core Services Management’ ([SRS-7-60]) for further processing.

Requirement ID: [SRS-7-505]

MG_MGMT_CM SHALL integrate the update of the virus definitions (LIST_MG_CIS_AV_MALWARE_DEFINITIONS) used by MG malware scanner with the existing capability

7.7.5.1 Interfaces

Requirement ID: [SRS-7-352]

MG_MGMT_CM MUST offer an interface ‘SMC Configuration Management’ that accepts an incoming ‘SMC Message’ in support of the operations ‘Configure OS’ (7.7.5.1.1), ‘Configure Protection Policy Enforcement Services” (7.7.5.1.2), ‘Configure Data Exchange Services’ (7.7.5.1.3) and ‘Configure Protection Services’ (7.7.5.1.4).

7.7.5.1.1 Configure OS

Requirement ID: [SRS-7-353]

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 MG is running on, and the applications running on the operating system.

Requirement ID: [SRS-7-354]

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]).

7.7.5.1.2 Configure Protection Policy Enforcement Services

Requirement ID: [SRS-7-355]

The interface ‘SMC Configuration Management’ MUST support an operation ‘Configure Protection Policy Enforcement Services’ that provides the capability to configure and manage MG_IFCPE (7.5.1.1) and MG_CIPE (7.5.3.1).

Requirement ID: [SRS-7-356]

The operation ‘Configure Protection Policy Enforcement Services’ MUST provide the capability to change, capture, duplicate, backup or restore the configuration of MG_IFCPE and MG_CIPE.

Requirement ID: [SRS-7-357]

The operation ‘Configure Protection Policy Enforcement 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]).

7.7.5.1.3 Configure Data Exchange Services

Requirement ID: [SRS-7-358]

The interface ‘SMC Configuration Management’ MUST support an operation ‘Configure Data Exchange Services’ that provides the capability to configure and manage MG_DEX ([SRS-7-1]).

Requirement ID: [SRS-7-359]

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

Requirement ID: [SRS-7-360]

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]).

7.7.5.1.4 Configure Protection Services

Requirement ID: [SRS-7-361]

The interface ‘SMC Configuration Management’ MUST support an operation ‘Configure Protection Services’ that provides the capability to configure and manage MG_CIS ([SRS-7-196]) and MG_PKCS ([SRS-7-294]).

Requirement ID: [SRS-7-362]

The operation ‘Configure Protection Services’ MUST provide the capability to change, capture, duplicate, backup or restore the configuration of MG_CIS and MG_PKCS.

Requirement ID: [SRS-7-363]

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-7-364]

The operation ‘Configure Protection Services’ MUST provide the capability to manage filters for MG_CIS.

Requirement ID: [SRS-7-365]

The management of filters for MG_CIS SHALL include:

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

Requirement ID: [SRS-7-456]

The operation ‘Configure Protection Services’ MUST provide the capability to manage XML artefacts for MG_CIS.

Requirement ID: [SRS-7-366]

The management of XML artefacts for MG_CIS SHALL include:

- Loading and removal;
- Validation against the corresponding XML Schema,
- Validation of any contained XML Digital Signature.

7.7.6 Cyber Defence

Requirement ID: [SRS-7-367]

MG_MGMT MUST provide a management capability MG_MGMT_CD that provides the capability to manage and respond to cyber-related attacks on the MG.

Requirement ID: [SRS-7-368]

MG_MGMT_CD SHALL pass outgoing Cyber Defence Messages to interface ‘Core Services Management’ ([SRS-7-60]) for further processing.

7.7.6.1 Interfaces

Requirement ID: [SRS-7-369]

MG_MGMT_CD MUST offer an interface ‘Cyber Defence’ that accepts an incoming ‘Cyber Defence Message’ in support of the operations ‘Assess’ (7.7.6.1.1), ‘Respond’ (7.7.6.1.2) and ‘Recover’ (7.7.6.1.3).

7.7.6.1.1 Assess

Requirement ID: [SRS-7-370]

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

Requirement ID: [SRS-7-371]

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

Requirement ID: [SRS-7-372]

The operation ‘Assess’ SHALL be able to support the aggregation of cyber-related data (e.g. logs from MG_IFCPE, MG_CIPE and MG_PKCS) to a central repository to facilitate proper analysis.

7.7.6.1.2 Respond

Requirement ID: [SRS-7-373]

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-7-374]

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-7-375]

The controlling of traffic flow by MG_MGMT_CD SHALL include:

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

7.7.6.1.3 Recover

Requirement ID: [SRS-7-376]

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 MG that were affected by the attack/fault.

7.7.7 Event Management

Requirement ID: [SRS-7-377]

MG_MGMT MUST provide a management capability MG_MGMT_EM that enables the management of events.

Requirement ID: [SRS-7-378]

MG_MGMT_EM SHALL collect events and support the forwarding of events to the EMS.

Requirement ID: [SRS-7-379]

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

Requirement ID: [SRS-7-380]

MG_MGMT_EM SHALL support SNMP v3 [IETF RFC 3412, 2002] and the Mail Monitoring MIB [IETF RFC 2789, 2000]

Requirement ID: [SRS-7-381]

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

Requirement ID: [SRS-7-382]

MG_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-7-383]

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

Requirement ID: [SRS-7-384]

MG_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-7-386]

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

Requirement ID: [SRS-7-387]

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