NATO Communications and Information Agency
Agence OTAN d'information et de communication

IEG Case C

IFB-CO-14314-IEG-C

BOOK II - PART IV SOW Annex A

SYSTEM REQUIREMENTS SPECIFICATION (SRS)

Table of Contents

NATO UNCLASSIFIED

Figures

Tables

1 Introduction

1.1 Purpose

This System Requirement Specification (SRS) describes the external behaviour of the system to be delivered under the IEG-C project, hereinafter referred to as 'IEG-C'. It also describes non-functional requirements, design constraints and other factors necessary to provide a comprehensive description of the requirements for the system.

This document supports increment 1 of Project 2014/0IS03102, which is included in Capability Package (CP) 9C0150, which covers the Information Exchange Gateway (IEG) Services for NATO SECRET to MISSION SECRET.

1.2 Scope

The Bi-SC CP9C0150 Project OIS03102 "Provide Information Exchange Service" increment 1 "Information exchange between NATO classified networks and NATO-led Mission Secret (MS) networks (Scenario C)" is to provide the IEG static capability to connect NATO CIS and Mission CIS at Secret level domain.

The scope of this document is to define the requirements for a standardized IEG-C architecture to provide a standardized gateway between NATO Secret (NS) networks and NATO-led Mission Secret (MS) networks for both Static and Deployable envioments that:

- Allows the Information Exchange between NATO Secret (NS) Network Domain and Mission Secret (MS) Network Domain instances implemented within the existing NATO Secret physical infrastructure at centralized locations;
- Releases information from NS to MS based on predefined criteria tailored to the specific Mission requirement; data failing to meet the release criteria shall be blocked and the internal domain notified accordingly;
- Allows the transfer of the information from MS to NS based on predefined criteria tailored to specific Mission requirement; data failing to meet the acceptance criteria shall be rejected or dropped and the sender notified accordingly. This functionality can be configurable depending on the operation.

1.3 Acronyms and Abbreviations

The acronyms and abbreviations used in this SRS are defined in Annex D of the Statement of Work.

1.4 Definitions

The definitions used in this SRS are defined in Annex E of the Statement of Work.

1.5 Overview

This SRS comprises 9 sections:

- Section 1 provide an introduction and describes the use of his document
- Section 2 provides a general description of the IEG-C, the roles involved and the project constraints.
- Section 3 provides an overview of the IEG-C Target Architecture and Logical Architecture.

- Section 4 specifies requirements for IEG-C components in general, interfaces, and integration of components.
- Section 5 specifies the non-functional requirements for the IEG-C.
- Section 6 specifies the functional requirements (including security functional requirements) for the Web Guard.
- Section 7 specifies the functional requirements (including security functional requirements) for the Mail Guard.
- Section 8 specifies the IEG-C security requirements.
- Section 9 specifies the IEG-C management requirements.
- Appendix A provides a general system description of the Web Guard.
- Appendix B provides an overview of relevant service interface profiles.
- Appendix C provides the security problem definition and security objectives for the IEG-C.
- Appendix D provides details of the Equipment Specifications.
- Appendix E provide a summary of the Component Names used in the SRS

1.6 SRS Conventions

The system requirements, defined in this document, are individually identified by a unique number which shall be used at all times as the specific reference for each.

No meaning is associated with the order of serial numbering. There could be gaps in numbering and requirement identifiers in a group do not have to be sequential.

Requirement identifiers are encapsulated in square brackets.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [IETF RFC 2119, 1997].

The requirements in this SRS have an identifier of the form [SRS-Section Number-Requirement Number], e.g. [SRS-1-228], and are enclosed within a box.

Requirement ID: [SRS-1-228]

Example SRS requirement.

The requirements in this SRS make use of logical names to describe the components of the system and their associated requirements. The logical names follow the naming used in the IEG-C Target Architecture [TR/2016/NSE010871/01, 2016], and a complete list of names is provided for reference in Appendix E.

1.7 Applicable References

The abbreviated document titles given in square brackets, […], are used to refer to documents in the reference lists in section 2 of Book II – Part IV Statement of Work (SOW).

1.8 Standards and Specifications

The standards and specifications are indicated in square brackets, […], and refer to documents in the reference lists in section 2 of Book II – Part IV Statement of Work (SOW).

1.9 Verification Methods

The requirements in this SRS will be verified through qualification, herein defined as an endorsement with a guarantee and supporting documentation that the item being qualified satisfies the specified requirement(s). The different verification methods applicable to the requirements herein are described in the following paragraphs.

Note: In some cases, more than one verification method might be required in order to verify fulfilment of a requirement.

1.9.1 Inspection

Inspection is the visual examination of an item (hardware and software) and associated descriptive documentation. Verification is based on the human senses (sight, touch) or other means that use simple measurement and handling methods. No stimulus is necessary. Passive resources such as meter rule, gauge may be used.

For Non-Developmental Items (NDI), Modified NDI and Developmental Items, hardware inspection is used to determine if physical constraints are met, and hardware and/or software, inspection is used to determine if physical quantity lists are met.

1.9.2 Analysis

Analysis is the review and processing of design products (documentation, drawings, presentations, etc.) or accumulated data obtained from other qualification methods, such as manufacturer's tests of a product to be mass-produced, to verify that the system/component design meets required design criteria.

1.9.3 Testing

Testing is the operation of the system, or a part of the system, under controlled and specified conditions, generally using instrumentation, other special test equipment or specific test patterns to collect data for later analysis. This verification method usually requires recorded results to verify that the requirements have been satisfied.

2 General System Description

2.1 Operational and Technical Overview

The IEG-C is a Data Loss Prevention guard at the interface between the (or a) NATO SECRET (NS) domain and a NATO-led 'mission' domain, such as 'Resolute Support' and KFOR. The guard approves or rejects the transmission of data between the two security domains based on either a STANAG-compliant trusted classification label, such as 'NATO <classification> Releasable to <mission>' or trusted source to trusted destination mediated by firewall rule sets. The reason for the trusted source/destination path is that not all current NATO services and apps are 'label aware'.

The overall requirement for the IEG-C is to allow a mission command structure to operate the full range of military command and control IT functions where the staff and users include NATO and non-NATO mission partners. All non-NATO mission partners will have security agreements with NATO such that they are authorised to access information classified up to NATO SECRET Releasable to

<Mission>. In such a situation, two IT systems are provided; one classified 'NATO SECRET' to process information that is required for the mission but not releasable to non-NATO partners (typically J2 data) and one classified <Mission> SECRET that is accessible to all authorised mission partners, both NATO and non-NATO.

For practical purposes, the majority of users are typically provided with access to the mission IT system. Users in the NS domain (both local and in the static NS domain) can be granted access to services and data in the <Mission> SECRET domain, but users in the <Mission> SECRET domain are prevented from any access to the NS domain. The NATO requirement for users with elevated privileges (e.g. system administrators) to have a security clearance higher than the level of the system they operate means that only NATO cleared users can be granted such permissions. Where both NS and <Mission> SECRET IT systems are provided, data transfer requirements typically require the IEG-C to be deployed to the mission HQ so that LAN-level transfer speeds can be provided between the two IT systems. Where a mission has no NS component, the IEG-C can be located at the supporting HQ at the reach-back or mission anchor location. Possible configurations are shown in the Figure 1 Possible IEG-C configurationsFigure 1 Possible IEG-C configurations:
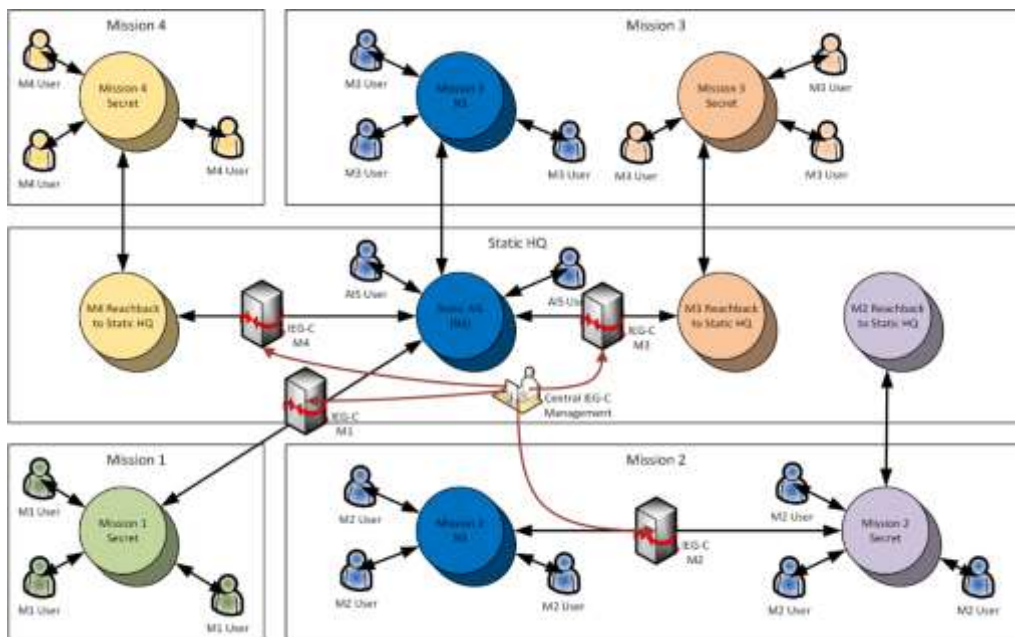
Figure 1 Possible IEG-C configurations

The IEG-C requirement and operational prototype solutions have evolved over many years to a situation where there are two main variants in operation today; those with a 'DMZ' and those without. In the 'without' case, a firewall and a mail guard are connected in parallel between the two security domains. The 'DMZ' configuration adds a third domain mediated by the firewall that contains the mail guard and other guards and proxies, such as an XML web-guard and web reverse proxy.

The objective of the IEG-C project is to modernise and standardise the configurations to a single layout as in Figure 2 IEG-C Management and ComponentsFigure 2 IEG-C Management and Components, and to add additional features required by, for instance, evolving security protection measures. It should be noted that configurations will never be fully identical as different missions will always operate different C2 tools and information exchange requirements due to the nature of the operation (Maritime-based, Land-based etc.). So there will be differences in the firewall rule sets and, of course, all missions have specific releasability labels.
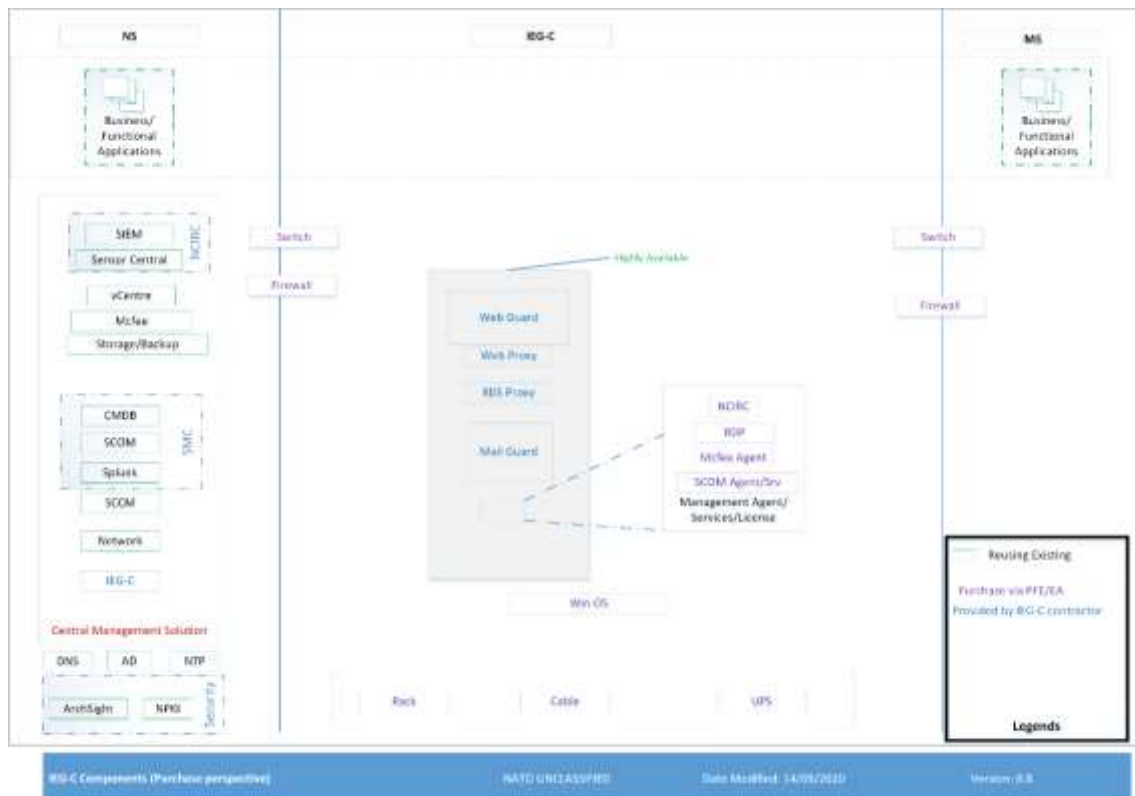
Figure 2 IEG-C Management and Components

As the IEG-C is a data release guard, it does not support any on-line users and, other than log files, only supports transient data. All of the IEG-C components will be centrally managed by a Boundary Services management team from a central location. IEG-C components and services will also be locally monitored. In case of loss of connectivity from central management team and the distant IEG-C, it will be possible to perform any management functions locally.

The logical layout and data flows of the IEG-C is shown in Figure 3Figure 3. Features to note are that physically separate firewalls are required for the interface to the NS domain and the interface to the <Mission> SECRET domain and that separate IEG-Cs are required for each mission. The diagram is illustrative of the data flows between the NS and <Mission> SECRET domains and shows both operational and management streams.
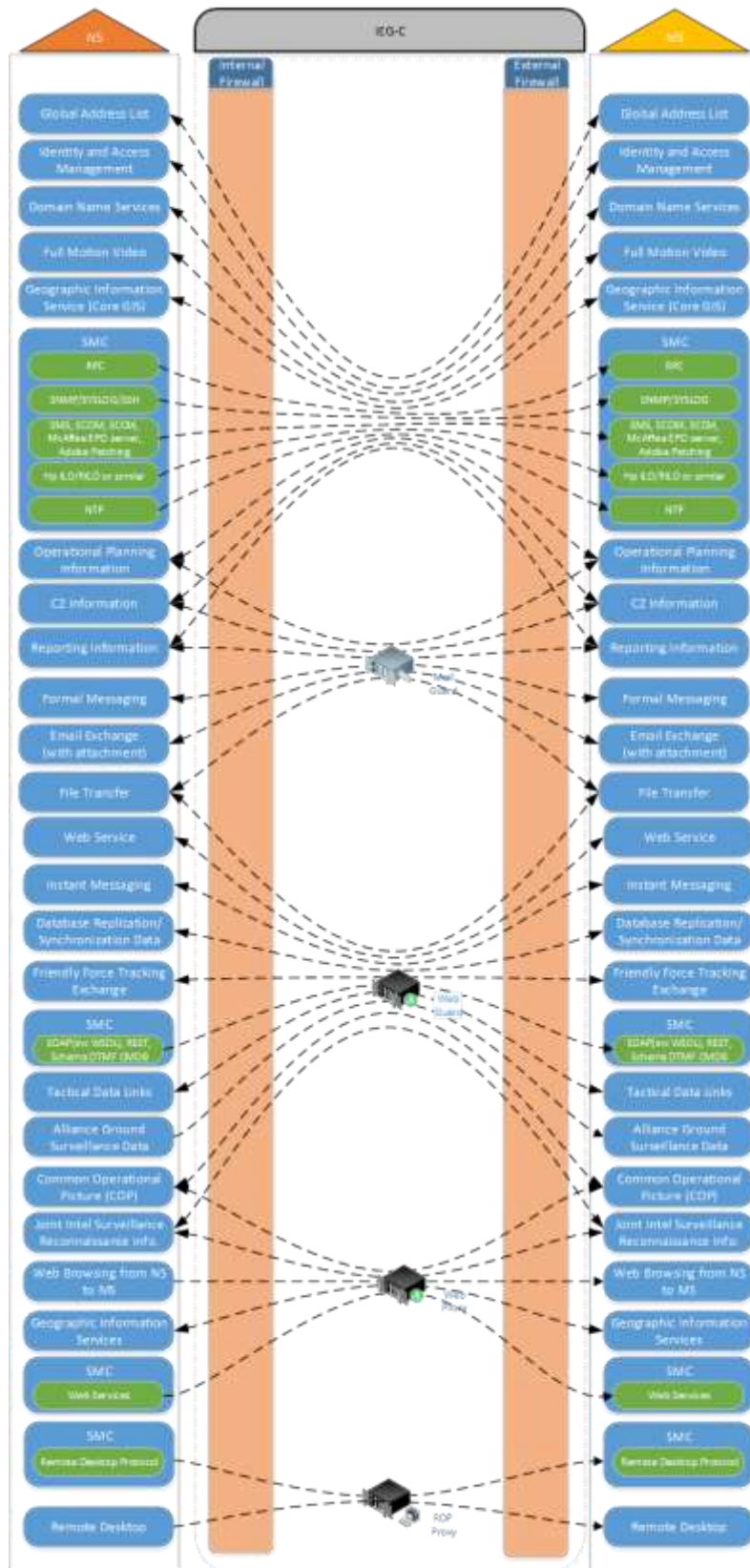
Figure 3 IEG-C Data Flows

2.2 Deployment Overview

The IEG Scenario C is intended to work on Secret level only. The IEG-C has three principal deployment options (as depicted in Figure 4Figure 4):

- in a static configuration where it acts as the interface between the static NS domain and MS domain at the mission HQ (e.g. IEG-C M1);
- in a deployed configuration where it acts as the interface between the NS domain and MS domain at the mission HQ (e.g. IEG-C M2); and
- in a static configuration where it acts as the interface between the static NS domain and the MS domain at the reach-back location (e.g. IEG-C M3 and IEG-C M4).
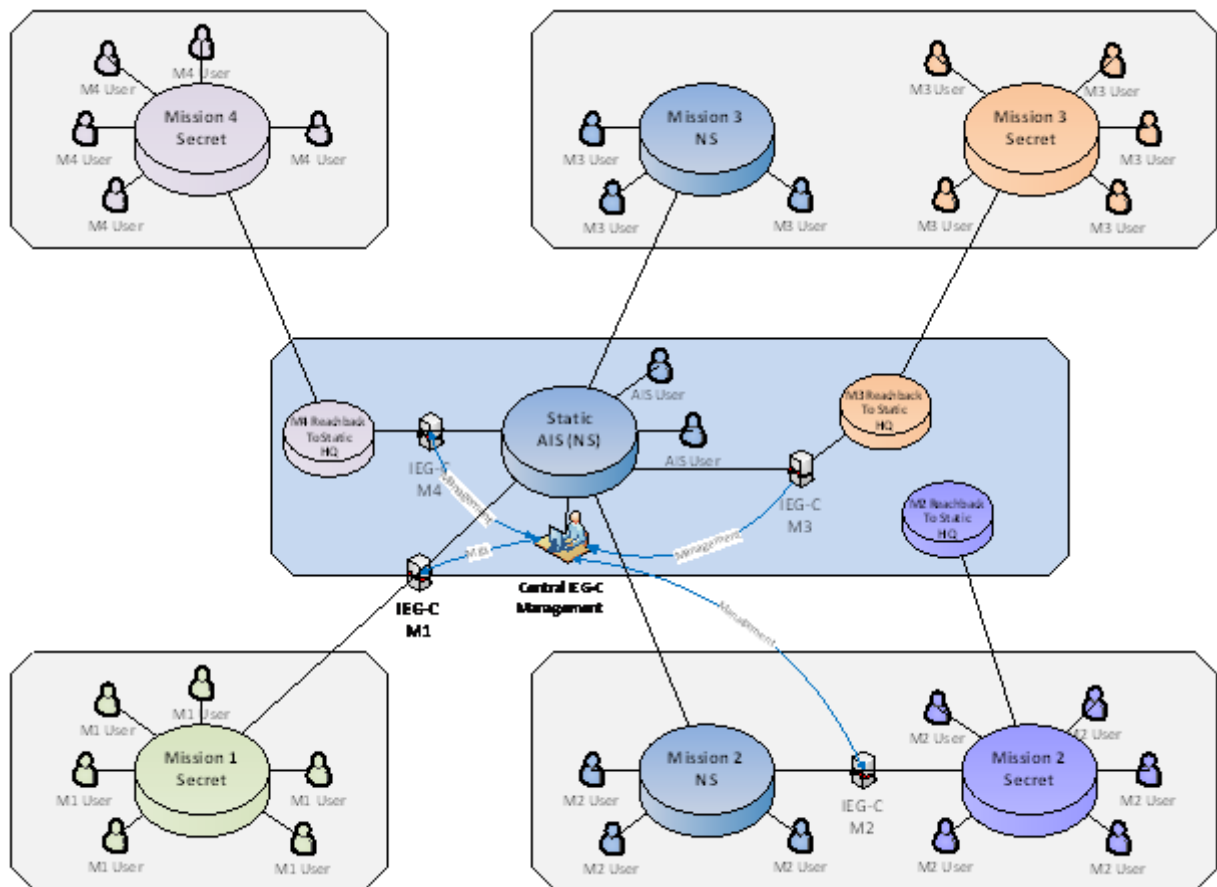
Figure 4 Principal modes of operation of the IEG-C

3 IEG-C Architecture

3.1 General

The IEG-C target architecture (TA, [TR/2016/NSE010871/01, 2016]) is described in terms of a set of composite IEG-C Architecture Building Blocks (ABBs), each of which has a set of associated functions, interfaces and attributes. The ABB methodology, as defined by NATO Enterprise Architecture (EA) Policy, Annex 9 of the Alliance C3 Policy, [NAC C-M(2015)0041-REV1, 2016], is used as the basis for defining an IEG-C Target Architecture.

The approach taken for describing the ABBs was driven by the need to design, implement and accredit a modular set of information assurance services, mediation services and associated service management and control services to enable information exchange between the NATO Secret (NS) network and NATO-led mission classified networks. The Target Architecture describes a standardized architecture for IEG-C addressing:

- Static implementation at centralized locations;
- IEG-C at deployable Point of Presence; and,
- IEG-C prototypes currently installed at static and deployed.

The ABBs are used within the Target Architecture to describe the overall functionality of the IEG-C and how each information exchange requirement (IER) can be supported through the IEG-C in terms of a pattern describing the interactions between ABBs and their service operations and interfaces. In turn, the architecture identifies the class of device (e.g. network switch, firewall, proxy, guard) which may be used to support each of the identified patterns, and associates the patterns with the IERs required to be supported by the IEG-C. Note that an IER may make use of more than one pattern.

Finally, the Target Architecture, derived from the ABBs, their functions, interfaces, attributes and patterns provided the basis for describing the system specification for IEG-C against which actual IEG-Cs can be procured.

3.2 IEG-C Primary Interfaces

The logical architecture allows for a standard gateway to be implemented that provides interfaces (see Figure 5Figure 5) between NATO Secret (NS) CIS (high domain) and NATO-led Mission Secret (MS) CIS (low domain) whereby the security of the NS CIS shall be improved by providing:

- standardized components;
  - o standardized hardware; and,
  - o standardized software.
- standardized configuration;
- centralized management; and,
- centralized maintenance.
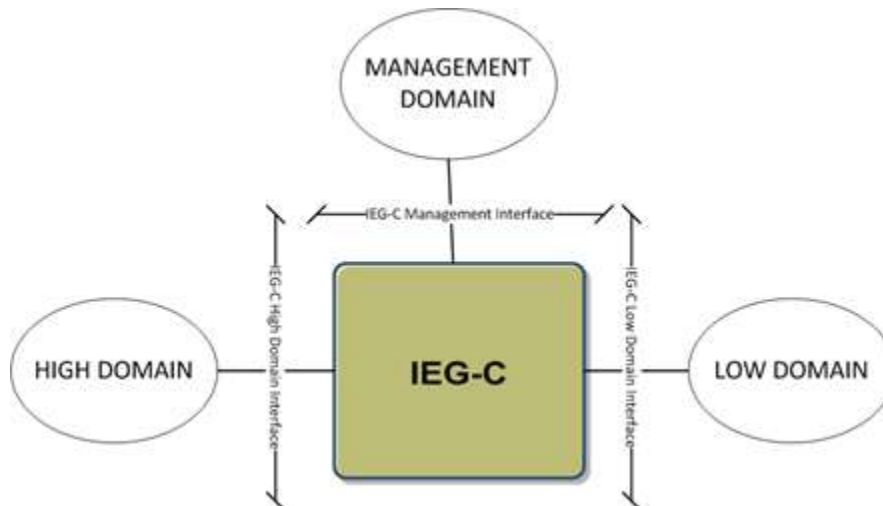
Figure 5 IEG-C Primary Interfaces

Requirement ID: [SRS-3-1]

The IEG-C SHALL provide a data exchange capability IEG-C_DEX that facilitates the mediation of data between the High Domain and the Low Domain.

Requirement ID: [SRS-3-2]

IEG-C_DEX SHALL offer the physical network interface IEG-C High Domain Interface [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_NET_HIGH) that provides Ethernet connectivity to the High Domain.

Requirement ID: [SRS-3-3]

IEG-C_DEX SHALL offer the physical network interfaces IEG-C Low Domain Interfaces [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_NET_LOW) that provides Ethernet connectivity to the Low Domains.

Requirement ID: [SRS-3-4]

IEG-C_DEX MAY offer the physical network interface IEG-C Management Interface [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_MGMT) that provides Ethernet connectivity to the High Domain.

Requirement ID: [SRS-3-5]

In the case that IEG-C_DEX cannot offer the physical network interface IEG-C_IF_MGMT, it SHALL offer a logical network interface IEG-C_IF_MGMT on top of IEG-C_IF_NET_HIGH.

Requirement ID: [SRS-3-6]

The IEG-C SHALL offer the following functionality as described in the IEG-C Architecture Building Blocks [NCIA TR/2016/NSE010871/01, 2017]:

- Provide CIS connectivity;
- Create Network Boundary;

NATO UNCLASSIFIED

- Create Domain Boundary;
- Protect Confidentiality of High Domain;
- Protect Integrity of High Domain;
- Protect Availability of High Domain;
- Mediate Data Exchange; and,
- Centralize Management.

Requirement ID: [SRS-3-101]

All IEG-C components SHALL support 1GbE.

Requirement ID: [SRS-3-102]

All IEG-C components SHALL be upgradeable, through the use of pluggable transceivers, to support 10GbE.

3.3 IEG-C Capabilities

Requirement ID: [SRS-3-7]

The design and architecture of the IEG-C for providing protected cross domain information exchange between NATO Secret and NATO-led Mission Secret SHALL be implemented in accordance with the self-protecting node principle [NAC AC/35-D/2004-REV3, 2013].

The critical technical capabilities for enabling protected cross domain information exchange are illustrated in Figure 6Figure 6.
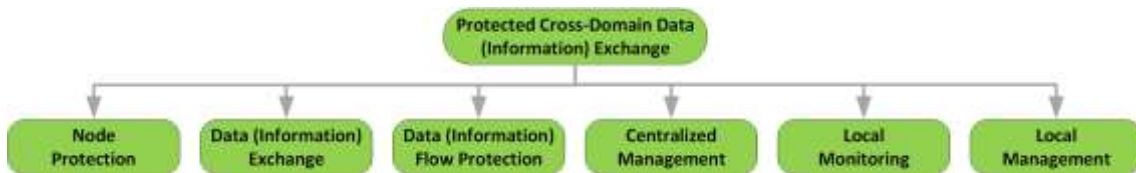
Figure 6 IEG-C Capabilities

The technical capabilities delivered by the IEG-C are summarised in Table 1.

Table 1 IEG-C Capabilities and Capability Statement

Capability Name	Capability Statement
Node Protection	The ability of the gateway to protect the infrastructure and to mitigate risks introduced by interconnecting NATO Secret and Mission secret networks.
Data (Information) Exchange	The ability of the gateway to ensure an efficient cross domain flow of data (information) between NATO Secret and Mission Secret for selected COI and Core Services.
Data (Information) Flow Protection	The ability of the gateway to enforce the protection policies, to prevent unauthorized and uncontrolled release of information, and to ensure that only the information intended to be exchanged are effectively transmitted under a controlled, security monitored regime (security label filtering compliant with NATO policy, document scanning, etc.).
Centralized Management	The ability of the gateway to be managed from a centralized system that provides enterprise level monitoring of information to support Service Management and Control (SMC) and Cyber Defence.
Local Monitoring	The ability to monitor all IEG-C components and services from a co-located monitoring suite, independent from the centralized management.
Local Management	Alternative solution to the Centralized Management to allow co-located support teams to perform (reduced) management activities if connectivity to central management is lost.

3.4 IEG-C Architecture Building Block Services

The IEG-C TA further subdivides the IEG-C ABB into the following ABBs:

- Data Exchange Services;
- Protection Services;
- Protection Policy Enforcement Services; and,
- Element Management Services.

The ABBs have been defined in a generic manner in order to support any information exchange requirements (IERs), specifically to:

- support the mediation of any type of data over any type of protocol;
- enforce the protection policy required for that information exchange requirement; and,
- centrally manage the IEG-C.

For each ABB a list of defined functions, service interfaces and service attributes is defined. The functionality provided by the IEG-C ABBS can be mapped to the IEG-C capabilities summarised in Table 1 as illustrated in Table 2.

Table 2 Mapping between IEG-C Capabilities and IEG-C ABB Services

	Data Exchange Services	Protection Services	Protection Policy Enforcement Services	Element Management Services
Node Protection	X	X		
Data (Information) Exchange	X			
Data (Information) Flow Protection		X	X	
Centralized Management				X

3.4.1 Data Exchange Services

The Data Exchange Services facilitates the mediation of data between a high network domain (High Domain) and a low network domain (Low Domain). The Data Exchange Services can be logically grouped to the following NATO C3 Taxonomy [NC3B AC/322-D(2019)0034 (INV), 2019] defined services classifications for supporting data mediation services:

- Communications Access Services;
- Infrastructure Services;
- SOA Platform Services; and,
- Business Support Services.

Requirement ID: [SRS-3-8]

The Data Exchange Services SHALL offer the following functionality to provide CIS Interconnectivity and Mediate Data Exchange:

- Exchange Email Services Data;
- Exchange Web Services Data;
- Provide Remote Desktop Access;
- Exchange Network Services Data; and,
- Exchange Text Based Collaboration Services Data

3.4.2 Protection Services

Requirement ID: [SRS-3-9]

The Protection Services SHALL provide the capability to protect data at the network layer and the application layer. The Protection Services consists of the following three atomic services:

- Intrusion Detection Services;
- Public Key Cryptographic Services; and,
- Content Inspection Services.

3.4.2.1 Intrusion Detection Services

Requirement ID: [SRS-3-10]

The Intrusion Detection Services SHALL offer the following functionality to provide protection for the integrity of the NATO Secret network and protection for availability of the NATO Secret network:

- Detect Malicious Activities and Faults;
- Prevent and mitigate Attacks and Faults

3.4.2.2 Public Key Cryptographic Services

Requirement ID: [SRS-3-11]

The Public Key Cryptographic Services SHALL offer the following functionality to provide protection for the confidentiality of the NATO Secret network and protection for the integrity of the NATO Secret network:

- Process Public Key Cryptographic Data
- Manage Cryptographic Keys

3.4.2.3 Content Inspection Services

Requirement ID: [SRS-3-12]

The Content Inspection Services SHALL offer the following functionality to provide protection for the confidentiality, integrity and availability of the NATO Secret network:

- Identify Content;
- Verify Content; and,
- Transform Content.

3.4.3 Policy Protection Enforcement Services

Requirement ID: [SRS-3-13]

The Protection Policy Enforcement Services SHALL enforce protection policies on mediated data.

Requirement ID: [SRS-3-14]

The Protection Policy Enforcement Services SHALL consider all aspects relevant to protection of confidentiality, integrity and availability. The Protection Policy Enforcement Services consists of the following two services:

- Information Flow Control Policy Enforcement (IFCPE) Services; and,
- Content Inspection Policy Enforcement (CIPE) Services.

3.4.4 IFCPE Services

Requirement ID: [SRS-3-15]

The IFCPE Services SHALL enforce Information flow policies (IFP), which constitute a subset of protection policies.

Requirement ID: [SRS-3-16]

The IFPs SHALL define the way information moves between the NATO Secret network and the Mission Secret network, and vice-versa based upon the following criteria:

- the subjects (for example, this may be the IP address of the source and destination, or originator and recipient domain for email or text-based collaboration chat, or the source and destination interfaces within the IEG-C where the IFP is being enforced) under control of the policy;
- the content (the data type i.e. XML, that is being exchanged by the Data Exchange Service supporting the information exchange requirement) under control of the policy; and
- the operations which cause information to flow to and from controlled subjects covered by the policy.

For each IEG-C an information flow control policy (IFP) is enforced. This is referred to as IEG-C_IFP. The IEG-C_IFP can be viewed as the union of the following three sub-policies:

- IEC-C_IFP_HL: for traffic flowing from the High Domain to the Low Domain;
- IEG-C_IFP_LH: for traffic flowing from the Low Domain to the High Domain; and,
- IEG-C_IFP_MGMT: for management traffic flowing between the Management Domain and the IEG-C.

Requirement ID: [SRS-3-17]

The Information Flow Control Policy Enforcement (IFCPE) Services SHALL enforce the following general IFPs:

- IEG-C_IFP_CA_HL - Communications Access Services High to Low IFP;
- IEG-C_IFP_CA_LH - Communications Access Services Low to High IFP;
- IEG-C_IFP_IS_HL - Infrastructure Services High to Low IFP;
- IEG-C_IFP_SOA_HL - SOA Platform Services High to Low IFP;
- IEG-C_IFP_SOA_LH - SOA Platform Services Low to High IFP;
- IEG-C_IFP_BS_HL - Business Support Services High to Low IFP;
- IEG-C_IFP_BS_LH - Business Support Services Low to High IFP; and,
- IEG-C_IFP_CS_MGMT - Core Services Management Services IFP.

3.4.5 CIPE Services

Requirement ID: [SRS-3-18]

The Content Inspection Policy Enforcement (CIPE) Services SHALL enforce Content Inspection Policies (CIPs) which define how the data mediated between the NATO Secret network and NATO-led Mission network is to be inspected.

Requirement ID: [SRS-3-19]

The CIPs SHALL be designed to protect the confidentiality of the NATO Secret network by inspecting data for unauthorised information that should not be released to the NATO-led Mission Network.

Requirement ID: [SRS-3-20]

The CIPs SHALL be designed to protect the integrity and availability of the NATO Secret network by identifying and verifying the structure of the data and removing or blocking malicious content.

Requirement ID: [SRS-3-21]

CIPE Services SHALL enforce the following general CIPs:

- IEG-C_CIP_SOA_HL - SOA Platform Services High to Low CIP;
- IEG-C_CIP_SOA_LH - SOA Platform Services Low to High CIP;
- IEG-C_CIP_BS_HL - Business Support Services High to Low CIP;
- IEG-C_CIP_BS_LH - Business Support Services Low to High CIP;
- IEG-C_CIP_COI-ES_HL - COI-Enabling Services High to Low CIP;
- IEG-C_CIP_COI-ES_LH - COI-Enabling Services Low to High CIP;
- IEG-C_CIP_COI_HL - COI-Specific Services High to Low CIP; and
- IEG-C_CIP_COI_LH - COI-Specific Services Low to High CIP.

3.4.6 Element Management Services

Requirement ID: [SRS-3-22]

The IEG-C Element Management Services SHALL provide interfaces that can be managed from a centralized management system to support activities such as Service Management and Control (SMC), Cyber-Defence, security policy administration, audit management and IEG-C configuration and maintenance.

Requirement ID: [SRS-3-25]

The IEG-C Element Management Services SHALL provide interfaces to support local management activities such as Service Management and Control (SMC), Cyber-

Defence, security policy administration, audit management and IEG-C configuration and maintenance, in case of loss of connectivity with the Central Management system.

Requirement ID: [SRS-3-23]

The Element Management Services SHALL support the different administrative roles that are required for managing the IEG-C.

Requirement ID: [SRS-3-24]

The administrative roles of the IEG-C SHALL be categorised as follows:

- System Administrator: responsible for installation, configuration and maintenance of the IEG-C;
- Local System Administrator: responsible for installation, configuration and maintenance of a subset of IEG-C's;
- Local System Maintainer: responsible for some maintenance activities of a subset of IEG-C's;
- Audit Administrator: responsible for regular review of IEG-C audit logs;
- CIS Security Administrator: responsible for performing the IEG-C CIS security-related tasks, such as security policy management;
- Cyber Defence Administrator: responsible for monitoring and performing cyber-related tasks; and,
- SMC Administrator: responsible for monitoring IEG-C services.
- Local SMC Administrator: responsible for monitoring a subset of IEG-C's services and components.

3.5 Patterns

The IEG-C ABBs can be combined into patterns which describe re-useable solutions (or components) to:

- support the mediation of any type of data over any type of protocol;
- enforce the protection policy required for that information exchange requirement; and,
- centrally and locally manage the IEG-C.

From a generic approach, patterns for combining the ABBs can be put together as shown in the IEG-C TA [TR/2016/NSE010871/01, 2016] APPENDIX B (listed below for reference):

- High to Low Node Protection Pattern
- High to Low Cross Domain Information Exchange Pattern
- Low to High Node Protection Pattern
- Low to High Cross Domain Information Exchange Pattern
- Management Pattern

However, the interfaces offered and the functionality provided by each of the composite ABBs and how the ABBs are combined are dependent upon the information exchange requirement (IER) that the IEG-C is required to support and the organizational policy to be enforced. As such, the patterns described in [TR/2016/NSE010871/01, 2016]

Appendix B have been tailored to specifically support the information exchange requirements that are required to be supported by the IEG-C (as listed below):

- Communications Access Services Pattern;
- SOA Platform Web Services Pattern;
- Business Support Services Email Pattern;
- Business Support Services Chat Pattern;
- Infrastructure Remote Desktop Access Pattern;
- SOA Platform High to Low Web Browsing Pattern;
- CIS Security Management Pattern; and,
- Service Management and Control (SMC) pattern.

These specific patterns are documented in Section 5.4.1 of the IEG-C TA [TR/2016/NSE010871/01, 2016] and are used as the basis for defining the requirements for the IEG-C components, the system interfaces offered by the IEG-C components and how the IEG-C components are integrated as specified in Section 4.

4 IEG-C Components, Interfaces and Integration

4.1 General

4.1.1 Components

Requirement ID: [SRS-4-1]

The IEG-C (depending upon the IERs and protection policies to be enforced for the CIS interconnection) SHALL consist of the following components:

- Firewalls;
- Network Switches;
- RDP Proxy;
- Web Proxy;
- Mail Guard; and,
- Web Guard.

Requirement ID: [SRS-4-2]

Only those IEG-C components, hence only the protocols, network services, and the information or data flows, required to support the information exchange requirements SHALL be configured and used through the interconnection.

Requirement ID: [SRS-4-3]

The IEG-C architecture and all of its components SHALL be compliant with "INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)" [NAC, AC/322-D/0030-REV5.

Requirement ID: [SRS-4-4]

The IEG-C and all of its components SHALL be configured in accordance with the "Technical and Implementation Directive for CIS Security" [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-4-225]

Unless otherwise identified during the Site Survey [SOW-673], the IEG-C and all of its components SHALL be certified to TEMPEST Level C, as defined in [SDIP-27/2].

Requirement ID: [SRS-4-5]

All IEG-C components SHALL gracefully shut down on notification from the Uninterruptible Power Supply (UPS).

Requirement ID: [SRS-4-226]

It SHALL be possible to trigger the graceful shut down from the central and local management solution.

Table 3 specifies the high level IEG-C TA ABBs (refer to Section 3.4) provided by each of the IEG-C components.

Table 3 IEG-C TA ABB mapping to IEG-C components

	Data Exchange Services	Protection Services	Policy Protection Services	Element Management Services
Firewall	X		X	X
Network Switch	X			X
RDP Proxy	X			X
Web Proxy	X	X	X	X
Mail Guard	X	X	X	X
Web Guard	X	X	X	X

Figure 7Figure 7 illustrates the association between the patterns identified in Section 3.5 and the IEG-C components required to support those patterns.
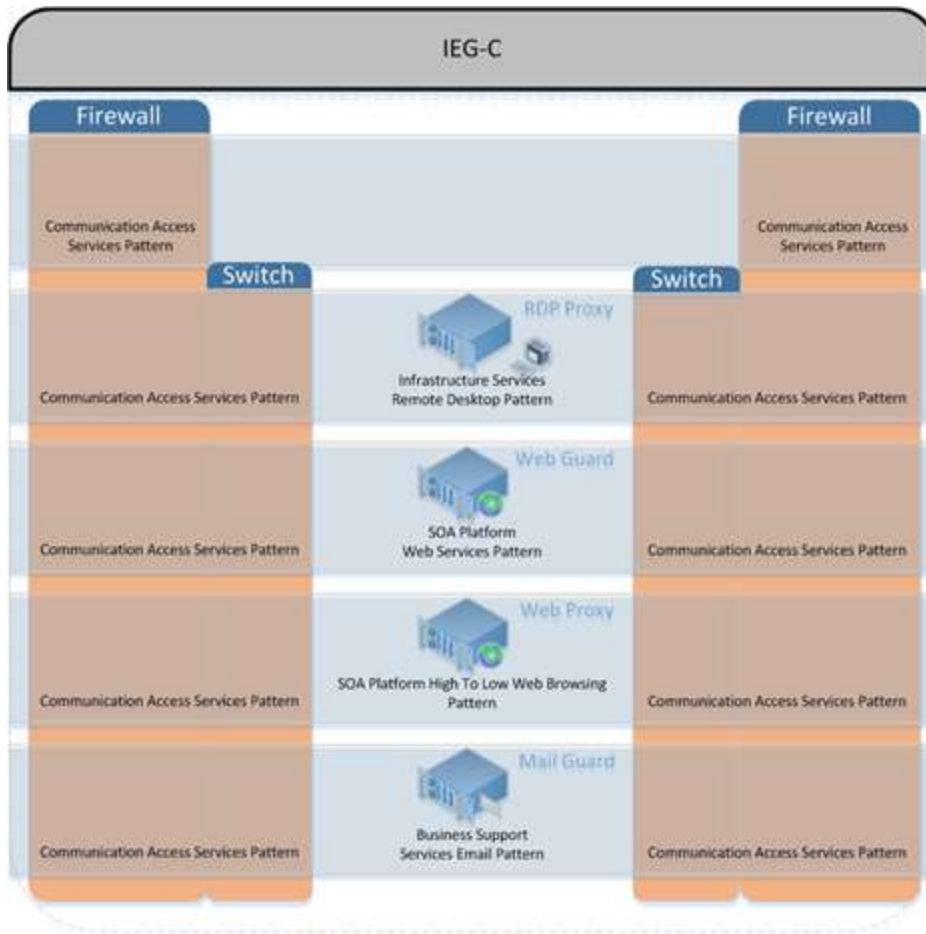
Figure 7 IEG-C components associated with the patterns

Requirement ID: [SRS-4-6]

The IEG-C SHALL provide supporting components required for the composition of an IEG-C (see Section 4.7.2).

4.1.2 System Interfaces

Figure 8Figure 8[1] below provides the system interfaces illustrating how the IEG-C components are connected based on the physical interfaces (see Section 3.2) offered by the IEG-C in order to support up a mission.

[1] *Note that this figure illustrates how future proxies or guards can be integrated into the IEG-C to support future information exchange requirements.*
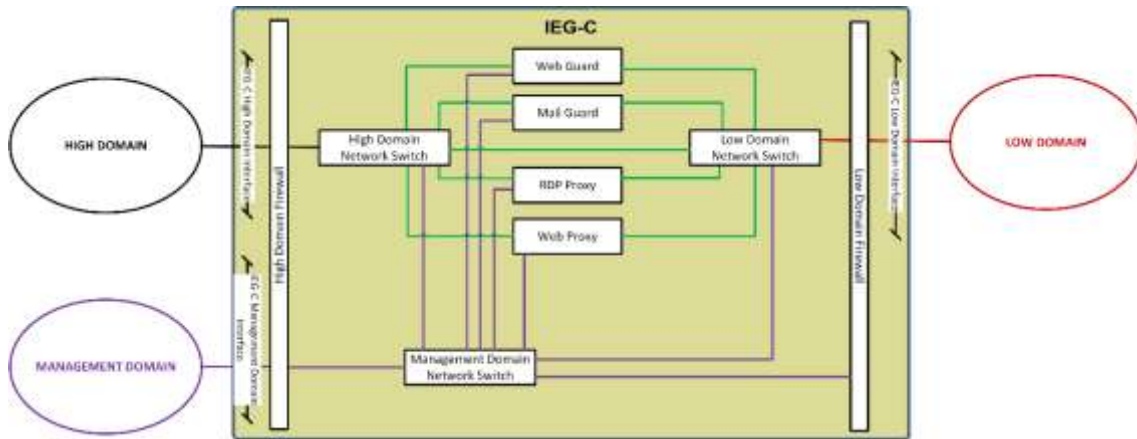
Figure 8 IEG-C Network Level System Interface

The IEG-C_DEX physical network interfaces (IEG-C High Domain Interface, IEG-C Low Domain Interfaces and Management Interface) depicted in Figure 5 above are further sub-divided into system (logical) interfaces provided by the Data Exchange Services (see Section 3.4.1) supporting connectivity to the high and low domains dependent upon the protocol being mediated across the IEG-C.

Table 4Table 4 shows a list of the application and management (SMC Service) protocols that will be arbitrated by the IEG-C, together with the primary component that will mediate the information using the protocol.

Table 4: Protocols Supported by the IEG-C

Protocol	Name	IEG-C Component	Service
DNS	Domain Name Services	Firewall	Domain Name Services
OCSP	Online Certificate Status Protocol	Firewall	PKI
LDAP	Lightweight Directory Access Protocol	Firewall	PKI
			Global Address List
			Identity and Access Management
HTTP	Hyper Text Transfer Protocol	Web Proxy	Web browsing from NS to MS
			Operational Planning information
			C2 Information
			Reporting Information
			Geographic Information Services
			Common Operational Picture
			JISR Replication
			SMC
		Web Guard	Web Service
			File Transfer
			Database Replication/Synchronization Data
			Friendly Force Tracking Exchange
			JISR Replication
			Geographic Information Services
			Common Operational Picture

Protocol	Name	IEG-C Component	Service
			SMC
SMTP	Simple Mail Transfer Protocol	Mail Guard	Email Exchange (with attachment)
			Formal Messaging (NMS)
			Operational Planning information
			C2 Information
			Reporting Information
			File Transfer
XMPP	eXtensible Message and Presence Protocol	Web Guard	Instant Messaging
RDP	Remote Desktop Protocol	RDP Proxy	Remote Desktop
			SMC
RTP	Real Time Protocol	Firewall	Full Motion Video
RTCP	Real Time Control Protocol	Firewall	Full Motion Video
Link 1	Link 1	Web Guard	Tactical Data Links
Link 11	Link 11	Web Guard	Tactical Data Links
Link 16	Link 16	Web Guard	Tactical Data Links
Link 22	Link 22	Web Guard	Tactical Data Links
JREAP	Joint Range Extension Applications Protocol	Web Guard	Tactical Data Links
OTH-GOLD	Over-The-Horizon GOLD	Web Guard	Tactical Data Links
FFTS	Friendly Force Tracking Systems	Web Guard	Tactical Data Links
NTP	Network Time Protocol	Firewall	SMC
SYSLOG	Syslog	Firewall	SMC
SNMP	Simple Network Management Protocol	Firewall	SMC
SSH	Secure Shell	Firewall	SMC
FTP	File Transport Protocol	Firewall	SMC
TELNET	Telnet	Firewall	SMC
RPC	Remote Procedure Call	Firewall	SMC
IPMI	Intelligent Platform Management Interface	Firewall	SMC
SCOM	System Center Operations Manager	Firewall	SMC
SCCM	System Center Configuration Manager	Firewall	SMC
WSUS	Window Server Update Services	Firewall	SMC

Protocol	Name	IEG-C Component	Service
CMDBf	Configuration Management Database Federation	Firewall	SMC
SMS	System Management Server	Firewall	SMC
EPO	Mc-Afee e-Policy Orchestrator	Firewall	SMC
AP	Adobe Patching	Firewall	SMC

Requirement ID: [SRS-4-7]

IEG-C_DEX SHALL offer User Datagram Protocol (UDP) [IETF RFC 768, 1980] and Internet Protocol (IP), IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interfaces 'Communications Access Services HL' and 'Communications Access Services LH' on top of IEG-C_IF_NET_HIGH and IEG-C_IF_NET_LOW, respectively.

Requirement ID: [SRS-4-224]

The IEG-C_DEX SHALL preserve the Differentiated Services field (DS Field) [IETF RFC 2474, 1998] in the IPv4 and IPv6 Headers.

Requirement ID: [SRS-4-8]

IEG-C_DEX SHALL offer HyperText Transport Protocol (HTTP), v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services HL' on top of 'Communications Access Services HL' and HyperText Transport Protocol (HTTP), v1.1 and v2. [IETF RFC 7230, 2014],[IETF RFC 7540, 2014] interface 'SOA Platform Services LH' on top of 'Communications Access Services LH'.

Requirement ID: [SRS-4-9]

The 'SOA Platform Services HL' and 'SOA Platform Services LH' interfaces SHALL support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-4-101]

The TLS Server identity (X.509 PKIX version 3.0 certificate, [IETF RFC 5280, 2008]) SHALL be validated, as per Section 6 of [IETF RFC 6125, 2011] following the best current practices documented in the "Recommendations for Secure Use of TLS and DTLS" [IETF RFC 7525, 2015(IETF)].

Requirement ID: [SRS-4-10]

IEG-C_DEX SHALL offer Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008] interface 'Business Support Services HL' on top of 'Communications Access Services HL' and Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008] interface 'Business Support Services LH' on top of 'Communications Access Services LH'.

Requirement ID: [SRS-4-11]

IEG-C_DEX SHALL offer Remote Desktop Protocol (RDP) [RDP Overview, 2019] interface 'Infrastructure Services HL' on top of 'Communications Access Services HL'.

Requirement ID: [SRS-4-102]

IEG-C_DEX SHALL offer an interface "Core Services" on top of 'Communications Access Services Management' that SHALL support the following protocols:

- DNS [IETF RFC 1035, 1987]
- OCSP [IETF RFC 6960, 2013]
- LDAP [IETF RFC 4510-4519, 2006]
- RTP [IETF RFC 3350, 2003]
- RTCP [IETF RFC 3350, 2003]
- JREAP [STANAG 5518]

Requirement ID: [SRS-4-12]

IEG-C_DEX SHALL offer UDP [IETF RFC 768, 1980] and IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interface 'Communications Access Services Management' on top of IEG-C_IF_MGMT.

Requirement ID: [SRS-4-13]

IEG-C_DEX SHALL offer an interface 'Core Services Management' on top of 'Communications Access Services Management' that SHALL support the following management protocols:

- Keyboard, video and mouse (KVM) over Internet Protocol (IP);
- Command Line interface (CLI) via Secure Shell (SSH) Transport Layer protocol [IETF RFC 4251, 2006];
- Simple Network Management Protocol (SNMP) Version 3 [IETF RFC 3410 – 3418, 2002];
- Syslog [IETF RFC 5424, 2009];
- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Network Time Protocol (NTP, [IETF RFC 5905, 2010]);
- Intelligent Platform Management Interface (IPMI, [IPMI V.2.0, 2013]);
- Hyper-Text Transport Protocol (HTTP) v1.1 Web interface [IETF RFC 7230, 2014] [IETF RFC 7231, 2014]
- Hyper-Text Transport Protocol (HTTP) v2 Web interface [IETF RFC 7540, 2014] ;
- Remote Desktop (RDP [RDP Overview, 2019];
- Remote Procedure Call (RPC, [IETF RFC 5531, 2009]).
- System Center Operations Manager
- Systems Center Configuration Manager
- Windows Server Update Services
- McAfee e-Policy Orchestrator
- Adobe Patching
- File Transfer Protocol [IETF RFC 959, 1985]
- Telnet [IETF RFC 854, 1983]

Table 4 below identifies the IEG-C_DEX Data Exchange Services interfaces offered by each of the IEG-C components.

Table 5 Data Exchange Services offered by IEG-C components

IEG-C Component	Data Exchange Services Interface	IEG-C TA Reference
Firewall	Communications Access Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.2 Section A.3.3.6
Network Switch	Communications Access Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.2 Section A.3.3.6
RDP Proxy	Communications Access Services Interface Infrastructure Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.3 Section A.3.3.2 Section A.3.3.6
Web Proxy	Communications Access Services Interface SOA Platform Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.4 Section A.3.3.2 Section A.3.3.6
Mail Guard	Communications Access Services Interface Business Support Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.5 Section A.3.3.2 Section A.3.3.6
Web Guard	Communications Access Services Interface SOA Platform Services Interface Communications Access Management Services Interface Core Services Management Interface	Section A.3.3.1 Section A.3.3.4 Section A.3.3.2 Section A.3.3.6

4.1.3 Integration

The IEG-C is a separate security domain from both the high domain and the low domain.

Requirement ID: [SRS-4-14]

Installation guidelines for "Selection and Installation of Equipment for the Processing of Classified Information" [SDIP-29/2] regarding equipment separation and installation requirements SHALL be adhered to.

Requirement ID: [SRS-4-15]

The IEG-C SHALL support a network architecture containing a de-militarized zone (DMZ).

The IEG-C Firewall is physically separated as a High Domain Firewall and a Low Domain Firewall.

Requirement ID: [SRS-4-17]

To support connectivity of the proxies and the guards to the high domain and the low domains the High Network Domain Switch and a Low Domain Network Switch SHALL be provided, respectively.

Requirement ID: [SRS-4-18]

The High Domain Switch SHALL be connected to the High Domain Firewall.

Requirement ID: [SRS-4-19]

The Low Domain Switch SHALL be connected to the Low Domain Firewall.

Requirement ID: [SRS-4-20]

The RDP Proxy SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) using separate physical network interfaces.

Requirement ID: [SRS-4-21]

The Web Proxy SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Firewall) using separate physical network interfaces.

Requirement ID: [SRS-4-22]

The Mail Guard SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) using separate physical network interfaces.

Requirement ID: [SRS-4-23]

The Web Guard SHALL be connected to both the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) via separate physical interfaces.

Requirement ID: [SRS-4-24]

The IEG-C shall include secure remote management capabilities providing the ability to monitor and control all IEG-C components remotely from central NATO management premises.

Requirement ID: [SRS-4-227]

The IEG-C shall include secure remote management capabilities providing the ability to integrate the monitoring all IEG-C components into a local NATO monitoring solution.

Requirement ID: [SRS-4-228]

The IEG-C shall include secure remote management capabilities providing the ability to manage all IEG-C components locally in case of loss of connectivity with the central management system.

Requirement ID: [SRS-4-25]

To support the (remote) management of the IEG-C, a Management Domain Network Switch SHALL be provided.

Requirement ID: [SRS-4-28]

The Management Domain Network Switch SHALL be connected to the High Domain Firewall.

Requirement ID: [SRS-4-29]

All IEG-C components SHALL have a connection to the Management Domain Switch.

Requirement ID: [SRS-4-30]

The IEG-C wired infrastructure for connecting IEG-C components (that are required to be connected together to support the information exchange requirements for the CIS interconnection) SHALL be based on Ethernet running over fibre optic and copper cables.

Requirement ID: [SRS-4-200

The IEG-C wired infrastructure for connecting IEG-C components (that are required to be connected together to support the information exchange requirements for the CIS interconnection) SHALL support VLANs.

4.1.4 External Interfaces

Figure 9Figure 9 illustrates the external interfaces, server-to-server, across the IEG-C, together with the associated IEG-C components that mediate the information exchange.
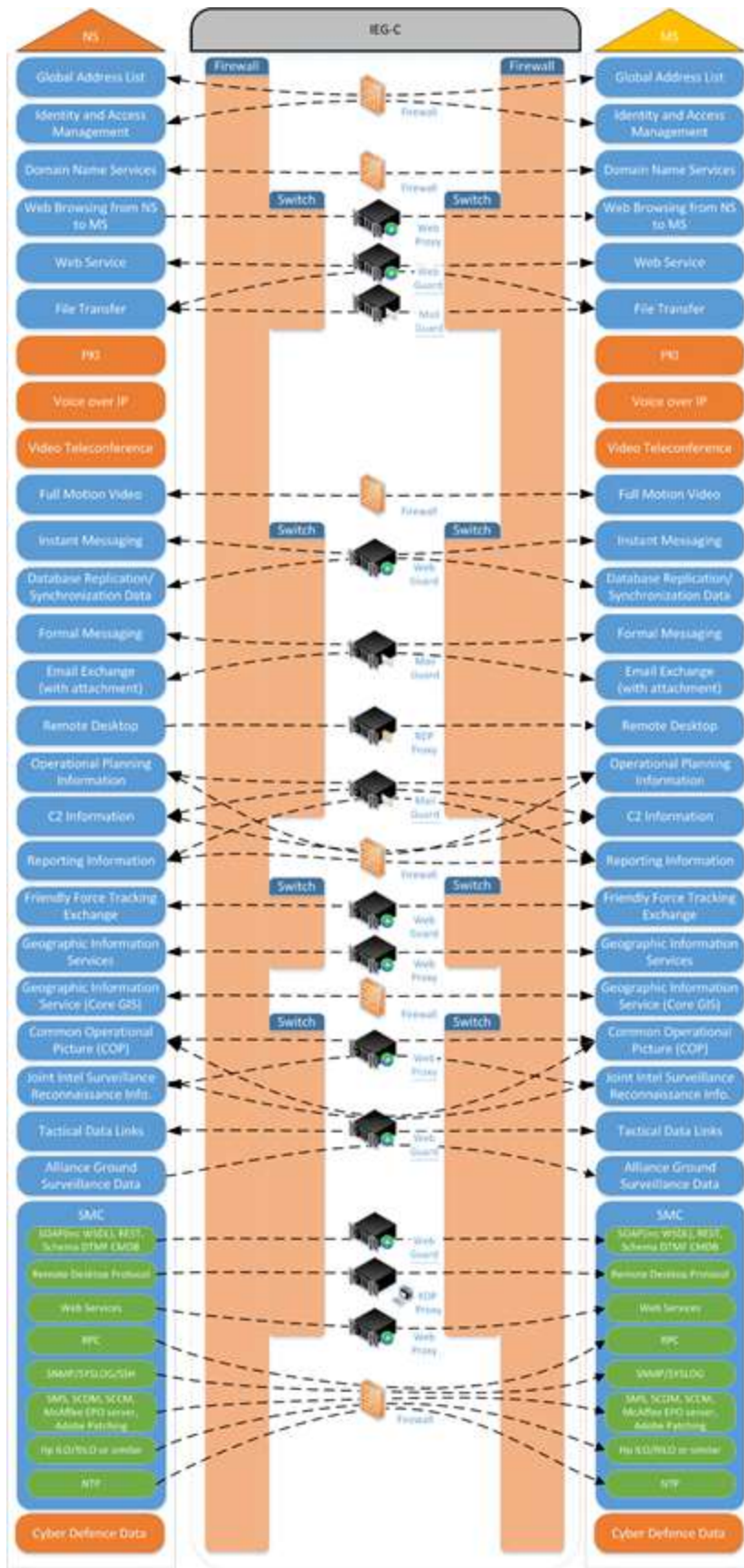
Figure 9 External interfaces, server-to-server, across the IEG-C

Requirement ID: [SRS-4-31]

The IEG-C SHALL be conformant with the service interface profiles (SIPs) and NATO Interoperability Standards and Profiles (NISPs) listed in APPENDIX B.

Requirement ID: [SRS-4-33]

The IEG-C SHALL interface and function correctly with the NATO Computer Incident Response Capability (NCIRC).

Requirement ID: [SRS-4-34]

The IEG-C SHALL interface and function correctly with the NATO Enterprise Service Management and Control (SMC) capability.

Requirement ID: [SRS-4-35]

The IEG-C SHALL interface and function correctly with the NATO Public Key Infrastructure (NPKI) capability.

Requirement ID: [SRS-4-36]

The IEG-C SHALL interface and function correctly with the NATO Enterprise Directory Services (NEDS) capability.

Requirement ID: [SRS-4-37]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Active Directory Domain Services (ADDS) capability.

Requirement ID: [SRS-4-38]

The IEG-C SHALL interface and function correctly with the Operational Network (ON) Automated Information System (AIS) and Mission Secret (MS) AIS mail exchange capability.

Requirement ID: [SRS-4-39]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Domain Name Services (DNS) capability.

Requirement ID: [SRS-4-40]

The IEG-C SHALL use fully qualified domain names (FQDN, [IETF RFC 1983, 1996]) for identifying all hosts, unless specifically requested not to.

Requirement ID: [SRS-4-41]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS web client and server capability providing SOAP-based and REST-based web services.

Requirement ID: [SRS-4-42]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS web client and server capability providing web browsing.

NATO UNCLASSIFIED

Requirement ID: [SRS-4-43]

The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Collaboration Services capability providing audio, voice and video services.

Requirement ID: [SRS-4-44]

The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Extensible Messaging and Presence Protocol (XMPP) capability for exchanging text-based collaboration services messages.

Requirement ID: [SRS-4-45]

The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Tactical Data Link (TDL) capability for exchanging TDL-formatted messages.

Requirement ID: [SRS-4-46]

The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Friendly Force Tracking (FFT) capability for exchanging FFT-formatted messages.

Requirement ID: [SRS-4-48]

The IEG-C SHALL interface and function correctly with the authoritative ON AIS Network Time Protocol (NTP) source.

4.2 Firewall

4.2.1 General

Requirement ID: [SRS-4-49]

The IEG-C Firewall components (High Domain Firewall and Low Domain Firewall) SHALL be the:

- Palo Alto Networks PA-3260 with redundant AC power supplies

A detailed description of this component is provided in Appendix D.

Requirement ID: [SRS-4-221]

The Firewall components SHALL support 10GbE.

Requirement ID: [SRS-4-222]

The Firewall components SHALL handle at least 90Gb throughput per 24 hour period.

Requirement ID: [SRS-4-223]

The Firewall components SHALL be able to sustain, on average, at least 6Gb/s throughput.

Requirement ID: [SRS-4-201]

The selected IEG-C High Domain and Low Domain Firewalls components SHALL include compatible rack mount kits and power cords.

Requirement ID: [SRS-4-51]

The IEG-C High Domain Firewall component Network Time Protocol (NTP) server SHALL be synchronized to a designated NTP server in the ON AIS domain.

Requirement ID: [SRS-4-52]

The IEG-C High Domain Firewall component SHALL be configured as the Authoritative Network Time Protocol (NTP) source for all IEG-C components (including the Low Domain Firewall) that require to be time synchronised.

4.2.2 Data Exchange Services

Requirement ID: [SRS-4-53]

The IEG-C High Domain Firewall and IEG-C Low Domain Firewall components SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

Requirement ID: [SRS-4-202]

The IEG-C High Domain Firewall and IEG-C Low Domain Firewall components SHALL mediate all Data Exchange Services that transition the IEG-C.

4.2.3 Protection Policy Enforcement Services

Requirement ID: [SRS-4-54]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be configurable to support the enforcement of the following IEG-C IFPs (see Section 3.4.4):

- IEG-C_IFP_CA_HL - Communications Access Services High to Low IFP;
- IEG-C_IFP_CA_LH - Communications Access Services Low to High IFP; and,
- IEG-C_IFP_CS_MGMT - Core Services Management Services IFP

Requirement ID: [SRS-4-55]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs to allow only authorized systems/hosts to exchange data between the high domain and the low domain.

Requirement ID: [SRS-4-56]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs in order to allow only those protocols and ports required to support the information exchange requirements for the high domain - low domain interconnection.

Requirement ID: [SRS-4-203]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs in order to allow only those application layer protocols and applications that are required to support the information exchange requirements for the high domain - low domain interconnection.

Requirement ID: [SRS-4204]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL identify application layer protocols and applications through application protocol inspection, which SHALL be based on the use of application signatures, application protocol decoding, and heuristics.

Requirement ID: [SRS-4-57]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and the IEG-C_IFP_SOA_LH IFPs in order to route authorised HTTP(S) application-level traffic to the appropriate IEG-C guard or proxy component (through the High Side Switch or appropriate Low Side Switch depending upon the source and destination of the HTTP(S) application-level traffic) in the DMZ.

Requirement ID: [SRS-4-58]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_BS_HL and the IEG-C_IFP_BS_LH IFPs in order to route authorised SMTP application-level traffic to the IEG-C Mail Guard component (through the High Side Switch or appropriate Low Side Switch depending upon the source and destination of the SMTP application-level traffic) in the DMZ.

Requirement ID: [SRS-4-59]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_IS_HL IFP in order to route authorised RDP application-level traffic to the IEG-C RDP Proxy component (through the High Side Switch depending upon the source and destination of the RDP application-level traffic) in the DMZ.

Requirement ID: [SRS-4-60]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CS_MGMT IFP in order to route authorised management traffic to the appropriate IEG-C component (through the Management Switch) in the DMZ.

Requirement ID: [SRS-4-61]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enforce the IEG-C IFPs configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.

4.2.4 Element Management Services

Requirement ID: [SRS-4-62]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be enabled and configured with the capability for being managed as specified in Section 9.

Requirement ID: [SRS-4-205]

The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be managed from the Service Operation Centre (SOC) using the current management tools (i.e. Palo Alto Networks Panorama).

4.2.5 Hardware and Software

Requirement ID: [SRS-4-63]

The IEG-C High Domain Firewall component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the high domain; one for the network connection to the High Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-64]

The IEG-C High Domain Firewall component network interfaces to the high domain SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-65]

The IEG-C High Domain Firewall component network interfaces to the High Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-66]

The IEG-C High Domain Firewall component network interface to the Management Domain Switch SHALL be a 1000-Base-SX gigabit Ethernet interface.

Requirement ID: [SRS-4-206]

The IEG-C Low Domain Firewall component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the low domain; one for the network connection to the Low Domain Network Switch; and, one for the network connection to the Management Domain Network Switch).

Requirement ID: [SRS-4-207]

The IEG-C Low Domain Firewall component network interfaces to the low domain SHALL be 1000-BaseSX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-208]

The IEG-C Low Domain Firewall component network interfaces to the Low Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

4.3 Network Switch

4.3.1 General

Requirement ID: [SRS-4-67]

The IEG-C Network Switch components (High Domain, Low Domain and Management) SHALL be selected from the following list of products:

- Dell Networking N1124T Switch
- Dell Networking S3048 Switch
- Dell Networking S3124F Switch
- Dell Networking S3148P Switch

Detailed descriptions of these component options are provided in Appendix D.

Requirement ID: [SRS-4-209]

The selected IEG-C Network Switch components SHALL include compatible rack mount kits and power cords.

Requirement ID: [SRS-4-68]

The IEG-C Network Switch components SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.3.2 Data Exchange Services

Requirement ID: [SRS-4-69]

The IEG-C Network Switch components SHALL enable the Data Exchange Services as specified in Table 4 (for that component).

4.3.3 Element Management Services

Requirement ID: [SRS-4-70]

The IEG-C High Domain Network Switch and Low Domain Network Switch components SHALL be enabled and configured with the capability for being managed as specified in Section 9.

4.3.4 Hardware and Software

Requirement ID: [SRS-4-71]

The IEG-C High Domain Switch component SHALL be configured to have at least five network interfaces (NICs: one for the network connection to the High Domain Firewall; one for the network connection to the Mail Guard; one for the network connection to the

Web Guard; one for the network connection to the server component; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-72]

The IEG-C High Domain Network Switch component network interface to the high domain firewall SHALL be 1000BASE-SX gigabit Ethernet interface.

Requirement ID: [SRS-4-73]

The IEG-C High Domain Network Switch component network interfaces to the Mail Guard, Web Guard, server component and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-74]

The IEG-C Low Domain Switch components SHALL be configured to have at least five network interfaces (NICs: one for the network connection to the Low Domain firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-75]

The IEG-C Low Domain Network Switch component network interface to the Low Domain Firewall SHALL be 1000BASE-SX gigabit Ethernet interface.

Requirement ID: [SRS-4-76]

The IEG-C Low Doman Network Switch component network interfaces to the Mail Guard, Web Guard, server component and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-77]

The IEG-C Management Domain Switch component SHALL be configured to have at least seven network interfaces (NICs: one for the network connection to the High Domain Firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component; one for the network connection to the High Domain Network Switch, one for the network connections to the Low Domain Network Switch and one for the network connection to the Low Domain Firewall).

Requirement ID: [SRS-4-78]

The IEG-C Management Domain Network Switch component network interface to the Firewall SHALL be a 1GbE interface.

Requirement ID: [SRS-4-79]

The IEG-C Management Domain Network Switch component network interfaces to the Mail Guard, Web Guard, server component, High Domain Switch and Low Domain Switches SHALL be 1GbE interfaces.

4.4 Web Proxy

4.4.1 General

Requirement ID: [SRS-4-81]

The IEG-C Web Proxy component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.4.2 Data Exchange Services

Requirement ID: [SRS-4-82]

The IEG-C Web Proxy component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

4.4.3 Protection Services

Requirement ID: [SRS-4-83]

The IEG-C Web Proxy component SHALL enable the capability to perform cryptographic operations and key management to support interception of Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.

Requirement ID: [SRS-4-229]

The IEG-C Web Proxy component 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-4-230]

The IEG-C Web Proxy component 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.

Requirement ID: [SRS-4-84]

The IEG-C Web Proxy component SHALL be configured to conform to the INFOSEC CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-4-85]

The IEG-C Web Proxy component SHALL be configured to 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-4-86]

The IEG-C Web Proxy component provided cryptographic mechanism SHALL be configured based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].

Requirement ID: [SRS-4-87]

The IEG-C Web Proxy component SHALL use a malware/virus scanner that is included in the NATO Information Assurance Product Catalogue (NIAPC) to check web content for malicious content.

4.4.4 Protection Policy Enforcement Services

Requirement ID: [SRS-4-89]

The IEG-C Web Proxy components SHALL enable the capability to be configured as a reverse web proxy from the high domain to the low domain.

Requirement ID: [SRS-4-90]

The IEG-C Web Proxy component SHALL be configurable to support the enforcement of the following IEG-C SOA Platform IFPs (see Section 3.4.4):

- IEG-C_IFP_SOA_HL - SOA Platform Services High to Low IFP; and,
- IEG-C_IFP_SOA_LH - SOA Platform Services Low to High IFP.

Requirement ID: [SRS-4-91]

The IEG-C Web Proxy component SHALL be configurable to support the enforcement of the following IEG-C SOA Platform CIP (see Section 3.4.5):

- IEG-C_CIP_SOA_LH - SOA Platform Services Low to High CIP.

Requirement ID: [SRS-4-92]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL IFP in order to guard HTTP application-level web browsing requests from the high domain to the low domain.

Requirement ID: [SRS-4-93]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_LH IFP in order to guard HTTP application-level web browsing responses from the low domain to the high domain.

Requirement ID: [SRS-4-94]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and IEG-C_IFP_SOA_LH IFPs to verify that the HTTP request (from the high domain to the low domain) and HTTP response (from the low domain to the high domain) can be released by checking high domain web client access control rules

against white or black lists (assuring only authorised high domain clients (or users) have access to the low domain web content).

Requirement ID: [SRS-4-95]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and IEG-C_IFP_SOA_LH IFPs to verify that the HTTP request (from the high domain to the low domain) and HTTP response (from the low domain to the high domain) can be released by checking low domain web server access control rules against white or black lists (assuring only authorised low domain web servers are published and made accessible for high domain clients).

Requirement ID: [SRS-4-96]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_LH IFP to enforce the IEG-C_CIP_SOA_LH CIP.

Requirement ID: [SRS-4-97]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_CIP_SOA_LH CIP to verify that all HTTP responses from the low domain to the high domain (to HTTP requests from the high domain to the low domain) do not contain any disallowed attachment types by checking against a white list or black list of attachment types.

Requirement ID: [SRS-4-98]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_CIP_SOA_LH CIP to verify that all HTTP responses from the low domain to the high domain (to HTTP requests from the high domain to the low domain) contain no malicious content.

Requirement ID: [SRS-4-231]

The IEG-C Web Proxy component SHALL ensure HTTP request or response does not contain any of the configured words/phrases.

Requirement ID: [SRS-4-232]

The IEG-C Web Proxy component SHALL inspect each of the HTTP request or response, including any attachments, for occurrences of any of the configured words/phrases.

Requirement ID: [SRS-4-233]

The IEG-C Web Proxy component 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 configured words/phrases in the http request or response and any attachments.

Requirement ID: [SRS-4-99]

The IEG-C Web Proxy component SHALL enforce the IEG-C SOA Platform IFPs and SOA Platform CIP configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.

4.4.5 Element Management Services

Requirement ID: [SRS-4-100]

The IEG-C Web Proxy component SHALL be enabled and configured with the capability for being managed as specified in Section 9.

4.4.6 Hardware and Software

Requirement ID: [SRS-4-101]

The IEG-C Web Proxy component SHALL be an appliance, or deployed on a physical server.

Requirement ID: [SRS-4-103]

The IEG-C Web Proxy component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connection to the Low Domain Switches; and, one for the network connection to the Management Domain Switch).

4.5 RDP Proxy

4.5.1 General

Requirement ID: [SRS-4-105]

The IEG-C RDP Proxy component SHALL be the Microsoft Windows Server 2016 (or later versions that are listed on the Approved Fielded Product List for the High Side) with the Remote Desktop Services server role.

Requirement ID: [SRS-4-106]

The IEG-C RDP Proxy component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.5.2 Data Exchange Services

Requirement ID: [SRS-4-107]

The IEG-C RDP Proxy component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

Requirement ID: [SRS-4-210]

Only configured users SHALL be allowed to connect to the RDP Proxy.

Requirement ID: [SRS-4-211]

Users SHALL be required to authenticate to the RDP Proxy in accordance with [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-4-212]

Authenticated users SHALL be required to authenticate to the RDP Proxy in accordance with [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-4-213]

An authenticated user SHALL only be able to connect to a configured set of network resources.

Requirement ID: [SRS-4-106]

Local client devices SHALL NOT be accessible on the remote desktop session.

4.5.3 Element Management Services

Requirement ID: [SRS-4-107]

The IEG-C RDP Proxy component SHALL be enabled and configured with the capability for being managed as specified in Section 9.

Requirement ID: [SRS-4-108]

The IEG-C RDP Proxy component SHALL generate an SSL Certificate Signing Request (CSR) to be signed by the appropriate E-NPKI Registration Authority (RA).

4.5.4 Hardware and Software

Requirement ID: [SRS-4-109]

The IEG-C RDP Proxy component SHALL be deployed on a physical server.

Requirement ID: [SRS-4-110]

The IEG-C RDP Proxy component server SHALL support (as a minimum) the Microsoft Windows Server 2016 R2 (or later versions that are listed on the Approved Fielded Product List for the High Side) 64-bit edition operating system.

Requirement ID: [SRS-4-111]

The IEG-C RDP Proxy component server SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

4.6 Web Guard

4.6.1 General

Requirement ID: [SRS-4-113]

The IEG-C Web Guard component SHALL comply with the functional requirements specified in Section 6.

Requirement ID: [SRS-4-114]

The IEG-C Web Guard component SHALL comply with the non-functional requirements specified in Section 5.3.

Requirement ID: [SRS-4-115]

The IEG-C Web Guard component SHALL comply with the security functional requirements specified in Section 6.8.

Requirement ID: [SRS-4-116]

The IEG-C Web Guard component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

Requirement ID: [SRS-4-118]

It SHALL be possible to enforce a separate 'WG security policy' (see section 6.2.1) per service/application mediated by the Web Guard.

4.6.2 Data Exchange Services

Requirement ID: [SRS-4-119]

The IEG-C Web Guard component SHALL enable the capability to support only those Data Exchange Services as listed in Table 4 (for that component) and specified in Section 6.4.

4.6.3 Protection Services

Requirement ID: [SRS-4-120]

The IEG-C Web Guard component Protection Services SHALL comply with the requirements specified in Section 6.6.

4.6.4 Protection Policy Enforcement Services

Requirement ID: [SRS-4-121]

The IEG-C Web Guard component Protection Policy Enforcement Services SHALL comply with the requirements specified in Section 6.5.

4.6.5 Element Management Services

Requirement ID: [SRS-4-122]

The IEG-C Web Guard component Element Management Services SHALL comply with the requirements specified in Section 6.7.

4.6.6 Hardware and Software

Requirement ID: [SRS-4-123]

The IEG-C Web Guard component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connection to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-124]

The IEG-C Web Guard component network interfaces to the High Domain Switch, Low Domain Switches and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

4.7 Mail Guard

4.7.1 General

Requirement ID: [SRS-4-126]

The IEG-C Mail Guard component SHALL be synchronised to the IEG-C Firewall component NTP source.

4.7.2 Data Exchange Services

Requirement ID: [SRS-4-127]

The IEG-C Mail Guard component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

4.7.3 Protection Services

Requirement ID: [SRS-4-128]

The IEG-C Mail Guard component SHALL use a malware/virus scanner that is included in the NATO Information Assurance Product Catalogue (NIAPC) to check email messages for malicious content.

Requirement ID: [SRS-4-129]

The IEG-C Mail Guard component SHALL enable the capability to configure the Content Inspection Services that will enforce the IEG-C Business Support and COI CIPs (refer to Section 4.7.4) depending on the information exchange requirements and the content inspection policy to be enforced for the CIS interconnection.

Requirement ID: [SRS-4-130]

The IEG-C Mail Guard component SHALL enable the capability to perform cryptographic operations and key management to support the validation of cryptographic bindings according to NISP Cryptographic Artefact Binding Profiles [ADatP-34(I), NISP Version 10, 2017].

Requirement ID: [SRS-4-131]

The IEG-C Mail Guard component SHALL be configured to conform to the INFOSEC CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-4-132]

The IEG-C Mail Guard component SHALL be configured to 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-4-133]

The IEG-C Mail Guard component provided cryptographic mechanism SHALL be configured based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].

4.7.4 Protection Policy Enforcement Services

Requirement ID: [SRS-4-134]

The IEG-C Mail Guard component SHALL be configurable to support the enforcement of the following IEG-C Business Support IFPs (see Section 3.4.4):

- MG_IFP_BS_HL - Business Support Services High to Low IFP; and,
- MG_IFP_BS_LH - Business Support Services Low to High IFP.

Requirement ID: [SRS-4-135]

The IEG-C Mail Guard component SHALL be configurable to support the enforcement of the following IEG-C Business Support CIPs (see Section 3.4.5):

- MG_CIP_BS_HL - Business Support Services High to Low CIP; and,
- MG_CIP_BS_LH - Business Support Services Low to High CIP.

Requirement ID: [SRS-4-136]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL IFP in order to guard SMTP application-level traffic from the high domain to the low domain.

Requirement ID: [SRS-4-137]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_LH IFP in order to guard SMTP application-level traffic from the low domain to the high domain.

Requirement ID: [SRS-4-138]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL and MG_IFP_BS_LH IFPs to verify that the email message can be forwarded between the high and low domain by checking originator access control rules against white or black lists.

Requirement ID: [SRS-4-139]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL and MG_IFP_BS_LH IFPs to verify that the email message can be transferred between the high and low domain by checking recipient access control rules against white or black lists.

Requirement ID: [SRS-4-140]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL IFP to enforce the MG_CIP_BS_HL CIP.

Requirement ID: [SRS-4-141]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL CIP to verify that all email messages to be released from the high domain to the low domain contain a security label that conforms to the access control rules to be enforced for the CIS interconnection.

Requirement ID: [SRS-4-142]

The IEG-C Mail Guard component SHALL enable the capability to select that the security label format is the STANAG 4774 confidentiality label XML format.

Requirement ID: [SRS-4-143]

The IEG-C Mail Guard component SHALL enable the capability to select that the STANAG 4774 confidentiality label is bound to the email message as specified in STANAG 4778 and NATO Interoperability Standards and Profiles (NISP) SMTP Binding Profile.

Requirement ID: [SRS-4-144]

The IEG-C Mail Guard component SHALL enable the capability to select that the STANAG 4774 confidentiality label is cryptographically bound to the email message as specified in NATO Interoperability Standards and Profiles (NISP) Cryptographic Artefact Binding Profiles.

Requirement ID: [SRS-4-145]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL CIP to verify that all email messages to be released from the high

domain to the low domain do not contain unauthorised information, such as 'dirty words'.

Requirement ID: [SRS-4-146]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_LH IFP to enforce the MG_CIP_BS_LH CIP.

Requirement ID: [SRS-4-147]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL and MG_CIP_BS_HL CIPs to verify that all email messages to be forwarded between the high domain and the low domain do not contain any disallowed attachment types by checking against a white list or black list of attachment types.

Requirement ID: [SRS-4-148]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_LH CIP to verify that all email messages (including email message header, body and allowed body parts) are well-formed, valid and contain no malicious content.

Requirement ID: [SRS-4-149]

Depending on the information exchange requirements the IEG-C SHALL be configurable to support the enforcement of the following IEG-C COI CIPs (see Section 3.4.5):

- IEG-C_CIP_COI-ES_HL - COI-Enabling Services High to Low CIP;
- IEG-C_CIP_COI-ES_LH - COI-Enabling Services Low to High CIP;
- IEG-C_CIP_COI_HL - COI-Specific Services High to Low CIP; and
- IEG-C_CIP_COI_LH - COI-Specific Services Low to High CIP.

Requirement ID: [SRS-4-150]

The IEG-C Mail Guard component SHALL enable the capability to configure the IEG-C_CIP_COI-ES_HL and IEG-C_CIP_COI_HL CIPs to verify that attachments contained in email messages to be released from the high domain to the low domain do not contain unauthorised information, such as 'dirty words', including classification markings.

Requirement ID: [SRS-4-151]

The IEG-C Mail Guard component SHALL enable the capability to configure the IEG-C_CIP_COI-ES_LH and IEG-C_CIP_COI_LH CIPs to verify that attachments contained in email messages are well-formed, valid and contain no malicious content.

Requirement ID: [SRS-4-152]

The IEG-C Mail Guard component SHALL enforce the IEG-C Business Support IFPs, Business Support CIPs and COI CIPs configured (depending upon the information

exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.

4.7.5 Element Management Services

Requirement ID: [SRS-4-153]

The IEG-C Mail Guard component SHALL be enabled and configured with the capability for being managed as specified in Section 9.

4.7.6 Hardware and Software

Requirement ID: [SRS-4-154]

The IEG-C Mail Guard component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-155]

The IEG-C Mail Guard component network interfaces to the High Domain Switch, Low Domain Switches and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

4.8 Management Workstation

The management workstation is deployed in the management domain and is used to manage multiple IEG-Cs.

Requirement ID: [SRS-4-214]

The IEG-C management workstation component SHALL be the Dell Optiplex 5070 SFF.

Requirement ID: [SRS-4-215]

The IEG-C management workstation monitor SHALL be the Dell P2419H Monitor.

Requirement ID: [SRS-4-216]

The IEG-C management workstation keyboard SHALL be the Dell KB216 Multimedia Keyboard.

Requirement ID: [SRS-4-217]

The IEG-C management workstation mouse SHALL be the Dell 6 Button Laser Mouse.

A detailed description of these components is provided in Appendix D.

4.9 Supporting Components

Supporting components of the IEG-C do not directly support the operational requirements provided by the IEG-C but are required for the overall composition of an IEG-C.

4.9.1 Server

Requirement ID: [SRS-4-156]

The IEG-C server SHALL be integrated with either

- HPE OneView and HPE Integrated Lights-Out (iLO); or
- Dell EMC OpenManage Enterprise and Dell Integrated Dell Remote Access Controller (iDRAC)

Requirement ID: [SRS-4-158]

The IEG-C server component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-159]

The IEG-C server component network interfaces to the High Domain Switch, Low Domain Switch and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-160]

The IEG-C server component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.9.2 Hypervisor

Requirement ID: [SRS-4-218]

Any IEG-C component MAY host a Type 1 Hypervisor, provided that the overall IEG-C system design meets the requirements of "Technical and Implementation Directive for CIS Security" [NAC AC/322-D/0048-REV3, 2019] (see SRS-4-4).

Requirement ID: [SRS-4-219]

The Type 1 Hypervisor for the server and the management workstation, if used, SHALL be the VMWare ESXi hypervisor.

4.9.3 Keyboard, Video and Mouse (KVM)

All management of the IEG-C components shall be performed remotely, therefore there is no requirement for a rack-based keyboard, monitor, mouse or KVM switch. However, future deployed versions of the IEG-C, that may be exercised as options, will require local management as a main or a backup solution, so there needs to be provision for the use of a rack that will allow the addition of rack-based keyboard, monitor, mouse or KVM switch.

4.9.4 Rack

Requirement ID: [SRS-4-165]

The IEG-C Rack component SHALL be the Server Equipment Cabinet

Detailed specifications of this component is provided in Appendix D.

Requirement ID: [SRS-4-167]

All IEG-C components SHALL be rack mounted.

4.9.5 Uninterruptible Power Supply (UPS)

Requirement ID: [SRS-4-168]

The IEG-C UPS component SHALL be the UPS APC Smart-UPS C 1500..

Detailed specifications of this component is provided in Appendix D.

Requirement ID: [SRS-4-220]

The IEG-C power distribution component SHALL be the Powerstrip Conteg.

Detailed specifications of this component is provided in Appendix D.

4.9.6 Cabling

Requirement ID: [SRS-4-169]

The IEG-C components providing 1000BASE-SX gigabit Ethernet physical interfaces SHALL be connected with multi-mode fibre optic cables.

Requirement ID: [SRS-4-172]

All network interfaces shall be implemented in accordance with [IEEE 802.3:2012], whereby, gigabit Ethernet interfaces shall support a maximum transmission unit (MTU) of 9000 bytes.

5 Non-Functional Requirements

5.1 Introduction

This chapter specifies the general non-functional requirements for the IEG-C (Section 5.2) and the specific non-functional requirements for the 'Web Guard Capability' (WG)[2] (Section 5.3) and the 'Mail Guard Capability' (Section 5.4). Depending on the nature of a requirement, requirements that are specified for the IEG-C may apply to the IEG-C as an integrated system of components, or to each of its individual components (including the WG), or to both. The specified components have been selected based on the current IEG-C configuration in NATO theatres. Therefore certain NFRs, e.g. performance efficiency requirements, do not need to be specified for these components.

[2] *Note that the abbreviation 'WG' stands for the capability, and not necessarily for a single (physical or virtual) system; in other words, a Web Guard Capability may be composed of more than one system. (See APPENDIX A for a general system description of the WG.)*

The Non-Functional Requirements (NFR) categorizes system/software product quality properties into the following characteristics:

- Performance efficiency – Sections 5.2.1 and 5.3.1;
- Compatibility-interoperability – Section 5.2.2;
- Usability – Sections 5.5 and 5.3.2;
- Reliability – Sections 5.2.4 and 5.3.3;
- Security – Sections 5.2.5 and 5.3.4;
- Maintainability – Sections 5.2.6 and 5.3.5;
- Portability – Section 5.2.7 and 5.3.6;
- Survivability – Section 5.2.8 and 5.3.7;
- Environment – Section 5.2.9;
- Equipment (Static) – Section 5.2.10;
- Equipment (DCIS) – Section 5.3.4.2.

Characteristic definitions in this section are based on ISO/IEC 25010:2011(E) - System and software quality models [ISO/IEC 25010, 2011].

5.2 IEG-C Non-Functional Requirements

5.2.1 Performance Efficiency

Description: Performance relative to the amount of resources used under stated conditions.

NOTE Resources can include other software products, the software and hardware configuration of the system, and materials (e.g. print paper, storage media).

5.2.1.1 Time Behaviour

Description: Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.

Requirement ID: [SRS-5-1]

The IEG-C SHALL have all functionality ready to use for an authorised user after invoking the system function within 5 minutes.

Requirement ID: [SRS-5-2]

The IEG-C SHALL execute the log-in function within 30 seconds.

Requirement ID: [SRS-5-300]

The IEG-C SHALL meet at a minimum the throughput levels defined for the individual data types shown Table 6Table 6 .

Table 6: IEG Capacity Requirements per Data Type

Data Type	Protocol	Mediator	Size (min- max)	Frequency
Directory (GAL)	LDAP	Firewall only	1KB - 10MB	12x/day
Identity & Access Mgmt	LDAP	Firewall only	<1KB	
Domain Name Services	DNS	Firewall only	<1KB	
Web browsing NS to MS	HTTP/S	Web Proxy	1KB-100MB	
File Transfer (RS)	FTP/HTTP	Web Guard	1KB-100MB	100/Day
File Transfer (other)	FTP/HTTP	Web Proxy	1KB-100MB	100/Day
Full motion video	STANAG 4609	Web Guard	188 byte	25000 /s
Instant Messaging	HTTP/S	Web Guard	<1Kb - 1Mb	1/day - 10/sec
Jchat / XMPP	XML	Web Guard	<1Kb - 1Mb	1/day - 10/sec
Formal Messaging	SMTP	Mail Guard	1KB-1MB	50/Day
Email (informal)	SMTP	Mail Guard	1kb-10Mb	2000/day
Remote Desktop	RDP	RDP Proxy	100KB streaming	5 concurrent sessions
IntelFS	HTTP	Web Guard	1KB-100MB	50/day
COP	Link-16, OTH-G	Web Guard		See air/maritime tracks
Maritime Tracks	OTG	Web Guard	1kb-10Mb	1package/30sec -5Min
Land Force Tracks	FFI/NFFI	Web Guard	<1KB	500 packets / 30 Sec
Air Tracks	Link-16, JREAP, OTH-Gold	Web Guard	<1Kb	<400 -500 packages/sec
Tactical Data Links	This is officially L16, L1, L11, L22	Web Guard	<1Kb	<400 -500 packages/sec
BMD Tracks	Link-16	DISG/Web Guard		See Air Tracks

Requirement ID: [SRS-5-301]

The IEG-C SHALL meet the minimum required throughput defined in Table 6Table 6, for at least 99.5% of its Operational time.

Requirement ID: [SRS-5-311]

The information contained in Table 6 SHALL be used to define key performance indicators (KPIs) for 'Availability', 'Quality' and 'Usage', as defined in [NCIA SMC TA, 2018].

5.2.1.2 Scalability

The system shall be scalable so that IEG-C capacity can be increased.

Requirement ID: [SRS-5-3]

The IEG-C SHALL be designed to allow future scalability.

Requirement ID: [SRS-5-4]

The IEG-C SHALL be expandable and scalable in performance (throughput and bandwidth).

Requirement ID: [SRS-5-5]

The IEG-C SHALL be capable of accommodating additional functionality the need for which may arise as well as future technological improvements.

Requirement ID: [SRS-5-6]

The IEG-C SHALL use an architecture that allows horizontal scalability and allows the same component to be deployed on multiple machines supporting the information exchange requirements in concert.

Requirement ID: [SRS-5-7]

In order to keep meeting the requirements on Time Behaviour in 5.2.1.1 it SHALL be possible to apply horizontal scalability without disrupting the services offered by the IEG-C.

Requirement ID: [SRS-5-9]

The IEG-C SHALL be Vertical Scalable, i.e. IEG-C SHALL be able to adapt its performance characteristics by adding additional system resources such as processing power, memory, disk capacity, or network capacity.

Requirement ID: [SRS-5-10]

The IEG-C SHALL be able to support additional system resources (introduction of additional storage capacity or server processing power) without having to modify the system architecture, replace existing components, interrupt or degrade current functional and performance requirements.

Requirement ID: [SRS-5-303]

The Platform SHALL be able to support a throughput increase of 10% every year for a period of 5 years with no degradation of the maximum latency.

Requirement ID: [SRS-5-329]

The IEG-C as a system SHALL support the use of multiple instances in parallel, providing same gateway services between identical Low and High domains and being operated in different physical locations.

Requirement ID: [SRS-5-330]

When multiple IEG-C are operated in parallel between identical Low and High domains, it SHALL be possible to identify per information flow, which IEG-C acts as the primary gateway and those which act as alternates.

Requirement ID: [SRS-5-331]

The fall back mechanism SHALL support a seamless transition from the primary IEG-C to an alternate IEG-C for users and system administrators.

Requirement ID: [SRS-5-332]

It SHALL be possible to identify on the monitoring system which IEG-C (primary or alternate) is currently servicing each of the information flows.

Requirement ID: [SRS-5-333]

The IEG-C SHALL be able to operate 72 hours in total isolation from any central management and monitoring system.

5.2.2 Compatibility-Interoperability

5.2.2.1 Interface Requirements

Interoperability is defined in ISO 25010 as the degree to which two or more systems, products or components can exchange information and use the information that has been exchanged. Description: Within NATO, interoperability is defined as, the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.

5.2.2.1.1 Principles of Alliance C3 Interoperability

The following principles are defined in Alliance Consultation Command and Control (C3) Interoperability Policy, 17th February 2015.

Use of an Architectural Approach to provide Coherence

- NATO C3 Interoperability Requirements (C3 IOR) shall be expressed in terms of the required sharing of information and ICT services and shall be identified and consolidated by the NATO Military Authorities (NMA) and Staffs within NATO capability requirement statements for execution by NATO and Nations.
- Architecture products shall serve to inform, guide and document interoperability of C3 Capabilities and ICT Services in their lifecycle.

Identification of Standards and Profiles as the basis for Interoperability Solutions

- Standards and profiles shall be included within the NATO Interoperability Standards and Profiles (NISP).
- NATO Enterprise entities shall ensure the service interface profiles associated with the C3 Capabilities and ICT Services they develop and provide are published in the NISP and are available for verification and validation testing to other NATO Enterprise entities and NATO Nations.
- NATO architectures shall utilise the agreed standards (STANAGs) and profiles from the NISP as appropriate to achieve the required interoperability of C3 Capabilities and ICT Services.
- Appropriate interoperability solutions and procedures to match C3 IOR over time shall be identified/developed and documented by the implementer and coordinated with the C3 Board as appropriate.
- NATO Enterprise entities shall implement and adopt the appropriate interoperability solutions and procedures to meet agreed C3 IOR. This will involve the achievement of semantic as well as syntactic, empirical and physical interoperability.

Verification and validation of Interoperability Solutions through Testing

- Interoperability of solutions to C3 IOR shall be verified and validated by testing regularly during the life cycle, in accordance with the provisions of this policy.
- Testing of the interfaces of C3 Capabilities and ICT Services shall be conducted, including testing against the agreed standards and profiles that are contained within the NISP. Testing at National level is a national responsibility and NATO is responsible for testing as a Host Nation.
-
- The status of interoperability testing of STANAGs is valuable information that must be recorded. To the extent possible, this information shall be included in the NISP.
- A harmonised spectrum of test capabilities shall be established and used to verify and validate NATO and national C3 interoperability. Test activities shall include technology demonstration and experimentation, standards development and implementation, system interoperability testing, field, pre-deployment and reference system testing.

The mandatory standards and profiles documented in the latest version of NISP will be used in the implementation of NATO Common Funded Systems. Participating nations agree to use the mandatory standards and profiles included in the NISP at the Service Interoperability Points and to use Service Interface Profiles among NATO and Nations to support the exchange of information and the use of information services in the NATO realm.

Requirement ID: [SRS-5-11]

The IEG-C SHALL use the existing interoperability profiles and provide any new profiles into the NATO Interoperability Standards and Profiles [ADatP-34] (NISP) volumes after all implementation is completed.

Requirement ID: [SRS-5-12]

The IEG-C software code and components SHALL comply with the latest version of the NATO Interoperability Standards and Profiles (NISP). Any deviation is to be justified and reviewed by the Technical Project Board.

Requirement ID: [SRS-5-13]

The IEG-C SHALL be compliant with NATO document AC/35-D/2002 "Directive on Security of Information".

Requirement ID: [SRS-5-14]

The IEG-C SHALL comply with NATO document "Primary Directive on CIS Security" [AC/35-D/2004-REV3].

Requirement ID: [SRS-5-15]

The IEG-C SHALL be compliant with the NATO document "INFOSEC Technical and Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools (ST)" [AC/322-D(2004)0030].

Requirement ID: [SRS-5-17]

The IEG-C SHALL be compliant with NATO document "Security within the North Atlantic Treaty Organisation" [NAC C-M(2002)49-COR12].

5.2.2.1.2 Information Exchange Requirements

Requirement ID: [SRS-5-18]

The IEG-C SHALL guarantee all incoming and outgoing formatted messages are valid according to the specified formats.

5.2.2.1.3 Security Services

Requirement ID: [SRS-5-19]

The IEG-C primary security services (access control, confidentiality, integrity, authentication, and non-repudiation) SHALL be supported by X.509

Requirement ID: [SRS-5-20]

The IEG-C X.509 support to primary security services SHALL be compliant with NPKI.

5.2.2.2 Handling Country Codes

STANAG 1059 [STANAG 1059] aims to provide unique 3-letter codes to distinguish geographical entities, nations and countries for use within NATO from 01 April 2004. Participating nations agreed to use the codes as defined in Annexes A and B of the STANAG, whenever it is necessary to use abbreviations in publications, documents, orders or other media, to identify geographical entities, nations and countries or any part of national forces.

Requirement ID: [SRS-5-21]

The IEG-C SHALL use country codes according to "Letter Codes for Geographical Entities" [STANAG 1059].

5.2.2.3 Time Synchronization

Requirement ID: [SRS-5-22]

The IEG-C SHALL provide accuracy of timing for messaging time stamps (e.g., time of receipt, send, release authorisation, etc.) to one millisecond. Other system-level functions (e.g., process synchronisation) may require additional accuracy as required for correct operation.

Requirement ID: [SRS-5-23]

The IEG-C SHALL synchronize its internal system clocks with a source on the ON using the Network Time Protocol (NTP).

5.2.3 Usability

5.2.3.1 Compliance with standards and Guide Lines

5.2.3.1.1 NCI Agency and NATO

Bi-SC AIS applications are developed as projects within the NCI Agency (NCIA) to be used by NATO users. Both NCIA and NATO have their own standards and guidelines that will influence or directly affect Bi-SC AIS applications' visual design. Although Bi-SC AIS applications can have their own identity, any new application needs to feel like other products NCIA or NATO have previously created and share the same organizational values.

Requirement ID: [SRS-5-24]

The visual design of the IEG-C SHOULD follow the recommendations and guidelines stated in the following Documents:

- NATO Visual Identity Guidelines [NATO VIG v3]

5.2.3.1.2 ISO standards

Requirement ID: [SRS-5-25]

The IEG-C icons included in the designed solution SHALL be compliant with the ISO 18152 standard series.

Requirement ID: [SRS-5-26]

The IEG-C SHALL be compliant with the ISO 9241 standard series. In particular:

Requirement ID: [SRS-5-27]

The IEG-C SHALL be compliant to ISO 9241-125:2017 for the presentation of information.

Requirement ID: [SRS-5-28]

The IEG-C SHALL be compliant to ISO 9241-13 for user guidance.

Requirement ID: [SRS-5-29]

The IEG-C SHALL be compliant to ISO 9241-14 for menu dialogues.

Requirement ID: [SRS-5-31]

The IEG-C SHALL be compliant to ISO 9241-143 for form filling dialogues

Requirement ID: [SRS-5-32]

The IEG-C SHALL be compliant to ISO 9241-171 for accessibility.

Requirement ID: [SRS-5-33]

The IEG-C SHALL follow the dialogue principles stated in ISO 9241-110.

5.2.3.2 Log-on procedures

Requirement ID: [SRS-5-34]

In applications where users must log-on to the system, log-on SHALL be a separate procedure that must be completed before a user is required to select among any operational options.

Requirement ID: [SRS-5-35]

Appropriate prompts for log-on SHOULD be automatically displayed on the user's terminal when accessing the application.

Requirement ID: [SRS-5-36]

User identification procedures SHALL be as simple as possible, consistent with adequate data protection.

Requirement ID: [SRS-5-37]

When required, the password SHALL not be echoed on the display. An asterisk (*) or similar symbol will be displayed for each character when inputting secure passwords during log-on.

Requirement ID: [SRS-5-38]

Users SHALL be provided feedback relevant to the log-on procedure that indicates the status of the inputs.

Requirement ID: [SRS-5-39]

If a user cannot log-on to a system, a prompt SHOULD be provided to explain the reason for this inability. Log-on processes SHOULD require minimum input from the user consistent with the requirements prohibiting illegal entry.

5.2.3.3 Log-off procedures

Requirement ID: [SRS-5-40]

When a user signals for system log-off, or application exit or shut-down, the system SHOULD check pending transactions to determine if data loss seems probable. If so, the computer SHOULD prompt for confirmation before the log-off command is executed.

5.2.4 Reliability

Description: Degree to which a system, product or component performs specified functions under specified conditions for a specified period of time.

NOTE 1 Adapted from ISO/IEC/IEEE 24765.

NOTE 2 Wear does not occur in software. Limitations in reliability are due to faults in requirements, design and implementation, or due to contextual changes.

NOTE 3 Dependability characteristics include availability and its inherent or external influencing factors, such as availability, reliability (including fault tolerance and recoverability), security (including confidentiality and integrity), maintainability, durability, and maintenance support.

For services, a failure is characterized by the inability of the Service to perform its operation.

For web-based applications, an error requiring the user to reload the browser shall be considered a failure.

Systems that require high reliability should also require high verifiability to make it easier to find defects that could compromise reliability.

For the Monitoring of reliability characteristics, the following definitions will be used:

a. Error (or Fault): A design or source code or hardware flaw or malfunction that causes a Failure of one or more Configuration Items. A mistake made by a person or a faulty Process that affects a CI is also an Error (human Error). For the IEG-C, Human Error is generally not taken into consideration in measuring the quality Performance.

b. Fault: see Error

c. Failure: Loss of ability to Operate to Specification, or to deliver the required output. The term Failure may be used when referring to Services, Processes, Activities, or Configuration Items.

d. Incident: An unplanned interruption to a service or reduction in the quality of a service. Failure of a Configuration Item that has not yet affected service is also an Incident — for example, Failure of one disk from a mirror set

e. Problem: A cause of one or more Incidents. The cause is not usually known at the time the Incident happens.

5.2.4.1 Availability

Description: Degree to which a system, product or component is operational and accessible when required for use.

Inherent Availability (Intrinsic): assumes ideal support (i.e., unlimited spares, no delays, etc.), only design related failures are considered: $Ai = MTBF/ (MTBF + MTTD+MTTRSy)$.

Operational Availability: considers logistics support, $A0 = MTBM / (MTBM + MDT)$.

- MTTD is the Mean Time To Diagnose.

- MTTRSy is the Mean Time To Restore (the System).

- MTBF is the Mean Time Between Failures.

- MTTR is the Mean Time Ro Repair as a function of design.

- MTBM is the Mean Time Between Maintenance, all corrective and preventive maintenance.

- MDT is the Mean Down Time, which includes the actual time to perform maintenance and accounts for any delays in getting the needed personnel, upgrades, installations, parts etc...

Requirement ID: [SRS-5-304]

The IEG-C SHALL exhibit a Mean-Time-Between-Failure (MTBF) characteristic of at least 8760 operational hours.

5.2.4.2 Inherent Availability

Requirement ID: [SRS-5-41]

The IEG-C SHALL be available in operational HQs, static and deployed, 24 hours a day, 7 days a week, with an availability rate of 99.5 %.

5.2.4.3 Operational Availability

Description: Operational Software to be in a state to perform a required function at a given point in time, under stated conditions of use.

Table 5 shows the levels of operational continuity for the desired availability:

Table 7 Levels of Operational Continuity per desired availability percentage

Level	Operational Continuity						Disaster Recovery	
	% Availability	Monthly Unplanned Downtime	Monthly Planned Downtime	Degraded Service	Max Restoration time	Max Allowable Data Loss	Recovery Time	Recovery Point
L1	99.99	<1 hr	<1 hr	None	1 hr	1 hr	N/A	N/A
L2	99.9	1 hrs	6 hrs	Minimal	2 hrs	4 hrs	4 hrs	8 hrs
L3	99	7 hrs	12 hrs	Some	4 hrs	8 hrs	12 hrs	24 hrs
L4	98	14 hrs	36 hrs	Allowed	12 hrs	24 hrs	48 hrs	48 hrs

Requirement ID: [SRS-5-42]

The IEG-C, including hardware, infrastructure and Operational Software, SHALL be available for use at static sites (via Data Centres) 24 hours per day, 365 days per year with an availability of 99.9% (Level 2 of Operational Continuity).

The IEG-C (including hardware, infrastructure and Operational Software) availability does not rely on enabling services external to the IEG-C. Hence, its availability depends solely of the intrinsic availability of the hardware and software elements that make the IEG-C.

Requirement ID: [SRS-5-318]

The IEG-C, as a system, SHALL have an availability of 99.95%.

5.2.4.4 Fault Tolerance

Description: Degree to which a system, product or component operates as intended despite the presence of hardware or software faults.

Requirement ID: [SRS-5-43]

The IEG-C SHALL, despite the presence of hardware or software faults in part of the IEG-C, continue to perform the unaffected IEG-C functions.

Requirement ID: [SRS-5-44]

The IEG-C Servers SHALL gracefully degrade in the condition where any dependent services and components are not available and notify the user of the limited functionality.

Requirement ID: [SRS-5-319]

Upon restoration of services, the IEG-C Servers SHALL become fully operational.

Requirement ID: [SRS-5-46]

The IEG-C SHALL provide a rate of fault occurrence of less than 2 failures for 1000 hours of operation in the IEG-C software components, with 95% confidence. A failure is defined as an error or cessation in the operation of the software requiring, as a minimum, a restart of the software (for example, a service) to recover.

Requirement ID: [SRS-5-47]

It SHALL be possible to correct any individual fault within the IEG-C within a period of time no greater than sixty (60) minutes.

5.2.4.5 Maturity

Description: Degree to which a system, product or component meets needs for reliability under normal operation.

NOTE: The concept of maturity can also be applied to other quality characteristics to indicate the degree to which they meet required needs under normal operation.

Requirement ID: [SRS-5-48]

The IEG-C SHALL exhibit a mean-time-between-failure (MTBF) characteristic of less than 2 failures every 7000 hours, and that SHALL not be affected by the total number of IEG-C instances which are active during that period. The MTBF measurement SHALL not include failures resulting from factors determined to be external to the IEG-C (e.g., loss of domain controller).

5.2.4.6 Recoverability

Description: Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.

NOTE Following a failure, a computer system will sometimes be down for a period of time, the length of which is determined by its recoverability.

Requirement ID: [SRS-5-50]

The IEG-C SHALL provide authorised users with the ability to perform full and/or incremental backups of the system's data and software without impacting system availability.

Requirement ID: [SRS-5-327]

The IEG-C backups SHALL be stored on the domain Disaster Recovery System (DRS) or, if the domain DRS is not available, a removable, local backup device.

Requirement ID: [SRS-5-334]

The IEG-C local backup dedicated hardware SHALL be removable in no more than 5 minutes, SHALL not exceed 5kg in weight and SHALL not exceed 30cmx30cmx30cm (Height, Wide, Deep).

Requirement ID: [SRS-5-51]

The IEG-C SHALL maintain full functionality and performance in the event of power failure(s) for a minimum of twenty (20) minutes, prior to initiating a graceful system shutdown.

Requirement ID: [SRS-5-52]

In case of a failure in the power supply to the IEG-C UPS, the IEG-C SHALL react at 50% battery level with a warning and at 30% battery level with going into graceful system shutdown..

Requirement ID: [SRS-5-53]

After going into graceful system shutdown caused by a power failure, the IEG-C SHALL have retained all the relevant data.

Requirement ID: [SRS-5-54]

The IEG-C SHALL provide automatic resumption of operation after power restoration, except where this violates security requirements.

Requirement ID: [SRS-5-55]

The IEG-C SHALL queue pending asynchronous (i.e. do not need immediate feedback) requests to an unavailable service and deliver them when the service becomes available again.

Requirement ID: [SRS-5-56]

The IEG-C SHALL provide a Mean Time To Repair (MTTR) after the failure of a critical component of four (4) hours or less.

Requirement ID: [SRS-5-57]

The IEG-C SHALL provide a maximum time to restore the service after the failure of a critical component of no greater than six (6) hours at the 95% confidence level.

Requirement ID: [SRS-5-58]

The IEG-C SHALL provide a Time-To-Repair (TTR) of no greater than eight (8) hours for servers and their components at 100% confidence level.

Requirement ID: [SRS-5-59]

In case of IEG-C failure the availability interruption SHALL not exceed two hours.

5.2.4.7 Robustness

Requirement ID: [SRS-5-60]

The IEG-C SHALL resume/retry IEG-C services in case of high latency/timeout/loss of network connectivity without loss of data. High latency is defined as latency exceeding one (1) minute.

Requirement ID: [SRS-5-61]

The IEG-C SHALL provide a Mean Time Between Maintenance (MTBM) for individual components of greater than six thousand (6000) hours of continuous operation where the required maintenance action excludes restart of the hardware and software.

Requirement ID: [SRS-5-62]

The IEG-C SHALL provide a MTBM of greater than thousand (1000) hours of continuous operation where the required maintenance action is only a restart of the hardware or software.

5.2.5 Security

Description: Security is defined as the capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and such that authorised persons or systems are not denied access to them.

As well as data stored in or by a product or system, security also applies to data in transmission.

For purposes of this SRS, the following definitions are used:

- Confidentiality: the property that information is not made available or disclosed to unauthorised individuals or entities.
- Integrity: the property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
- Non-repudiation: the measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipients.
- Accountability: the degree to which actions of an entity can be traced uniquely to the entity.
- Authenticity: the degree to which the identity of a subject or resource can be proved to be the one claimed.

The following INFOSEC functionalities will be provided by the BI-SC AIS:

- Confidentiality. Military-grade NATO IP cryptographic equipment (NICE) will provide confidentiality to User data as well as cryptographic separation between security Domains (for example, NATO SECRET, NATO UNCLASSIFIED. MISSION SECRET). Information exchange between these security domains will be achieved through appropriate boundary protection services (BPS). As a minimum, NICE will be located at each boundary between the local area networks (LANs) and the NATO wide area network (WAN). This will ensure that all User data will be encrypted prior to transmission across the NATO WAN. Software application layer mechanisms will be used for Community-of-Interest (COI) separation.
- Integrity. Digital signatures and authentication services will be used by various protocols (e.g., SNMP, IPSEC) to provide integrity and strong authentication to User data and network configurations. The NATO Public Key Infrastructure (NPKI) will enable these specific security services.

Infrastructure security as provided by the Bi-SC AIS Infrastructure will be transparent to the IEG-C.

Requirement ID: [SRS-5-63]

The IEG-C SHALL comply with security settings, installation guides and configuration guidelines listed in the latest approved version of the NCIA CSSL Security Configuration Catalogue.

Requirement ID: [SRS-5-64]

The IEG-C components SHALL be configured with the latest security patches and updated with the latest security guidelines from the NATO Information Assurance Technical Centre (NIATC).

Requirement ID: [SRS-5-65]

The IEG-C SHALL be capable of operating within the NS and MS WAN environment (including servers, network, services and workstations) in the presence of the currently approved NATO Security Settings (target version to be provided by the Purchaser during the Design Stage). Any deviations from the approved security settings SHALL be identified by the Contractor prior to testing and SHALL be subject to approval of the Purchaser.

NATO UNCLASSIFIED

5.2.5.1 Authenticity

5.2.5.1.1 General

Definitions:

- User: refers to a person having access to the operating system (an OS User) and IEG-C Services. Each User of the IEG-C is assigned Access Rights based on its Role, the Permissions within that Role, and optionally the organization of the User.
- Role: Defined by a set of permissions (i.e., access to objects and functionality) to perform certain operations.

The primary roles in the IEG-C are those defined in Section 3.4.6: System Administrator, Audit Administrator, CIS Security Administrator, Cyber Defence Administrator, and SMC Administrator.

Where in the requirements that follow the general term "IEG-C Administrator" is used to denote one of the primary roles, the reader shall substitute the general term for the applicable primary role based on the requirement.

5.2.5.1.2 Authentication Processing

Requirement ID: [SRS-5-66]

The IEG-C SHALL uniquely Identify and Authenticate Users.

Requirement ID: [SRS-5-67]

The IEG-C SHALL allow an IEG-C Administrator to manage (create, update, delete) IEG-C User Accounts, password details, and assign User Roles to User Account and manage general access privileges of individual User Accounts.

Requirement ID: [SRS-5-68]

The IEG-C SHALL support the application of a password policy.

Requirement ID: [SRS-5-69]

The IEG-C SHALL be configurable to deny the re-use of a specified previous passwords.

Requirement ID: [SRS-5-70]

IEG-C SHALL be configurable to lock user accounts after a specified number of unsuccessful authentication attempts.

Requirement ID: [SRS-5-71]

IEG-C passwords SHALL be stored in encrypted form.

Requirement ID: [SRS-5-72]

IEG-C SHALL support the locking of accounts that are no longer required for a specified period of time after which they SHALL be deleted.

Requirement ID: [SRS-5-73]

The IEG-C SHALL support the protection of User credentials in transit.

Requirement ID: [SRS-5-74]

The IEG-C SHALL provide privileged IEG-C accounts (e.g., system and security administrator accounts).

Requirement ID: [SRS-5-75]

The IEG-C SHALL allow authenticated Users to manage their password.

Requirement ID: [SRS-5-305]

The IEG-C SHALL implement Identity and Access Management (IAM) according to the requirements on IAM as specified in the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-5-306]

In support of the authentication and authorization of users, the IEG-C and its sub-components SHALL support authentication and authorization based on the RADIUS protocol [IETF RFC 2865, 2000].

Requirement ID: [SRS-5-308]

The IEG-C SHALL implement multifactor user authentication in accordance with in the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-5-309]

The implementation of multifactor authentication by the IEG-C SHALL integrate with the multifactor authentication solution as it is in use in the NATO Enterprise.

5.2.5.2 Audit and Accountability

Requirement ID: [SRS-5-76]

The IEG-C SHALL generate audit records for auditable events, addressing, among others, the following events:

- system start-up (including re-starts) and shutdown;
- log-on (including log-on attempts) and log-off of individual users
- changes to permissions and privileges of users and groups;

- changes to security relevant system management information(including audit functions);
- start-up and shutdown of the audit function;
- any access to security data;
- deletion, creation or alteration of the security audit records;
- changes to system date and time;
- unsuccessful attempts to access system resources;

Requirement ID: [SRS-5-77]

Audit tracing in the IEG-C SHALL be permanently effective.

Requirement ID: [SRS-5-78]

The IEG-C SHALL protect the information from unauthorised modification or deletion.

Requirement ID: [SRS-5-79]

The IEG-C SHALL establish access permissions to audit information.

Requirement ID: [SRS-5-80]

The IEG-C SHALL associate individual user identities to auditable events in the event log.

Requirement ID: [SRS-5-81]

The IEG-C SHALL include the date and time of each auditable event in the event log.

Requirement ID: [SRS-5-82]

The IEG-C SHALL alert an IEG-C Administrator on failed attempts at log-on.

Requirement ID: [SRS-5-83]

The IEG-C SHALL create and maintain an archive of audit information.

Requirement ID: [SRS-5-84]

The IEG-C SHALL support the retaining of audit information for a specified period of time.

5.2.5.2.1 User Audit Log

Requirement ID: [SRS-5-85]

The IEG-C SHALL record in traceable logs all selected transactions, database activities, technical events (e.g., dataset synchronisation, directory replication) and accessing of data.

Requirement ID: [SRS-5-86]

If so configured, the IEG-C SHALL log all configurations changes with the trace to persons or systems.

5.2.5.2.2 System Audit Log

Requirement ID: [SRS-5-87]

The IEG-C SHALL generate and maintain an Audit Log for each of the following auditable events, SHALL associate individual User identities to those events, and SHALL include date and time of the event, type of event, User identity, and the outcome (success or failure) of the event:

- System start-up and shutdown,
- the start/end time of usage of system applications (system components) by individual Users
- Changes to permissions and privileges of Users and groups,
- Changes to security relevant system management function,
- Configuration changes,
- Any access to audit log,
- Deletion, creation or alteration of the security audit records,
- All privileged operations,
- All updates of IEG-C access rights,
- All attempts to delete, write or append the Audit files.

Requirement ID: [SRS-5-88]

The IEG-C SHALL use integrity checking countermeasures to ensure that the Audit Log has been archived successfully.

Requirement ID: [SRS-5-89]

The IEG-C SHALL support the following warning system events based on configurable limits:

- Network bandwidth low;
- Percentage of disk space left;
- Percentage of table space left.

5.2.5.3 Application Security

5.2.5.3.1 Session Management

Requirement ID: [SRS-5-90]

Sessions SHALL be invalidated when the user logs out.

Requirement ID: [SRS-5-91]

Sessions SHALL timeout after a specified period of inactivity.

5.2.5.3.2 Input validation

Requirement ID: [SRS-5-92]

The runtime environment or parser SHALL not be susceptible to XML and XPath injection.

Requirement ID: [SRS-5-93]

The IEG-C SHALL have defences against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)

5.2.5.3.3 Data Protection

Requirement ID: [SRS-5-94]

Sensitive data SHALL be sanitized from memory as soon as it is no longer needed.

5.2.5.3.4 Communications Security

Requirement ID: [SRS-5-95]

A certificate path SHALL be built and validated from a trusted CA to each Transport Layer Security (TLS) server certificate, and each server certificate SHALL match the Fully Qualified Domain Name of the server.

Requirement ID: [SRS-5-96]

Failed TLS connections SHALL not fall back to an insecure connection.

Requirement ID: [SRS-5-97]

Certificate paths SHALL be built and validated for all client certificates using configured trust anchors and revocation information.

5.2.5.3.5 Business Logic

Requirement ID: [SRS-5-98]

The application logic SHALL have protection mechanisms against application crashing, memory access violations (buffer overflow) and unexpected exceptions such as data destruction and resource depletion (Memory, CPU, Bandwidth, Disk Space, etc.).

Requirement ID: [SRS-5-99]

The application SHALL have sufficient access controls to prevent elevation of privilege attacks.

5.2.6 Maintainability

Description: Degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers

NOTE 1 Modifications can include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications. Modifications include those carried out by specialized support staff, and those carried out by business or operational staff, or end users.

NOTE 2 Maintainability includes installation of updates and upgrades.

NOTE 3 Maintainability can be interpreted as either an inherent capability of the product or system to facilitate maintenance activities, or the quality in use experienced by the maintainers for the goal of maintaining the product or system.

5.2.6.1 Modularity

Description: Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components.

The system should be composed of discrete components such that a change to one component has minimal impact on other components.

Requirement ID: [SRS-5-100]

The IEG-C SHALL be composed of discrete components such that a change to one component has minimal impact on other components.

Requirement ID: [SRS-5-166]

Any IEG-C component SHALL not exceed 2U height. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.

Requirement ID: [SRS-5-320]

Any IEG-C component SHALL not exceed 20kg. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.

Requirement ID: [SRS-5-321]

Any IEG-C component using forced airflow (fan) cooling SHALL be of front-rear type.

Requirement ID: [SRS-5-322]

All IEG-C component SHALL have dual power supply module. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.

5.2.6.2 Manageability

The system should facilitate efficient and effective management of its operations.

Requirement ID: [SRS-5-101]

The IEG-C SHALL be able to report its status (healthy, warnings, errors) and 'capacity' related aspects for the [IT] resources used (disk, memory, CPU, network) and the application aspects addressed (load, transactions, users) to the NATO EMS environment (in addition to any project specific requirements).

Requirement ID: [SRS-5-102]

The IEG-C SHALL ensure that the application provides management of Personal Information (e.g., User profile and expertise information) held within the IEG-C.

5.2.6.3 Supportability

The system should be easy to support by support personnel.

Requirement ID: [SRS-5-103]

The IEG-C SHALL support remote configuration of all IEG-C components and updates using Microsoft System Center Configuration Manager (SCOM) if available on the platform.

Requirement ID: [SRS-5-104]

IEG-C software assets (including different versions) SHALL have a unique SWID tag assigned.

Requirement ID: [SRS-5-105]

The IEG-C SHALL support collection and reporting of asset inventory metrics for all IEG-C components using Microsoft System Centre Configuration Manager, unless an IEG-C component does not support SCOM, including:

- Memory
- Operating System
- Peripherals
- Services
- Login tracking
- Software existence and usage
- Licensing

5.2.7 Portability

Description: Portability is defined as the capability of the software product to be transferred from one environment to another.

5.2.7.1 Adaptability

Description: Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.

Requirement ID: [SRS-5-106]

The IEG-C SHALL be effective and efficient in the adaptation for different or evolving hardware, software or other operational or usage environments.

Requirement ID: [SRS-5-107]

The IEG-C architecture SHALL be designed to permit upgrading for use of new communication, processing and storage technologies during its operational lifetime.

5.2.7.2 Installability

Description: Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.

Requirement ID: [SRS-5-108]

The IEG-C SHALL be equipped with an Installation Guide.

Requirement ID: [SRS-5-109]

The IEG-C Installation Guide SHALL explain all actions to take in order to install and configure the IEG-C, including COTS components. Every action SHALL be followed by a description (text and/or screenshots) of the feedback which will be displayed.

Requirement ID: [SRS-5-110]

The IEG-C Installation Guide SHALL describe:

- Prerequisites for installing the IEG-C. (e.g., the necessary OS access right to be able to install the IEG-C)
- The necessary software, drivers, etc. to install the IEG-C
- How to address integration in the 'environment' (node) - like configuration of monitoring and backup functions
- The (environment specific) configuration changes necessary on the system and the environment
- The required disc space.

Requirement ID: [SRS-5-111]

The IEG-C Installation Guide SHALL describe how to configure the system backbone to be able to run the IEG-C.

Requirement ID: [SRS-5-112]

The IEG-C Installation Guide SHALL contain a description of all configuration files. The following points SHALL be described:

- The location of the configuration file
- The content of the configuration file
- The available settings of the items in the configuration file and their meaning
- How to change the configuration file

Requirement ID: [SRS-5-113]

Two copies of the SWID tag file SHALL be installed on each system that the IEG-C software is installed on. The first copy of the tag file SHALL be accessible in the top level directory of the installed software package itself and the second copy of the tag file SHALL be installed in a platform dependent file system location as:

 <file system location>\regid.1997-08.int.nato\<tagfilename>."

Requirement ID: [SRS-5-114]

The IEG-C SHALL provide a capability to completely uninstall IEG-C application(s)/component(s). The IEG-C uninstallation capability SHALL remove all program files and folders, registry entries, program and group folders, as appropriate, retaining all shared and system files.

Requirement ID: [SRS-5-115]

The IEG-C uninstallation capability SHALL not adversely impact other installed applications.

Requirement ID: [SRS-5-116]

The IEG-C SHALL store IEG-C temporary files only in the IEG-C's temporary folders in configurable locations.

Requirement ID: [SRS-5-117]

An IEG-C System Administrator SHALL be able to successfully deploy (i.e., install and configure) a component in the IEG-C within a time frame of one (1) working day after receiving a maximum of five (5) days of training per component.

For Deployable CIS (DCIS), systems and composing modules are being re-configured from scratch each time there is a new mission. To this purpose, an automation and orchestration solution is being used. This tool uses blueprints using API and scripts to connect to elements over different types of interfaces (iLO ports, serial ports, SSH, RESTful, ...) to configure these step-by-step.

Requirement ID: [SRS-5-323]

The IEG-C SHALL be configurable from scratch using the DCIS orchestration and automation toolset.

Requirement ID: [SRS-5-324]

The IEG-C SHALL include an NSAB/NOS endorsed quick erase feature allowing the complete erasure of all configuration, stored data and software.

Requirement ID: [SRS-5-325]

The quick erase feature SHALL not take longer than 30 minutes.

Requirement ID: [SRS-5-326]

The quick erase feature SHALL not erase IEG-C backups.

5.2.7.3 Internationalisation

Requirement ID: [SRS-5-118]

All software and documentation to be provided by the Contractor under this project SHALL be in English (US) version.

5.2.8 Survivability

Requirement ID: [SRS-5-119]

The IEG-C SHALL automatically detect the availability and re-establishment of network connectivity and SHALL initiate subsequent tasks as though network connectivity had not been lost.

5.2.9 Environment

Requirement ID: [SRS-5-121]

The IEG-C SHALL support the use of IPv6 without impaired functionality and performance within a network environment.

Requirement ID: [SRS-5-122]

The IEG-C SHALL be compliant to the requirements specified in this SRS in a virtualized server environment (virtual servers).

5.2.10 Equipment

Requirement ID: [SRS-5-123]

The IEG-C equipment SHALL NOT be damaged nor suffer loss of data, when any of the ambient temperature and humidity conditions contravene operating limits while power is available.

Requirement ID: [SRS-5-124]

The IEG-C support staff SHALL be able to manually resume normal operation of the IEG-C equipment within five (5) minutes from when ambient temperature and humidity conditions return to within operating limits.

5.3 Web Guard Non-Functional Requirements

This section details the additional, Web Guard specific, non-functional requirements, over and above those specified in section 5.2.

5.3.1 Performance Efficiency

5.3.1.1 Capacity

Description: Degree to which the maximum limits of a product or system parameter meet requirements.

NOTE Parameters can include the number of items that can be stored, the number of concurrent users, the communication bandwidth, throughput of transactions, and size of database.

Requirement ID: [SRS-5-125]

The WG SHALL support the concurrent processing of low-to-high and high-to-low traffic and meet the performance objectives for both traffic flows.

Requirement ID: [SRS-5-126]

The WG SHALL support the concurrent execution of low-to-high and high-to-low policy enforcement and meet the performance objectives for each.

Requirement ID: [SRS-5-127]

The WG SHALL support the concurrent execution of all functionality offered by the building blocks Data Exchange Services, Protection Policy Enforcement Services, Protection Services and Element Management Services.

Requirement ID: [SRS-5-128]

On interface WG_IF_NET_HIGH (see 6.4.1.2) the WG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-129]

On interface WG_IF_NET_LOW (see 6.4.1.3) the WG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-131]

The WG SHALL allow an IEG-C System Administrator to perform system management functions regardless of the load on the WG.

Requirement ID: [SRS-5-132]

The WG SHALL support the information exchange of HTTP messages with body size up to ten (10) GB.

Requirement ID: [SRS-5-133]

The WG SHALL support parallel processing of HTTP messages, i.e. it SHALL be possible for the WG to subject multiple different HTTP messages to policy enforcement at the same time.

5.3.1.2 Time Behaviour

Description: Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.

5.3.1.2.1 Definitions

Processing time

Let the *'WG processing of an HTTP message'* (or simply *'HTTP message processing'*) be the following sequence:

For a given HTTP message *H*:

- Subject *H* to policy enforcement; and
- If *H* violates the WG security policy: generate (but not send) the appropriate HTTP error message.

Let the *'WG processing time of an HTTP message'* or simply *'HTTP message processing time'* (notation: T_WG_Proc) be the time measured in order for the WG to complete the sequence *'HTTP message processing'* above.

When it is written that the *'WG processes an HTTP message'*, this means the same as subjecting an HTTP message to *'HTTP message processing'*. Therefore, the time it takes for the WG to process an HTTP message is equal to T_WG_Proc.

Let the *'WG processing times'* be the processing times that the WG is able to offer.

Throughput

Let the *'WG throughput'*, or simply *'throughput'* be the number of HTTP messages that the WG can process per given time period.

Forwarding time

Let the *'WG forwarding time of an HTTP message'* or simply *'HTTP message forwarding time'* (notation: $T\_WG\_Forward$) be the time measured in order for the WG to complete the following sequence:

For a given HTTP message *H*:

- Receive *H* at WG_IF_NET_HIGH or WG_IF_NET_LOW;
- If necessary queue *H*; and then
- Execute *'HTTP message processing'* for *H*;
- Then, if *H* did not violate the WG security policy:
    - If necessary queue *H*; and then
    - Forward *H* onto the low domain or high domain respectively.
- Else, if *H* did violate the WG policy:
    - If necessary queue the associated HTTP error message; and then
    - Forward the HTTP error message onto the high domain or low domain respectively.

When it is written that the *'WG forwards an HTTP message'*, this means the same as completing the sequence above.

The *'HTTP message forwarding time'* is equal to the *'HTTP message processing time'* plus the time it takes to receive, queue and forward HTTP messages. (The 'HTTP message forwarding time' is similar to the concept of 'response time' (i.e. 'processing time' + 'queueing time').)

Let the *'WG forwarding times'* be the forwarding times that the WG is able to offer.

5.3.1.2.2 Message size categories

Throughput, processing time and forwarding time depend on message size. Therefore this SRS distinguishes a number of message size categories for the WG.

Let the following terminology denote size categories for HTTP messages. The size categories are determined by the size of the HTTP body.

- Very small HTTP messages: *0 <= HTTP body size <= 150 KB;*
- Small HTTP messages: *150 KB < HTTP body size <= 10 MB;*
- Medium HTTP messages: *10 MB < HTTP body size <= 50 MB;*
- Large HTTP message: *50 MB < HTTP body size <= 100 MB;*

- Very large HTTP messages: *100 MB < HTTP body size <= 10 GB.*

The size categories are based on HTTP body size because that is the part of the HTTP message that is determined by the message size of the product that is being exchanged by the Web Guard between the low and high domain.

5.3.1.2.3 'Normal load' and 'peak load'

Normal load

In this SRS the *'normal load'* is the load on the WG (in terms of HTTP messages to be forwarded) that can be assumed to exist under normal traffic conditions. This SRS defines a *'normal load'* for each size category from 5.3.1.2.2, which is referred to as the *'size category normal load'* (*SCNL*). Then, the 'total normal load' (notation *TNL*) is the sum of all size category normal loads that the WG can be subjected to simultaneously.

The following *'load characteristics'* are distinguished in order to characterize the traffic that comprises the normal load (note that not all load characteristics have to apply to a normal load simultaneously):

- *Average message size;*
- *Maximum message size;* (For the size category *normal load* this is bound by the maximum message size in the category. For the *TNL* this is bound by the maximum message size of the 'very large HTTP messages' category.)
- *Number of messages per time unit;*
- *Message size distribution;*
- *Message type distribution.*

When it is written that the WG 'supports a normal load', this means that the *WG throughput*, the *WG processing times* and the *WG forwarding times* are such that the WG is able to support a continuous normal load without degradation in performance.

Peak load

Let *'peak load'* be a multiple of the normal load (in terms of its load characteristics), during a limited period of time.

5.3.1.2.4 Requirements for WG forwarding times, throughput and processing times

Requirement [SRS-5-134] below specifies the requirements for supporting the normal load per message size category.

Requirement ID: [SRS-5-134]

The WG SHALL support[3] the following normal loads per message size category:

[3] *When it is written that the WG 'supports a normal load', this means that the* WG throughput, *the* WG processing times *and the* WG forwarding times *are such that the WG is able to support a continuous normal load without degradation in performance.*

- Very small HTTP messages: a *SCNL* of 35000 HTTP messages per minute with average message size 15 KB.
- Small HTTP messages: a *SCNL* of 180 HTTP messages per minute with average message size 5 MB.

- Medium HTTP messages: a *SCNL* of 30 HTTP messages per minute with average message size 30 MB.
- Large HTTP messages: a *SCNL* of 10 HTTP messages per minute with average message size 70 MB.
- Very large HTTP messages: a *SCNL* of 2 HTTP messages per minute with average message size 300 MB.

Requirement ID: [SRS-5-135]

The WG SHALL meet the requirements in [SRS-5-133] under a total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 7 MB;
- *TNL* maximum message size <= 10 GB;
- *TNL* message size distribution: 80% of *TNL* < 150 KB; 95% of *TNL* < 30 MB; 98% of *TNL* < 300 MB.

Requirement ID: [SRS-5-136]

Per size category the average *HTTP message processing time T_WG_Proc-Average* SHALL meet the following constraints under the size category normal loads from [SRS-5-133]:

- Very small HTTP messages: *T_WG_Proc-Average* < 200 milliseconds;
- Small HTTP messages: *T_WG_Proc-Average* < 3000 milliseconds;
- Medium HTTP messages: *T_WG_Proc-Average* < 15000 milliseconds;
- Large HTTP messages: *T_WG_Proc-Average* < 60000 milliseconds;
- Very large HTTP messages: *T_WG_Proc-Average* < 240000 milliseconds.

Requirement ID: [SRS-5-137]

The WG SHALL meet the requirements on *HTTP message processing time* in [SRS-5-135] under a total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 7 MB;
- *TNL* maximum message size <= 10 GB;
- *TNL* message size distribution: 80% of *TNL* < 150 KB; 95% of *TNL* < 30 MB; 98% of *TNL* < 300 MB.

Requirement ID: [SRS-5-138]

If an HTTP message *H* is processed by the WG that is too large for the category 'Very large HTTP messages', the WG SHALL:

- continue to operate;
- be responsive to commands issued by a System Administrator;
- meet the requirements in [SRS-5-133] under the total normal load *TNL*;

NATO UNCLASSIFIED

- and MAY terminate the processing of *H* in order to do so.

5.3.1.2.5 Requirements for peak load

The following 3 requirements specify the extent to which a peak load may impact the WG throughput, processing times or forwarding times. The peak loads are based on the normal loads from requirement [SRS-5-133]. Each requirement is followed by a rationale.

Requirement ID: [SRS-5-139]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *WG throughput* for that size category SHALL meet the following constraints for the peak load stated, while not rejecting HTTP traffic:

- Very small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Medium HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Very large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.

Rationale behind [SRS-5-138]: A peak load may require the WG to divert part of its resources to peak load handling, e.g. managing messages queues, potentially affecting resources dedicated to throughput. This requirement aims to limit the impact of a peak load on the WG's throughput. (Because of the temporary nature of a peak load, it may be possible to temporarily make additional system resources available to handle the overhead introduced by the peak load.)

Requirement ID: [SRS-5-140]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *HTTP message forwarding time T_WG_Forward-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting HTTP traffic:

- Very small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 10% when compared to the *SCNL*.
- Small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds,

> *T_WG_Forward-Average* SHALL increase at most 20% when compared to the *SCNL*.
> - Medium HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 30% when compared to the *SCNL*.'
> - Large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 40% when compared to the *SCNL*.
> - Very large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 50% when compared to the *SCNL*.

Rationale behind [SRS-5-139]: A peak load implies message queues and hence an increase in forwarding time. This requirements aims to limit the impact on the forwarding times. (Because of the temporary nature of a peak load, it may be possible to temporarily make resources available to increase throughput such that an increase in forwarding time can be limited.)

Requirement ID: [SRS-5-141]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *HTTP message processing time T_WG_Proc-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting HTTP traffic:

> - Very small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 5% compared to normal load.
> - Small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 10% compared to normal load.
> - Medium HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 20% compared to normal load.
> - Large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 30% compared to normal load.
> - Very large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 40% compared to normal load.

Rationale behind [SRS-5-140]: While under peak load it may not be acceptable for certain types of information exchange, e.g. 'near real time' messaging, to have the processing time increased. While for requirements [SRS-5-138] and [SRS-5-139] it is possible to meet those requirements at the cost of processing time (e.g. the number of message processing threads may be increased such that throughput is maintained

however per message thread the processing time drops), this requirement aims to limit the increase of the processing times while under peak load.

Requirement ID: [SRS-5-142]

During peak loads that are larger in size or longer in duration than those specified in [SRS-5-138] , [SRS-5-139] and [SRS-5-140] , the WG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject HTTP traffic in order to do so.

Requirement ID: [SRS-5-143]

If peak loads for multiple size categories take place simultaneously, the WG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject HTTP traffic in order to do so.

Requirement ID: [SRS-5-144]

It SHALL be possible to configure an upper size limit, L, such that the WG SHALL reject messages that exceed L.

5.3.1.2.6 Requirements on impact of logging

Requirement ID: [SRS-5-145]

The impact of logging by the WG on its performance SHALL remain within the following limits, for the following log severity levels [RFC 5424]:

- For severity levels 'Emergency' (0), 'Alert' (1), 'Critical' (2), 'Error' (3), 'Warning' (4): no impact on performance;
- For severity levels 'Notice' (5) and 'Informational' (6): a decrease in throughput of at most 40%.
- For severity level 'Debug' (7): a decrease in throughput of at most 80%.

5.3.1.3 Scalability

Requirement ID: [SRS-5-146]

The WG SHALL be scalable such that when an increase in traffic occurs, capacity can be increased in order to keep meeting the requirements on Time Behaviour in 5.3.1.2.

Requirement ID: [SRS-5-147]

The WG architecture SHALL support horizontal scalability and allow for multiple instances of the WG to be deployed on multiple machines, supporting the information exchange requirements in concert.

Requirement ID: [SRS-5-148]

The WG SHALL be vertically scalable, i.e. the WG SHALL be able to adapt its performance characteristics by having additional system resources added such as processing power, memory, disk capacity, or network capacity.

Requirement ID: [SRS-5-149]

In order to keep meeting the requirements on Time Behaviour in 5.3.1.2 it SHALL be possible to apply horizontal scalability without disrupting the services offered by any active WG.

Requirement ID: [SRS-5-150]

The horizontal scaling of the WG SHALL NOT introduce any additional WG management overhead.

Requirement ID: [SRS-5-151]

The WG SHALL be dimensioned and configured to be able to scale in performance and support the following per a year for three years without degradation of performance as specified in section 5.3.1.2:

- a 200% increase in the *SCNL* (normal load for each HTTP message size category);
- a 50% increase in message size.

5.3.2 Usability

5.3.2.1 Usability

Description: Extent to which an interactive system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

Requirement ID: [SRS-5-152]

The WG SHALL have a high degree of learnability, making it very easy to use for System Administrators even the first time.

5.3.3 Security

5.3.3.1 Audit and Accountability

5.3.3.1.1 Log Configuration

Requirement ID: [SRS-5-156]

The WG SHALL notify a System Administrator by e-mail when the audit log reaches 75% of its maximum permitted size.

Requirement ID: [SRS-5-310]

The WG System Administrator address SHALL be configurable.

Requirement ID: [SRS-5-157]

The WG SHALL provide a configuration option to set the maximum permitted size of the audit log.

5.3.3.2 Integrity

Requirement ID: [SRS-5-158]

The WG SHALL contain residual information protection mechanisms to ensure that purged information is no longer accessible.

Requirement ID: [SRS-5-159]

The WG SHALL ensure that newly created objects do not contain information that should not be accessible (i.e. information that has been logically deleted).

5.3.4 Maintainability

5.3.4.1 Analysability

Description: Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

NOTE Implementation can include providing mechanisms for the product or system to analyse its own faults and provide reports prior to a failure or other event.

The system shall be effective and efficient in the possibility to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

Requirement ID: [SRS-5-161]

WG log messages SHALL contain initiating module information, Date/Time (Z), system instance, (log) message, category/severity, user (invoker of function), and context information (like mission/session, service/function, parameters, and trace-log).

5.3.5 Portability

Description: Portability is defined as the capability of the software product to be transferred from one environment to another.

5.3.5.1 Installability

Description: Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.

Requirement ID: [SRS-5-162]

A WG System Administrator SHALL be able to successfully deploy (i.e., install and configure to a predefined configuration) the WG within a time frame of one (1) working days after receiving a maximum of five (5) days of training.

5.4 Mail Guard Non Functional Requirements

5.4.1 Performance Efficiency

5.4.1.1 Capacity

The degree to which the maximum limits of a product or system parameter meet requirements.

NOTE Parameters can include the number of items that can be stored, the number of concurrent users, the communication bandwidth, throughput of transactions, and size of database.

Requirement ID: [SRS-5-208]

The MG SHALL support the concurrent processing of low-to-high and high-to-low traffic and meet the performance objectives for both traffic flows.

Requirement ID: [SRS-5-209]

The MG SHALL support the concurrent execution of low-to-high and high-to-low policy enforcement and meet the performance objectives for each.

Requirement ID: [SRS-5-210]

The MG SHALL support the concurrent execution of all functionality offered by the building blocks Data Exchange Services, Protection Policy Enforcement Services, Protection Services and Element Management Services.

Requirement ID: [SRS-5-211]

On interface MG_IF_NET_HIGH (see section 7.1.2) the MG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-212]

On interface MG_IF_NET_LOW (see section 7.1.2) the MG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-213]

The MG SHALL queue SMTP messages in the event that policy enforcement functionality is unavailable.

Requirement ID: [SRS-5-214]

The MG SHALL allow an IEG-C System Administrator to perform system management functions regardless of the load on the MG.

Requirement ID: [SRS-5-215]

The MG SHALL support the information exchange of SMTP messages with body size up to ten (10) MB.

Requirement ID: [SRS-5-216]

The MG SHALL support parallel processing of SMTP messages, i.e. it SHALL be possible for the MG to subject multiple different SMTP messages to policy enforcement at the same time.

5.4.1.2 Time Behaviour

The degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.

5.4.1.2.1 Definitions

Processing time

Let the '*MG processing of an SMTP message*' (or simply '*SMTP message processing*') be the following sequence:

For a given SMTP message *M*:

- Subject *M* to policy enforcement; and
- If *M* violates the MG security policy: generate (but not send) the appropriate SMTP error message.

Let the '*MG processing time of an SMTP message*' or simply '*SMTP message processing time*' (notation: T_MG_Proc) be the time measured in order for the MG to complete the sequence '*SMTP message processing*' above.

When it is written that the 'MG processes an SMTP message', this means the same as subjecting an SMTP message to '*SMTP message processing*'. Therefore, the time it takes for the MG to process an SMTP message is equal to T_MG_Proc.

Let the '*MG processing times*' be the processing times that the MG is able to offer.

Throughput

Let the '*MG throughput*', or simply '*throughput*' be the number of SMTP messages that the MG can process per given time period.

Forwarding time

Let the '*MG forwarding time of an SMTP message*' or simply '*SMTP message forwarding time*' (notation: $T\_MG\_Forward$) be the time measured in order for the MG to complete the following sequence:

For a given SMTP message *M*:

- Receive *M* at MG_IF_NET_HIGH or MG_IF_NET_LOW;
- If necessary queue *M*; and then
- Execute '*SMTP message processing*' for *M*;
- Then, if *M* did not violate the MG policy:
  - If necessary queue *M*; and then
  - Forward *M* onto the low domain or high domain respectively.

o Else, if *M* did violate the MG policy:
   ▪ If necessary queue the associated SMTP error message; and then
   ▪ Forward the SMTP error message onto the high domain or low domain, as required.

When it is written that the '*MG forwards an SMTP message*', this means the same as completing the sequence above.

The '*SMTP message forwarding time*' is equal to the '*SMTP message processing time*' plus the time it takes to receive, queue and forward SMTP messages. (The 'SMTP message forwarding time' is similar to the concept of 'response time' (i.e. 'processing time' + 'queueing time').)

Let the '*MG forwarding times*' be the forwarding times that the MG is able to offer.

5.4.1.2.2 Message size categories

Througput, processing time and forwarding time depend on message size. Therefore this SRS distinguishes a number of message size cagetories for the MG.

Let the following terminology denote size categories for SMTP messages. The size categories are determined by the size of the encoded SMTP (MIME) body.

- Small SMTP messages: *0 KB < SMTP body size <= 100 KB*;
- Medium SMTP messages: *100 MB < SMTP body size <= 500 KB*;
- Large SMTP message: 500 KB *< SMTP body size <= 10 MB*;

5.4.1.2.3 'Normal load' and 'peak load'

Normal load

In this SRS the '*normal load*' is the load on the MG (in terms of SMTP messages to be forwarded) that can be assumed to exist under normal traffic conditions. This SRS defines a 'normal load' for each size category from 5.4.1.2.2, which is referred to as the '*size category normal load*' (*SCNL*). Then, the '*total normal load*' (notation *TNL*) is the sum of all size category normal loads that the MG can be subjected to simultaneously.

The following '*load characteristics*' are distinguished in order to characterize the traffic that comprises the normal load (note that not all load characteristics have to apply to a normal load simultaneously):

- *Average message size*;
- *Maximum message* size; (For the *size category normal load* this is bound by the maximum message size in the category. For the *TNL* this is bound by the maximum message size of the 'very large SMTP messages' category.)
- *Number of messages per time unit;*
- *Message size distribution*;
- *Message type distribution.*

When it is written that the MG '**supports a normal load**', this means that the *MG throughput*, the *MG processing times* and the *MG forwarding times* are such that the MG is able to support a continuous normal load without degradation in performance.

Peak load

Let '*peak load*' be a multiple of the normal load (in terms of its load characterisitcis), during a limited period of time.

5.4.1.2.4 Requirements for MG forwarding times, throughput and processing times

Requirement ID: [SRS-5-217]

The MG SHALL support[1] a total normal load, *TNL*, with the following normal loads per message size category:

- Small SMTP messages: a *SCNL* of 22 SMTP messages per minute with average message size 70 KB.
- Medium SMTP messages: a *SCNL* of 4 SMTP messages per minute with average message size 250 KB.
- Large SMTP messages: a *SCNL* of 1 SMTP messages per minute with average message size 1 MB.

Requirement ID: [SRS-5-218]

The MG SHALL support the total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 250 KB;
- *TNL* maximum message size <= 10 MB;
- *TNL* message size distribution: 80% of *TNL* < 100 KB; 95% of *TNL* < 500 KB; 98% of *TNL* < 2.5 MB.

Requirement ID: [SRS-5-219]

Per size category the average *SMTP message processing time T_MG_Proc-Average* SHALL meet the following constraints under the size category normal loads from [SRS-5-217]:

- Small SMTP messages: *T_MG_Proc-Average* < 200 milliseconds;
- Medium SMTP messages: *T_MG_Proc-Average* < 3000 milliseconds;
- Large SMTP messages: *T_MG_Proc-Average* < 15000 milliseconds;

Requirement ID: [SRS-5-220]

The MG SHALL meet the requirements on *SMTP message processing time* in [SRS-5-219] under a total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 250 KB;
- *TNL* maximum message size <= 1 MB;

---

[1] When it is written that the MG 'supports a normal load', this means that the *MG throughput*, the *MG processing times* and the *MG forwarding times* are such that the MG is able to support a continuous normal load without degradation in performance.

- *TNL* message size distribution: 80% of *TNL* < 100 KB; 95% of *TNL* < 500 KB; 98% of *TNL* < 2.5 MB.

Requirement ID: [SRS-5-221]

If an SMTP message *M* is processed by the MG that is too large for the category 'Large SMTP messages', the MG SHALL:

- continue to operate;
- be responsive to commands issued by a System Administrator;
- meet the requirements in [SRS-5-219] under the total normal load *TNL*;
- and MAY terminate the processing of *M* in order to do so.

5.4.1.2.5 Requirements for peak load

The following 3 requirements specify the extent to which a peak load may impact the MG throughput, processing times or forwarding times. The peak loads are based on the normal loads from requirement [SRS-5-217]. Each requirement is followed by a rationale.

Requirement ID: [SRS-5-222]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *MG throughput* for that size category SHALL meet the following constraints for the peak load stated, while not rejecting SMTP traffic:

- Small SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Medium SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Large SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.

Rationale behind [SRS-5-222]: A peak load may require the MG to divert part of its resources to peak load handling, e.g. managing messages queues, potentially affecting resources dedicated to throughput. This requirement aims to limit the impact of a peak load on the MG's throughput. (Because of the temporary nature of a peak load, it may be possible to temporarily make additional system resources available to handle the overhead introduced by the peak load.)

Requirement ID: [SRS-5-223]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *SMTP message forwarding time T_MG_Forward-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting SMTP traffic:

- Small SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Forward-Average* SHALL increase at most 20% when compared to the *SCNL*.
- Medium SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Forward-Average* SHALL increase at most 30% when compared to the *SCNL*.
- Large SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Forward-Average* SHALL increase at most 40% when compared to the *SCNL*.

Rationale behind [SRS-5-223]0: A peak load implies longer message queues and hence an increase in forwarding time. This requirement aims to limit the impact on the forwarding times. (Because of the temporary nature of a peak load, it may be possible to temporarily make resources available to increase throughput such that an increase in forwarding time can be limited.)

Requirement ID: [SRS-5-224]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *SMTP message processing time T_MG_Proc-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting SMTP traffic:

- Small SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Proc-Average* SHALL increase at most 10% compared to normal load.
- Medium SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Proc-Average* SHALL increase at most 20% compared to normal load.
- Large SMTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_MG_Proc-Average* SHALL increase at most 30% compared to normal load.

Requirement ID: [SRS-5-225]

During peak loads that are larger in size or longer in duration than those specified in [SRS-5-222], [SRS-5-223] and [SRS-5-224], the MG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject SMTP traffic in order to do so.

Requirement ID: [SRS-5-226]

If peak loads for multiple size categories take place simultaneously, the MG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject SMTP traffic in order to do so.

Requirement ID: [SRS-5-227]

It SHALL be possible to configure an upper message size limit, L, such that the MG SHALL reject messages that exceed the size limit L.

5.4.1.2.6 Requirements on impact of logging

Requirement ID: [SRS-5-228]

The impact of logging by the MG on its performance SHALL remain within the following limits, for the following syslog severity levels [RFC 5424]:

- For severity levels 'Emergency' (0), 'Alert' (1), 'Critical' (2), 'Error' (3), 'Warning' (4): no impact on performance;
- For severity levels 'Notice' (5) and 'Informational' (6): a decrease in throughput of at most 40%.
- For severity level 'Debug' (7): a decrease in throughput of at most 80%.

5.4.1.3 Scalability

Requirement ID: [SRS-5-229]

The MG SHALL be scalable such that when an increase in traffic occurs, capacity can be increased in order to keep meeting the requirements on Time Behaviour in 5.4.1.2.

Requirement ID: [SRS-5-230]

The MG architecture SHALL support horizontal scalability and allow for multiple instances of the MG to be deployed on multiple machines, supporting the information exchange requirements and MG policy in concert.

Requirement ID: [SRS-5-231]

The MG SHALL be vertically scalable, i.e. the MG SHALL be able to adapt its performance characteristics by having additional system resources added such as processing power, memory, disk capacity, or network capacity.

Requirement ID: [SRS-5-232]

In order to keep meeting the requirements on Time Behaviour in 5.4.1.2 it SHALL be possible to apply horizontal scalability without disrupting the services offered by any active MG.

Requirement ID: [SRS-5-233]

The horizontal scaling of the MG SHALL NOT introduce any additional MG management overhead.

Requirement ID: [SRS-5-328]

The MG SHALL be dimensioned and configured to be able to scale in performance and support the following per year, for three years, without degradation of performance as specified in section 5.4.1.2:

- a 100% increase in the SCNL (normal load for each SMTP message size category);
- a 50% increase in message size.

5.4.2 Usability

5.4.2.1 Usability

The extent to which an interactive system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

Requirement ID: [SRS-5-234]

The MG SHALL have a high degree of learnability, making it very easy to use for System Administrators even the first time.

Requirement ID: [SRS-5-235]

The MG SHALL score above 80% in user success rate without external support, for System Administrators that have received standard training.

5.4.3 Reliability

5.4.3.1 Fault Tolerance

Requirement ID: [SRS-5-236]

The MG SHALL continue to receive and queue messages in the event of unavailability of recipient side networking.

Requirement ID: [SRS-5-237]

The MG SHALL continue to dequeue and send messages in the event of unavailability of originator side networking.

5.4.4 Security

5.4.4.1 Audit and Accountability

5.4.4.1.1 Log Configuration

Requirement ID: [SRS-5-238]

The MG SHALL notify a System Administrator by e-mail when the audit log reaches 75% of its maximum permitted size.

Requirement ID: [SRS-5-239]

The MG SHALL provide a configuration option to set the maximum permitted size of the audit log.

5.4.4.2 Integrity

Requirement ID: [SRS-5-240]

The MG SHALL contain residual information protection mechanisms to ensure that purged information is no longer accessible.

Requirement ID: [SRS-5-241]

The MG SHALL ensure that newly created objects do not contain information that has been purged.

5.4.5 Maintainability

5.4.5.1 Analysability

The degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

NOTE Implementation can include providing mechanisms for the product or system to analyse its own faults and provide reports prior to a failure or other event.

The system shall be effective and efficient in the possibility to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

Requirement ID: [SRS-5-242]

Alert messages triggered by the MG (e.g., error, warning, notification and informational messages) SHALL contain initiating module information, context sensitive help or directives on where to find answers and solutions.

Requirement ID: [SRS-5-243]

MG log messages SHALL contain initiating module information, Date/Time(Z), system instance, (log) message, category/severity, user (invoker of function), context information (for example, mission/session, service/function, parameters, and trace-log).

5.4.6 Portability

The portability is defined as the capability of the software product to be transferred from one environment to another.

5.4.6.1 Installability

The degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.

Requirement ID: [SRS-5-507]

A MG System Administrator SHALL be able to successfully deploy (i.e., install and configure) the MG within a time frame of one (1) working day after receiving a maximum of five (5) days of training.

6 Web Guard Functional Requirements

6.1 Background

6.1.1 Introduction

This chapter describes the functional requirements for a 'Web Guard Capability' (WG)[4]. For a general system description of the WG, including a common information exchange scenario supported by the WG, see APPENDIX A. 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 Web Guard capability are captured in WG patterns. The patterns are described in Section 6.3. In each pattern the WG enforces a number of policies. An overview of the policies is provided in Section 6.2.

[4] *Note that the abbreviation 'WG' stands for the capability, and not necessarily for a single (physical or virtual) system; in other words, a Web Guard Capability may be composed of more than one system.*

Due to the choice for an IEG-C architecture based on a DMZ, and the WG being part of that DMZ, the operations at the external interfaces of the WG 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 WG patterns. The next section explains the use of the interfaces and operations for the WG and IEG-C.

6.1.2 Domains, interfaces and operations

The IEG-C TA [NCIA TR/2016/NSE010871/01, 2017] assumes a DMZ architecture. Figure 10Figure 10 shows the logical placement of the WG in the DMZ, the interfaces of IEG and WG, and the domains to which the IEG-C and WG interface. The WG interfaces to the high side of the DMZ at WG_IF_NET_HIGH, and to the low side of the DMZ at WG_IF_NET_LOW.
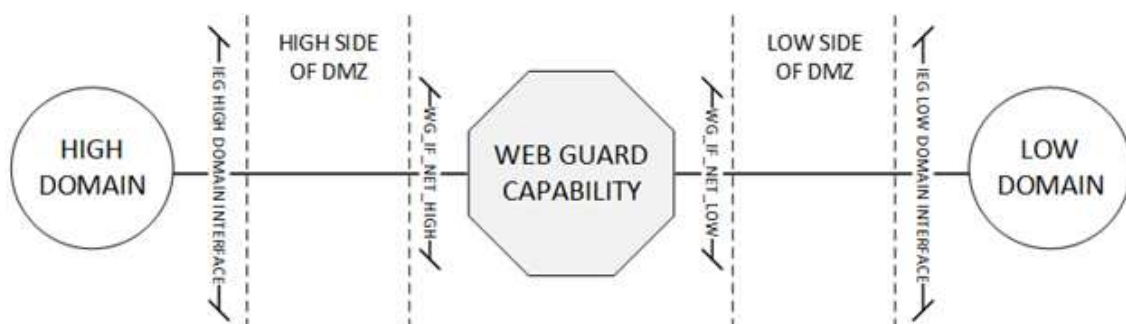
Figure 10 WG in DMZ architecture: domains and interfaces

Note that the WG 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 WG_IF_NET_HIGH and WG_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 6 provides an overview.

Table 8 Subset of logical IEG-C ABB interfaces supported by WG interfaces

WG interfaces (Section A.5)	Supported subset of logical interfaces from IEG-C ABB 'Data Exchange Services'	Note on security domains
WG_IF_NET_HIGH	- Communications Access Services HL Interface - Communications Access Services LH Interface - SOA Platform Services HL Interface - SOA Platform Services LH Interface	From the point of view of the WG, the high side DMZ and the high domain are the same security domain referred to as 'high domain'.
WG_IF_NET_LOW	- Communications Access Services HL Interface - Communications Access Services LH Interface - SOA Platform Services HL Interface - SOA Platform Services LH Interface.	From the point of view of the WG, the low side DMZ and the low domain are the same security domain referred to as 'low domain'.
WG_IF_MGMT (Not shown in Figure 10.)	Management interface	The management interface can be implemented as a logical interface on top of WG_IF_NET_HIGH in which case – from the point of view of the WG - 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 WG – the management domain is considered a separate security domain referred to as 'management domain'.

In the DMZ architecture in Figure 10, 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 WG 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 WG as shown in Table 6. 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 of [NCIA TR/2016/NSE010871/01, 2017]). So even though both sides of the DMZ are external to the WG, the operations that apply to the WG are 'ReceiveInternalNetwork' and 'ForwardInternalNetwork'.

Figure 11Figure 11 illustrates the logical interface 'Communications Access Services HL interface' and its operations supporting the traffic flow from the high domain to the low domain.
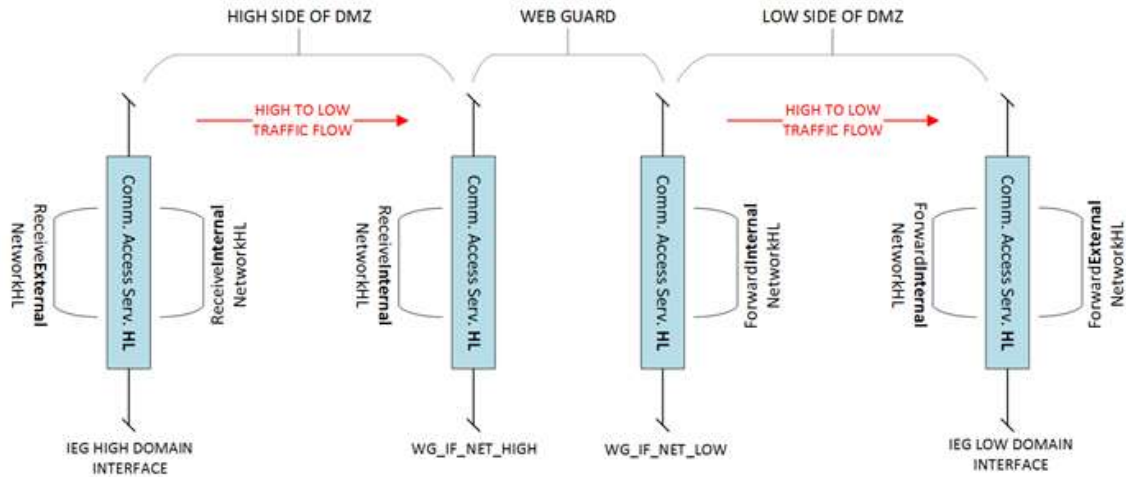
Figure 11 Operations at instances of the interface 'Communication Access Services HL' for traffic flowing from the high to the low domain

Figure 12Figure 12 illustrates the logical interface 'Communications Access Services LH interface' and its operations supporting the traffic flow from the low domain to the high domain.
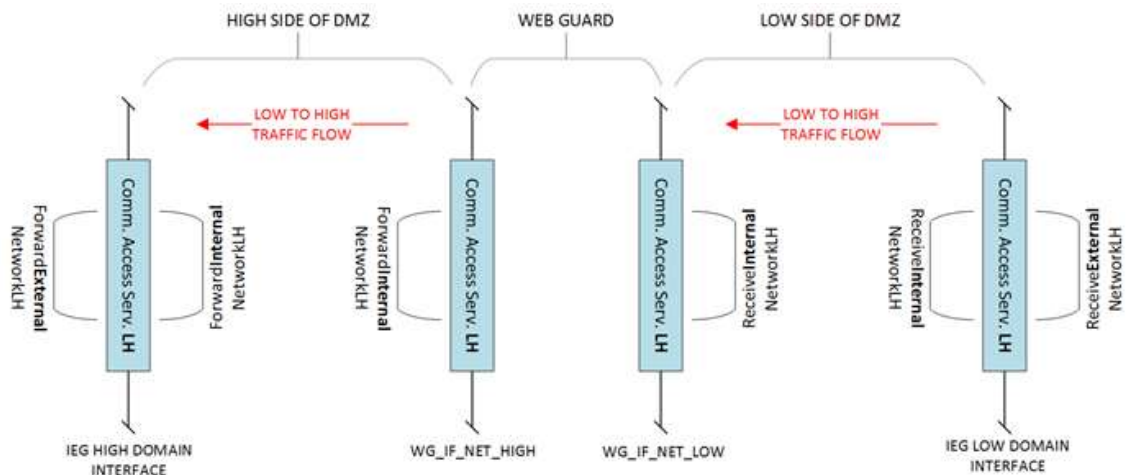
Figure 12 Operations at instances of the interface 'Communication Access Services LH' for traffic flowing from the low to the high domain

6.2 WG Policy Enforcement

6.2.1 WG security policy

The WG enforces a security policy. This policy is referred to as the 'WG security policy' (see Section A.2.1). Regarding the enforcement of the WG security policy on low-to-high and high-to-low traffic[5] (Figure A.3), the WG security policy is composed of two types of policies:

[5] Note that the WG also needs to enforce a security policy with respect to local access control (in support of system administration, system audit and self-protection (see 6.8)). The local access control policy is considered a part of the WG security policy, however may be administered separately from the policies listed in 6.2.

- Information flow control policies (Section 6.2.2);
- Content inspection policies (Section 6.2.3).

6.2.2 WG information flow control policies

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

- The sub-policy that pertains to high-to-low traffic, referred to as 'WG_IFP_HL';
- The sub-policy that pertains to low-to-high traffic, referred to as 'WG_IFP_LH'; and
- The sub-policy that pertains to management traffic, referred to as 'WG_IFP_MGMT'.

All three policies can be broken down further into sub-polices. Table 7 provides an overview of all IFPs and their scope; each IFP is covered in Section 6.5.2.

Table 9 IFPs enforced by WG and their scope

Policy	Union of sub-policies	Scope
WG_IFP	WG_IFP_HL	High to low traffic
	WG_IFP_LH	Low to high traffic
	WG_IFP_MGMT	Management traffic (related to management of the WG itself).
WG_IFP_MGMT	WG_IFP_MGMT_IN	Management traffic destined for WG
	WG_IFP_MGMT_OUT	Management traffic leaving WG
WG_IFP_HL	WG_IFP_CA_HL	High to low HTTP traffic
	WG_IFP_SOA_HL	HTTP messages transferred from high to low
WG_IFP_LH	WG_IFP_CA_LH	Low to high HTTP traffic
	WG_IFP_SOA_LH	HTTP messages transferred from low to high
WG_IFP_CA_HL	WG_IFP_CA_HL_IN	Transfer-in high to low HTTP traffic for processing by WG
	WG_IFP_CA_HL_OUT	Transfer-out high to low HTTP traffic processed by WG
WG_IFP_CA_LH	WG_IFP_CA_LH_IN	Transfer-in low to high HTTP traffic for processing by WG
	WG_IFP_CA_LH_OUT	Transfer-out low to high HTTP traffic processed by WG

6.2.3 WG content inspection policies

The content inspection policy (CIP) that is enforced by the WG is referred to as 'WG_CIP'. The policy WG_CIP is the union of the policies 'WG_CIP_HL' and 'WG_CIP_LH', see Table 8.

Table 10 WG content inspection policies

Policy	Union of sub-policies	Scope
WG_CIP	WG_CIP_HL	HTTP messages transferred from high to low
	WG_CIP_LH	HTTP messages transferred from low to high

Note that the outcome of the enforcement of IFPs WG_IFP_SOA_HL and WG_IFP_SOA_LH depends on the outcome of the enforcement of WG_CIP in the sense

that WG_IFP_SOA_HL and WG_IFP_SOA_LH will not permit traffic flow when traffic violates WG_CIP (see requirements [SRS-6-136] and [SRS-6-137]).

Section 6.6.1 specifies the functional requirements of the WG for the ABB 'Content Inspection Services'. The enforcement functionality of the WG related to this ABB is:

- XML schema validation;
- HTTP header vetting;
- label validation; and
- detection of malware.

The enforcement of XML schema validation, HTTP header vetting, and label validation is referred to as the 'common WG information exchange scenario, see A.2.2. However, this chapter adds malware detection as required enforcement functionality.

The WG provides the enforcement functionality through the application of content filters that enforce the content inspection policies WG_CIP_HL and WG_CIP_LH. In order to be able to group functional requirements per WG functionality, WG_CIP_HL and WG_CIP_LH are split into sub-policies as per Table 9; each CIP is described in Section 6.5.4. The selection of sub-policies depends on the information exchange scenario that will be supported. The sub-policies in Table 9 assume the common WG information exchange scenario that is described in A.4, augmented with malware detection.

Table 11   Further breakdown of WG content inspection policies in support of the common WG information exchange scenario (described in A.4), augmented with malware detection

Policy	Union of sub-policies	Scope	WG functionality
WG_CIP_HL	WG_CIP_HL_LV	HTTP message body	Label validation
	WG_CIP_HL_HV	HTTP message headers	HTTP header vetting
WG_CIP_LH	WG_CIP_LH_SV	HTTP message body	XML schema validation
	WG_CIP_LH_HV	HTTP message headers	HTTP header vetting
	WG_CIP_LH_MD	HTTP message headers and body	Malware detection

6.2.4 Support for enforcement of WG_CIP_LH_LV, WG_CIP_HL_SV, and WG_CIP_HL_MD

Sections 6.5.3 and Section 6.6.1 cover the policies from Table 11Table 11. Information exchange scenarios that require the WG functionalities label validation, XML schema validation, or malware detection in the direction opposite to the one covered in Table 11Table 11, can be supported by implementing policy enforcement for the associated sub-policies WG_CIP_LH_LV, WG_CIP_HL_SV, and WG_CIP_HL_MD respectively. Functional requirements that describe policy enforcement based on WG_CIP_LH_LV, WG_CIP_HL_SV, and WG_CIP_HL_MD are not included in this document, however can be formulated in a similar fashion to those that cover the enforcement of the policies in Table 11Table 11.

6.3 WG Patterns

6.3.1 Main Patterns

Three main patterns comprise the WG. Each pattern is a combination of two sub-patterns, see Table 10.

Table 12 Patterns that comprise the WG

Pattern	Combination of sub-patterns	Depicted in
WG High to Low Pattern	WG High to Low Node Self Protection Pattern	Figure 13
	WG High to Low Cross Domain Information Exchange Pattern	
WG Low to High Pattern	WG Low to High Node Self Protection Pattern	Figure 15
	WG Low to High Cross Domain Information Exchange Pattern	
WG Management pattern	WG Management Self Protection Pattern	Figure 17
	WG Element Management Services Pattern	Figure 18

The WG patterns enforce the information flow control and content inspection policies that are described in Sections 6.2.2 and 6.2.3. Therefore it shall be noted that support for the enforcement of additional policies (6.2.4) may require a modification to the patterns.

6.3.2 WG High to Low Pattern

The policy WG_IFP_HL is enforced in the WG High to Low Pattern (depicted in Figure 13). The pattern is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

(In order to clarify the sequence of the pattern, the following formatting is used: <u>interfaces</u> are underlined and *operations* are in italic.)

- [START] Data Exchange Services -> <u>Communications Access Services HL</u> -> *ReceiveInternalNetworkHL*
- Protection Policy Enforcement Services -> <u>IFCPE Services High to Low</u> -> *Enforce HL Communications IFCPE* [IFP: WG_IFP_CA_HL_IN]
- Data Exchange Services -> <u>SOA Platform Services HL</u> -> *ReceiveWebContentHL*
- Protection Services -> <u>Public Key Cryptographic Services</u> -> *Verify / Decrypt*
- (Required if TLS connection is used or content is digitally signed)
- Protection Policy Enforcement Services -> <u>IFCPE Services High to Low</u> -> *Enforce HL SOA Platform IFCPE* [IFP: WG_IFP_SOA_HL]
- Protection Policy Enforcement Services -> <u>CIPE Services High to Low</u> -> *Enforce HL SOA CIPE* [CIP: WG_CIP_HL]
- Protection Services -> <u>Content Inspection Services</u> -> *Initialize / Filter / Halt*
- Protection Services -> <u>Public Key Cryptographic Services</u> -> *Verify*
- (Required if digital signature must be verified)
- Data Exchange Services -> <u>SOA Platform Services HL</u> -> *ForwardWebContentHL*
- Protection Services -> <u>Public Key Cryptographic Services</u> -> *Encrypt/Sign*
- (Required if TLS connection is used or if content is to be signed by the WG)
- Protection Policy Enforcement Services -> <u>IFCPE Services High to Low</u> -> *Enforce HL Communications IFCPE* [IFP: WG_IFP_CA_HL_OUT]

- Data Exchange Services -> Communications Access Services HL ->
ForwardInternalNetworkHL [END]

Note that the pattern starts with the operation 'ReceiveInternalNetworkHL' and ends with the operation 'ForwardInternalNetworkHL'; this is in line with Figure 11.

Traffic will follow the pattern from [START] to [END] if no policy violation occurs. In case a policy violation occurs, traffic flow is interrupted according to Figure 13:

- If enforcement of WG_IFP_CA_HL_IN or WG_IFP_CA_HL_OUT results in a policy violation, traffic will be rejected and an action shall be executed as specified in [SRS-6-116].
- If enforcement of WG_IFP_SOA_HL results in a policy violation, an HTTP error message may be generated according to [SRS-6-138]. Note that [SRS-6-138] includes the option to silently drop traffic. Figure 13Figure 13 however assumes an HTTP error message is generated.
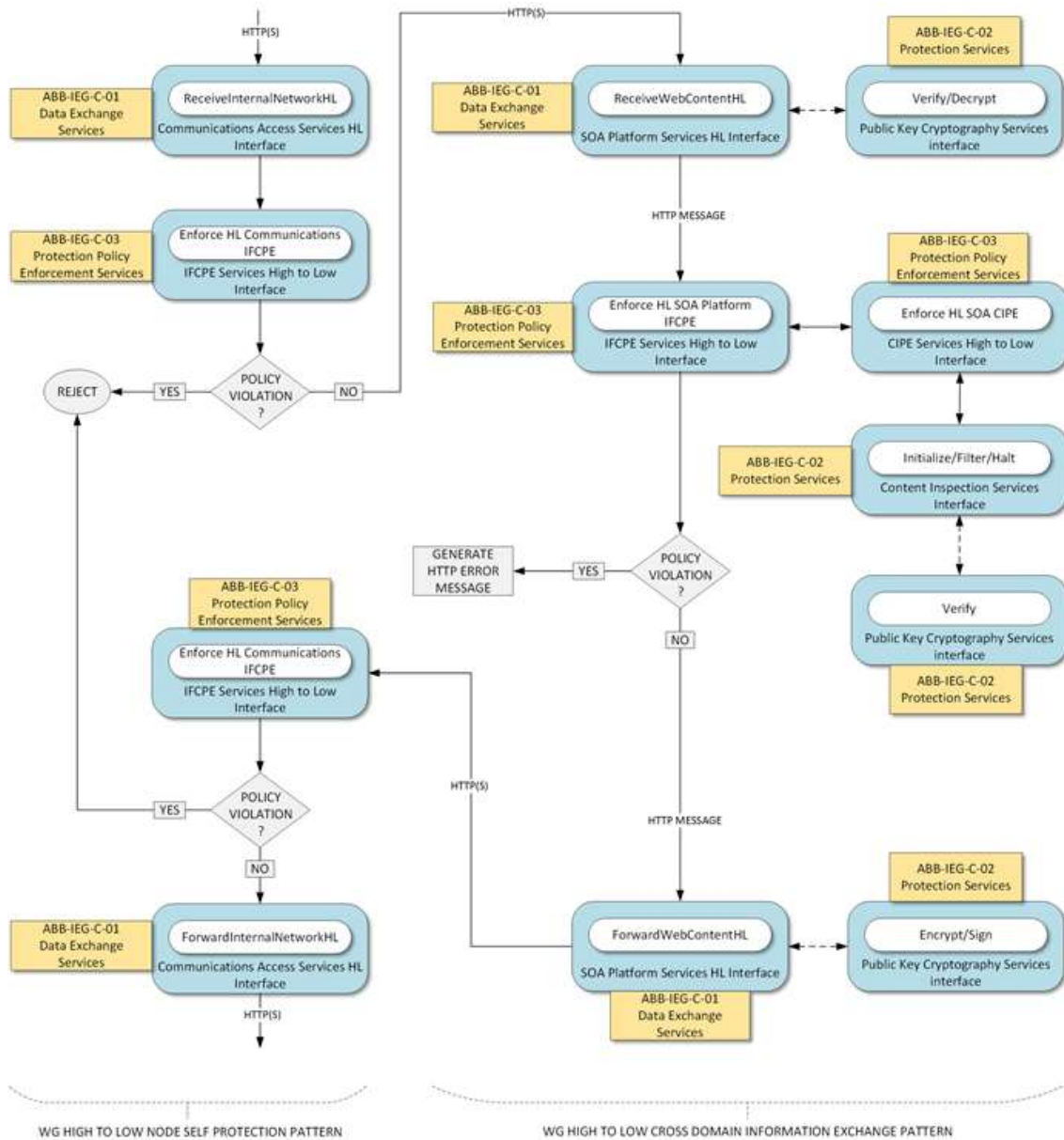
Figure 13 WG High to Low Pattern (combination of 'WG High to Low Node Self Protection Pattern' and 'WG High to Low Cross Domain Information Exchange pattern')

HTTP error messages are sent as response messages, therefore they will not continue to follow the WG High to Low Pattern. Instead they will follow part of the WG Low to High Pattern. The WG Low to High Pattern is depicted in full in Figure 15Figure 15; the part that is relevant to the sending of HTTP error messages is included as a sub-pattern in Figure 14Figure 14.

Figure 14 shows the composed pattern for the generation and sending of HTTP error messages that occur during high to low traffic flow processing. The pattern is composed of two sub-patterns: a WG High to Low sub-pattern in which the error message is generated, and a WG Low to High sub-pattern in which the error message is sent.
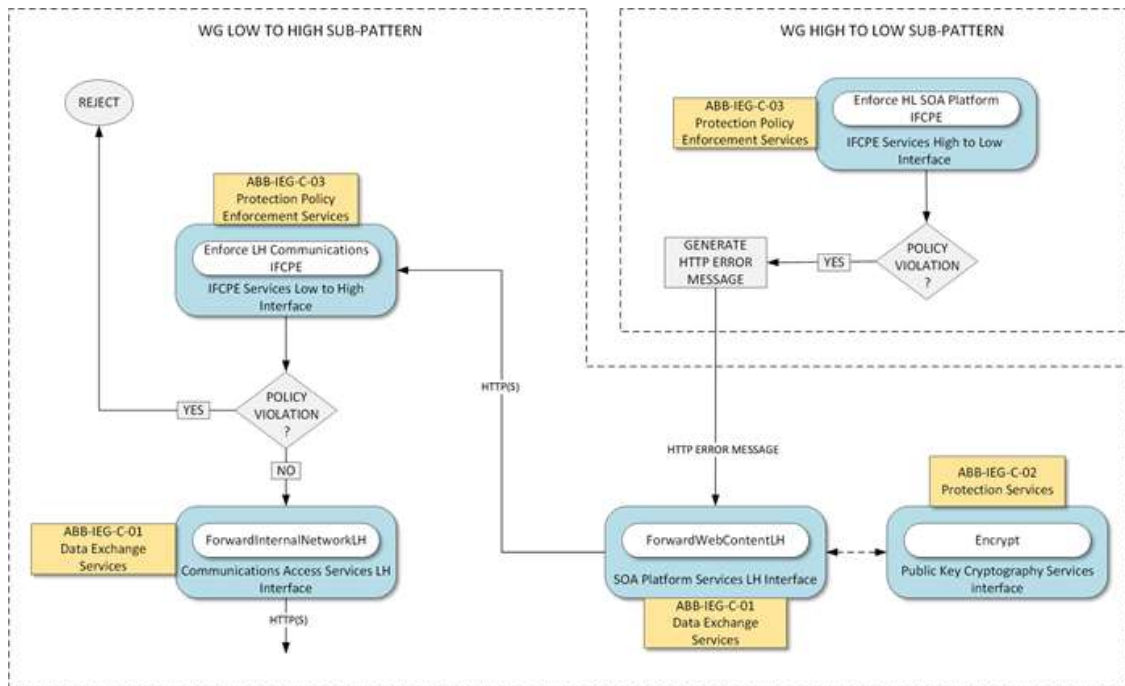
Figure 14 Pattern for generation and sending of HTTP error messages that occur during high to low traffic flow processing

6.3.3 WG Low to High Pattern

The policy WG_IFP_LH is enforced in the WG Low to High Pattern (depicted in Figure 15). The pattern is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

(In order to clarify the sequence of the pattern, the following formatting is used: interfaces are underlined and *operations* are in italic.)

- [START] Data Exchange Services -> Communications Access Services LH -> *ReceiveInternalNetworkLH*
- Protection Policy Enforcement Services -> IFCPE Services Low to High -> *Enforce LH Communications IFCPE* [IFP: WG_IFP_CA_LH_IN]
- Data Exchange Services -> SOA Platform Services LH -> *ReceiveWebContentLH*
- Protection Services -> Public Key Cryptographic Services -> *Verify / Decrypt* (Required if TLS connection is used or content is digitally signed)
- Protection Policy Enforcement Services -> IFCPE Services Low to High -> *Enforce LH SOA Platform IFCPE* [IFP: WG_IFP_SOA_LH]
- Protection Policy Enforcement Services -> CIPE Services Low to High -> *Enforce LH SOA CIPE* [CIP: WG_CIP_LH]
- Protection Services -> Content Inspection Services -> *Initialize / Filter / Halt*
- Data Exchange Services -> SOA Platform Services LH -> *ForwardWebContentLH*
- Protection Services -> Public Key Cryptographic Services -> *Encrypt*
- (Required if TLS connection is used)
- Protection Policy Enforcement Services -> IFCPE Services Low to High -> *Enforce LH Communications IFCPE* [IFP: WG_IFP_CA_LH_OUT]
- Data Exchange Services -> Communications Access Services LH -> *ForwardInternalNetworkLH* [END]

Note that the pattern starts with the operation 'ReceiveInternalNetworkLH' and ends with the operation 'ForwardInternalNetworkLH'; this is in line with Figure 12.

Traffic will follow the pattern from [START] to [END] if no policy violation occurs. In case a policy violation occurs, traffic flow is interrupted according to Figure 15:

- If enforcement of WG_IFP_CA_LH_IN or WG_IFP_CA_LH_OUT results in a policy violation, traffic will be rejected and an action shall be executed as specified in [SRS-6-116].
- If enforcement of WG_IFP_SOA_LH results in a policy violation, an HTTP error message may be generated according to [SRS-6-138]. Note that [SRS-6-138] includes the option to silently drop traffic. Figure 15~~Figure 15~~ however assumes an HTTP error message is generated.
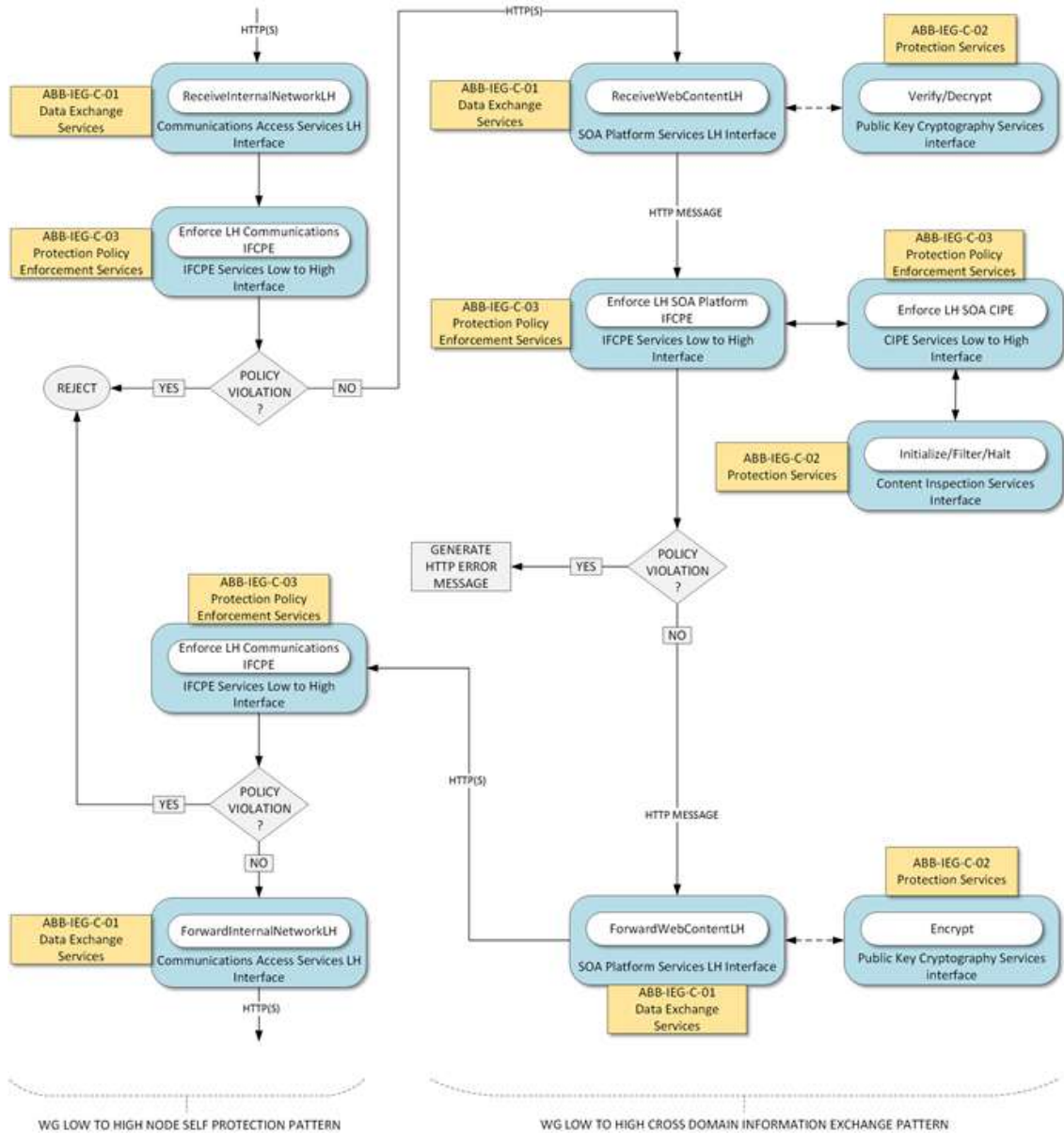
Figure 15   WG Low to High Pattern (combination of 'WG Low to High Node Self Protection Pattern' and 'WG Low to High Cross Domain Information Exchange Pattern')

HTTP error messages are sent as response messages, therefore they will not continue to follow the WG Low to High Pattern. Instead they will follow part of the WG High to Low. The WG High to Low Pattern is depicted in full in Figure 13Figure 13; the part that is relevant to the sending of HTTP error messages is included as a sub-pattern in Figure 16Figure 16

Figure 16Figure 16 shows the composed pattern for the generation and sending of HTTP error messages that occur during low to high traffic flow processing. The pattern is composed of two sub-patterns: a WG Low to High sub-pattern in which the error message is generated, and a WG High to Low sub-pattern in which the error message is sent.
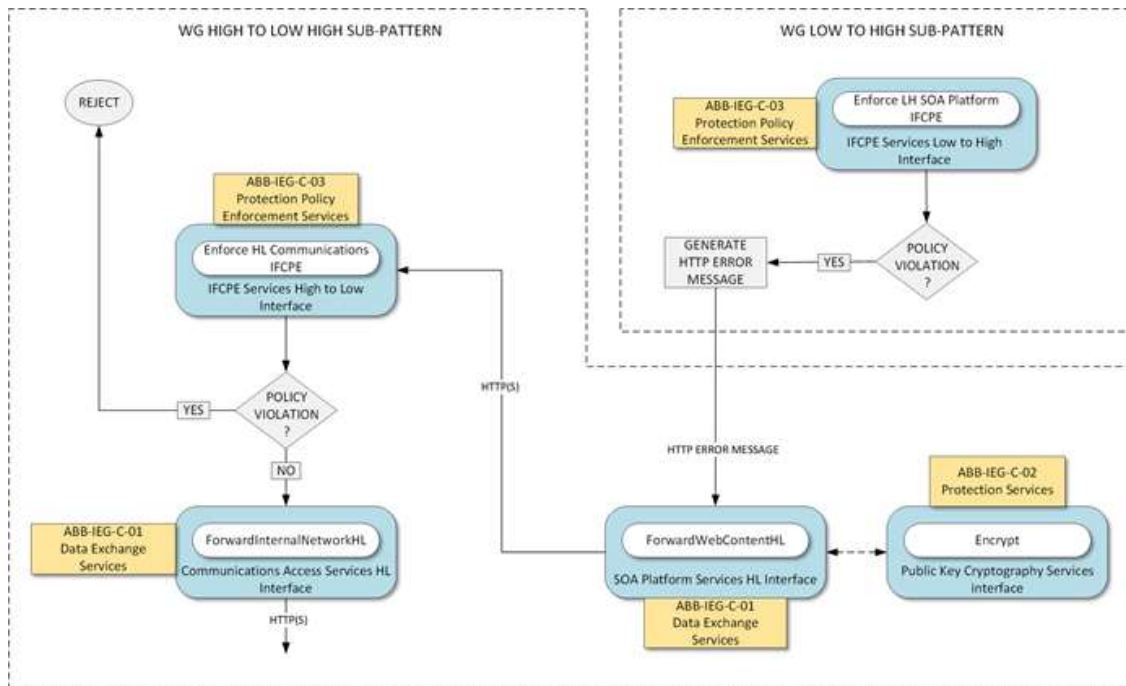
Figure 16 Pattern for generation and sending of HTTP error messages that occur during low to high traffic flow processing

6.3.4 WG Management Pattern

The WG Management Pattern is composed of the 'WG Management Self Protection Pattern' (Figure 17Figure 17) and the 'WG Element Management Services Pattern' (Figure 18Figure 18). The 'WG Management Self Protection Pattern' enforces the policy WG_IFP_MGMT, and the 'WG Element Management Services Pattern' enables management of the operating system and the WG ABBs. Management services at the WG are offered by the ABB 'Element Management Services' (see 6.7). The WG Management Pattern also applies to management traffic initiated at the WG with external destination (related to the operations described in Sections 6.7.7 and 6.7.8).

6.3.4.1 WG Management Self Protection Pattern

Figure 17Figure 17 shows the 'WG Management Self Protection Pattern'. The pattern forwards incoming management traffic to the 'WG Element Management Services Pattern'. Traffic that is output by the 'WG Element Management Services Pattern' is picked up again by the 'WG Management Self Protection Pattern'. It is composed of the following ABBs, interfaces and operations (sub-policies that are enforced are shown [between brackets]):

(In order to clarify the sequence of the pattern, the following formatting is used: interfaces are underlined and *operations* are in italic.)

- [START] Data Exchange Services -> Communications Access Services Management -> ReceiveNetworkManagement
- Protection Policy Enforcement Services -> IFCPE Services Management -> EnforceManagemenCommunicationstIFCPE [IFP: WG_IFP_MGMT_IN] -> 'WG Element Management Services Pattern'
- Processing by 'WG Element Management Services Pattern' (Figure 18)

- 'WG Element Management Services Pattern' -> Protection Policy Enforcement Services -> IFCPE Services Management -> EnforceManagementCommunicationsIFCPE [IFP: WG_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 WG_IFP_MGMT_IN or WG_IFP_MGMT_OUT results in a policy violation, traffic will be rejected and an action shall be executed as specified in [SRS-6-116].
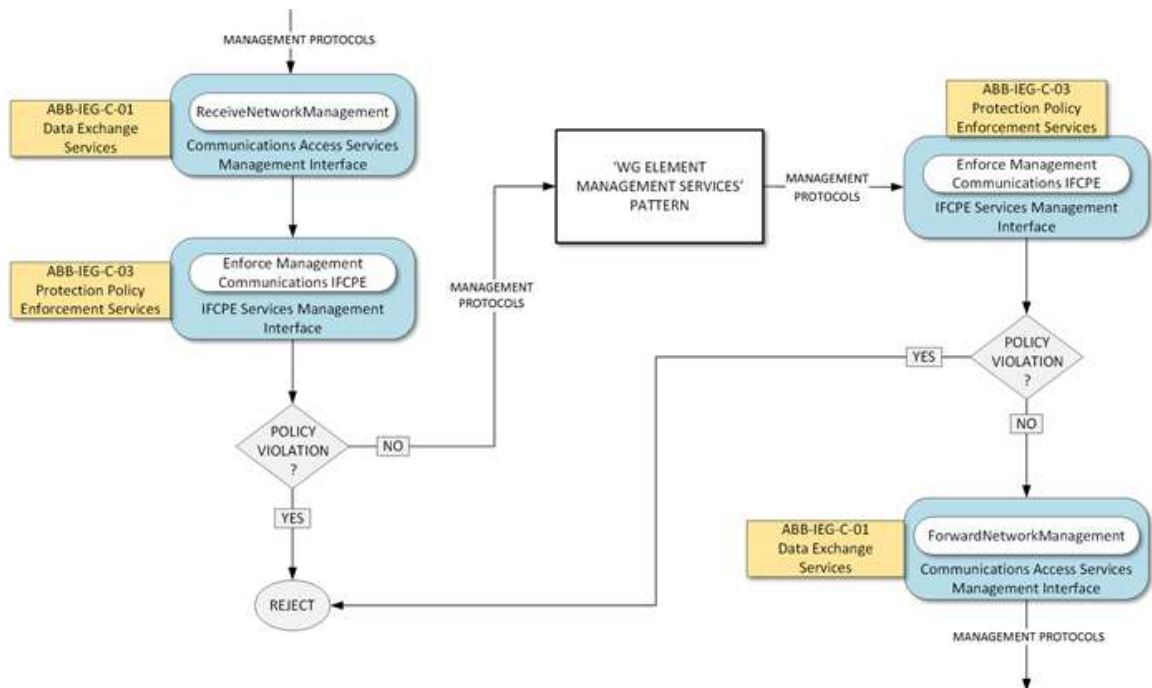
Figure 17 WG Management Self Protection Pattern; this pattern is connected to the pattern 'WG Element Management Services' and enforces an IFP on incoming and outgoing management traffic

6.3.4.2 WG Element Management Services Pattern

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

(In order to clarify the sequence of the pattern, the following formatting is used: interfaces are underlined and operations are in italic.)

- 'WG Management Self Protection Pattern' - > [START] Data Exchange Services -> Core Services Management -> ReceiveManagementContent
- Protection Services -> Public Key Cryptographic Services -> Verify / Decrypt (Required if SSH or TLS connection is used, or content is digitally signed)
- Element Management Services -> CIS Security -> Manage Protection Policies / Review / Manage Public Key Material

OR:

- Element Management Services -> <u>SMC Configuration Management</u> -> Configure OS / Configure Protection Policy Enforcement Services / Configure Data Exchange Services / Configure Protection Services

OR:

- Element Management Services -> <u>Event Management</u> -> Log / Alert / Report

OR:

- Element Management Services -> <u>Cyber Defence</u> -> Assess / Response / Recover

OR:

- Element Management Services -> <u>Performance Management</u> -> Monitor / Meter / Track Messages
- Data Exchange Services -> <u>Core Services Management</u> -> ForwardManagementContent
- Protection Services -> <u>Public Key Cryptographic Services</u> -> Encrypt
- (Required if SSH or TLS connection is used)
- [END] -> 'WG Management Self Protection Pattern'
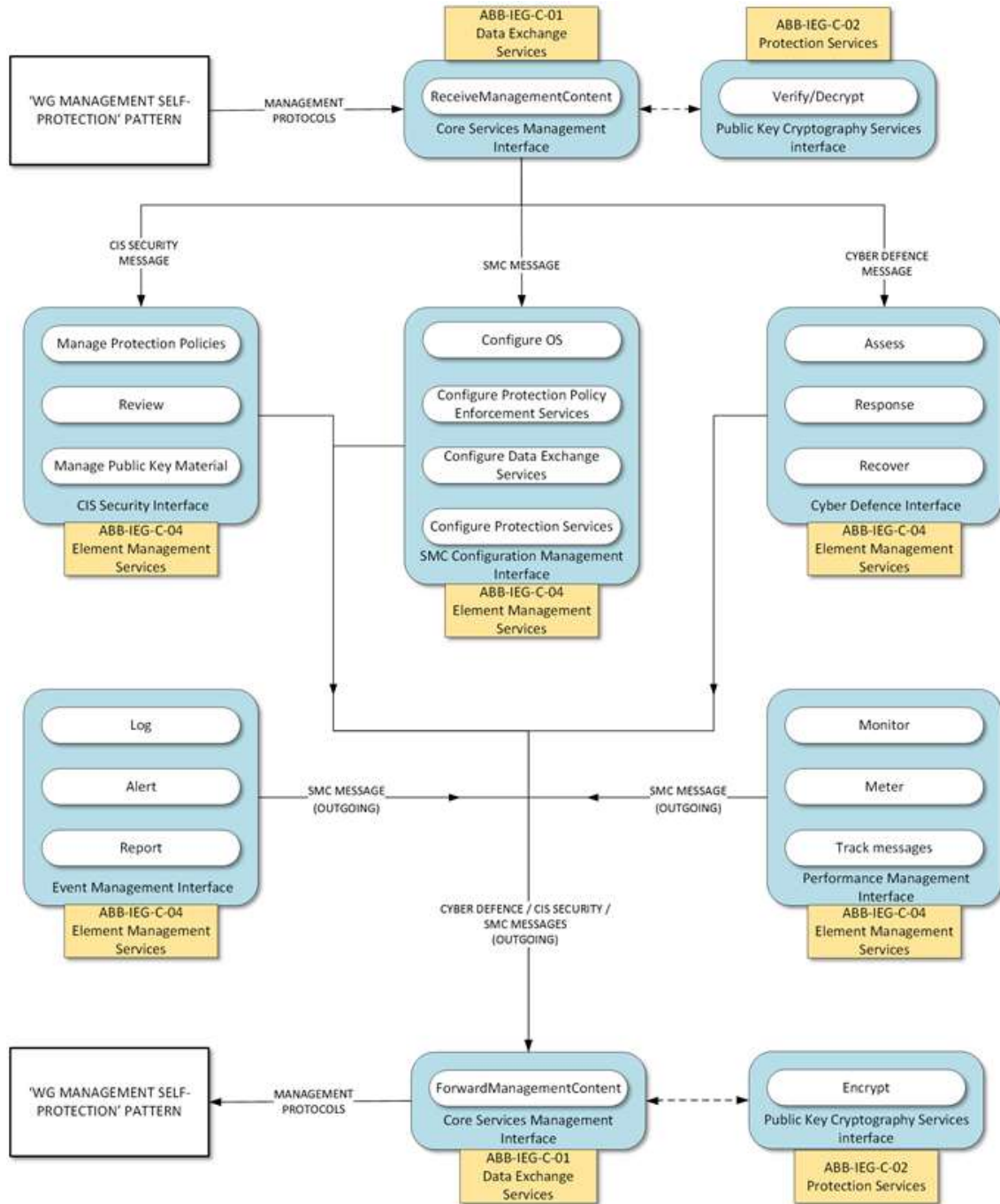
Figure 18 WG Element Management Services Pattern; this pattern takes input from and outputs to the 'WG Management Self Protection Pattern'

6.3.4.3 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;
- 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 messages 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 WG per IEG-C ABB and assume the WG patterns from Section 6.5. Note that in Section 6.3 the terms 'high domain' and 'low domain' are to be interpreted according to Table 6.

6.4 Data Exchange Services

6.4.1 Data Exchange Services

6.4.1.1 WG_DEX

Requirement ID: [SRS-6-1]

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

6.4.1.2 WG_IF_NET_HIGH

Requirement ID: [SRS-6-2]

WG_DEX MUST offer a physical network interface WG_IF_NET_HIGH that provides Ethernet connectivity to the high domain.

Requirement ID: [SRS-6-3]

WG_IF_NET_HIGH MUST support an operation 'ReceiveHigh' that receives (transfer-in) data from the high domain for processing by the WG.

Requirement ID: [SRS-6-4]

WG_IF_NET_HIGH MUST support an operation 'ForwardHigh' that forwards (transfer-out) data that has been processed by the WG to the high domain.

6.4.1.3 WG_IF_NET_LOW

Requirement ID: [SRS-6-5]

WG_DEX MUST offer a physical network interface WG_IF_NET_LOW that provides Ethernet connectivity to the low domain.

Requirement ID: [SRS-6-6]

WG_IF_NET_LOW MUST support an operation 'ReceiveLow' that receives (transfer-in) data from the low domain for processing by the WG.

Requirement ID: [SRS-6-7]

WG_IF_NET_LOW MUST support an operation 'ForwardLow' that forwards (transfer-out) data that has been processed by the WG to the low domain.

6.4.1.4 WG_IF_MGMT

Requirement ID: [SRS-6-8]

WG_DEX SHOULD offer a physical network interface WG_IF_MGMT that provides Ethernet connectivity to the management domain.

Requirement ID: [SRS-6-9]

If WG_DEX does not offer a physical network interface WG_IF_MGMT, it MUST offer a logical network interface WG_IF_MGMT on top of WG_IF_NET_HIGH.

Requirement ID: [SRS-6-10]

WG_IF_MGMT MUST support an operation 'ReceiveManagement' that receives data from the management domain for processing by the WG.

Requirement ID: [SRS-6-11]

WG_IF_MGMT MUST support an operation 'ForwardManagement' that forwards data that has been processed by the WG to the management domain.

6.4.2 Communications Access Services

6.4.2.1 Communications Access Services HL

Requirement ID: [SRS-6-12]

WG_DEX MUST offer a TCP/IP [IETF RFC 791, 1981], [IETF RFC 2460, 1998], [IETF RFC 7414, 2015] over Ethernet interface 'Communications Access Services HL' on top of WG_IF_NET_HIGH and WG_IF_NET_LOW.

6.4.2.1.1 ReceiveInternalNetworkHL

Requirement ID: [SRS-6-13]

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

Requirement ID: [SRS-6-14]

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

6.4.2.1.2 ForwardInternalNetworkHL

Requirement ID: [SRS-6-15]

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

Requirement ID: [SRS-6-16]

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

6.4.2.2 Communications Access Services LH

Requirement ID: [SRS-6-17]

WG_DEX MUST offer a TCP/IP [IETF RFC 791, 1981], [IETF RFC 2460, 1998], [IETF RFC 7414, 2015] over Ethernet interface 'Communications Access Services LH' on top of WG_IF_NET_LOW and WG_IF_NET_HIGH.

6.4.2.2.1 ReceiveInternalNetworkLH

Requirement ID: [SRS-6-18]

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

Requirement ID: [SRS-6-19]

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

6.4.2.2.2 ForwardInternalNetworkLH

Requirement ID: [SRS-6-20]

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

Requirement ID: [SRS-6-21]

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

6.4.3 SOA Platform Services

6.4.3.1 SOA Platform Services HL

Requirement ID: [SRS-6-22]

WG_DEX MUST offer a HyperText Transport Protocol (HTTP) v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services HL' on top of 'Communications Access Services HL'.

Requirement ID: [SRS-6-23]

The interface 'SOA Platform Services HL' and its operations SHALL be conformant to the following service interface profiles (SIPs), see Appendix B.3:

- Service Interface Profile for Security Services;
- Service Interface Profile for REST Security Services;
- Service Interface Profile for Messaging (SOAP);
- Service Interface Profile for REST Messaging.

6.4.3.1.1 ReceiveWebContentHL

Requirement ID: [SRS-6-24]

The interface 'SOA Platform Services HL' MUST support an operation 'ReceiveWebContentHL' that provides HTTP connectivity on the high domain.

Requirement ID: [SRS-6-25]

The operation 'ReceiveWebContentHL' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-26]

The operation 'ReceiveWebContentHL' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-27]

After receiving an HTTP message, the operation 'ReceiveWebContentHL' SHALL pass the HTTP message to the interface 'IFCPE Services High to Low' ([SRS-6-71]) for further processing.

Requirement ID: [SRS-6-28]

The operation 'ReceiveWebContentHL' SHALL persist the HTTP TCP/IP connection from an HTTP client in the high domain until:

- an HTTP Response is received at the interface 'SOA Platform Services LH' (6.4.3.2) and processed by the operation 'ForwardWebContentLH' (6.4.3.2.3); or
- the HTTP TCP/IP connection is timed out by the HTTP client.

Requirement ID: [SRS-6-29]

In support of the use of HTTP persistent connections, the WG SHALL be able to correlate HTTP request and response messages that belong to the same HTTP connection initiated in the high domain.

Requirement ID: [SRS-6-30]

The operation 'ReceiveWebContentHL' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.3.1.2 ForwardWebContentHL

Requirement ID: [SRS-6-31]

The interface 'SOA Platform Services HL' MUST support an operation 'ForwardWebContentHL' that provides HTTP connectivity on the low domain.

Requirement ID: [SRS-6-32]

After receiving an HTTP Request message from the interface 'IFCPE Services High to Low', the operation 'ForwardWebContentHL' SHALL initiate a new HTTP connection - including the HTTP message - to an HTTP server on the low domain. The new HTTP connection SHALL not use the stateful HTTP protocol attributes associated with the connection in [SRS-6-28].

Requirement ID: [SRS-6-33]

After receiving an HTTP Response message from the interface 'IFCPE Services High to Low', the operation 'ForwardWebContentHL' SHALL forward the HTTP message to the low domain using the persisted HTTP connection ([SRS-6-43]).

Requirement ID: [SRS-6-34]

The operation 'ForwardWebContentHL' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-35]

The operation 'ForwardWebContentHL' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-36]

The operation 'ForwardWebContentHL' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.3.2 SOA Platform Services LH

Requirement ID: [SRS-6-37]

WG_DEX MUST offer a HyperText Transport Protocol (HTTP), v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services LH' on top of 'Communications Access Services LH'.

Requirement ID: [SRS-6-38]

The interface 'SOA Platform Services LH' and its operations SHALL be conformant to the following service interface profiles (SIPs), see Appendix A.3:

- Service Interface Profile for Security Services;
- Service Interface Profile for REST Security Services;
- Service Interface Profile for Messaging (SOAP);
- Service Interface Profile for REST Messaging.

6.4.3.2.1 ReceiveWebContentLH

Requirement ID: [SRS-6-39]

The interface 'SOA Platform Services LH' MUST support an operation 'ReceiveWebContentLH' that provides HTTP connectivity on the low domain.

Requirement ID: [SRS-6-40]

The operation 'ReceiveWebContentLH' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-41]

The operation 'ReceiveWebContentLH' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-42]

After receiving an HTTP message, the operation 'ReceiveWebContentLH' SHALL pass the HTTP message to the interface 'IFCPE Services Low to High' (6.5.1.2.2) for further processing.

Requirement ID: [SRS-6-43]

The operation 'ReceiveWebContentLH' SHALL persist the HTTP TCP/IP connection from an HTTP client in the high domain until:

- an HTTP Response is received at the interface 'SOA Platform Services HL' ([SRS-6-22]) and processed by the operation 'ForwardWebContentHL' (6.4.3.1.3); or
- the HTTP TCP/IP connection is timed out by the HTTP client.

Requirement ID: [SRS-6-44]

In support of the use of HTTP persistent connections, the WG SHALL be able to correlate HTTP Request and Response messages that belong to the same HTTP connection initiated in the low domain.

Requirement ID: [SRS-6-45]

The operation 'ReceiveWebContentLH' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.3.2.2 ForwardWebContentLH

Requirement ID: [SRS-6-46]

The interface 'SOA Platform Services LH' MUST support an operation 'ForwardWebContentLH' that provides HTTP connectivity on the high domain.

Requirement ID: [SRS-6-47]

After receiving an HTTP Request message from the interface 'IFCPE Services Low to High', the operation 'ForwardWebContentLH' SHALL initiate a new HTTP connection - including the HTTP message - to an HTTP server on the high domain. The new HTTP connection SHALL not use the stateful HTTP protocol attributes associated with the connection in [SRS-6-43].

Requirement ID: [SRS-6-48]

After receiving an HTTP Response message from the interface 'IFCPE Services Low to High', the operation 'ForwardWebContentLH' SHALL forward the HTTP message to the high domain using the persisted HTTP connection ([SRS-6-43]).

Requirement ID: [SRS-6-49]

The operation 'ForwardWebContentLH' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-6-50]

The operation 'ForwardWebContentLH' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-51]

The operation 'ForwardWebContentLH' MUST support error handling as specified in [IETF RFC 7231, 2014].

6.4.4 Communications Access Services Management

6.4.4.1 Communications Access Services Management

Requirement ID: [SRS-6-52]

WG_DEX MUST offer UDP [IETF RFC 768, 1980] and IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interface 'Communications Access Services Management' on top of WG_IF_MGMT.

6.4.4.1.1 ReceiveNetworkManagement

Requirement ID: [SRS-6-53]

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 WG.

Requirement ID: [SRS-6-54]

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

6.4.4.1.2 ForwardNetworkManagement

Requirement ID: [SRS-6-55]

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

Requirement ID: [SRS-6-56]

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

6.4.5 Core Services Management

6.4.5.1 Core Services Management

Requirement ID: [SRS-6-57]

WG_DEX MUST offer an interface 'Core Services Management' on top of 'Communications Access Services Management'.

Requirement ID: [SRS-6-58]

The interface 'Core Services Management' MUST support the following management protocols:

- Transport Layer protocol [IETF RFC 4251, 2006];
- 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) v1.1 Web interface [IETF RFC 7230, 2014] [IETF RFC 7231, 2014]; Hyper-Text Transport Protocol (HTTP) v2 Web interface, [IETF RFC 7540, 2014]~~
- ~~Remote Desktop (RDP).~~

Requirement ID: [SRS-6-59]

The interface 'Core Services Management' MAY support the following management protocol:

- Intelligent Platform Management Interface (IPMI) [IPMI V2.0, 2013];
- Remote Desktop (RDP).
- Hyper-Text Transport Protocol (HTTP) v1.1 Web interface [IETF RFC 7230, 2014] [IETF RFC 7231, 2014]; Hyper-Text

Transport Protocol (HTTP) v2 Web interface, [IETF RFC 7540, 2014]

- Remote Procedure Call (RPC).
- Keyboard, video and mouse (KVM) over Ethernet;
- Command Line interface (CLI) via Secure Shell (SSH)

6.4.5.2 ReceiveManagementContent

Requirement ID: [SRS-6-60]

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

Requirement ID: [SRS-6-61]

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

Requirement ID: [SRS-6-62]

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

Requirement ID: [SRS-6-63]

The operation 'ReceiveManagementContent' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

Requirement ID: [SRS-6-64]

The operation 'ReceiveManagementContent' SHALL pass management content in the form of a management message to the appropriate interface offered by WG_MGMT ([SRS-6-252]) for further processing.

6.4.5.3 ForwardManagementContent

Requirement ID: [SRS-6-65]

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

Requirement ID: [SRS-6-66]

After receiving a management message from one of the interfaces offered by WG_MGMT ([SRS-6-252]), the operation 'ForwardManagementContent' SHALL forward the management message, as payload of the appropriate management protocol, to the management domain.

Requirement ID: [SRS-6-67]

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

Requirement ID: [SRS-6-68]

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

Requirement ID: [SRS-6-69]

The operation 'ForwardManagementContent' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).

6.5 Protection Policy Enforcement Services

6.5.1 Information Flow Control Policy (IFP) Enforcement

6.5.1.1 WG_IFCPE

Requirement ID: [SRS-6-70]

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

- Mediate the flow of information between WG_IF_NET_HIGH and WG_IF_NET_LOW in accordance with the WG information flow policy WG_IFP;
- Control incoming and outgoing management traffic at WG_IF_MGMT in accordance with the WG information flow policy WG_IFP.

Requirement ID: [SRS-6-71]

The design of WG_IFCPE SHALL be such that the enforcement of policies WG_CIP_LH_LV and WG_CIP_HL_SV can be supported (see 6.2.4).

6.5.1.2 IFCPE Services High to Low

Requirement ID: [SRS-6-72]

For the flow of information from WG_IF_NET_HIGH to WG_IF_NET_LOW, WG_IFCPE MUST offer an interface 'IFCPE Services High to Low' that accepts information for further processing.

6.5.1.2.1 Enforce HL Communications IFCPE

Requirement ID: [SRS-6-73]

The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL Communications IFCPE' that enforces the policy WG_IFP_CA_HL.

Requirement ID: [SRS-6-74]

The operation 'Enforce HL Communications IFCPE' SHALL enforce the policy WG_IFP_CA_HL_IN on the following information flow:

- Source: Communications Access Services HL Interface -> ReceiveInternalNetworkHL;
- Destination: SOA Platform Services HL Interface -> ReceiveWebContentHL;
- Information: HTTP(S) traffic;
- Operation: pass HTTP(S) traffic by ensuring the following conditions:
  - WG_IFP_CA_HL_IN permits information flow.

Requirement ID: [SRS-6-75]

The operation 'Enforce HL Communications IFCPE' SHALL enforce the policy WG_IFP_CA_HL_OUT on the following information flow:

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

Requirement ID: [SRS-6-500]

If WG_IFP_CA_HL_IN or WG_IFP_CA_HL_OUT do not permit information flow, the WG SHALL execute the actions specified in WG_IFP_CA_HL.

Requirement ID: [SRS-6-76]

For every action taken, the operation 'Enforce HL Communications IFCPE' SHALL invoke the operation 'Log' 6.7.7.1.1) at the interface 'Event Management' (6.7.7.1) and log the action.

Requirement ID: [SRS-6-77]

If WG_IFP_CA_HL does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' (6.7.7.1) and log the outcome O_WG_IFCPE (6.6.2.4).

Requirement ID: [SRS-6-78]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_CA_HL

6.5.1.2.2 Enforce HL SOA Platform IFCPE

Requirement ID: [SRS-6-79]

The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL SOA Platform IFCPE' that enforces the policy WG_IFP_SOA_HL.

Requirement ID: [SRS-6-80]

Prior to enforcing WG_IFP_SOA_HL, WG_IFCPE SHALL completely reassemble all chunks of an HTTP message-body that was received with chunked transfer encoding.

Requirement ID: [SRS-6-81]

The operation 'Enforce HL SOA Platform IFCPE' SHALL enforce the policy WG_IFP_SOA_HL on the following information flow:

- Source: SOA Platform Services HL Interface->ReceiveWebContentHL;
- Destination: SOA Platform Services HL Interface >ForwardWebContentHL;
- Information: HTTP Messages;
- Operation: pass HTTP Messages from source to destination ensuring the following conditions:
  - the HTTP Message has been processed by the WG content inspection policy enforcement capability WG_CIPE (6.5.3.1) based on the content inspection policy WG_CIP_HL ([SRS-6-144]);
  - Based on the outcome of processing by WG_CIPE, WG_IFP_SOA_HL permits the release of the HTTP Message to the low domain.
  - In case of an HTTP response message, pass message only if it was preceded by an HTTP request message that was passed as part of the enforcement of WG_IFP_SOA_LH ([SRS-6-97]).

Requirement ID: [SRS-6-82]

The operation 'Enforce HL SOA Platform IFCPE' MUST support the invocation of the operation 'Enforce HL SOA CIPE' at the interface 'CIPE Services High to Low' (6.5.3.2). The operation 'Enforce HL SOA CIPE' SHALL take as input:

- The HTTP message that is being processed;
- The policy WG_CIP_HL.

Requirement ID: [SRS-6-83]

If WG_IFP_SOA_HL does not permit the release of information, the WG SHALL execute the actions specified in WG_IFP_SOA_HL.

Requirement ID: [SRS-6-84]

For every action taken, the operation 'Enforce HL SOA Platform IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-85]

If WG_IFP_SOA_HL does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-86]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_SOA_HL.

6.5.1.3 IFCPE Services Low to High

Requirement ID: [SRS-6-87]

For the flow of information from WG_IF_NET_LOW to WG_IF_NET_HIGH, WG_IFCPE MUST offer an interface 'IFCPE Services Low to High' that accepts information for further processing.

6.5.1.3.1 Enforce LH Communications IFCPE

Requirement ID: [SRS-6-88]

The interface 'IFCPE Services Low to High' MUST support an operation 'Enforce LH Communications IFCPE' that enforces the policy WG_IFP_CA_LH.

Requirement ID: [SRS-6-89]

The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy WG_IFP_CA_LH_IN on the following information flow:

- Source: Communications Access Services LH Interface -> ReceiveInternalNetworkLH;
- Destination: SOA Platform Services LH Interface -> ReceiveWebContentLH;
- Information: HTTP(S) traffic;
- Operation: pass HTTP(S) traffic by ensuring the following conditions:
  - WG_IFP_CA_LH_IN permits information flow.

Requirement ID: [SRS-6-90]

The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy WG_IFP_CA_LH_OUT on the following information flow:

- Source: SOA Platform LH Interface -> ForwardWebContentLH;
- Destination: Communications Access Services LH Interface -> ForwardNetworkLH;
- Information: HTTP(S) traffic;
- Operation: pass HTTP(S) traffic by ensuring the following conditions:
  - WG_IFP_CA_LH_OUT permits information flow.

Requirement ID: [SRS-6-91]

If WG_IFP_CA_LH_IN or WG_IFP_CA_LH_OUT do not permit information flow, the WG SHALL execute the actions specified in WG_IFP_CA_LH.

Requirement ID: [SRS-6-92]

For every action taken, the operation 'Enforce LH Communications IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-93]

If WG_IFP_CA_LH does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-94]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_CA_LH.

6.5.1.3.2 Enforce LH SOA Platform IFCPE

Requirement ID: [SRS-6-95]

The interface 'IFCPE Services Low to High' MUST support an operation 'Enforce LH SOA Platform IFCPE' that enforces the policy WG_IFP_SOA_LH.

Requirement ID: [SRS-6-96]

Prior to enforcing WG_IFP_SOA_LH, WG_IFCPE SHALL completely reassemble all chunks of an HTTP message-body that was received with chunked transfer encoding.

Requirement ID: [SRS-6-97]

The operation 'Enforce LH SOA Platform IFCPE' SHALL enforce the policy WG_IFP_SOA_LH on the following information flow:

- Source: SOA Platform Services LH Interface->ReceiveWebContentLH;
- Destination: SOA Platform Services LH Interface >ForwardWebContentLH;
- Information: HTTP Messages;
- Operation: pass HTTP Messages from source to destination ensuring the following conditions:
  - the HTTP Message has been processed by the WG content inspection policy enforcement capability WG_CIPE (6.5.3.1) based on the content inspection policy WG_CIP_LH ([SRS-6-151]).
  - Based on the outcome of processing by WG_CIPE, WG_IFP_SOA_LH permits the import of the HTTP Message to the high domain.
  - In case of an HTTP response message, pass message only if it was preceded by an HTTP request message

that was passed as part of the enforcement of
WG_IFP_SOA_HL ([SRS-6-81]).

Requirement ID: [SRS-6-98]

The operation 'Enforce LH SOA Platform IFCPE' MUST support the invocation of the
operation 'Enforce LH SOA CIPE' at the interface 'CIPE Services Low to High'
(6.5.3.2). The operation 'Enforce LH SOA CIPE' SHALL take as input:

- The HTTP message that is being processed;
- The policy WG_CIP_LH.

Requirement ID: [SRS-6-99]

If WG_IFP_SOA_LH does not permit the release of information, the WG SHALL
execute the actions specified in WG_IFP_SOA_LH.

Requirement ID: [SRS-6-100]

For every action taken, the operation 'Enforce LH SOA Platform IFCPE' SHALL invoke
the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and
log the action.

Requirement ID: [SRS-6-101]

If WG_IFP_SOA_LH does not permit the release of information due to a policy
violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event
Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-102]

The WG SHALL ensure that no illicit information flows exist to circumvent the
enforcement of WG_IFP_SOA_LH.

6.5.1.4 IFCPE Services Management

Requirement ID: [SRS-6-103]

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

6.5.1.4.1 Enforce Management Communications IFCPE

Requirement ID: [SRS-6-104]

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

Requirement ID: [SRS-6-105]

The operation 'Enforce Management Communications IFCPE' SHOULD enforce the
policy WG_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:
  - WG_IFP_MGMT_IN permits information flow.

Requirement ID: [SRS-6-106]

The operation 'Enforce Management Communications IFCPE' SHOULD enforce the policy WG_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:
  - WG_IFP_MGMT_OUT permits information flow.

Requirement ID: [SRS-6-107]

If WG_IFP_MGMT_IN or WG_IFP_MGMT_OUT do not permit information flow, the WG SHALL execute the action specified in WG_IFP_MGMT.

Requirement ID: [SRS-6-108]

For every action taken, the operation 'Enforce Management Communications IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-109]

If WG_IFP_MGMT does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).

Requirement ID: [SRS-6-110]

The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_MGMT.

6.5.2 Information flow control policies

Requirement ID: [SRS-6-111]

WG_IFP SHALL be configurable.

Requirement ID: [SRS-6-112]

WG_IFP SHALL specify the actions ACTIONS that need to be executed by WG_IFCPE.

Requirement ID: [SRS-6-113]

For each action in ACTIONS it SHALL be possible to:

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

Requirement ID: [SRS-6-114]

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

- WG_IFP_CA_LH_IN;
- WG_IFP_CA_LH_OUT;
- WG_IFP_CA_HL_IN;
- WG_IFP_CA_HL_OUT;
- WG_IFP_MGMT_IN;
- WG_IFP_MGMT_OUT;
- WG_IFP_SOA_LH;
- WG_IFP_SOA_HL.

Requirement ID: [SRS-6-115]

WG_IFP SHALL specify the level of granularity of the outcome O_WG_IFCPE. It SHALL be possible for WG_IFCPE to distinguish within O_WG_IFCPE:

- The sub-policy ([SRS-6-114]) 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-6-116]

The policies WG_IFP_CA_HL, WG_IFP_CA_LH and WG_IFP_MGMT SHALL specify:

- That an information flow (as described in 6.5.1.2.2, 6.5.1.3.2 and 6.5.1.4.2 respectively) is not permitted if the outcome O_WG_IFCPE constitutes a policy violation;
- The action the WG shall take in case information flow is not permitted. The possible actions SHALL include:
  o Silently drop traffic;
  o Reset the TCP/IP connection.

Requirement ID: [SRS-6-117]

The policy WG_IFP_CA_HL_IN SHALL specify the actions ACTIONS_WG_CA_HL_IN that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-74]).

Requirement ID: [SRS-6-118]

ACTIONS_WG_CA_HL_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_HL_IN.

Requirement ID: [SRS-6-119]

The policy WG_IFP_CA_HL_OUT SHALL specify the actions ACTIONS_WG_CA_HL_OUT that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-75]).

Requirement ID: [SRS-6-120]

ACTIONS_WG_CA_HL_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_HL_OUT.

Requirement ID: [SRS-6-121]

The policy WG_IFP_CA_LH_IN SHALL specify the actions ACTIONS_WG_CA_LH_IN that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-89]).

Requirement ID: [SRS-6-122]

ACTIONS_WG_CA_LH_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_LH_IN.

Requirement ID: [SRS-6-123]

The policy WG_IFP_CA_LH_OUT SHALL specify the actions ACTIONS_WG_CA_LH_OUT that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-90]).

Requirement ID: [SRS-6-124]

ACTIONS_WG_CA_LH_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_LH_OUT.

Requirement ID: [SRS-6-125]

The policy WG_IFP_MGMT_IN SHALL specify the actions ACTIONS_WG_MGMT_IN that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in [SRS-6-105].

Requirement ID: [SRS-6-126]

ACTIONS_WG_MGMT_IN SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-MGT_IN.

Requirement ID: [SRS-6-127]

The policy WG_IFP_MGMT_OUT SHALL specify the actions ACTIONS_WG_MGMT_OUT that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in [SRS-6-106].

Requirement ID: [SRS-6-128]

ACTIONS_WG_MGMT_OUT SHALL include the following actions:

- Filter traffic based on the ruleset RULESET_WG_IFCPE-MGT_OUT.

Requirement ID: [SRS-6-129]

The policy WG_IFP_CA_HL SHALL specify RULESET_WG_IFCPE-CA_HL_IN and RULESET_WG_IFCPE-CA_HL_OUT.

Requirement ID: [SRS-6-130]

RULESET_WG_IFCPE-CA_HL_IN and RULESET_WG_IFCPE-CA_HL_OUT SHALL be configurable.

Requirement ID: [SRS-6-131]

The policy WG_IFP_CA_LH SHALL specify RULESET_WG_IFCPE-CA_LH_IN and RULESET_WG_IFCPE-CA_LH_OUT.

Requirement ID: [SRS-6-132]

RULESET_WG_IFCPE-CA_LH_IN and RULESET_WG_IFCPE-CA_LH_OUT SHALL be configurable.

Requirement ID: [SRS-6-133]

The policy WG_IFP_MGMT SHALL specify RULESET_WG_IFCPE-MGT_IN and RULESET_WG_IFCPE-MGT_OUT.

Requirement ID: [SRS-6-134]

RULESET_WG_IFCPE-MGT_IN and RULESET_WG_IFCPE-MGT_OUT SHALL be configurable.

Requirement ID: [SRS-6-135]

Each of the rulesets RULESET_WG_IFCPE-CA_HL_IN, RULESET_WG_IFCPE-CA_HL_OUT, RULESET_WG_IFCPE-CA_LH_IN, RULESET_WG_IFCPE-CA_LH_OUT, RULESET_WG_IFCPE-MGT_IN, RULESET_WG_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-6-136]

The policy WG_IFP_SOA_HL SHALL specify:

- That a release of information to the low domain is not permitted if O_WG_CIPE_HL ([SRS-6-148]) constitutes a policy violation;
- The action the WG shall take in case of a policy violation, see [SRS-6-138].

Requirement ID: [SRS-6-137]

The policy WG_IFP_SOA_LH SHALL specify:

- That an import of information to the high domain is not permitted if O_WG_CIPE_LH ([SRS-6-155]) constitutes a policy violation;
- The action the WG shall take in case of a policy violation, see [SRS-6-138].

Requirement ID: [SRS-6-138]

The policies WG_IFP_SOA_HL and WG_IFP_SOA_LH SHALL specify the action the WG shall take in case of a policy violation. The possible actions SHALL include:

- Silently drop traffic;
- Send an HTTP error response of a specific type;
  - The type of HTTP error message SHALL be configurable.
- Send a custom HTTP error message;
  - The contents of the custom HTTP error message SHALL be configurable.
  - It SHALL be possible to include the items in [SRS-6-163].

6.5.3 Content Inspection Policy (CIP) Enforcement

6.5.3.1 WG_CIPE

Requirement ID: [SRS-6-139]

The WG MUST provide a content inspection policy enforcement (CIPE) capability WG_CIPE that enables the WG to manage and schedule the routing of content through content filters (by WG_CIS ([SRS-6-190])) in accordance with the WG content inspection policy WG_CIP.

Requirement ID: [SRS-6-140]

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

Requirement ID: [SRS-6-395]

If WG_CIPE does not conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012], the proposed functional specification of the WG_CIPE SHALL be described in the bid response.

Requirement ID: [SRS-6-397]

The WG_CIPE SHALL be able to be configured to support the "Content Inspection Policy Enforcement Profile for a Medium Assurance NATO XML-Labelling Guard" [NC3A TR/2012/SPW007959/03].

Requirement ID: [SRS-6-141]

WG_CIPE SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_CIP.

Requirement ID: [SRS-6-142]

WG_CIPE SHALL ensure that enforcement actions are executed in the order as specified in WG_CIP ([SRS-6-159]).

6.5.3.2 CIPE Services High to Low

Requirement ID: [SRS-6-143]

For the flow of information from WG_IF_NET_HIGH to WG_IF_NET_LOW, WG_CIPE MUST offer an interface 'CIPE Services High to Low' that accepts information for further processing.

6.5.3.2.1 Enforce HL SOA CIPE

Requirement ID: [SRS-6-144]

The interface 'CIPE Services High to Low' MUST support an operation 'Enforce HL SOA CIPE' that enforces the policy WG_CIP_HL.

Requirement ID: [SRS-6-145]

The operation 'Enforce HL SOA CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-6-194]) provided by WG_CIS ([SRS-6-190]):

- Operation 'Initialize' ([SRS-6-199]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in WG_CIS;
- Operation 'Filter' ([SRS-6-201]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA;
- Operation 'Halt' ([SRS-6-203]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in WG_CIS.

Requirement ID: [SRS-6-146]

WG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy WG_CIP_HL.

Requirement ID: [SRS-6-147]

For every action taken, the operation 'Enforce HL SOA CIPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-148]

WG_CIPE SHALL inform WG_IFCPE of the outcome O_WG_CIPE_HL of the enforcement of WG_CIP_HL based on WG_CIP ([SRS-6-163]).

Requirement ID: [SRS-6-149]

WG_CIPE SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log O_WG_CIPE_HL.

6.5.3.3 CIPE Services Low to High

Requirement ID: [SRS-6-150]

For the flow of information from WG_IF_NET_LOW to WG_IF_NET_HIGH, WG_CIPE MUST offer an interface 'CIPE Services Low to High' that accepts information for further processing.

6.5.3.3.1 Enforce LH SOA CIPE

Requirement ID: [SRS-6-151]

The interface 'CIPE Services Low to High' MUST support an operation 'Enforce LH SOA CIPE' that enforces the policy WG_CIP_LH.

Requirement ID: [SRS-6-152]

The operation 'Enforce LH SOA CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-6-194]) provided by WG_CIS ([SRS-6-190]):

- Operation 'Initialize' ([SRS-6-199]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in WG_CIS;
- Operation 'Filter' ([SRS-6-201]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA;
- Operation 'Halt' ([SRS-6-203]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in WG_CIS.

Requirement ID: [SRS-6-153]

WG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy WG_CIP_LH.

Requirement ID: [SRS-6-154]

For every action taken, the operation 'Enforce LH SOA CIPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.

Requirement ID: [SRS-6-155]

WG_CIPE SHALL inform WG_IFCPE of the outcome O_WG_CIPE_LH of the enforcement of WG_CIP_LH based on WG_CIP ([SRS-6-163]).

Requirement ID: [SRS-6-156]

WG_CIPE SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log O_WG_CIPE_LH.

6.5.4 Content inspection policies

Requirement ID: [SRS-6-157]

WG_CIP SHALL be configurable.

Requirement ID: [SRS-6-158]

WG_CIP SHALL specify the actions ACTIONS that need to be executed by WG_CIS.

Requirement ID: [SRS-6-159]

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

Requirement ID: [SRS-6-160]

For each action in ACTIONS it SHALL be possible to:

- Enable or disable the action.

- Instruct WG_CIPE to ignore the outcome of the execution of the action by WG_CIS (as received from WG_CIS ([SRS-6-206])).
- If the outcome of the execution of the action by WG_CIS is a policy violation: instruct WG_CIPE to continue the enforcement of WG_CIP, or to stop.

Requirement ID: [SRS-6-161]

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

- WG_CIP_LH_SV;
- WG_CIP_LH_HV;
- WG_CIP_LH_MD;
- WG_CIP_HL_HV;
- WG_CIP_HL_LV.

Requirement ID: [SRS-6-162]

It SHALL be possible to enable or disable the enforcement of each sub-policy in ([SRS-6-161]).

Requirement ID: [SRS-6-163]

WG_CIP SHALL specify the level of granularity of the outcomes O_WG_CIS ([SRS-6-205]), O_WG_CIPE_HL ([SRS-6-148]) and O_WG_CIPE_LH ([SRS-6-155]). It SHALL be possible for WG_CIS to distinguish within O_WG_CIS, O_WG_CIPE_HL and O_WG_CIPE_LH:

- The WG_CIS capability that determined a policy violation (WG_CIS_SV ([SRS-6-208]), WG_CIS_HV ([SRS-6-213]), WG_CIS_LV ([SRS-6-219]), and WG_CIS_MD ([SRS-6-508]);
- 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.

Requirement ID: [SRS-6-164]

The policy WG_CIP_LH_SV SHALL specify the actions ACTIONS_WG_LH_SV that need to be performed by WG_CIS_SV.

Requirement ID: [SRS-6-165]

ACTIONS_WG_LH_SV SHALL include the following actions:

- Check the HTTP message body for XML well-formedness;
- Validate the HTTP message body against a list of W3C XML Schemas LIST_WG_CIS_SV-XS;
  - Select LIST_WG_CIS_SV-XS based on the URI in the HTTP message startline.
- Check that the namespace of the root node belongs to a list of allowed namespaces LIST_WG_CIS_SV-NS;
  - Select LIST_WG_CIS_SV-NS based on the URI in the HTTP message startline.

NATO UNCLASSIFIED

Requirement ID: [SRS-6-166]

WG_CIP_LH_SV SHALL specify LIST_WG_CIS_SV-XS.

Requirement ID: [SRS-6-167]

LIST_WG_CIS_SV-XS SHALL be configurable.

Requirement ID: [SRS-6-168]

WG_CIP_LH_SV SHALL include the option to specify a LIST_WG_CIS_SV-XS for a given URI.

Requirement ID: [SRS-6-169]

WG_CIP_LH_SV SHALL specify LIST_WG_CIS_SV-NS.

Requirement ID: [SRS-6-170]

LIST_WG_CIS_SV-NS SHALL be configurable.

Requirement ID: [SRS-6-171]

WG_CIP_LH_SV SHALL include the option to specify a LIST_WG_CIS_SV-NS for a given URI.

Requirement ID: [SRS-6-172]

The policy WG_CIP_HL_HV SHALL specify the actions ACTIONS_WG_HL_HV that need to be performed by WG_CIS_HV.

Requirement ID: [SRS-6-173]

ACTIONS_WG_HL_HV SHALL include the following actions based on RULESET_WG_CIS_HV-HL:

- Verify the information attributes in [SRS-6-214] ;
- Add or rewrite a header line;
- Remove a header line;
- Add or rewrite a value;
- Remove a value;
- Translate a URI to another value;
- Normalize the 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-6-174]

WG_CIP_HL_HV SHALL specify RULESET_WG_CIS_HV-HL.

Requirement ID: [SRS-6-175]

RULESET_WG_CIS_HV-HL SHALL be configurable.

Requirement ID: [SRS-6-176]

The policy WG_CIP_LH_HV SHALL specify the actions ACTIONS_WG_LH_HV that need to be performed by WG_CIS_HV.

Requirement ID: [SRS-6-177]

ACTIONS_WG_LH_HV SHALL include the following actions based on RULESET_WG_CIS_HV-LH:

- Verify the information attributes in [SRS-6-214] ;
- Add or rewrite a header line;
- Remove a header line;
- Add or rewrite a value;
- Remove a value;
- Translate a URI to another value;
- Normalize the 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-6-178]

WG_CIP_LH_HV SHALL specify RULESET_WG_CIS_HV-LH.

Requirement ID: [SRS-6-179]

RULESET_WG_CIS_HV-LH SHALL be configurable.

Requirement ID: [SRS-6-180]

Each of the rulesets RULESET_WG_CIS_HV-HL and RULESET_WG_CIS_HV-LH SHALL include:

- Whitelist of allowed values for the information attributes in [SRS-6-214] ;
- Whitelist of allowed header lines;
- Header lines that shall be present in the message header;
- Header lines that shall not be present in the message header;
- Rules on the start line:
  - Format MUST be according to [IETF RFC 7230, 2014], or [IETF RFC 7540, 2014], depending on the version;
  - Allowed values for the scheme;
  - Allowed values for HTTP version;
  - All case-insensitive parts MUST be lowercase;
  - Maximum length of URI;
  - Maximum number of arguments in URI;
  - Whitelist of allowed URIs;
  - Value to translate a given URI to;
  - Unneeded whitespace SHALL not be present;
  - Allowed values for 'Status Codes;
  - Allowed values for 'Reason String''.
- Rules on the header lines:
  - Remove headers that are not on the whitelist;
  - Remove values that are not on the whitelist;
  - Values that must be added (or rewritten) if not present;

- o Value to translate a given URI to;
- o Maximum length of header;
- o Whitelist of allowed character sets;
- o All case-insensitive parts MUST be lowercase;
- o Host header line: MUST match hostname in start-line URI;
- o Content-Length header line: value MUST be correct.

Requirement ID: [SRS-6-181]

The policy WG_CIP_HL_LV SHALL specify the actions ACTIONS_WG_HL_LV that need to be performed by WG_CIS_LV.

Requirement ID: [SRS-6-182]

ACTIONS_WG_HL_LV SHALL include the following actions:

- Verify that the syntax of the confidentiality metadata label conforms to ADatP-4774 "Confidentiality Metadata Label Syntax" [STANAG 4774];
- Verify that the binding mechanism used conforms to ADatP-4778 "Metadata Binding Mechanism" [STANAG 4778];
- Verify that the binding profile that is applied conforms to "XML Signature Cryptographic Artefact Profile" in [STANAG 4778 SRD.2];
- Validate the *BindingInformation* element (see [STANAG 4778]) against a list of W3C XML Schemas LIST_WG_CIS_LV-XS.
- Verify that the value of any *TransformAlgorithm* attribute is allowed according to a list of allowed values LIST_WG_CIS_LV-TR as specified in [STANAG 4778 SRD.2];
- Verify that the value of any *CanonicalizationMethodAlgorithm* attribute is allowed according to a list of allowed values LIST_WG_CIS_LV-CM as specified in [STANAG 4778 SRD.2];
- Verify that the value of any *DigestMethodAlgorithm* attribute is allowed according to a list LIST_WG_CIS_LV-DM as specified in [STANAG 4778 SRD.2];
- Verify that the value of any *SignatureMethodAlgorithm* attribute used for a digital signature is allowed according to a list LIST_WG_CIS_LV-SM_PKI as specified in [STANAG 4778 SRD.2];
- Verify that the value of any *SignatureMethodAlgorithm* attribute used for a keyed-hash message authentication code (HMAC) is allowed according to a list LIST_WG_CIS_LV-SM_HMAC as specified in [STANAG 4778 SRD.2];
- Check the validity of certificates against a certificate revocation list LIST_WG_CIS_LV-CRL or by using OCSP;
- Evaluate the binding according to [STANAG 4778] and [STANAG 4778 SRD.2]. Evaluation SHALL include:
  - o Identify the complete set of data objects *S* that are labelled (i.e. for each data object *DO* in *S* there is a confidentiality metadata label *CL* identified that is bound to *DO*).

- o For each data object *DO* in *S*, associate the information attributes in ([SRS-6-233]) with *DO*.
- For each data object *DO* in *S*, verify the values of the information attributes in ([SRS-6-233]) against a Metadata Policy Information File (MPIF) MPIF_NATO;
- For each data object *DO* in *S*, verify that *DO* can be released to the low domain based on RULESET_WG_CIS_LV;
- Sanitize the body of the HTTP message based on RULESET_WG_CIS_LV; (Note that the rule set RULESET_WG_CIS_LV will specify whether or not data sanitization shall take place.)
- In the case of sanitization of a file for which a filename has been specified of the form <FILENAME.EXTENSION>, modify the filename to '<FILENAME-SANITIZED_STRING-TIMESTAMP.EXTENSION>' with 'SANITIZED_STRING' and 'TIMESTAMP' as defined in RULESET_WG_CIS_LV.
- Modify BindingInformation for *DO* based on RULESET_WG_CIS_LV;
- Before release of a data object *DO* to the low domain, apply a canonicalization-without-comments [W3C Canonical XML Version 1,1, 2008] transform to *DO*.

Requirement ID: [SRS-6-183]

WG_CIP_HL_LV SHALL specify the lists:

- LIST_WG_CIS_LV-XS;
- LIST_WG_CIS_LV-TR;
- LIST_WG_CIS_LV-CM;
- LIST_WG_CIS_LV-DM;
- LIST_WG_CIS_LV-SM_PKI;
- LIST_WG_CIS_LV-SM_HMAC;
- LIST_WG_CIS_LV-CRL.

Requirement ID: [SRS-6-184]

All lists in [SRS-6-183] SHALL be configurable.

Requirement ID: [SRS-6-185]

WG_CIP_HL_LV SHALL specify the metadata policy information file MPIF_NATO.

Requirement ID: [SRS-6-187]

WG_CIP_HL_LV SHALL specify RULESET_WG_CIS_LV.

Requirement ID: [SRS-6-188]

RULESET_WG_CIS_LV SHALL be configurable.

Requirement ID: [SRS-6-189]

RULESET_WG_CIS_LV SHALL specify:

- The clearance level of the low domain (based on the classification level of the low domain and the clearance levels of the actors in the low domain) in accordance with [STANAG 4774];
- One or more additional (alternative) clearance levels of the low domain, if required.
- The clearance level of the high domain (based on the classification level of the high domain and the clearance levels of the actors in the high domain);
- One or more additional (alternative) clearance levels of the high domain, if required.
- Given a data object *DO* to which a confidentiality metadata label *CL* is bound, the requirements *R* that the values of the information attributes in CL ([SRS-6-233]) must meet in order for *DO* to be releasable from the high domain to the low domain.
  - *R* SHALL be expressed in terms of values of the information attributes in *CL* ([SRS-6-233]) and values that comprise the clearance levels of the low and the high domain;
  - It SHALL be possible to express *R* in terms of a series of AND and OR statements.
- Rules for releasing a data object for which the binding is granular (as defined in [STANAG 4778]);
- Rules for releasing a data object that has an alternative confidentiality metadata label bound to it;
- Whether or not a confidentiality metadata label and associated binding information for *DO* shall be removed before release of *DO*.
- Whether or not signatures shall be removed before release of *DO*.
- Whether or not data sanitization shall be applied;
- If data sanitization shall be applied:
  - 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 SHOULD 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 SHOULD provide a content-filter capability as specified in the NATO CIPE functional specification in [NC3A TN-1486, 2012].

Requirement ID: [SRS-6-396]

If WG_CIPE does not conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012], the proposed functional specification of the WG_CIPE SHALL be described in the bid response.

Requirement ID: [SRS-6-398]

The WG_CIPE SHALL be able to be configured to support the "Content Inspection Policy Enforcement Profile for a Medium Assurance NATO XML-Labelling Guard" [NC3A TR/2012/SPW007959/03].

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.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

IFB-CO-14314-IEG-C
Book II – Part IV SOW Annex A SRS

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.

NATO UNCLASSIFIED

Book II, Part IV SOW Annex A, Page 146

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;

NATO UNCLASSIFIED

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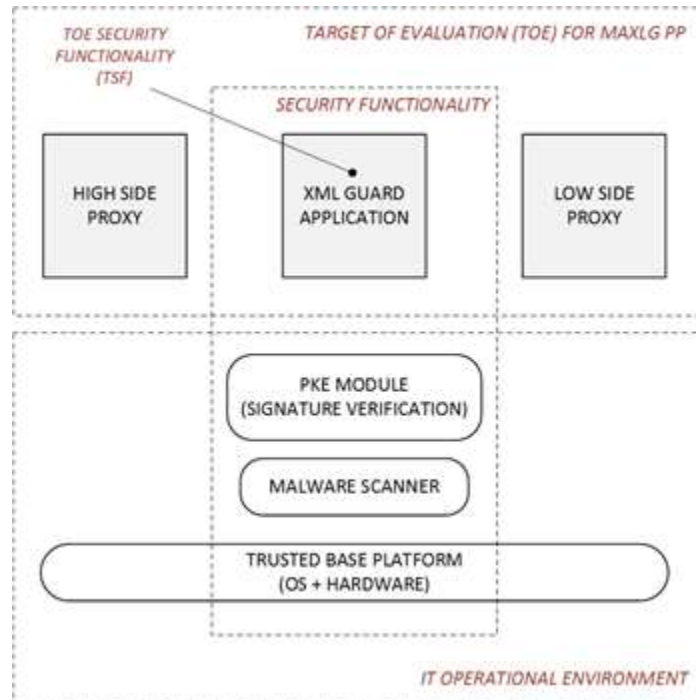
Figure 19   TOE, TSF and IT operational environment defined in [NCIA TN-1485 v1.1, 2012]

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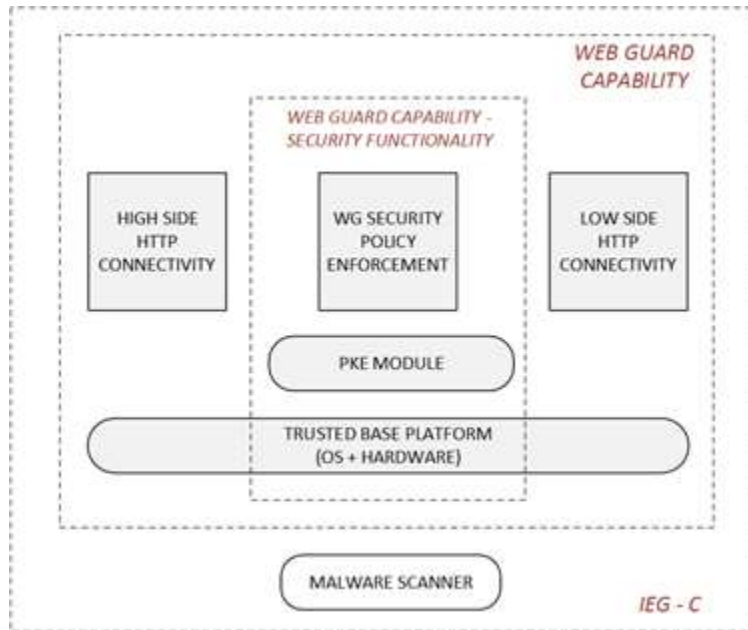
Figure 20 Interpretation of TOE, TSF and IT operational environment for the WG

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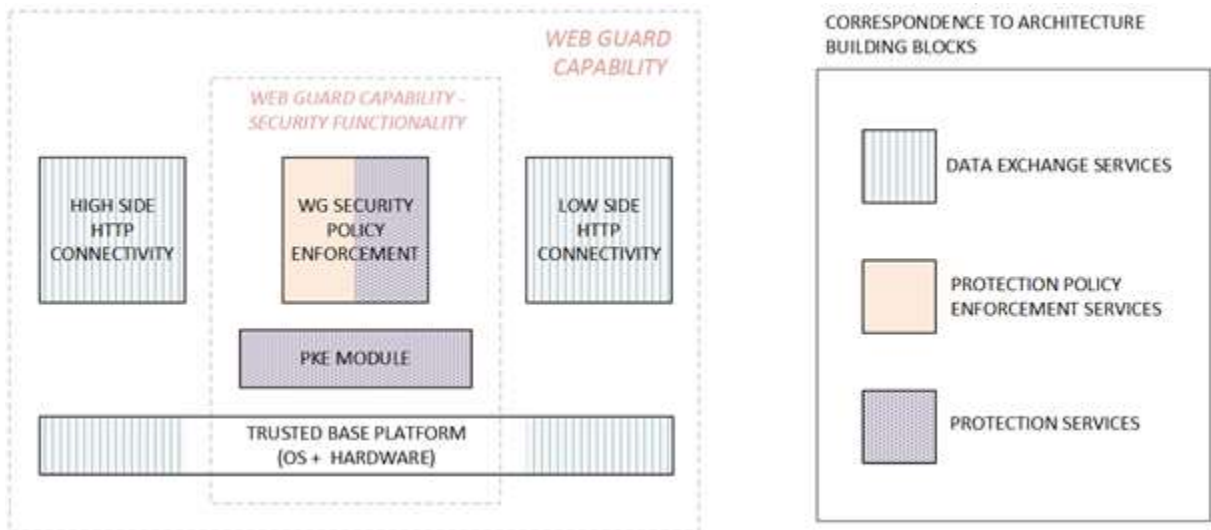
Figure 21 Correspondence between the WG components in Figure 20 and the IEG-C ABBs

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-6-377] 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 22Figure 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 18Table 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 22Figure 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 22Figure 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 18Table 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 23Figure 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.
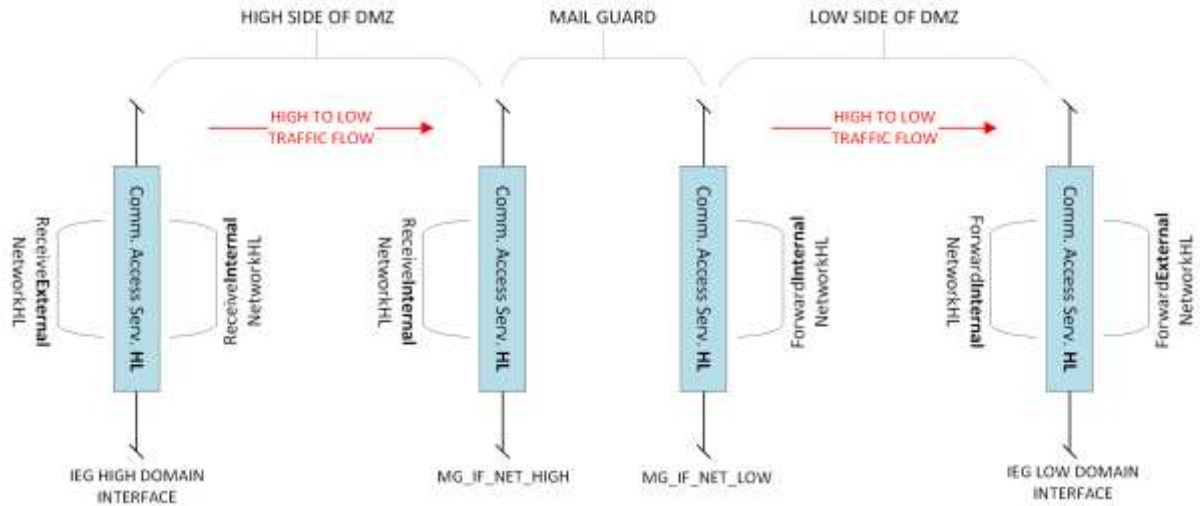
Figure 23: Operations at instances of the interface 'Communication Access Services HL' for traffic flowing from the high to the low domain

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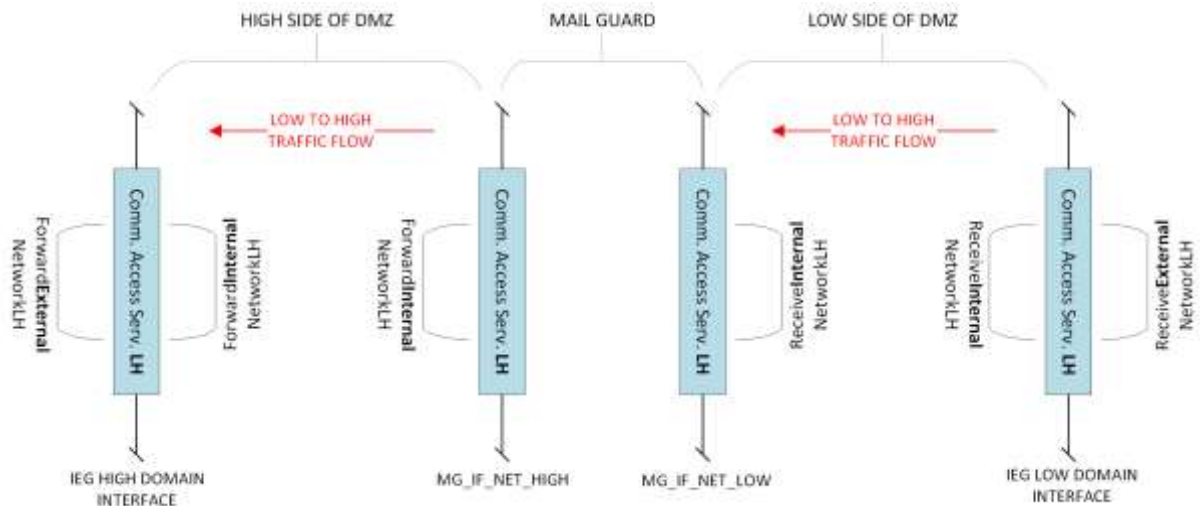
Figure 24: Operations at instances of the interface 'Communication Access Services LH' for traffic flowing from the low to the high domain

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:

---

[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.

- Information flow control policies (Section 7.2.2)
- 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 19Table 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 20Table 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~~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~~.

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~~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~~Figure 26~~
	MG Low to High Cross Domain Information Exchange Pattern	
MG Management pattern	MG Management Self Protection Pattern	Figure 27~~Figure 27~~
	MG Element Management Services Pattern	Figure 28~~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~~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].
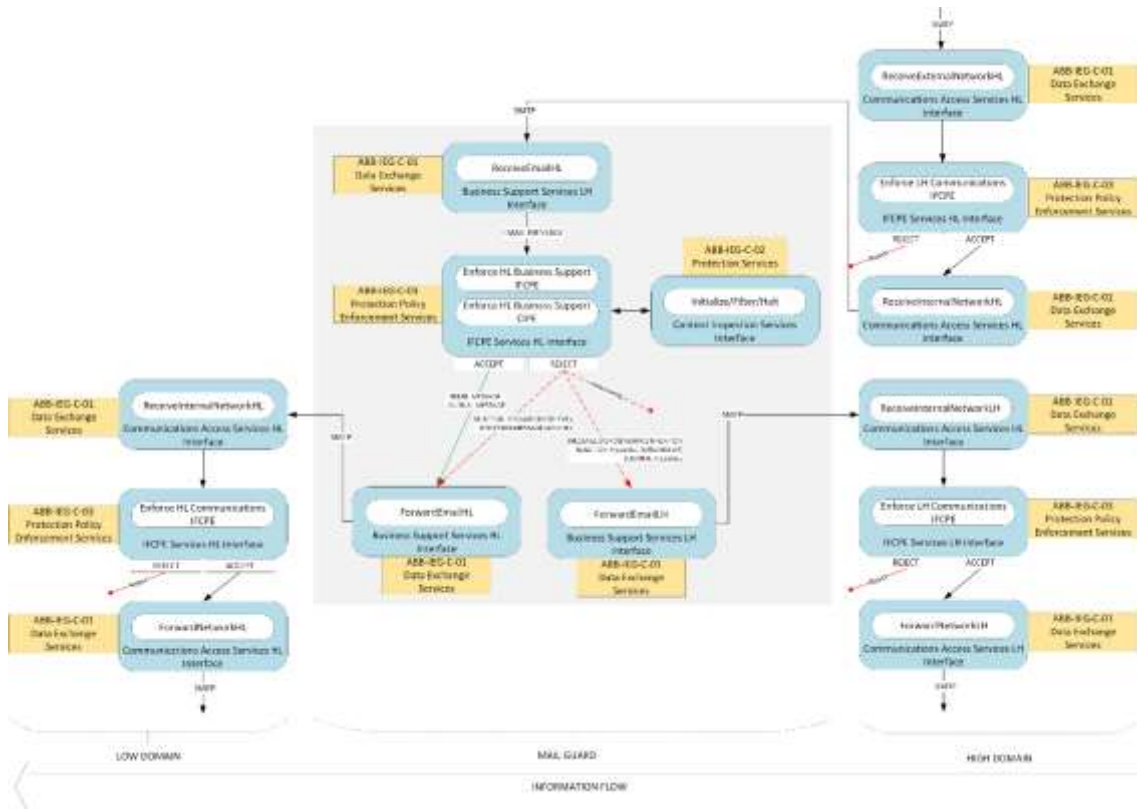
Figure 25: Transfer Informal Email Service High To Low

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

---

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

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.

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 attachments 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 26Figure 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].
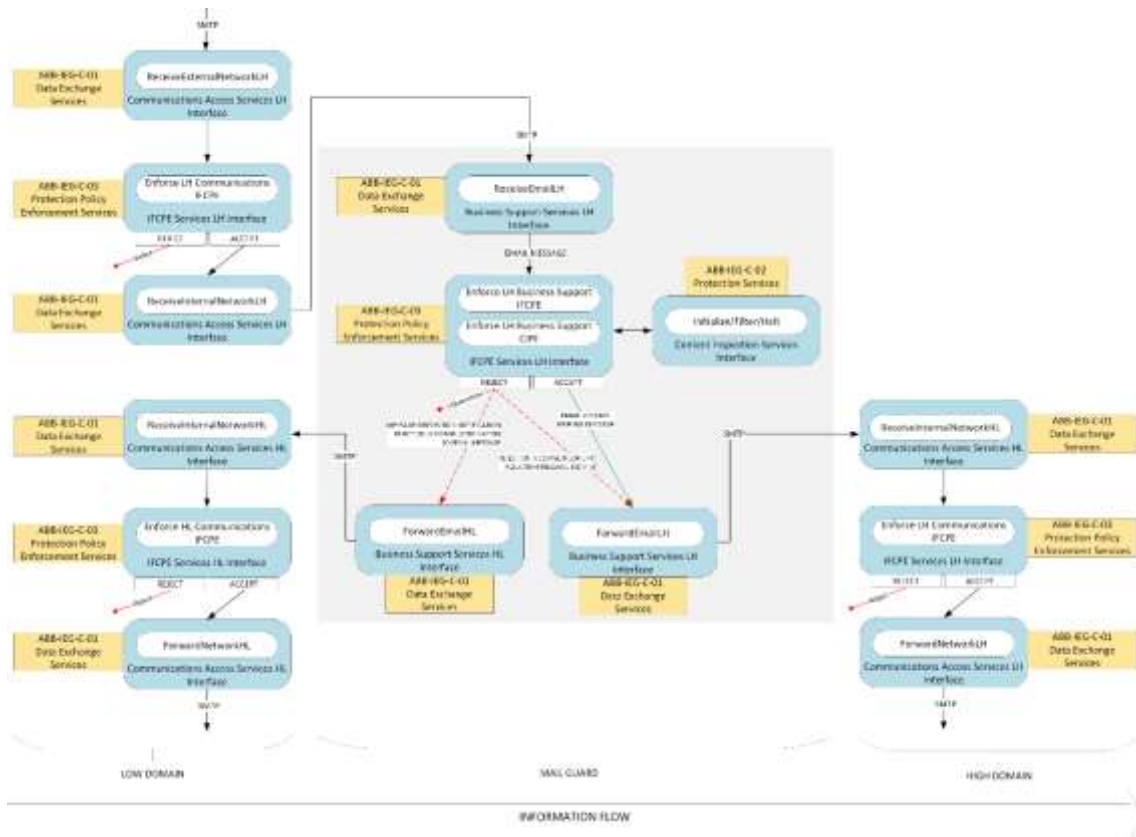
Figure 26: Transfer Informal Email Service Low To High

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.

---

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

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 27Figure 27) and the 'MG Element Management Services Pattern' (Figure 28Figure 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 27Figure 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 28Figure 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].
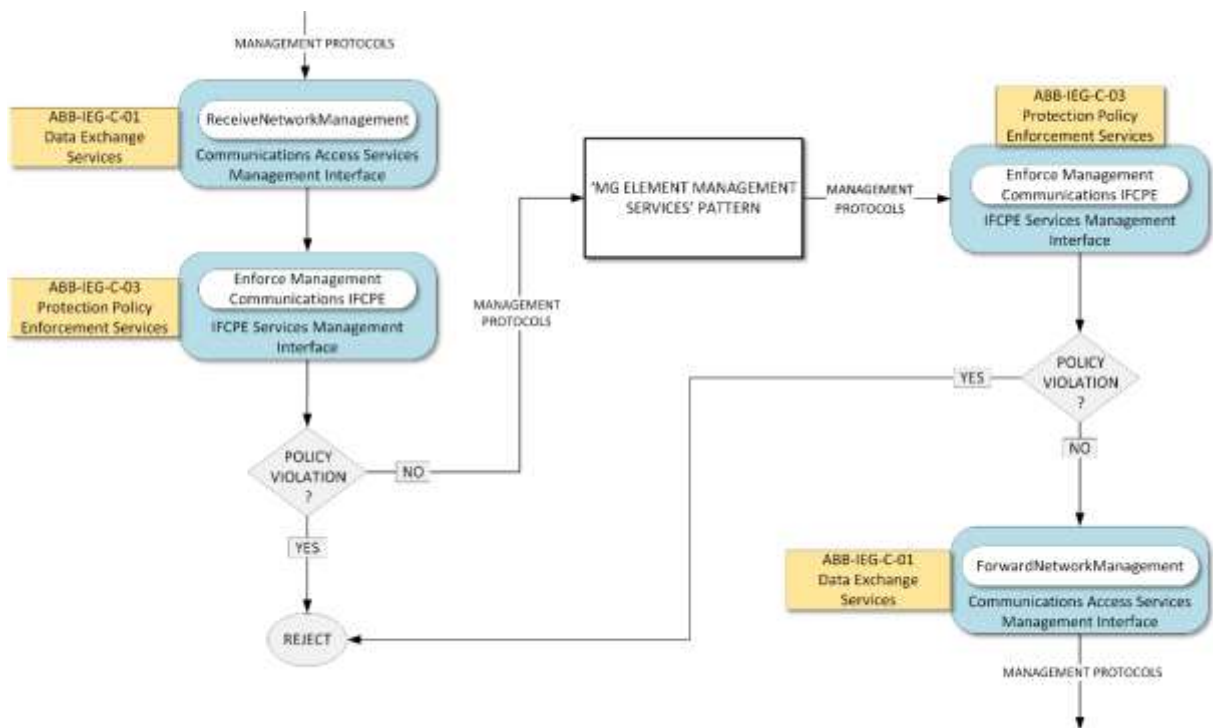
Figure 27: MG Management Self Protection Pattern; this pattern is connected to the pattern 'MG Element Management Services' and enforces an IFP on incoming and outgoing management traffic

7.3.4.2 MG Element Management Services Pattern

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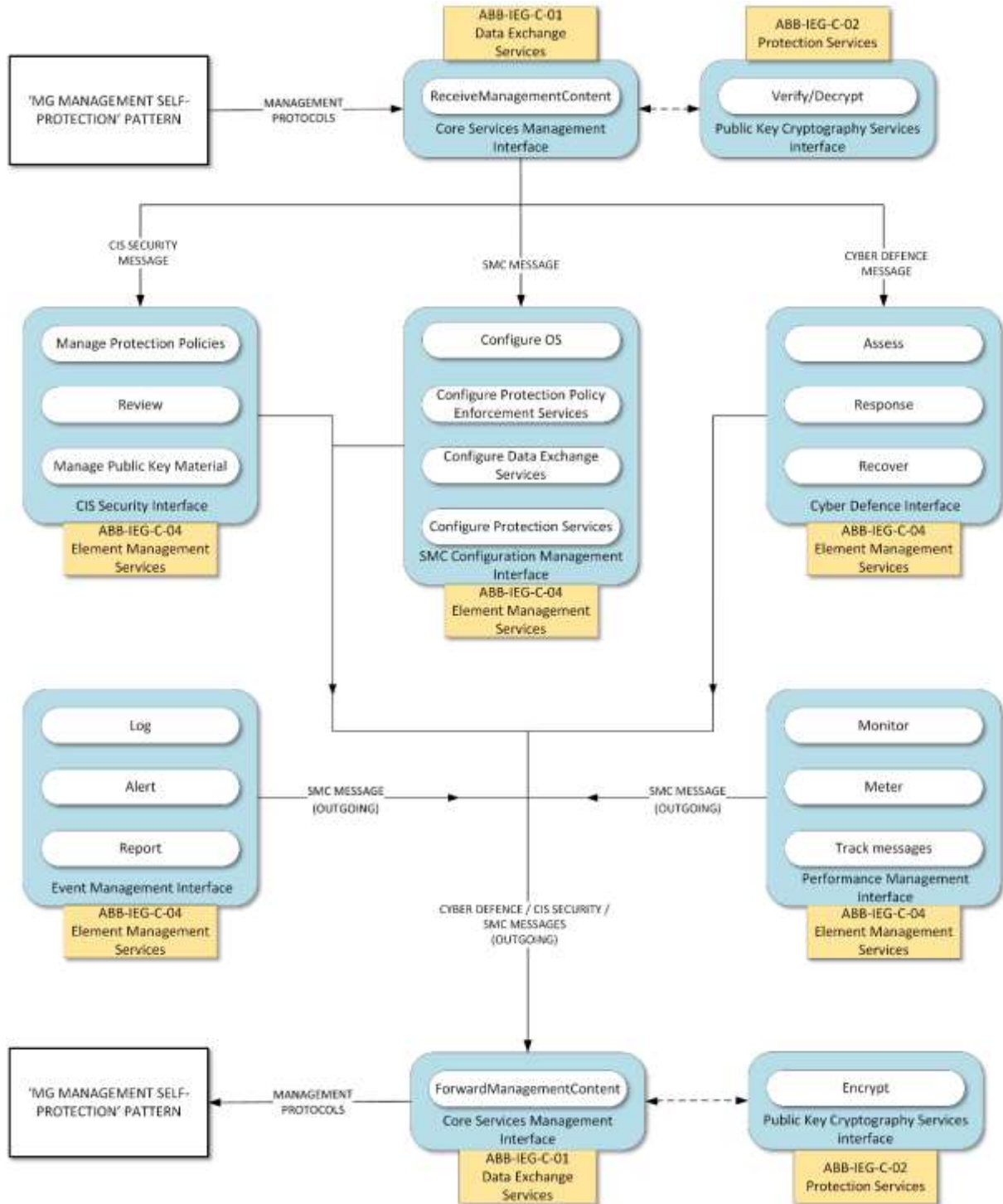
Figure 28: MG Element Management Services Pattern; this pattern takes input from and outputs to the 'MG Management Self Protection Pattern'

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

- 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 18Table 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 IEG-C_IFP_BS_EMAIL _HL.

Requirement ID: [SRS-7-94]

The operation 'Enforce HL Business Support IFCPE' SHALL enforce the policy IEG-C_IFP_BS_EMAIL _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, IEG-C_IFP_BS_EMAIL _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 IEG-C_IFP_BS_EMAIL _HL does not permit the release of information, the MG SHALL execute the actions specified in IEG-C_IFP_BS_EMAIL _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 IEG-C_IFP_BS_EMAIL _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 IEG-C_IFP_BS_EMAIL _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:
    - o 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:
    - o 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 SHOULD conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012].

Requirement ID: [SRS-7-508]

If WG_CIPE does not conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012], the proposed functional specification of the WG_CIPE SHALL be described in the bid response.

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-7-187]).

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 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 SHOULD 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 Transfer Protocol [IETF RFC 5321, 2008].

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 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 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:
  - o 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]
  - o 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, or
- 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 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]).

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.

Requirement ID: [SRS-7-388]

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

Requirement ID: [SRS-7-389]

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

- SLA compliance reports;
- Error/exception reports;
- Service usage reports;

Requirement ID: [SRS-7-390]

Other customizable reports based on captured metrics which can be filtered and sorted based on various criteria.

Requirement ID: [SRS-7-391]

MG_MGMT_EM SHALL pass outgoing SMC Messages to interface 'Core Services Management' ([SRS-7-60]) for further processing.

7.7.7.1 Interfaces

Requirement ID: [SRS-7-392]

MG_MGMT_EM MUST offer an interface 'Event Management' that generates and forwards 'SMC Messages' in support of the operations 'Log' (7.7.7.1.1), 'Alert' (7.7.7.1.2) and 'Report' (7.7.7.1.3).

7.7.7.1.1 Log

Requirement ID: [SRS-7-393]

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-7-394]

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

Requirement ID: [SRS-7-395]

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 MG_MGMT_EM).

Requirement ID: [SRS-7-396]

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

Requirement ID: [SRS-7-397]

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-7-398]

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

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

7.7.7.1.2 Alert

Requirement ID: [SRS-7-399]

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-7-400]

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-7-401]

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-7-402]

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

7.7.7.1.3 Report

Requirement ID: [SRS-7-403]

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-7-404]

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

7.7.8 Performance Management

Requirement ID: [SRS-7-405]

MG_MGMT MUST provide a management capability MG_MGMT_PM that enables the management of the performance and capacity of the MG.

Requirement ID: [SRS-7-406]

MG_MGMT_PM SHALL provide customizable dashboards for monitoring selected statistics and metrics for MG services.

Requirement ID: [SRS-7-407]

MG_MGMT_PM SHALL pass outgoing SMC Messages to interface 'Core Services Management' ([SRS-7-60] for further processing.

7.7.8.1 Interfaces

Requirement ID: [SRS-7-408]

MG_MGMT_PM MUST offer an interface 'Performance Management' that generates and forwards 'SMC Messages' in support of the operations 'Monitor'(7.7.8.1.1), 'Meter' (7.7.8.1.2) and 'Track Messages' (7.7.8.1.3.

7.7.8.1.1 Monitor

Requirement ID: [SRS-7-409]

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 MG.

Requirement ID: [SRS-7-410]

The operation 'Monitor' SHALL support the real-time monitoring of MG services against expected KPI, SLA or other metric thresholds as configured.

Requirement ID: [SRS-7-411]

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

Requirement ID: [SRS-7-412]

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

7.7.8.1.2 Meter

Requirement ID: [SRS-7-413]

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-7-414]

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

Requirement ID: [SRS-7-415]

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-7-416]

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-7-417]

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

7.7.8.1.3 Track Messages

Requirement ID: [SRS-7-418]

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-7-419]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all SMTP messages from the high domain to the low domain.

Requirement ID: [SRS-7-420]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all delivery reports and status notifications from the low domain to the high domain.

Requirement ID: [SRS-7-421]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all SMTP messages from the low domain to the high domain.

Requirement ID: [SRS-7-422]

The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all delivery reports and status notifications from the high domain to the high domain.

Requirement ID: [SRS-7-423]

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

7.8 Security Functional Requirements

7.8.1 Introduction

The security functional requirements for the MG are drawn from the Protection Profile for the IEG-C defined in section 8.

Requirement ID: [SRS-7-424]

The MG SHALL be evaluated to EAL4(+) based on the Protection Profile defined in Section 8.

7.8.2 Requirements

7.8.2.1 Infrastructure Platform

Requirement ID: [SRS-7-425]

The MG SHALL include malware/virus protection for its server.

Requirement ID: [SRS-7-426]

The MG malware/virus protection SHALL be maintained/updated from the NATO Service Operation Centre (SOC).

7.8.2.2 Trusted Base Platform (TBP)

Requirement ID: [SRS-7-428]

The MG SHALL protect components and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.

Requirement ID: [SRS-7-429]

The MG SHALL 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.

Requirement ID: [SRS-7-430]

The MG SHALL provide mechanisms that control a user's logical access to the Mail Guard and to explicitly deny access to specific users when appropriate.

7.8.2.3 Policy Enforcement Module

Requirement ID: [SRS-7-431]

The MG SHALL be capable of maintaining protection policy enforcement if it is unable to communicate with the Policy Enforcement module which provided it the policy.

Requirement ID: [SRS-7-432]

The MG SHALL enable the enforcement of information flows email messages.

Requirement ID: [SRS-7-433]

The MG SHALL enable the enforcement of content inspection of email messages.

Requirement ID: [SRS-7-434]

The MG SHALL validate the origin, integrity and binding [STANAG 4778] of a confidentiality label [STANAG 4774] to a data object before it is used.

Requirement ID: [SRS-7-506]

The MG SHALL validate a confidentiality label [STANAG 4774] against the corresponding SPIF before it is used.

7.8.2.4 Data Protection Module

Requirement ID: [SRS-7-435]

The MG Data Protection Module SHALL provide a NATO approved cryptographic sub-component 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].

Requirement ID: [SRS-7-436]

The MG Data Protection Module cryptographic sub-component SHALL be validated to at least FIPS 140-2 Level 2 [FIPS 140-2, 2001], or otherwise verified to an equivalent level of functionality and assurance by a NATO nation COMSEC authority.

Requirement ID: [SRS-7-437]

The MG Data Protection Module SHALL provide capability to protect against disclosing or transmitting information in violation of the policy.

Requirement ID: [SRS-7-438]

The MG SHALL provide mechanisms that mitigate attempts to exhaust its resources.

Requirement ID: [SRS-7-439]

The MG Data Protection Module SHALL provide capability to protect against gaining inappropriate access to one or more networks, endpoints, or services, such as through transmitting malicious executable code, scripts, or commands.

7.8.2.5 Protected Communications

Requirement ID: [SRS-7-440]

The MG SHALL ensure that is protection policy information is transmitted to the Policy Enforcement Module in a secure and timely manner so that there is assurance that the correct policy is being enforced.

Requirement ID: [SRS-7-441]

The MG SHALL ensure that communications are not subject to unauthorized modification or disclosure.

Requirement ID: [SRS-7-442]

The MG SHALL provide a means to ensure that administrators are not communicating with some other entity pretending to be the MG when supplying identification and authentication data.

7.8.2.6 Authentication

Requirement ID: [SRS-7-443]

The MG SHALL validate the identity of other peer entities prior to distributing data to them.

Requirement ID: [SRS-7-444]

The MG SHALL provide a means to detect and reject the replay of authentication data as well as other security data and attributes.

Requirement ID: [SRS-7-445]

The MG SHALL use a NPKI provided device certificate to validate its identity to other peer entities.

Requirement ID: [SRS-7-446]

The MG SHALL validate the identity of other peer identities by validating the peer entities device certificate to an NPKI trust point

7.8.2.7 Audit

Requirement ID: [SRS-7-447]

The MG SHALL provide measures for generating and storing audit information for security relevant events that will record access attempts to MG-protected resources by users.

7.8.2.8 Management

There are no Management security functional requirements identified for the Mail Guard.

7.8.2.9 Trusted Update

Requirement ID: [SRS-7-448]

The MG firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Requirement ID: [SRS-7-449]

The MG SHALL ensure the integrity of its update packages prior to installation.

8 Security Requirements

8.1 General

Requirement ID: [SRS-8-2]

Utilisation of modern IA techniques and compliancy with the cyber-defence services SHALL be followed.

8.2 Interconnection of Networks

Requirement ID: [SRS-8-3]

The IEG-C SHALL consider and apply the following directions, guidance and obligation within the INFOSEC technical and implementation directive for the interconnection of networks:

- AC/322-D(2004)0024-REV3-COR1 "CIS Security Technical and Implementation Directive on the NATO PKI Certificate Policy"
- AC/35-D/1021-REV3, dated 31 Jan 2012 "Guidelines for the security accreditation of communication and information systems (CIS)"
- AC/35 D/2004 Rev3 15 Nov 2013 "Primary Directive on CIS Security"
- AC/322-D/0047-REV2 (INV) 11 March 2009 "INFOSEC Technical & Implementation Directive on cryptographic security and cryptographic mechanisms"

8.3 Protection Profile

8.3.1 Applicability of Protection Profiles relevant for IEG-C

For the purposes of specifying the security requirements for an IEG-C an approach based upon the National Information Assurance Partnership (NIAP) Protection Profile (PP) scheme [NIAP] has been adopted. The IEG-C consists of a number of components to provide a solution for automated cross-domain information exchange between NATO Secret and NATO-led Mission Secret networks while offering the required level of assurance for the interconnection. These components have been identified and functionally specified in Section 4. NIAP contains a number of PPs that are applicable for IEG-C components as listed below:

- Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V.1.2, 2016]
- Protection Profile for General Purpose Operating Systems [NIAP PP_OS_V.4.1, 2016]
- Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP CPP_FW_V.1.0, 2015]
- Collaborative Protection Profile for Network Devices [NIAP CPP_ND_V.1.0, 2015]
- Collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) [NIAP PP_NDCP_IPP_EP_V.2.1, 2016]
- Standard Protection Profile for Enterprise Security Management Policy Management [NIAP PP_ESM_V.2.1, 2013]
- Standard Protection Profile for Enterprise Security Management Access Control [NIAP PP_ESM_AC_V.2.1, 2013]

To support industry in developing a commercial alternative to the NC3A Medium Assurance XML Labelling Guard, NATO developed a Common Criteria (CC) Protection Profile [NCIA TN-1485 v1.1, 2012]. The NATO PP can be used as a target specification for the implementation of a CC Evaluation Assurance Level (EAL) 4+ evaluation of commercial products that provide a Web Guard capability in an IEG-C.

The main purpose for specifying the security requirements based on the NIAP-approved PP scheme is to be able to re-use existing, up-to-date and agreed profiles in order to establish a consistent approach for describing the security requirements and evaluating the IEG-C capability to meet those security requirements. The security requirements have been developed as a result of analysing and assessing, from the NIAP and NATO PPs, the security objectives based on identified threats, assumptions and organizational security policies deemed applicable for an IEG-C capability and commensurate with the threats that may be active within the operational environment that the IEG-C will be deployed.

The PP scheme provides rationale whereby the PP illustrates how the security objectives are addressed by security functional requirements (SFRs). Each security requirement specified for the IEG-C will identify the security objectives detailed in Section 8.3.4 and list (by reference) the security functional requirements (SFRs), specified in the appropriate NIAP or NATO PP, relevant to that security requirement where applicable. It is not the intention to map all SFRs defined in each of the relevant PPs for the following reasons:

• The definitions for the PP Target of Evaluation (TOE) and the TOE Security Functionality (TSF) are influenced by assumptions within the IT operational environment defined in the TOE that may not be applicable to the IEG-C; and,
• SFRs may be defined for TSF components that do not exist in the IEG-C TOE.

The security requirements for specifying the security functionality required by the IEG-C are written in a manner that reflects the overall objective intended by an SFR. This means that SFRs that are too implementation-specific, for example an SFR that refers to a particular protocol and version that differs from the protocol version required to be supported by the IEG-C, are still relevant and can still be referenced without the need to rewrite the SFR.

8.3.2 Target of Evaluation (TOE) Overview

The IEG-C is composed of a number of IEG-C components that contain logical sub-components, providing overlapping capabilities for the IEG-C components, which have different relevance for enforcing the security functional requirements (SFRs). The logical sub-components are:

• Trusted Base Platform - consists of the operating system (OS) kernel, the tools and applications which are part of the OS, and the hardware, on which the OS runs.
• Policy Enforcement Module - central component for enforcing security requirements of the IEG-C. It is application software that implements the protection policies (IFPs and CIPs). This module provides functionality described by the Protection Policy Enforcement Services [NCIA TR/2016/NSE010871/01, 2017].
• Data Protection Module – helps to protect confidentiality, integrity and availability of the High Domain. The Data Protection Module provides functionality to process cryptographically protected data and implement specific scanning for malicious contents. This module includes the capabilities described for the PKE and Malware Scanner modules as specified in [NCIA TN-1485 v1.1, 2012] and provides the functionality described by the Protection Services [[NCIA TR/2016/NSE010871/01, 2017].

The TOE Security Functionality (TSF) of the TOE (illustrating the IEG-C components and the relationships with the logical sub-components) is highlighted in Figure 22 for an IEG-C .
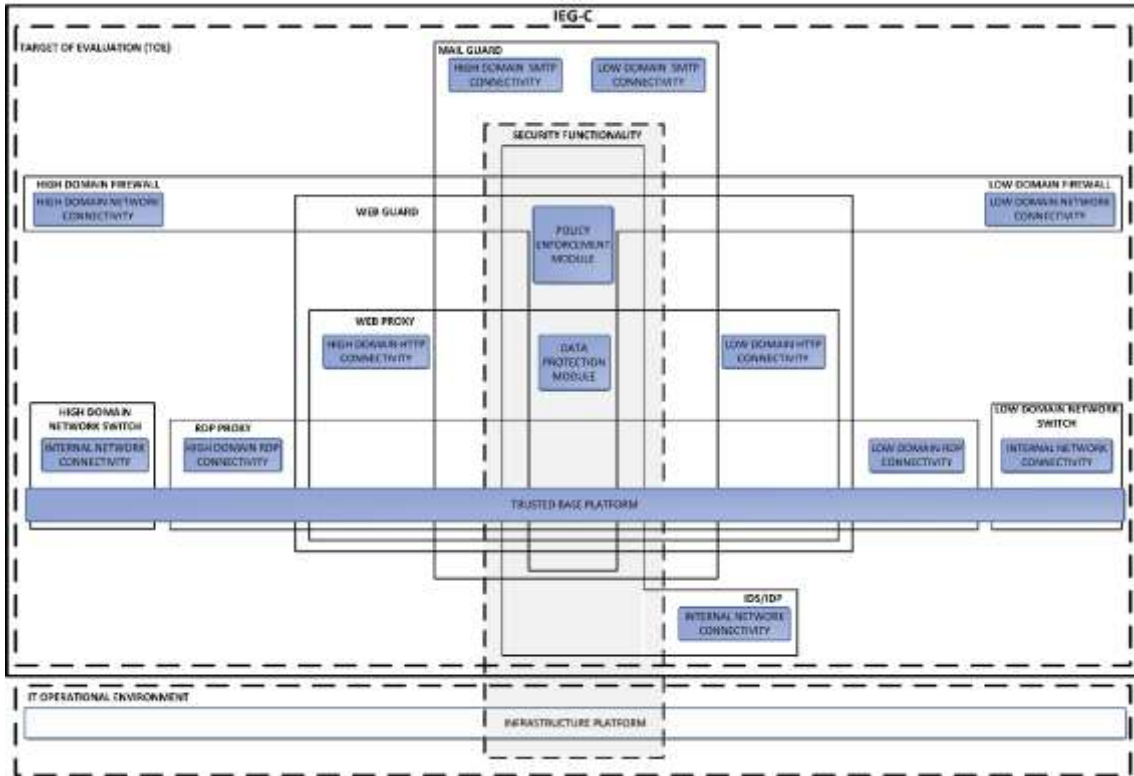
Figure 29 TOE, TSF and Operational Environment for a static IEG-C

Figure 22 illustrates the Infrastructure Platform component as part of the TSF provided by the operational environment.

Table 16 below lists the sub-components that are part of the TSF for a static IEG-C and illustrates which IEG-C components, provided as a part of the TOE, relates to those sub-components.

Table 23 IEG-C TSF sub-components for static and deployed IEG-C

	Trusted Base Platform	Policy Enforcement Module	Data Protection Module
High Domain Firewall	X	X	X
Low Domain Firewall	X	X	X
High Domain Network Switch	X		
Low Domain Network Switch	X		
RDP Proxy	X		
Web Proxy	X		X
Web Guard	X	X	X

	Trusted Base Platform	Policy Enforcement Module	Data Protection Module
Mail Guard	X	X	X
Intrusion Detection / Prevention System	X	X	X
Management	X	X	X

8.3.3 Security Problem Definition

8.3.3.1 Threats

The security threats identified in Appendix C.1.1 SHALL be addressed by the TOE or its operational environment.

8.3.3.2 Assumptions

The specific conditions identified in Appendix C.1.2 are assumed to exist in a PP-compliant TOE environment.

8.3.3.3 Organizational Security Policies

Appendix C.1.3 lists applicable Organizational Security Policies (OSPs) provided.

8.3.4 Security Objectives

Appendix C.2 describes the Security Objectives and the associated security functional requirements (SFRs) that address the Security Objectives.

8.3.5 Security Functional Requirements

If applicable, for each security requirement the source(s) from the PPs is identified (the associated SFRs are referenced through the relationship with the Security Objectives listed in Appendix C.2). The security requirements are categorised into the logical sub-components identified in the TSF and IT operational environment, and the underlying functionality that the TOE provides, as illustrated in Figure 24. Each security requirement identifies to which IEG-C component(s) the requirement is applicable.
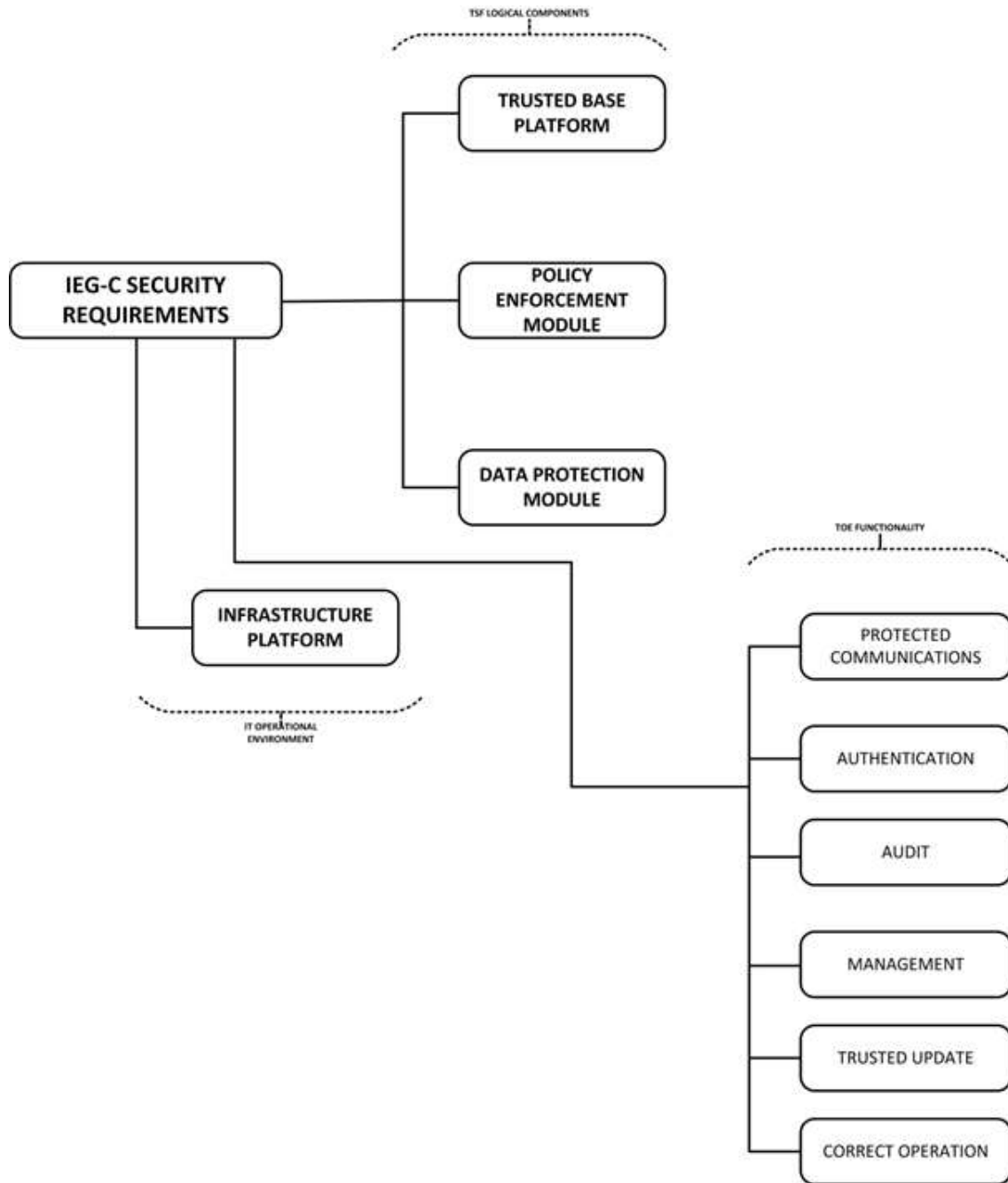
Figure 30 Graphical representation of security requirements to TSF and IT Operational Environment components and TOE functionality

8.3.5.1 Infrastructure Platform

Table 24 Infrastructure Platform: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-1] The IEG-C SHALL be located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the IEG-C.	A.PHYSICAL_PROTECTION A.PHYSICAL_ACCESS_MANAGED OE.PHYSICAL_ACCESS_MANAGED	X								
Requirement ID: [SRS-8-51] The Infrastructure Platform SHALL provide a NATO approved malware scanning capability [NC3B AC/322-D(2004)0019 (INV), 2004].	P.ANALYZE OE.MALWARE_SCANNER OE.ROBUST								X	
Requirement ID: [SRS-8-52] The Infrastructure Platform SHALL provide capability to ensure that only authorized communications are allowed between the high and low networks.	OE.NO_TOE_BYPASS OE.CONNECTIONS		X							

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-4] The Infrastructure Platform SHALL provide reliable time data to the IEG-C.	OE.SYSTIME	X								

8.3.5.2 Trusted Base Platform (TBP)

Table 25 Trusted Base Platform: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-5] The IEG-C is a distributed system, therefore, the TBP SHALL implement measures to protect against eavesdropping between components of the IEG-C that are distributed.	A.PLATFORM O.TRUSTED_COMMUNICATIONS O.TRUSTED_PATH O.DATAPROT	X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-6] The TBP consists of hardware (processors, memory, and devices), firmware and the operating system(s). The TBP SHALL be configured according to relevant NATO guidance and directives [NAC AC/322-D/0048-REV3, 2019]		X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-7] The TBP SHALL protect components and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.	O.ACCESSID O.AUTH	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-8] The TBP SHALL 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.	O.PROTECTED_STORAGE O.ACCESSID O.AUTH	X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-9] The TBP SHALL provide reliable time data to all components of the IEG-C.		X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-10] The TBP SHALL provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	O.TOE_ROBUST_ACCESS	X	X	X	X	X	X	X	X	X

8.3.5.3 Policy Enforcement Module

Table 26 Policy Enforcement Module: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-11] The IEG-C SHALL be able to recognize and discard invalid or malicious input provided by users.	O.OFLOWS	X								X
Requirement ID: [SRS-8-12] The IEG-C SHALL be capable of maintaining protection policy enforcement if it is unable to communicate with the Policy Enforcement module which provided it the policy.	O.MAINTAIN	X	X				X	X	X	
Requirement ID: [SRS-8-13] The IEG-C SHALL provide a mechanism to identify and rectify contradictory policy data.	O.CONSISTENT	X								X
Requirement ID: [SRS-8-14] The IEG-C SHALL enable enforcement of information flow between the IEG-C components.	O.MEDIATE_FLOW O.MESSAGE_VETTING	X	X				X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-15] The IEG-C SHALL enable enforcement of content inspection between the IEG-C components.	O.REVERSE_PROXY O.MINIMAL_PROXY O.MESSAGE_VETTING	X	X				X	X	X	X
Requirement ID: [SRS-8-16] The IEG-C SHALL validate the origin, integrity and binding [STANAG 4778 of a security label [STANAG 4774] to a data object before it is used.	O.VALID_LABEL	X					X	X		

8.3.5.4 Data Protection Module

Table 27 Data Protection Module: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-17] The Data Protection Module SHALL provide a NATO approved cryptographic sub-component 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 A.PKI_NATO_COMPLIANT O.CRYPTO_NATO_APPROVED	X	X	X		X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-18] The Data Protection Module cryptographic sub-component is validated according validated to at least FIPS 140-2 Level 2 [FIPS 140-2, 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 A.PKI_NATO_COMPLIANT	X	X	X		X	X	X	X	X
Requirement ID: [SRS-8-19] The Data Protection Module SHALL provide capability to protect against network-based reconnaissance (probing for information about a monitored network or its endpoints), such as through use of various scanning or mapping techniques. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	O.SYSTEMT_MONITORING O_ANALYZE O_REACT OE.MALWARE_SCANNER	X							X	

NATO UNCLASSIFIED

IFB-CO-14314-IEG-C
Book II – Part IV SOW Annex A SRS

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-20] The Data Protection Module SHALL provide capability to protect against attacks that are targeted at obstructing the normal function of monitored networks, endpoints, or services, such as through denial of service attacks. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	O.SYSTEMT_MONITORING O_ANALYZE O_REACT OE.MALWARE_SCANNER	X							X	
Requirement ID: [SRS-8-21] The Data Protection Module SHALL provide capability to protect against disclosing or transmitting information in violation of the policy.	O.VALID_LABEL	X					X	X		
Requirement ID: [SRS-8-22] The IEG-C SHALL apply analytical processes to network traffic data collected from monitored networks and derive conclusions about potential intrusions or network traffic policy violations.	O.ANALYZE	X							X	X

NATO UNCLASSIFIED

Book II, Part IV SOW Annex A, Page 255

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-23] The IEG-C shall provide mechanisms that mitigate attempts to exhaust resources provided by the TOE (e.g., resulting in denying access to high network resources).	O.RESOURCE_SHARING	X					X	X	X	
Requirement ID: [SRS-8-24] The Data Protection Module SHALL provide capability to protect against gaining inappropriate access to one or more networks, endpoints, or services, such as through transmitting malicious executable code, scripts, or commands. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	O.SYSTEMT_MONITORING O_ANALYZE O_REACT OE.MALWARE_SCANNER	X					X	X	X	

8.3.5.5 Protected Communications

Table 28 Protected Communications: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-25]	O.DISTRIB	X	X				X	X	X	X

Requirement	Objective									
The IEG-C SHALL ensure that is protection policy information is transmitted to the Policy Enforcement Module in a secure and timely manner so that there is assurance that the correct policy is being enforced.										
Requirement ID: [SRS-8-26] The IEG-C SHALL ensure that communications between distributed components of the TOE are not subject to unauthorized modification or disclosure.	O.TRUSTED_COMMUNICATIONS	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-27] The IEG-C SHALL provide a means to ensure that administrators are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.	O.TRUSTED_PATH	X	X	X	X	X	X	X	X	X

8.3.5.6 Authentication

Table 29 Authentication: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-28] The IEG-C SHALL provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.	O.AUTH	X								X
Requirement ID: [SRS-8-29] The IEG-C SHALL contain the ability to validate the identity of other TOE components prior to distributing data to them.	O.ACCESSID	X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-30] The IEG-C SHALL provide a means to detect and reject the replay of authentication data as well as other TSF data and security attributes.	O.REPLAY_DETECTION	X					X	X		

8.3.5.7 Audit

Table 30 Audit: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-31] The IEG-C SHALL provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.	O.AUDIT_GENERATION	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-32] The IEG-C shall provide the capability to protect audit information.	O.AUDIT_PROTECTION	X								X

8.3.5.8 Management

Table 31 Management: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-36] The IEG-C SHALL provide an administrator role to isolate administrative actions, and to make the administrative functions available locally and remotely.	O.ADMIN_ROLE	X								X
Requirement ID: [SRS-8-37] The IEG-C SHALL provide all the functions and facilities necessary to support the administrators in their management of the security of the IEG-C, and restrict these functions and facilities from unauthorized use.	O.MANAGE	X								X
Requirement ID: [SRS-8-38] The IEG-C SHALL display an advisory warning regarding use of the IEG-C.	O.DISPLAY_BANNER	X								X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-39] The configuration of, and all changes to, the IEG-C and its development evidence SHALL be analysed, tracked, and controlled throughout the IEG-C's development.	O.CHANGE_MANAGEMENT	X								X
Requirement ID: [SRS-8-40] The IEG-C SHALL provide a mode from which recovery or initial start-up procedures can be performed.	O.MAINT_MODE	X								X
Requirement ID: [SRS-8-41] The IEG-C SHALL collect and store information about all events that may indicate a policy violation related to misuse, inappropriate access, or malicious activity on monitored networks.	O.SYSTEM_MONITORING	X								X

8.3.5.9 Trusted Update

Table 32 Trusted Update: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-42] The Infrastructure Platform firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	A.REGULAR_UPDATES OE.UPDATES	X	X						X	
Requirement ID: [SRS-8-50] The IEG-C firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	A.REGULAR_UPDATES O.UPDATES	X	X	X	X	X	X	X	X	

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-43] The IEG-C SHALL ensure the integrity of their update packages. OSs are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant IEG-Cs provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.	O.INTEGRITY	X	X	X	X	X	X	X	X	

8.3.5.10 Correct Operation

Table 33 Correct Operation: requirements, sources (including SFRs, if applicable) and applicability to IEG-C components

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-44] The IEG-C SHALL provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.		X	X	X	X	X	X	X	X	X

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
Requirement ID: [SRS-8-45] The IEG-C SHALL undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE does not allow attackers with medium attack potential to violate the TOE's security policies.	O.VULNERABILITY_ANALYSIS	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-46] The IEG-C SHALL undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.	O.THOROUGH_FUNCTIONAL_ TESTING	X	X	X	X	X	X	X	X	X
Requirement ID: [SRS-8-47] The IEG-C SHALL respond appropriately to its analytical conclusions about policy violations.	O.REACT	X							X	
Requirement ID: [SRS-8-48] The IEG-C SHALL ensure that any information contained in a protected resource is	O.RESIDUAL_INFORMATION	X	X				X	X	X	

Requirement	Sources	IEG-C	Firewall	Network Switch	RDP Proxy	Web Proxy	Web Guard	Mail Guard	IDS	Management
not released when the resource is reallocated; this includes that no residual information from a previously relayed message is transmitted.										
Requirement ID: [SRS-8-49] The TSF SHALL maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure.	O.SELF_PROTECTION	X	X				X	X		

9 Management Requirements

9.1 General

The management of the IEG-C can be categorised into the following categories for providing the functionality required to be supported by the IEG-C administrators performing the different administrative management roles (further specified in [SRS-3-24]):

- Service Management and Control (SMC);
- Communications and Information (CIS) Security; and,
- Cyber Defence.

Requirement ID: [SRS-9-1]

All Management capabilities MUST provide support for multiple concurrent administrators with access control to enable simultaneous access to the management capability from potentially distributed consoles with appropriately administered levels of access.

Requirement ID: [SRS-9-2]

Figure 32 illustrates the interfaces that MUST be provided by the IEG-C for managing the IEG-C remotely and locally.
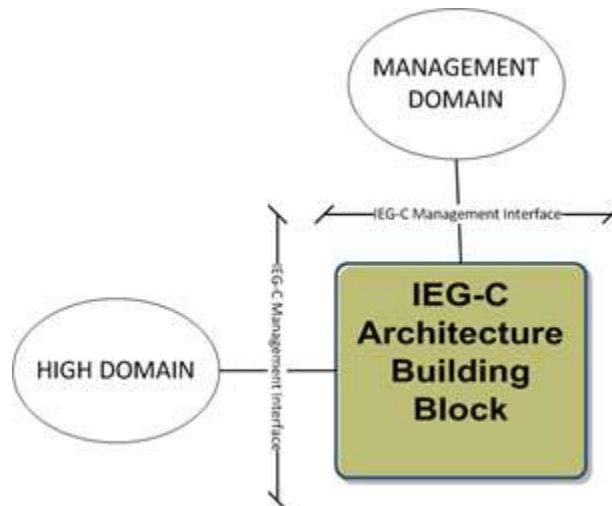
Figure 31 Management Interfaces exposed by IEG-C ABB

Requirement ID: [SRS-9-3]

The IEG-C MUST provide the capability to be managed remotely from a central location on the HIGH DOMAIN.

Requirement ID: [SRS-9-4]

To support remote management from a central location the IEG-C MUST offer the physical (or logical) IEG-C Management Interface implemented on top of the IEG-C High Domain Interface as described in Section 3.2.

Requirement ID: [SRS-9-5]

The IEG-C MUST provide the capability to be managed locally.

Requirement ID: [SRS-9-6]

To support local management the IEG-C MUST offer a physical network interface providing Ethernet connectivity to the management users on a separate security domain depicted as the MANAGEMENT DOMAIN in Figure 32

Requirement ID: [SRS-9-7]

The IEG-C Management Interface MUST support the operation 'ReceiveNetworkManagement' as specified in [NCIA TR/2016/NSE010871/01, 2017] section A.2.2.3.

Requirement ID: [SRS-9-8]

The IEG-C Management Interface MUST support the operation 'ForwardNetworkManagement' as specified in [NCIA TR/2016/NSE010871/01, 2017] section A.2.2.3.

Requirement ID: [SRS-9-9]

The IEG-C Management Interface SHALL be managed using one or more of the following protocols:

- HyperText Transport Protocol (HTTP) [IETF RFC 7230, 2014];
- Secure Shell Protocol (SSH) [IETF RFC 4251, 2006];
- Remote Desktop Protocol;
- Keyboard, Video and Mouse (KVM) over Ethernet;
- Simple Network Management Protocol (SNMP) v3 [IETF RFC 3410 – 3418, 2002].

Requirement ID: [SRS-9-10]

Remote Management traffic MUST be encrypted.

Requirement ID: [SRS-9-11]

The IEG-C Management Interface MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).

Requirement ID: [SRS-9-12]

The IEG-C Management Interface MUST support Datagram Transport Layer Security (DTLS, [IETF RFC 6353, 2011]).

Requirement ID: [SRS-9-13]

The IEG-C MUST offer the 'Communications Access Management' Interface on top of the IEG-C Management interface.

Requirement ID: [SRS-9-14]

The IEG-C MUST offer the 'Core Services Management' Interface on top of the 'Communications Access Management' Interface

Requirement ID: [SRS-9-15]

The IEG-C MUST support the 'ReceiveManagementContent' operation to provide connectivity for administrators on the MANAGEMENT DOMAIN.

Requirement ID: [SRS-9-16]

The operation 'ReceiveManagementContent' SHALL pass management content to the appropriate interface (see Sections 9.2, [SRS-9-83] and [SRS-9-98]).

Requirement ID: [SRS-9-17]

The IEG-C MUST support the 'ForwardManagementContent' operation that forwards management traffic to the MANAGEMENT DOMAIN.

Requirement ID: [SRS-9-18]

After receiving management content from the appropriate interface (see Sections 9.2, [SRS-9-83] and [SRS-9-98].), the operation 'ForwardManagementContent' SHALL forward the management content to the MANAGEMENT DOMAIN.

9.2 Service Management and Control

9.2.1 Management and Control functions

Effective management of the IEG-C and its services is critical. The ability to monitor and manage IEG-C services' performance and availability, configure and control IEG-C services for automating and improving end-to-end processes cross domain is a core capability provided by the IEG-C.

The IEG-C Element Management Services provide a suite of capabilities needed to facilitate Service Management and Control (SMC) Services and ensure that the Data Exchange Services, Protection Policy Enforcement Protection Services, and Protection Services are up and running, are accessible and available and that they are operating performing within agreed upon Quality of Service and Service Level Agreement (SLA) parameters for the IEG-C.

The IEG-C Element Management Services provide the following management and control functions:

- Configuration Management
- Event Management (including Logging, Alerting and Reporting)
- Performance and Capacity Management (including Monitoring, Metering and Message Tracking)

9.2.2 Configuration Management

In ITIL terms, Configuration Management is the process responsible for maintaining information about the Configuration Items (CI) required to deliver a Service, including their Relationships with one another. This information is managed throughout the lifecycle of the CI, and it typically stored in a Configuration Management Database (CMDB).

The Configuration Management process is most concerned with configuring, deploying and later decommissioning Data Exchange Services and Protection Services and their supporting platform. The IEG-C needs to provide the ability to change, capture, duplicate, backup or restore the configuration of the Data Exchange Services and Protection Services. The IEG-C needs to provide the ability to manage the operating systems that the IEG-C services are running on.

Requirement ID: [SRS-9-19]

An Enterprise CMDB already exists, and SHALL be used as the underpinning of the Platform's configuration management as well.

Requirement ID: [SRS-9-20]

The IEG-C SHALL support the Enterprise Configuration Management via an interface with the Enterprise configuration management database (BMC ITSM Atrium CMDB) to track IEG-C assets and their configuration information.

Requirement ID: [SRS-9-21]

The IEG-C MUST offer an interface 'SMC Configuration Management' that accepts an incoming 'SMC Message' for further processing.

Requirement ID: [SRS-9-22]

The 'SMC Configuration Management' Interface MUST provide the capability to manage the underlying operating system(s) hosting all the services provided by the IEG-C.

Requirement ID: [SRS-9-23]

The 'SMC Configuration Management' Interface MUST provide the capability to configure, deploy and decommission Data Exchange Services depending upon the information exchange requirement(s) that is (are) being supported.

Requirement ID: [SRS-9-24]

The 'SMC Configuration Management' Interface MUST provide the capability to configure, deploy and decommission Protection Services depending upon the information exchange requirement(s) that is (are) being supported.

Requirement ID: [SRS-9-25]

The 'SMC Configuration Management' Interface MUST provide the capability to provides the ability to change, capture, duplicate, backup or restore the configuration of the Protection Policy Enforcement Services depending upon the information exchange requirement(s) that is (are) being supported.

Requirement ID: [SRS-9-26]

The 'SMC Configuration Management' Interface MUST support the following operations:

- 'Configure OS';
- 'Configure Data Exchange Services';
- 'Configure Protection Services'; and,
- 'Configure Protection Policy Enforcement Services'.

Requirement ID: [SRS-9-27]

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]);
- Remote Desktop Protocol (RDP);
- Intelligent Platform Management Interface (IPMI, [IPMI V2.0, 2013]);

- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).

Requirement ID: [SRS-9-28]

The operation 'Configure OS' SHALL support the management of the IEG-C hardware (virtual or physical) and software resources including configuration of common services provided by the operating system (OS) for applications running on the operating system. These common services include application execution, input/output operations, file system, communication, resource allocation, control access to OS resources and time synchronisation.

Requirement ID: [SRS-9-29]

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]).

Requirement ID: [SRS-9-30]

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-9-31]

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]).

Requirement ID: [SRS-9-32]

The IEG-C 'SMC Configuration Management' Interface SHALL pass outgoing SMC Messages to the interface 'Core Services Management' for further processing.

9.2.3 Event Management

In ITIL terms, an "event" can be defined as any detectable or discernible occurrence that has significance for the management of the infrastructure or the delivery of a Service. Event Management is the process that monitors all events that occur throughout the Platform. It allows for normal operation, but also detects and escalates exception conditions.

For the Platform, Event Management includes:

- Logging,
- Alerting
- Reporting

Requirement ID: [SRS-9-34]

The IEG-C SHALL collect events generated from all IEG-C services and forward them to the Enterprise Event Management System.

Requirement ID: [SRS-9-35]

The IEG-C SHOULD support monitoring based on the Microsoft System Center Operations Manager (SCOM).

Requirement ID: [SRS-9-36]

The IEG-C SHALL support SNMP v3 [IETF RFC 3412, 2002] with standards-based and proprietary-specific Management Information Bases (MIBs).

Requirement ID: [SRS-9-37]

The IEG-C SHALL provide a toolset which allows Administrators to define, filter, correlate and group events according to their context, criticality, source and impacts.

Requirement ID: [SRS-9-38]

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

Requirement ID: [SRS-9-39]

The IEG-C MUST offer an interface 'SMC Event Management' that accepts an incoming 'SMC Message' for further processing.

Requirement ID: [SRS-9-40]

The 'SMC Event Management' Interface MUST support the following operations:

- 'Log';
- 'Alert'; and,
- 'Report'.

9.2.3.1 Logging

Logging is the act of keeping a log, which is a file that records either events that occur in software or messages between different users. In the simplest case, messages are written to a single log-file.

Requirement ID: [SRS-9-41]

The IEG-C SHALL support Data Exchange Services logging for monitoring access requests for information from both the High Domain and the Low Domain.

Requirement ID: [SRS-9-42]

The IEG-C SHALL provide the capability to examine recorded historical logs and archives.

Requirement ID: [SRS-9-43]

The IEG-C 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-9-44]

The IEG-C SHALL log request and response attributes to include:

- time-stamp;
- source and target address(es);
- URL;
- Operation;
- Size; and
- Unique request id (extracted from the request/response or automatically generated by the IEG-C Logging Services).

Requirement ID: [SRS-9-45]

The IEG-C SHALL also provide functionality to log attributes extracted from the payload.

Requirement ID: [SRS-9-46]

The IEG-C SHALL provide functionality to log selectively whole messages based on pre-configured criteria or filter (e.g. policy based).

Requirement ID: [SRS-9-47]

The IEG-C SHALL provide a log analysis tool that allows a search for log events based on combinations of search criteria across all fields in the log record format supported by this system.

Requirement ID: [SRS-9-49]

The IEG-C SHALL provide the capability to aggregate generated log messages for all instances of services of IEG-C.

Requirement ID: [SRS-9-50]

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

- Syslog Message [IETF RFC 5424, 2009]; and,
- Hypertext Transport Protocol Message (HTTP/1.1, [IETF RFC 7230, 2014], HTPP/2.0 [IETF RFC 7540, 2015]).

Requirement ID: [SRS-9-51]

The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Log' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.3.2 Alerting

The IEG-C and the services hosted on it, will have certain expectations of service availability, performance, security and other parameters. These may be expressed as Key Performance Indicators (KPI), Service Level Agreements (SLA) or other metrics.

The Alerting functionality of the IEG-C SMC capability is closely tied to the Monitoring functionality, in which the "health" of the system is continually evaluated. In all cases, when the acceptable threshold for a service (or the IEG-C) is detected to be approaching or reached, the system will automatically generate an Alert event.

An Alert can either be a:

- "Warning" (indicating that it is necessary to take action in order to prevent an exception occurring); or,
- "Exception" (indicating that the service is currently operating below the normal predefined parameters/indicators)

While this functionality is closely related to the Event Management system, there are some unique requirements for the IEG-C, including the ability to alert on intrusion attacks.

Requirement ID: [SRS-9-52]

The IEG-C SHALL provide a toolset to configure rule based event filtering, and to automate alert triggering capabilities.

Requirement ID: [SRS-9-53]

The IEG-C SHALL provide functionality to generate alerts associated with IEG-C services to include:

- breach of performance or capacity thresholds;
- SLAs can't be met; and
- specific mechanisms to enforce SLAs were activated (e.g. throttling).

Requirement ID: [SRS-9-54]

The IEG-C SHALL provide functionality to generate an alert about stalled processes (e.g. a compromised content filter).

Requirement ID: [SRS-9-55]

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

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]
- Syslog [IETF RFC 5424, 2009];

Requirement ID: [SRS-9-56]

The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Alert' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.3.3 Reporting

An SMC system needs to provide thorough, highly customizable reports for compliance, auditing, billing, service value determination, and so on.

The Reporting component is distinct from the Monitoring component in that Monitoring occurs in real time, while Reporting (usually) happens *post facto.*

Requirement ID: [SRS-9-57]

The IEG-C SHALL provide operational and historical reports on events.

Requirement ID: [SRS-9-58]

The IEG-C SHALL provide a toolset allowing for custom report building and saving.

Requirement ID: [SRS-9-59]

The IEG-C SHALL be able to generate

- 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-9-60]

The IEG-C SHALL be able to provide performance trend analysis.

Requirement ID: [SRS-9-61]

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

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]
- Comma Separated Values (CSV)

Requirement ID: [SRS-9-62]

The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Report' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.4 Performance and Capacity Management

In order to be able to identify problems and bottlenecks in the network or service infrastructure the need for sophisticated traffic monitoring and performance analysis platform was identified. The IEG-C System Administrators require insight into basic performance parameters, including network utilization levels (instantaneous, peak, average or trends), statistics on the collected traffic (protocol distribution, to/from information, packet lengths or errors), network response times and measured throughputs, error counters of interfaces etc.

Such a capability will provide immediate identification of potential bottlenecks or outages, and enable the IEG-C System Administrators to take proactive measures to circumvent

bottlenecks or to throttle down low priority traffic in case overall bandwidth is not sufficient to satisfy all communication requirements.

For the Platform, Performance and Capacity Management includes:

- Monitoring
- Metering

Requirement ID: [SRS-9-63]

The IEG-C MUST offer an interface 'SMC Performance Management' that accepts an incoming 'SMC Message' for further processing.

Requirement ID: [SRS-9-64]

The 'SMC Performance Management' Interface MUST support the following operations:

- 'Monitor'; and
- 'Meter';

9.2.4.1 Monitoring

Monitoring observes and tracks the operations and activities of end users on the IEG-C, thus providing a way to supervise the overall processes that are performed.

Requirement ID: [SRS-9-65]

The IEG-C SHALL monitor the status and quality of service, (including availability, performance, and utilisation) of the IEG-C infrastructure and the IEG-C Services hosted on the IEG-C.

Requirement ID: [SRS-9-66]

The IEG-C SHALL provide functionality for real time monitoring of IEG-C Services against expected KPI, SLA, or other metric thresholds as configured.

Requirement ID: [SRS-9-67]

The IEG-C SHALL provide visibility on usage patterns over daily, monthly and variable periods. This toolset shall support trend and abnormal behaviour analysis.

Requirement ID: [SRS-9-68]

The IEG-C SHALL provide customizable dashboards for monitoring selected statistics and metrics for IEG-C services.

Requirement ID: [SRS-9-69]

The IEG-C SHALL provide the capability to monitor requests for information access attempts cross domain through the IEG-C services.

Requirement ID: [SRS-9-70]

The IEG-C SHALL provide functionality to monitor service faults and exceptions.

Requirement ID: [SRS-9-71]

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

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]

Requirement ID: [SRS-9-72]

The IEG-C 'SMC Performance Management' Interface SHALL pass outgoing 'Monitor' SMC Messages to the interface 'Core Services Management' for further processing.

9.2.4.2 Metering

Metering measures levels of resource utilization consumed by service subscribers. Measured data is stored for summarizing and analysing.

Requirement ID: [SRS-9-73]

The IEG-C SHALL be able to collect and present the statistics on service utilisation broken down by end user or system which can be used for metering, billing and other purposes.

Requirement ID: [SRS-9-74]

The IEG-C SHALL aggregate collected statistics for a given end user or system or group of end user or system over specified periods of time.

Requirement ID: [SRS-9-75]

The IEG-C SHALL archive and make available for retrieval and reporting collected and aggregated statistics.

Requirement ID: [SRS-9-76]

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

- Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]

Requirement ID: [SRS-9-77]

The IEG-C 'SMC Performance Management' Interface SHALL pass outgoing 'Meter' SMC Messages to the interface 'Core Services Management' for further processing.

9.3 CIS Security Management

Requirement ID: [SRS-9-78]

The IEG-C SHALL provide the capability to allow the CIS Security Administrator to fulfil their role.

Requirement ID: [SRS-9-79]

The IEG-C MUST offer an interface 'CIS Security' that accepts an incoming 'CIS Security Message' for further processing.

Requirement ID: [SRS-9-80]

The 'Cyber Defence' Interface MUST support the following operations:

- 'Manage Public Key Material';
- 'Manage Protection Policies'; and,
- 'Review'.

9.3.1 Manage Public Key Material

Requirement ID: [SRS-9-81]

The IEG-C SHALL provide the Security administrator the ability to perform all necessary functions regarding the management of cryptographic key material.

Requirement ID: [SRS-9-82]

The management of key material SHALL be compliant with CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-9-84]

The IEG-C 'CIS Security' Interface SHALL pass outgoing 'Manage Public Key Material' CIS Security Messages to the interface 'Core Services Management' for further processing.

9.3.2 Manage Protection Policies

Requirement ID: [SRS-9-85]

The IEG-C SHALL provide the capability for a Security administrator to manage the full lifecycle of the Information Flow Control Policies and the Content Inspection Policies that are required to be enforced by the Protection Policy Enforcement Services dependent upon the information exchange requirements.

Requirement ID: [SRS-9-86]

The IEG-C SHALL provide the capability to support the creation, modification and deletion of the protection policies including the activation and de-activation of those protection policies.

Requirement ID: [SRS-9-87]

The IEG-C 'Manage Protection Policies' operation SHALL also support backing up and restoring of policies.

Requirement ID: [SRS-9-88]

The IEG-C SHALL provide the Security administrator with the capability to manage the Protection Services with tasks such as update IDS signatures, anti-virus signatures, manage content filters and patch hardware and software.

Requirement ID: [SRS-9-200]

The patching of IEG-C components SHAL be performed centrally from the Service Operation Centre (SOC).

Requirement ID: [SRS-9-89]

The operation 'Manage Protection Policies' SHALL support CIS Security Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-90]

The IEG-C 'CIS Security' Interface SHALL pass outgoing 'Manage Protection Policies' CIS Security Messages to the interface 'Core Services Management' for further processing.

9.3.3 Review

Requirement ID: [SRS-9-91]

The IEG-C SHALL provide the capability to the Audit manager to review audit logs.

Requirement ID: [SRS-9-92]

The operation 'Review' SHALL support CIS Security Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

9.4 Cyber Defence Management

Requirement ID: [SRS-9-93]

The IEG-C SHALL provide the capability to allow the Cyber Defence Administrator to fulfil their role.

Requirement ID: [SRS-9-94]

The IEG-C MUST offer an interface 'Cyber Defence' that accepts an incoming 'Cyber Defence Message' for further processing.

Requirement ID: [SRS-9-95]

The 'Cyber Defence' Interface MUST support the following operations:

- 'Assess';
- 'Respond'; and,
- 'Recover'.

9.4.1 Assess

Requirement ID: [SRS-9-96]

The IEG-C SHALL provide the Cyber Defence administrator with the capability to assess damage and attacks/faults identifying IEG-C components that have been affected by attacks and faults.

Requirement ID: [SRS-9-97]

The IEG-C SHALL support analysis and evaluation of attacks.

Requirement ID: [SRS-9-201]

For all its components the IEG-C SHALL support the generation 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-9-98]

For all its components the IEG-C SHALL 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-9-202]

For all its components the IEG-C SHALL support the ingestion of cybersecurity-related log, alert, and event data in the SIEM solution that is operated by NCSC.

Requirement ID: [SRS-9-203]

For all its components the IEG-C SHALL ensure that all cybersecurity-related log, alert, and event data can be parsed correctly by the SIEM solution that is operated by NCSC.

Requirement ID: [SRS-9-99]

The operation 'Assess' SHALL support Cyber Defence Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-100]

The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Assess' Cyber Defence Messages to the interface 'Core Services Management' for further processing.

9.4.2 Respond

Requirement ID: [SRS-9-101]

The IEG-C SHALL provide the Cyber Defence administrator with the required functionality to take the required action to dynamically mitigate the risk identified by a suspected attack/fault.

Requirement ID: [SRS-9-102]

The IEG-C SHALL provide the capability to control traffic flows including termination, throttling to a certain level of bandwidth or with a certain delay, redirection, or otherwise modify the flow for the purpose of stopping or mitigating an attack or fault.

Requirement ID: [SRS-9-103]

The IEG-C SHALL provide capability for traffic flows to be terminated or limited in capacity in order to stop or reduce the effect of an attack or a fault.

Requirement ID: [SRS-9-105]

The operation 'Respond' SHALL support Cyber Defence Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-106]

The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Respond' Cyber Defence Messages to the interface 'Core Services Management' for further processing.

9.4.3 Recover

Requirement ID: [SRS-9-107]

The IEG-C SHALL provide the Cyber Defence administrator with the required functionality to take the required action to recover from an attack/fault.

Requirement ID: [SRS-9-108]

The IEG-C SHALL provide the capability to restore IEG-C components that were affected by an attack/fault.

Requirement ID: [SRS-9-109]

The operation 'Recover' SHALL support Cyber Defence Messages of the following types:

- Secure Shell (SSH, [IETF RFC 4253, 2006]);
- Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]);
- HTTP over TLS ([IETF RFC 2818, 2000]).

Requirement ID: [SRS-9-110]

The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Recover' Cyber Defence Messages to the interface 'Core Services Management' for further processing.

9.5 Audit Management

Requirement ID: [SRS-9-111]

The IEG-C SHALL provide the capability to allow the Audit Administrator to fulfil their role.

Requirement ID: [SRS-9-112]

The IEG-C SHALL be interoperable with NATO auditing and system management tools.

Requirement ID: [SRS-9-113]

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

Requirement ID: [SRS-9-114]

The IEG-C 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-9-115]

The IEG-C SHALL provide the capability to appropriately classify and protect audit information in accordance with NATO security policy.

Requirement ID: [SRS-9-116]

The IEG-C SHALL include mechanisms to protect audit logs from unauthorised access, modification and deletion.

Requirement ID: [SRS-9-117]

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

Requirement ID: [SRS-9-118]

The IEG-C SHALL provide reliable time stamps and the capability for the Audit Administrator to set the time used for these time stamps.

Requirement ID: [SRS-9-119]

The IEG-C SHALL generate and maintain an audit log for each of the general auditable events:

- IEG-C start-up and shutdown
- IEG-C 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
- Creation, modification or deletion of audit log records
- Invocation of privileged operations
- Modification to IEG-C access rights
- Unauthorised attempts to access IEG-C system files

Requirement ID: [SRS-9-204]

All audit logs SHALL record the date, time, details of change and the user.

Requirement ID: [SRS-9-120]

The IEG-C SHALL generate and maintain an audit log for each of the 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-9-121]

The IEG-C SHALL generate and maintain an audit log for each of the 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 Intrusion Detection Services IDS signatures
- Updates of Content Inspection Services content filters
- Failed certificate path validation and revocation

Requirement ID: [SRS-9-122]

The IEG-C SHALL generate and maintain an audit log for each of the 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-9-123]

The IEG-C SHALL archive the audit log after a period of time as configured by the Audit Administrator.

Requirement ID: [SRS-9-124]

By default the audit log SHALL be archived daily.

Requirement ID: [SRS-9-125]

The IEG-C SHALL automatically back up audit logs at configurable intervals.

Requirement ID: [SRS-9-126]

The IEG-C SHALL provide integrity checking countermeasures to ensure that the audit log has been archived correctly.

Requirement ID: [SRS-9-127]

The IEG-C SHALL alert the Audit Administrator when the audit log exceeds a configurable percentage of the configurable maximum permitted size.

Requirement ID: [SRS-9-128]

By default the configurable percentage SHALL be 90% of the configurable maximum permitted size.

APPENDIX A: Web Guard General System Description

A.1 Purpose of the system

A.1.1 Introduction

This section provides a general overview of the expected role and functionality of an implementation of a 'Web Guard Capability' (WG). Note that the abbreviation 'WG' stands for the capability, and not necessarily for a single (physical or virtual) system; in other words, a Web Guard Capability may be composed of more than one system.

A.1.2 Enabling cross-domain information exchange

The WG is part of the Information Exchange Gateway (IEG) case C (IEG-C) and enables information exchange between communities-of-interest (COIs) in the NATO Secret ('High') and Mission Secret ('Low') network domains. The WG does not mediate all traffic that passes through the IEG-C; a subset of the information transfer is handled by the WG. This subset is characterized by:

- the COIs that exchange information;
- the protocol used (HTTP);
- the type of information exchange scenario used by the COI; and
- the use of NATO labelling [STANAG 4774], [STANAG 4778], i.e. the WG mediates information transfer for information that is labelled following the [STANAG 4774], [STANAG 4778].

For example, the WG will not mediate e-mail traffic or directory service traffic, however it is able to mediate HTTP traffic with labelled HTTP message content, see Section A.2. HTTP traffic with unlabelled HTTP message content will be handled be a separate proxy, i.e. Web Proxy, see section 4.4. Figure A.1 illustrates the role of the Web Guard Capability in the IEG-C.
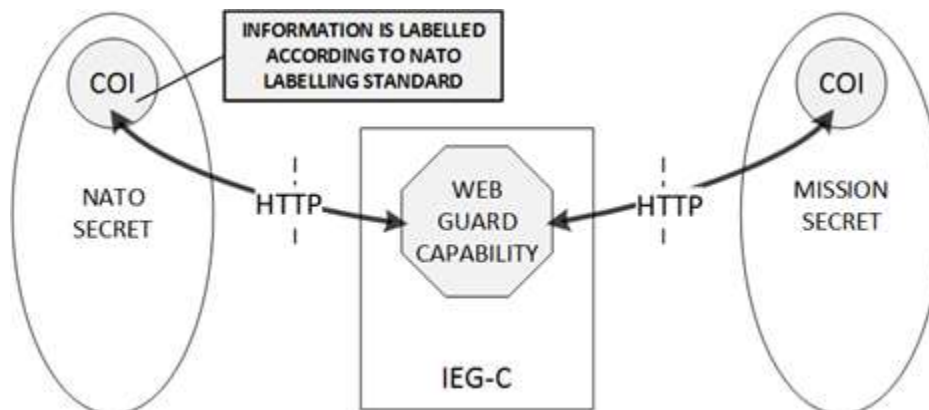
Figure 32 The Web Guard Capability is part of the IEG-C and handles the subset of the IEG-C information transfer that is labelled according to the NATO Labelling standard [STANAG 4774] and transferred over HTTP

A.1.3 Cross-domain solution

The WG offers a cross-domain solution (CDS) that is based on the use of labels (conformant to [STANAG 4774]), following the concept of Object Level Protection (OLP, [NCIA TR-2012-SPW008418-29, 2014]). The key function of the WG is to allow

automated data exchange between two network enclaves that belong to different security domains. From the WG's perspective one enclave is defined as the high domain, and the other enclave as the low domain.

In an information-exchange scenario involving a high domain and a low domain, also called a cross-domain information exchange, the following threats to the high domain are recognized:

- Leakage of confidential information from the high domain to the low domain;
- Degradation of the integrity or availability of resources in the high-security domain.

Figure A.2 illustrates these threats.
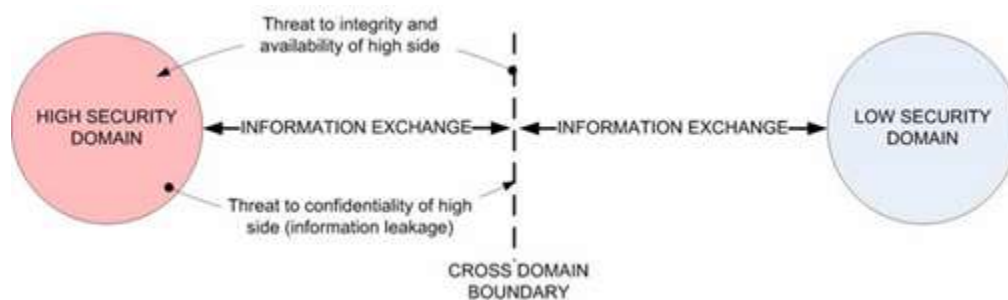
Figure 33 Identification of threats in a cross-domain information exchange

The purpose of the WG is to enable cross-domain information exchange by mediating traffic flows, while offering sufficient protection against the threats mentioned above by enforcing an appropriate security policy. In the case of high-to-low traffic, when information crosses the cross-domain boundary, the information is considered to have been 'released to the low domain'. Note that in the case of an IEG-C deployment, the WG is integrated in the IEG and the cross-domain boundary viewed from the WG's perspective may not coincide with the cross-domain boundary as viewed from the IEG's perspective. For all practical purposes, when this SRS states that information has been "released" by the WG to the low domain, this means that the WG has verified (or ensured) that the information is releasable to the low domain regardless of any potential further processing by other components in the IEG.

A.1.4 Security objective

The security objective of the WG is to protect the confidentiality of information, and the integrity and availability of resources in the high-security domain. The integrity and availability of the high domain is protected by allowing only those messages that have a white-listed message format to pass from the low domain to the high-security domain. In addition, constraints are set on the contents of the message. This is captured in a security policy.

The confidentiality of information is protected when messages pass from the high domain to the low domain by validating the confidentiality metadata label[7] that is bound to the information. Depending on the values contained in the label, the security policy in effect and the WG's functionality/configuration, the WG rejects the release of information, accepts it, or sanitizes the information by removing the parts that are in conflict with the security policy. See Section A.3.5 for an explanation of the data sanitization functionality.

(Note that data sanitization functionality is considered optional functionality for a WG developed based on this SRS.)

[7] *The meaning of the term 'confidentiality metadata label' is defined in [STANAG 4774]. A confidentiality metadata label is also known as a 'sensitivity label'. In this document the simplified term 'label' is also used and is understood to mean 'confidentiality metadata label'.*

A.1.5 Label handling

From the WG's point of view each attempted transfer of data from the high to the low domain is considered a request for information release. In order to make the information-release decision to reject, accept or sanitize, the WG validates a confidentiality metadata label that is bound to the information. The label and the binding mechanism must comply with the ([STANAG 4774], [STANAG 4778]). Depending on the information exchange scenario, the services in the COIs that use the WG to transfer information, and the security policy in effect, the WG can leave the confidentiality metadata label unaltered, remove it, or create a new (potentially modified) label. (Removal of the label is an option if the label will not be processed any further in the low domain. If the WG has sanitized information before release, and the low domain requires released information to be labelled, the WG will have to create a new label and bound it to the information before release.) If digital signatures are used, this means the WG must include the functionality to generate signatures in addition to signature verification.

Note that the way the WG handles labels depends on the labelling profile that is applied by the COIs; the [STANAG 4778] defines a number of labelling profiles and some of them allow for the co-existence of (COI-)application specific labels (that do not conform to [STANAG 4774]) and a label that will only be handled by the WG. In general the WG will not interpret (or modify) any (COI-) application specific labels, and will only handle labels that conform to the [STANAG 4774].

From now on in this document, when the term 'label' is used, it is implied to be a label that conforms to the [STANAG 4774] unless otherwise indicated.

A.2 Scope of the system

A.2.1 HTTP Proxy

To the COI services that make use of the WG (in either the high or the low domain), the WG acts as a hypertext transfer protocol (HTTP) 1.1 proxy [IETF RFC 7230, 2014]. The specific behaviour of the WG with respect to HTTP connectivity however, will also be influenced by the security policy that is enforced by the WG (from now on also referred to as the 'WG security policy'). The WG mediates HTTP traffic between HTTP clients and HTTP servers that reside in the high or low domain. The WG security policy pertains to both directions that HTTP messages can flow. For messages flowing from high to low, the enforcement of the WG security policy is referred to as 'high to low enforcement'. For messages flowing from low to high, it is referred to as 'low to high enforcement', see Figure A.3.
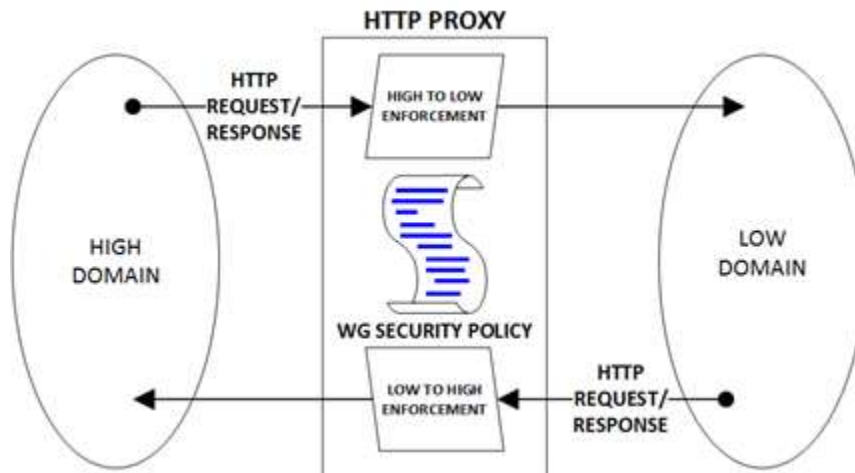
Figure 34 The WG provides HTTP proxy functionality to both domains, and enforces a security policy on traffic flowing in both directions

A.2.2 Types of security policy enforcement

For both directions of traffic flow, the WG security policy determines the security policy enforcement functionality that is enabled. The WG offers the following types of security policy enforcement functionality:

- HTTP header vetting (see [SRS-6-213]);
- Label validation (see [SRS-6-219]), potentially resulting in 'Data sanitization', i.e. removing the parts of the XML-formatted HTTP message body that are in conflict with the WG security policy. (Data sanitization is considered optional functionality for a WG based on the functional requirements in chapter 5.3, see [SRS-6-236]).
- XML schema validation (see [SRS-6-208]).

A.3 WG viewed as access-control mechanism

A.3.1 Access-control functionality

For the purpose of explaining the security policy enforcement functionality of the WG in more detail, this paragraph explains how the WG can be viewed as an access-control mechanism when mediating traffic flows between the high and low domains[8]. Here, it is important to note that the access control decision is made at the domain level, i.e. all initiators and targets are subject to the same domain security policy (based on their domain membership). In the case of high to low enforcement, a request to release information I_HL can be viewed as a request to provide the low domain access[9] to I_HL. Similarly, an attempt to transfer information I_LH from the low to the high domain can be viewed as a request to provide the high domain access to I_LH. Taking this point of view, the WG can be viewed as an implementation of a classic access-control mechanism consisting of an access-control policy (i.e. the WG security policy), an access-control decision function (ADF) and an access-control enforcement function (AEF) as shown in Figure A.4. The WG connects the high and low domains and, given the available access-control information (ACI), mediates access requests from initiators to targets located in either of the two domains.

[8] The type of access control described here is different from user access control; the WG will implement user access control in support of system administration, but it will not implement user

access control in the sense of taking credentials of a sending or receiving user (in either low or high domain) into account when enforcing the WG security policy.

[9] Whether or not information is actually accessed by a target in the low domain after release (e.g. a low domain user opens a file) is irrelevant to the decision to release the information (which essentially says that any low domain user is authorized to access the information). The act of releasing information to the low domain means that any target in the low domain may now access the information if so desired.
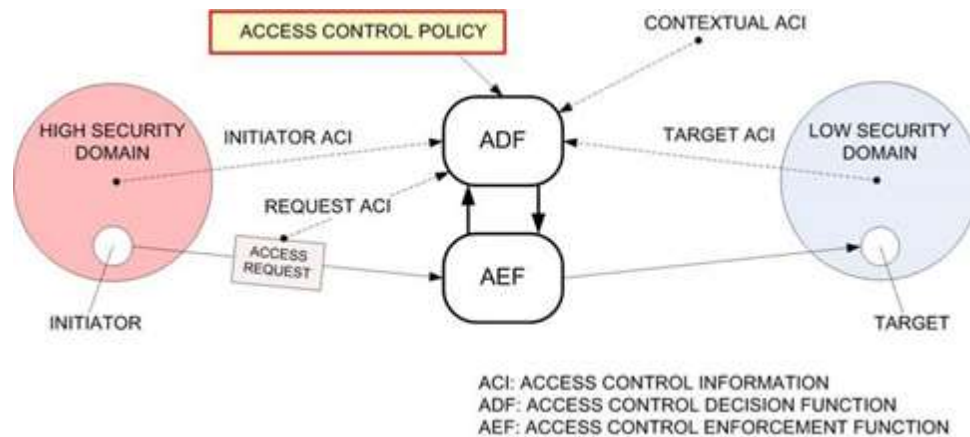
Figure 35 The WG can be viewed as an access-control mechanism connecting two security domains; initiator and target may be located in either domain10 depending on the actual access request

[10] Note that the figure uses the terms 'high security domain' and 'low security domain'. In the text these are referred to as 'high domain' and 'low domain' respectively.

An access request whose initiator is located in the high domain is also called an *information release request*. An access-control decision that grants access to a release request is called a *release of information* or simply a *release*.

A description of the ADF, AEF and ACI for the WG is given below for the types of security policy enforcement functionality for both directions of traffic flow.

A.3.2 HTTP header vetting

The access requests supported by the AEF of the WG are HTTP 1.1 request messages and HTTP response messages.

If the initiator of the access request is in the low domain, only a pre-defined set of HTTP message header lines with corresponding values is allowed. This set is defined in the WG security policy. The ADF tries to match each header line against this set. If it fails, access is denied for the particular header line and it is removed, or the header line is vetted (i.e. rewritten to conform to the WG security policy). As a result of this process an HTTP message with a transformed message header may be forwarded to the high domain.

If the initiator of the access request is in the high domain a similar process takes place. As a result of this process an HTTP message with a transformed message header may be forwarded to the low domain.

A.3.3 XML schema validation

If the initiator of the access request is in the low domain, only permitted XML document types are allowed for HTTP message bodies that are XML. This is defined in the WG security policy in the form of a list of allowed XML schema [W3C WD-xmlschema11-1, 2006] definitions. The ADF performs an XML schema validation. If the validation fails, access is denied for the entire HTTP message.

A.3.4 Label validation

If the initiator is in the high domain, the ACI is in fact a pair consisting of the contents of the HTTP request or response message and also one or more labels. In the context of information release the label provides information about the security-classification levels and categories of the information contained in the body of the HTTP message. For each labelled object in the HTTP message, the WG validates the label by checking its conformance to the [STANAG 4774], verifying the digital signature (if present) and by comparing the security-classification levels and the assigned categories against the WG security policy in order to determine its decision to reject, release or (optionally) sanitize.

A.3.5 Data sanitization

If the initiator is in the high domain, the ADF and AEF can work at a different level of granularity depending on the contents of the HTTP message body. If the HTTP message body is not XML, a single-access decision is made for the entire HTTP message and the decision is to either reject or release the entire HTTP message. However, if the HTTP message body is XML, the NATO labelling standard [STANAG 4778] allows for binding labels to individual information items in the XML infoset [W3C REC-xml-infoset, 2004]. If this is done, the AEF is able to act on every information item individually: individual information items for which the label is such that release to the low side is not allowed by the WG security policy, can be removed so that an HTTP message with a transformed message body results. This process is referred to as 'data sanitization'. The sanitized HTTP message can then be released to the low domain. Note that it is still possible to reject the entire HTTP message if one of the individual information items cannot be released.

Data sanitization is considered optional functionality for a WG based on the functional requirements in chapter 5.3, see [SRS-6-236]).

A.3.6 Process to determine if a label is in conflict with the WG security policy

The WG security policy expresses the requirements that (the values within) labels must meet in order for the labelled information to be released to the low domain[11]. These requirements are expressed in terms of the values that comprise the clearance level of the low domain. (The clearance level of a domain typically reflects the ownership of the domain, its classification and the coalition that makes use of the domain.) If for a given label L these requirements are not met, the information object that is labelled with L is rejected or (optionally) sanitized by the WG. The way in which these requirements are captured in the WG security policy as well as the mechanism that is used to verify if a label meets those requirements, can be implemented in different ways.

[11] *In theory it is also possible that the WG security policy expresses, for a given label, requirements on the clearance level of the low domain. However, in order to make a release decision for all requests for information release, such an approach would require support for all possible label values and that may not be feasible. Therefore, it is assumed that the WG security policy expresses requirements on the values of the label.*

A.4 Common information exchange scenario supported by the WG

A common information exchange scenario that is supported by the WG is referred to as the 'bi-directional cross-domain XML web content' scenario based on HTTP POST. In this scenario, XML-formatted data is transported in the body of HTTP POST requests or associated HTTP response messages. An example of such XML-formatted data are Simple Object Access Protocol (SOAP) messages [W3C Note SOAP, 2000].

In the bi-directional XML web content scenario, the producers and consumers of the web content that are located in either of the two security domains exchange XML-formatted messages over HTTP. The WG acts as an HTTP proxy and the web content producers and consumers have to be configured accordingly. The web content is contained in the body of an HTTP POST message or an HTTP response message.

In this scenario two cases of message processing are distinguished depending on the origin of the HTTP POST request:

- The case in which the HTTP POST request is sent from the low domain is called "low to high web content processing".
- The case in which the HTTP POST request is sent from the high domain is called "high to low web content processing".

The security functionality that is enforced in this scenario is as follows:

- Low to High enforcement:
  - o HTTP header vetting;
  - o XML schema validation.
- High to Low enforcement:
  - o Label validation;
  - o HTTP header vetting.

The XML-formatted messages that are sent from the high to the low domain are labelled according to the [STANAG 4774]. Figure 37 shows the data transfers and processing that is involved in the case "low to high web content processing".
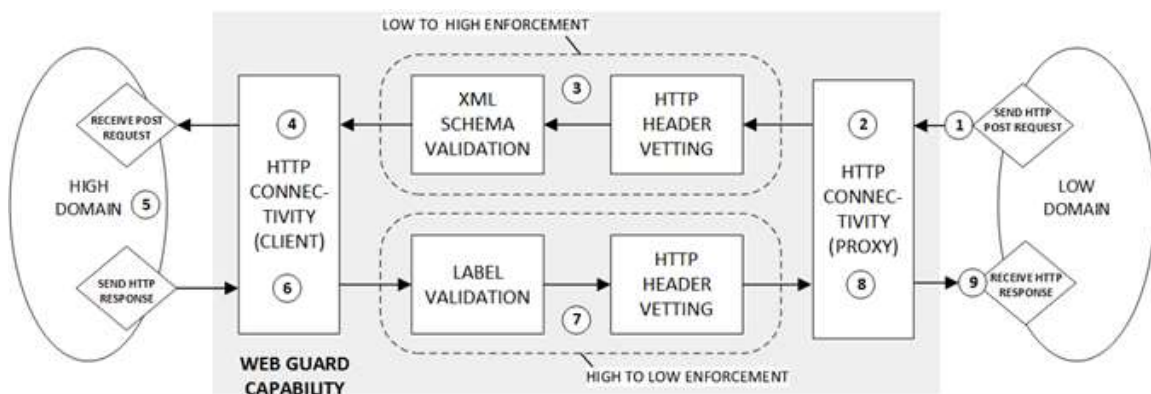
Figure 36 Low to high web content processing based on HTTP POST

The order of processing is as follows (see numbered steps in Figure A.5):

1. A web content consumer located in the low domain initiates the HTTP connection by sending a message in the body of an HTTP POST request message to a web content producer in the high domain.

2. HTTP connectivity (proxy): the HTTP POST request message is mediated by the WG that functions as an HTTP proxy to the web content consumer in the low domain.

3. Low to high enforcement: the WG enforces the WG security policy and performs validation of the messages:

    3.1. HTTP header vetting: the WG checks the HTTP headers for conformance to the WG security policy, and modifies and removes headers if necessary.

    3.2. XML schema validation: the WG checks if message body is XML. If so, it checks the compliance of the message body with predefined XML schemas. If the message body is not XML, the message is rejected.

4. HTTP connectivity (client): on behalf of the web content consumer in the low domain the WG acts as an HTTP client to the web content producer in the high domain.

5. The web content producer located in the high domain receives the HTTP POST request and sends a labelled XML web content message in the body of an HTTP response message to the WG; the target is the web content consumer in the low domain.

6. HTTP connectivity (client): the HTTP response message is received by the WG.

7. High to low enforcement: the WG enforces the WG security policy and performs validation of the messages: this requires the validation of HTTP message body and label.

    7.1. Label validation: the WG validates the label. This includes:

    - The validation of the digital signature of the label;
    - The validation of the conformance of the label (and bindings) to the [STANAG 4774], [STANAG 4778];
    - The validation of the binding(s) of the label to the contents of the HTTP message body;
    - The validation of the values in the label against the metadata policy that governs the information exchange; this policy specifies the label values that can be used, and their allowed usage, and is typically captured in a metadata policy information file (MPIF)[12]. The validation may include processing of an alternative label if the values of the originator label are not supported by the WG (i.e. they are not defined in the MPIF for this information exchange scenario). If neither originator nor alternative label is supported by the WG, the information release request will be rejected;
    - The validation of the conformance of the labelled content to the WG security policy (i.e. whether or not the values of the label imply that release to the low domain is allowed). If the WG security policy is such that the release of the content of the HTTP message body must be denied, the HTTP message is not transferred. If the WG security policy allows for parts of the message body to be released, data sanitization may be executed.

    7.2. <u>HTTP message header vetting</u>: the WG checks the HTTP headers for conformance to the access-control policy, and modifies or removes headers if necessary.

8. <u>HTTP connectivity (proxy)</u>: in its role of HTTP proxy, the WG sends the response message to the web content consumer in the low domain.

9. The low domain web content consumer receives the HTTP response.

Note that the description of steps above assumes that a consumer will request web content from a producer. However, the WG does not distinguish between a consumer or producer when enforcing the WG security policy, hence in the case of "low to high web content processing" the HTTP POST request message can also be initiated by a producer in the low domain if there is a requirement to do so (e.g. push web content). Similar considerations apply to the case 'high to low web content processing'.

The case 'high to low web content processing' contains the same steps and processes as 'low to high web content processing', however the traffic flow is in the opposite direction:

- the HTTP connection is initiated in the high domain by sending an HTTP POST request;
- the WG acts an HTTP proxy to the initiator in the high domain;
- Label validation takes place for the message body of the HTTP POST request instead of the HTTP response.

Note that the scenario based on HTTP POST that is described above is an example scenario. Scenarios based on other HTTP methods will be supported by the WG, for which similar steps and diagrams as for Figure A.6 can be developed.

The enforcement of the WG security policy is transparent to producers and consumers of web content. The WG does not authenticate producers or consumers of web content, however the set of producers and consumers that is reachable from either domain can be defined as part of the WG security policy based on a whitelist of URIs.

The sending of HTTP error messages - in case the enforcement of the WG security policy leads to a denial of an HTTP request – is governed by the WG security policy that specifies for a given deployment of the WG whether or not to send error messages, and if so which types are allowed and what the contents of their payload can be.

A.5 WG interfaces and external services

A.5.1 Standard interfaces

The WG offers the following standard interfaces (depicted in Figure A.6):

- WG_IF_NET_HIGH: This is a network interface that connects the WG to a network enclave belonging to the high domain. This interface is also called the 'high network interface'.
- WG_IF_NET_LOW: This is a network interface that connects the WG to a network enclave belonging to the low domain. This interface is also called the 'low network interface'.

- WG_IF_LOCAL_MGMT: This interface is intended for local system-administration purposes of the WG.
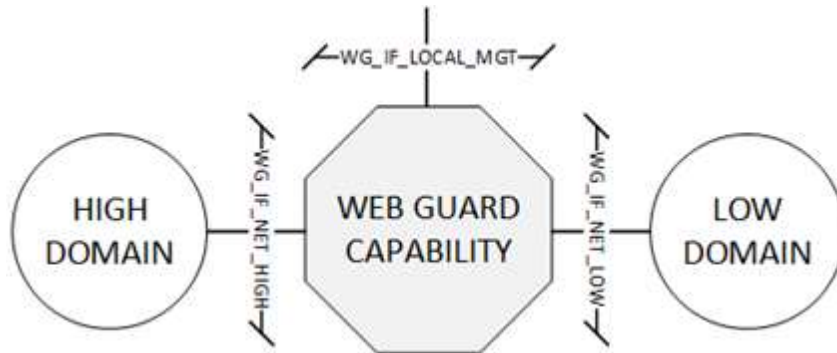
Figure 37 Network and local management interfaces of the WG

Note that depending on the type of deployment of the WG or its integration in the IEG-C, the interfaces in Figure A.6 can be physical or logical interfaces. For example, if the WG is implemented in a virtual machine, WG_IF_LOCAL_MGMT is a logical interface because it will then be accessed through the physical local management interface of the host of the virtual machine. (The physical local management interface consists of a directly attached keyboard and display console.)

A.5.2 Management interface

In addition to the standard interfaces from Section A.5.1, the WG has a (remote) management interface WG_IF_MGMT. The interface WG_IF_MGMT can be a dedicated physical interface, or a logical interface on top of WG_IF_NET_HIGH. (The WG is managed from the administrative high domain or from a dedicated management domain). WG_IF_MGMT supports remote management of the WG, and connections to the following external services:

- The IEG-C Domain Management System (DMS) in order to report on the key performance indicators 'Availability', 'Quality' and 'Usage' [NCIA SMC TA, 2018];
- REST-based Web Services for
    o the retrieval of XML schemas in support of XML schema validation;
    o Information on the metadata policy[13] (i.e. the policy that governs the values of the metadata that comprise the label);
- An OCSP responder provided by E-NPKI for obtaining the revocation status of X.509 digital certificates;
- An LDAP directory service (NATO Enterprise Directory Service (NEDS)) for:
    o The retrieval of X.509 certificates and associated revocation material;
    o Information on the metadata policy[13] (i.e. the policy that governs the values of the metadata that comprise the label);

[13] *This information can for example be captured at the WG in the form of a metadata policy information file (MPIF). For metadata in the context of sensitivity labels, such an MPIF is also commonly referred to as a security policy information file (SPIF).*

The interface WG_IF_MGMT is visualized in Figure A.7.
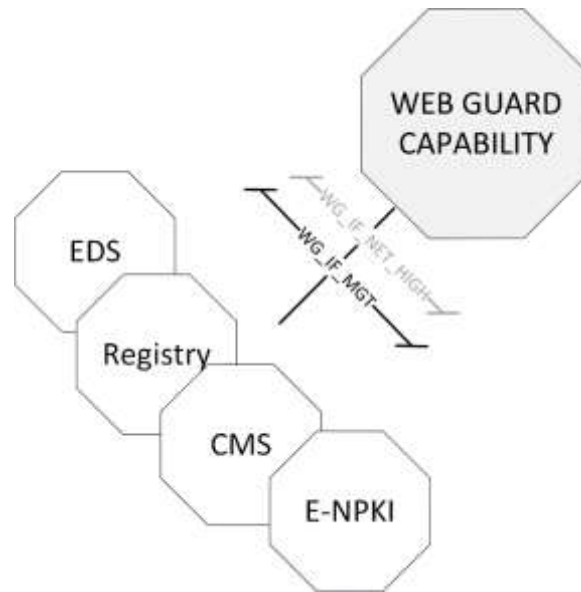
Figure 38 The management interface WG_IF_MGMT can be implemented as a physical interface or a logical interface on top of WG_IF_NET_HIGH; it supports remote management and connections to EDS, Registry, CMS and E-NPKI

A.5.3 Existing Capabilities

An implementation of the WG by NC3A (former NCIA) is operational as a component in an IEG-C at a number of locations. The implementation is referred to as 'NC3A MAXLG' (medium assurance XML-Labelling Guard). The NC3A MAXLG partially provides the functionality of the WG as specified in Chapter 6.3, e.g. the NC3A MAXLG supports an older version of the NATO labelling standard [STANAG 4774].

A.6 Dependencies

A.6.1 Availability of Enterprise NATO PKI

The Enterprise NATO PKI (E-NPKI) must be available to support the information exchange enabled by the WG.

A.6.2 Availability of a malware scanner

A malware scanner helps to protect the integrity and availability of the high domain by implementing specific scanning (such as virus-scanning) for malicious content that can be transmitted from the low domain. Although the WG provides filtering of messages delivered from the low to the high domain based on white listing of message types, it does not provide by itself any protection for the high domain against malicious content that might be injected from the low domain. Therefore, if a malware scanning capability is required for the information exchange scenario supported by the WG, it must be provided separately compliant with [NC3B AC/322-D(2004)0019 (INV), 2004].

A.6.3 Relationship with NC3A MAXLG

The WG is the replacement of the NC3A MAXLG in theatre. The requirements in the WG SRS are based on architecture building blocks (ABBs). The ABBs that are used for the WG are described in [NCIA TR/2016/NSE010871/01, 2016]. In order to understand how the architecture of the NC3A MAXLG relates to the ABBs used for the WG, Figure

39Figure 39 illustrates this relationship. It shows the system architecture of the NC3A Medium Assurance XML-Labelling Guard (MAXLG) (excluding system management components) with each component in the figure marked according to the accompanying legend which expresses the relationship with the ABBs.

Note that the HTTP connectivity component in the NC3A MAXLG implements both HTTP client and proxy connectivity. It does not implement HTTPS. The Public Key Cryptography Services are implemented in the form of a Public Key Encryption (PKE) module.

The 'WG High to Low Pattern' can be followed through the figure from left to right. Similarly, the 'WG Low to High Pattern' can be followed from right to left.
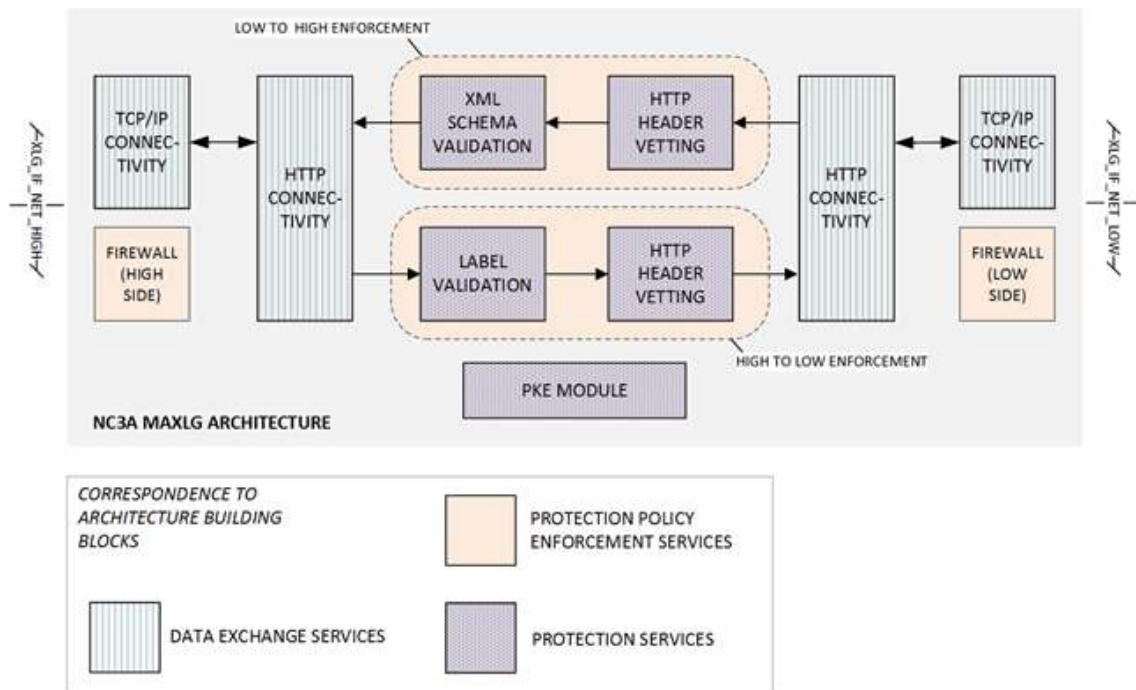
Figure 39 Relationship between NC3A MAXLG system architecture and IEG-C ABBs

APPENDIX B: Service Interface Profiles

B.1 Introduction

NATO communication and information systems (CIS) operate in a heterogeneous environment, with service providers and service consumers operating under multiple different frameworks and application contexts. Systems deployed onto NATO networks are subject to an appropriate security approval and/or accreditation process addressing the confidentiality, integrity and availability of security objectives where different available technologies and mechanisms can be used to apply security.

To ensure interoperability between services, both within NATO, and between NATO and its partners, there is a need to define a standard (and standards-based) profile which will be mandatory for all service operations in the federated mission environment. Service Interface Profiles (SIPs) have been designed to specify new and existing security technologies and mechanisms that offer a security framework that is implementation-independent, and can be used to support interoperability.

SIPs are published as Agency Technical Instructions (INSTR TECH) and are living documents that are periodically reviewed and updated.

In the case were a SIP has not been defined for a specific service, an FMN Service Instructions (SIs), which provides guidance how to implement the service in federated Mission Networks to enable the effective and efficient sharing of information, may be used.

This Appendix defines the SIPs and SIs that are applicable to the IEG-C in order to ensure cross-domain interoperability.

The SIPs and Sis that are applicable to the IEG-C are those that relate to proxies or guards that are hosted within the IEG-C. As identified in section 6.3, Table 10, the following are the initial IEG-C guards and proxies:

- RDP Proxy
- Web Guard
- Web Proxy
- Mail Guard

For services that the IEG-C does not mediate through the use of a proxy or guard, SIPs and SIs are not applicable. For example, the IEG-C may allow the flow of directory information between the High and Low Domains, however the SIP for Enterprise Directory Services is not applicable to the IEG-C as it does not proxy or guard the directory information exchange. Note that the directory services in the High and Low Domains which are exchanging directory information should be compliant with the SIP for Enterprise Directory Services, however this is beyond the scope of this Target Architecture.

B.2 RDP Proxy

There is no current SIP or SI for the remote desktop protocol, and consequently there is no requirement on the RDP proxy.

B.3 Web Guard

The following SIPs are applicable to the IEG-C Web Guard:

1. INSTR TECH 06.02.01 Service Interface Profile for Security Services, 4th February 2015

2. INSTR TECH 06.02.02 Service Interface Profile for REST Security Services, 4th February 2015

3. INSTR TECH 06.02.06 Service Interface Profile for Messaging (SOAP), 4th February 2015

4. INSTR TECH 06.02.07 Service Interface Profile for REST Messaging, 4th February 2015

In particular, these SIPs are applicable to the following interfaces and operations of the IEG-C Data Exchange Services ABB:

- SOA Platform Services HL Interface
  - ReceiveWebContentHL
  - ForwardWebContentHL

- SOA Platform Services LH Interface
    - o ReceiveWebContentLH
    - o ForwardWebContentLH

B.4 Web Proxy

The following SIPs are applicable to the IEG-C Web Proxy:

1. INSTR TECH 06.02.01 Service Interface Profile for Security Services, 4th February 2015

2. INSTR TECH 06.02.02 Service Interface Profile for REST Security Services, 4th February 2015

3. INSTR TECH 06.02.06 Service Interface Profile for Messaging (SOAP), 4th February 2015

4. INSTR TECH 06.02.07 Service Interface Profile for REST Messaging, 4th February 2015

In particular, these SIPs are applicable to the following interfaces and operations of the IEG-C Data Exchange Services ABB:

- SOA Platform Services HL Interface
    - o ReceiveWebContentHL
    - o ForwardWebContentHL
- SOA Platform Services LH Interface
    - o ReceiveWebContentLH
    - o ForwardWebContentLH

B.5 Mail GUARD

The following SI is applicable to the IEG-C Mail Guard:

1. FMN Spiral 1 Service Instructions for Informal Messaging, 18th February 2016

In particular, this SI is applicable to the following interfaces and operations of the IEG-C Data Exchange Services ABB:

- Business Support Service HL Interface
    - o ReceiveEmailHL
    - o ForwardEmailHL
- Business Support Service LH Interface
    - o ReceiveEmailLH
    - o ForwardEmailLH

B.6 Future Proxies/Guards

If additional guard and/or proxies are introduced into the IEG-C architecture to support other information exchange requirement, additional SIPs may be applicable.

APPENDIX C: IEG-C Protection Profile

C.1 Security Problem Definition

C.1.1 Threats

Threats	Description	Source
T.ADDRESS_MASQUERADE	A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.	[NCIA TN-1485 v1.1, 2012]
T. ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.	[NCIA TN-1485 v1.1, 2012]
T.AUDIT_COMPROMISE	An attacker may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	[NCIA TN-1485 v1.1, 2012]
T.COVERT_CHANNEL	An attacker on the high network may initiate an illicit flow of unauthorised information from the high network enclave to the low network enclave as a result of exploiting a covert channel in the IEG.	[NCIA TN-1485 v1.1, 2012] modified
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by an attacker.	[NCIA TN-1485 v1.1, 2012]
T.FLAWED_IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE may occur, leading to flaws that may be exploited by an attacker.	[NCIA TN-1485 v1.1, 2012]
T.INFORMATION_LEAK	A low network attacker may carry out a network-based attack against the high network enclave in order to obtain unauthorised information.	[NCIA TN-1485 v1.1, 2012] modified
T.MALICIOUS_TSF_COMPROMISE	An attacker may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	[NCIA TN-1485 v1.1, 2012]
T.MASQUERADE	An attacker may masquerade as an administrator in order to gain unauthorized access to data or TOE resources.	[NCIA TN-1485 v1.1, 2012]
T.MALWARE_INJECTION	Malicious software, such as viruses and worms, may be introduced into the high domain from the low domain.	[NCIA TN-1485 v1.1, 2012]
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behaviour being undiscovered thereby causing potential security vulnerabilities.	[NCIA TN-1485 v1.1, 2012]
T.RECONNAISSANCE	A low network attacker may obtain unauthorised information about resources (e.g. IP addresses, port numbers, system names, system date/time, products, versions) in the high network enclave e.g. by using network scanning techniques, network traffic monitoring, etc.	[NCIA TN-1485 v1.1, 2012] modified
T.REPLAY	An attacker may gain inappropriate access to the TOE by replaying administrator's authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or IA attributes (e.g., captured as transmitted during the course of legitimate use).	[NCIA TN-1485 v1.1, 2012]
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	[NCIA TN-1485 v1.1, 2012]
T.RESOURCE_EXHAUSTION	An attacker may block others from accessing system resources	[NCIA TN-1485 v1.1, 2012]
T.SECURITY_LABEL_TAMPERING	A high network attacker may modify a security label. For example the security label may be modified so that it binds wrong IA attributes to information in such a way that the IA attributes conform to the release level and as a consequence unauthorised information may be illicitly released to the low network enclave.	[NCIA TN-1485 v1.1, 2012] modified
T.SPOOFING	An attacker may misrepresent itself as the TOE to obtain administrator's identification and authentication data.	[NCIA TN-1485 v1.1, 2012]
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.	[NCIA TN-1485 v1.1, 2012]
T.UNAUTHORIZED_ACCESS	A low network attacker may gain access to unauthorised information	[NCIA TN-1485 v1.1, 2012] modified

T.UNIDENTI FIED_ACTI ONS	The administrator may not have ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	[NCIA TN-1485 v1.1, 2012]
T.UNKNOW N_STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.	[NCIA TN-1485 v1.1, 2012]
T.NETWOR K_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it. A low network attacker may carry out a network-based attack against resources available on the high network thereby compromising the system integrity and availability.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016] Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016] [NCIA TN-1485 v1.1, 2012] modified
T.NETWOR K_EAVESD ROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016] Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016]
T.LOCAL_A TTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016] Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016]
T.PHYSICAL _ACCESS	An attacker may try to access sensitive data at rest.	Protection Profile for Application Software Version 1.2 [NIAP PP_APP_V1.2, 2016]

T.LIMITED_ PHYSICAL_ ACCESS	An attacker may attempt to access data on the IEG while having a limited amount of time with the physical device.	Protection Profile for General Purpose Operating Systems [NIAP, PP_OS_V.4.1, 2016] modified
T.UNAUTHO RIZED_ADM INISTRATO R_ACCESS	Threat agents may attempt to gain administrator access to the firewall by nefarious means such as masquerading as an administrator to the firewall, masquerading as the firewall to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between the firewall and a network device. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the firewall and the network on which it resides.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.WEAK_CR YPTOGRAP HY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.UNTRUST ED_COMMU NICATION_ CHANNELS	Threat agents may attempt to target firewalls that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the firewall itself.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.WEAK_AU THENTICATI ON_ENDPO INTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the firewall itself could be compromised.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP,

		CPP_ND_V.1.0, 2015]
T.UPDATE_ COMPROMI SE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.UNDETEC TED_ACTIVI TY	Threat agents may attempt to access, change, and/or modify the security functionality of the firewall without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.SECURIT Y_FUNCTIO NALITY_CO MPROMISE	Threat agents may compromise credentials and firewall data enabling continued access to the firewall and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or firewall credentials for use by the attacker.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.PASSWO RD_CRACKI NG	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the firewall. Having privileged access to the firewall provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.SECURIT Y_FUNCTIO NALITY_FAI LURE	A component of the firewall may fail during start-up or during operations causing a compromise or failure in the security functionality of the firewall, leaving the firewall susceptible to attackers.	Collaborative Protection Profile for Stateful Traffic

		Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices [NIAP, CPP_ND_V.1.0, 2015]
T.NETWORK_DISCLOSURE	An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported. Sensitive information on a protected network might be disclosed resulting from disclosure/transmitted information in violation of policy, such as sending unencrypted credit card numbers. The IPS TOE will be capable of inspecting packet payloads for data strings and patterns of characters.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) [NIAP, PP_NDCP_IPP_EP_V.2.1, 2016]
T. NETWORK_ ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services. An attacker may attempt to gain inappropriate access to one or more networks, endpoints, or services, such as through brute force password guessing attacks, or by transmitting malicious executable code, scripts, or commands. If malicious external devices are able to communicate with devices on the protected network, then those devices may be susceptible to the unauthorized disclosure of information.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls [NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) [NIAP, PP_NDCP_IPP_EP_V.2.1, 2016]
T.NETWORK_MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.	Collaborative Protection Profile for Stateful Traffic Filter Firewalls

	Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services, (e.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools, and botnets).	[NIAP, CPP_FW_V.1.0, 2015] Collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) [NIAP, PP_NDCP_IPP_EP_V.2.1, 2016]
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources. Though most IPS will provide some protection from DDoS (distributed denial of service) attacks, providing protection against DDoS attacks is not a requirement for conformant TOEs, as this is best counteracted by firewalls, cloud computing and design. Note however that DoS protection is required.	Collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) [NIAP, PP_NDCP_IPP_EP_V.2.1, 2016]
T.ADMIN_ERROR	The security features offered by the TOE may be rendered irrelevant if a malicious or careless administrator configures or operates the TOE in a manner that is inconsistent with the defined security requirements. For example, they may fail to enable encrypted communications, configure an appropriate password policy, or assign excessive administrative privileges to a user who does not require them. While the TSF cannot truly prevent such incidents, the distribution of clear administrative guidance is expected to reduce unintentional errors, and the display of an acceptable use banner (with clearly enumerated consequences for unacceptable use) may deter some malicious activity.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.EAVES	An Enterprise Security Management architecture will almost certainly require data to be transmitted between remote devices in order to function. The TOE may distribute policies to be enforced to remote Access Control products. It may receive user attributes or session data from elsewhere in the environment, and it may write audit data to a centralized repository that is located remotely. If this data is not protected by a sufficiently secure trusted channel, it may be subject to involuntary disclosure. An attacker with access to this data can use it for reconnaissance purposes or to replay known valid information in an attempt to impersonate a valid user or entity. The Operational Environment will almost certainly require data to be transmitted between remote devices in order to function. The TOE may receive policies to enforce from a remote source. It will receive user attributes or session data from elsewhere in the environment, and it will write audit data to a centralized repository that is located remotely. If this data is not protected by a sufficiently secure trusted channel when in transit, it may be subject to involuntary disclosure. An attacker with access to this data can use it for reconnaissance	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013] Standard Protection Profile for Enterprise Security Management Access Control

	purposes or to replay known valid information in an attempt to impersonate a valid user or entity.	[NIAP, PP_ESM_aC_V. 2.1, 2013]
T.UNAUTH	If the TSF does not appropriately identify, authenticate, and authorize its administrators, there will not be assurance that its management functions are being performed appropriately. A poorly designed or implemented authentication function will allow an attacker to illegitimately access the TSF and attempt to perform management functions. A poorly designed or implemented data protection function will allow access control checks to be bypassed allowing for privilege escalation. Regardless of the method by which an attacker gains illegitimate access to the ability to create policies, the resulting compromise of the integrity of the organization's access control policies is the same. The primary purpose of deploying the TOE is to enforce access control against objects that reside in the Operational Environment. It does this by providing mechanisms to intercept subject requests to perform operations against objects and determine whether a defined access control policy should allow the request to occur. If these activities are subverted or bypassed, or if the TOE is incapable of controlling access to the expected level of granularity, then all or some of the Operational Environment will function as if the TOE did not exist. This situation allows for objects being accessed without proper authorization.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013] Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.DISABLE	In order to enforce access control against objects, the TOE must reside in a logical location that will allow it to intercept requests. The types of resources to which access is being controlled may require the TOE to reside locally to these resources. If the TOE is located on an endpoint system, the threat of the TOE being disabled is magnified. This is due to the fact that endpoint systems are less likely to perpetually remain in controlled access environments. When the assurance of physical access control is diminished, the risk of an attacker attempting to access the system is increased. If the TOE runs as a process that can be terminated or if its files can be moved, altered, or removed from the operating system's start-up sequence, a user will have the ability to circumvent access control enforcement.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.NOROUTE	In cases where the TOE is located remotely from other ESM components, a risk may be present. If connections between the TOE and remote resources are disrupted, the TOE may not be able to properly enforce its security functions. Worse yet, the threat of discontinuity can be realized by denial of service or by simply unplugging physical cables. It can also be very easily performed inadvertently and by individuals far removed from the operation of the TOE itself. Because of this, the TOE must have some way to maintain continuity of operations in the event of a virtually inevitable service outage.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.FALSIFY	The Policy Management product must communicate with the TOE in order to distribute policies that the TOE will be responsible for enforcing. In order to provide assurance that a policy has been received and will be enforced, the TOE should be able to provide some evidence of policy receipt and consumption to the Policy Management product. However, if the format of this receipt is sufficiently generic or the communications channel is not sufficiently protected from disclosure, an attacker may intercept the distribution of the policy and return a false receipt to the Policy Management product. The result of this is that the TOE does not enforce the correct policy and nothing appears amiss from a management perspective, potentially making the security breach more difficult to detect.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V. 2.1, 2013]
T.WEAKPOL	The Standard Protection Profile for Enterprise Security Management Access Control specifies a variety of technology types and the minimum sets of subjects, objects, operations, and attributes in order to define sufficiently detailed policies for each technology type. A Policy Management product must be capable of creating policies	Standard Protection Profile for Enterprise Security

	that provide the same level of detail that a compatible Access Control product can consume. An insufficiently detailed policy is an ineffective access control mechanism because it either allows unintended activity or incorrectly restricts legitimate usage.	Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.CONTRADICT	An access control policy can potentially contain many different complex rules that permit and forbid access to various objects. A consequence of this is that a policy may contain rules that contradict one another. For example, a rule may exist that allows a particular user the ability to run a particular program on a host while another rule in the same policy may exist that forbids all members of a group that user belongs to from running the same program. If a policy that contains such a contradiction is consumed by an Access Control product, it may create an unpredictable result.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.FORGE	When an Access Control product receives what appears to be updated policy information from the TOE, the Access Control product must have some assurance of the authenticity of the policy and the identity of the sender. If the communications channel is not sufficiently protected or the mechanism by which the TOE provides a guarantee of a policy's integrity is not sufficiently robust, an attacker who is aware of the syntax used to transmit a policy may be able to forge an arbitrarily fake one and have an Access Control product consume it. If this occurs, an Access Control product may be configured to enforce a permissive fake policy that allows unauthorized access, to enforce a restrictive fake policy that prevents legitimate activities from being performed, or to consume an incorrectly formatted policy and either terminate or allow an attacker access to memory space within the system on which the Access Control product resides. When the TOE receives what appears to be updated policy information, the TOE must have some assurance of the authenticity of the policy and the identity of the sender. If the communications channel is not sufficiently protected or the mechanism by which the TOE validates the identity of the policy's source is not sufficiently robust, an attacker who is aware of the syntax used to transmit a policy may be able to forge an arbitrarily fake one and have the TOE consume it. If this occurs, the TOE may be configured to enforce a permissive fake policy that allows unauthorized access, to enforce a restrictive fake policy that prevents legitimate activities from being performed, or to consume an incorrectly formatted policy.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013] Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V.2.1, 2013]
T.WEAKIA	The ability of the TSF to define administrative privileges does not prevent malicious use if the TSF's authentication function can be subjected to brute force guessing. The TSF must provide sufficient login frustration mechanisms to limit the ability of an attacker to authenticate to the TOE through brute force.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]
T.MASK	Part of the reason for implementing an Enterprise Security Management solution within an organization is to provide transparency and accountability. Because of this, the TOE is expected to provide the capability to monitor and audit enforcement of its functionality. If an attacker is able to alter audit data or prevent it from being recorded, then they can begin to probe a system for weaknesses with a reduced risk of discovery. Similarly, if the TOE does not identify and audit anomalous or malicious actions taken against the TSF, then the potential exists for its behaviour to be altered without detection. If this were to occur, there would be no assurance that its security functions were operating properly.	Standard Protection Profile for Enterprise Security Management Policy Management [NIAP, PP_ESM_V.2.1, 2013]

	Part of the reason for implementing an ESM solution within an organization is to provide transparency and accountability. Because of this, the TOE is expected to provide the capability to monitor and audit enforcement of its access control policies. If an attacker is able to confound audit data by exploiting previously-discussed attack vectors (impersonating Secure Configuration Management to reconfigure the TOE's audit ability, compromising a trusted channel to any remote audit repository to divert or rewrite data, disabling a part of the TOE responsible for auditing, or deleting or modifying local audit logs), then they can begin to probe a system for policy weaknesses with a reduced risk of discovery. Similarly, if the TOE does not identify and audit anomalous or malicious actions taken against itself, then the potential exists for its behaviour to be altered without detection. If this were to occur, there would be no assurance that its access control enforcement was functioning properly.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_aC_V.2.1, 2013]
T.OFLOWS	The TOE is responsible for accepting input from potentially a variety of sources. If an attacker can replay policy data or modify legitimate policy data in transit, then the TSF may be enforcing an incorrect policy. This presents the attacker an opportunity to access data without authorization.	Standard Protection Profile for Enterprise Security Management Access Control [NIAP, PP_ESM_AC_V.2.1, 2013]

C.1.2 Assumptions

Assumptions	Description	Source
A.CRYPTOGRAPHY_MODULE_VALIDATED	The cryptographic module is validated according validated to at least FIPS 140-2 Level 2 [FIPS 140-2, 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]	[NCIA TN-1485 v1.1, 2012] modified
A.CRYPTOGRAPHY_NATO_APPROVED	The TOE uses 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].	[NCIA TN-1485 v1.1, 2012]
A.NO_TOE_BYPASS	Information cannot flow between the high network enclave and the low network enclave without passing through the TOE. Ref: [NAC AC/322-D/0030-REV5]	[NCIA TN-1485 v1.1, 2012]
A.PHYSICAL_ACCESS_MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2001-REV2, 2008], [NAC AC/35-D/1030, 2005].	[NCIA TN-1485 v1.1, 2012]
A.PKI_NATO_COMPLIANT	The PKI complies with the NATO directives and guidelines on use of Public-Key Infrastructure, including [NAC C-M(2003)32, 2003], and [NAC AC/322-D(2004)0024-REV3-COR1, 2018].	[NCIA TN-1485 v1.1, 2012]
A.TRUSTED_LABELER	A labeller is trusted to only create security labels in accordance with the NATO policy and respective directives and guidelines with assurance commensurate with the value of the information that he can create labels for. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2002-REV4, 2012], [NAC AC/35-D/1032, 2005] [STANAG 4774], [STANAG 4778}.	[NCIA TN-1485 v1.1, 2012]
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE. The OS is configured according to relevant NATO guidance and directives [AC/322-D/0048-REV3, 2019]	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified

		[NCIA TN-1485 v1.1, 2012] modified
A.PROPER_ USER	The user of the IEG is not wilfully negligent or hostile, and uses the functionality provided by the IEG in compliance with NATO policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified
A.TRUSTED _ADMIN	The administrator of the IEG is not careless, wilfully negligent or hostile, and administers the OS within compliance of NATO policy.	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified [NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
A.PHYSICA L_PROTEC TION	The IEG is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the IEG's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the IEG and the data it contains.	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
A.LIMITED_ FUNCTIONA LITY	The IEG is assumed to provide networking, filtering and guarding functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the IEG should not provide computing platform for general purpose applications (unrelated to IEG core functionality).	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified [NCIA TN-1485 v1.1, 2012] modified
A.REGULAR _UPDATES	The IEG firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
A.ADMIN_C REDENTIAL S_SECURE	The administrator's credentials (private key) used to access the firewall are protected by the host platform on which they reside.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015]
A.CONNEC TIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.	[NIAP PP_NDCP_IPP_ EP_V.2.1, 2016]
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment.	[NIAP PP_ESM_V.2.1, 2013] [NIAP PP_ESM_AC_V .2.1, 2013]
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE. The administrators of the IEG-C can be categorised into the following roles: System Administrator: responsible for installation, configuration and maintenance of the IEG-C; Audit Administrator: responsible for regular review of IEG-C audit logs;	[NIAP PP_ESM_V.2.1, 2013] modified [NIAP PP_ESM_AC_V .2.1, 2013] modified

	CIS Security Administrator: responsible for performing the IEG-C CIS security-related tasks, such as security policy management; Cyber Defence Administrator: responsible for monitoring and actioning cyber-related tasks; and, SMC Administrator: responsible for monitoring IEG-C services.	

C.1.3 Organizational Security Policies

Organizational Security Policy	Description	Source
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE. Reference: [NAC AC/322-D/0048-REV3, 2019]	[NCIA TN-1485 v1.1, 2012]
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels. Reference: [NAC AC/322-D/0030-REV5]	[NCIA TN-1485 v1.1, 2012]
P.CLASSIFICATION	The IEG must limit the access to information based on IA attributes included in a label and the information flow control policy as defined in the Protection Policy Enforcement Services. The access rules enforced shall prevent a subject from accessing information which is of higher sensitivity than it is operating at and prevent a subject from causing information from being downgraded to a lower sensitivity. Reference: [NAC AC/35-D/2002-REV4, 2012]	[NCIA TN-1485 v1.1, 2012]
P.CRYPTOGRAPHY	The TOE shall use NATO-approved and validated 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. Reference: [NAC AC/322-D(2007)0002-REV1, 2015]	[NCIA TN-1485 v1.1, 2012]
P.VULNERABILITY_ ANALYSIS	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential. Reference: [NAC AC/322-D/0048-REV3, 2019]	[NCIA TN-1485 v1.1, 2012]
P.ACCESS_ BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. Reference: [AC/322-D/0048-REV3, 2019] Appendix 1 Annex 1 page 1-29	[NIAP CPP_FW_V.1.0, 2015] [NIAP PP_ESM_V.2.1, 2013] [NIAP CPP_ND_V.1.0, 2015] [NCIA TN-1485 v1.1, 2012]
P.ANALYZE	Analytical processes and information to derive conclusions about potential intrusions must be applied and appropriate response actions taken.	[NIAP PP_NDCP_IPP_ EP_V.2.1, 2016]
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.	[NIAP PP_ESM_AC_V .2.1, 2013]

C.2 Security Objectives

C.2.1 Security Objectives for the TOE

Security Objective	Description	Source
O.ADMIN_ROLE	The TOE will provide an administrator role to isolate administrative actions, and to make the administrative functions available locally and remotely.	[NCIA TN-1485 v1.1, 2012] (FMT_SMR.2)
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.	[NCIA TN-1485 v1.1, 2012] (FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FAU_STG.3,

		FAU_STG.4(1), FAU_STG.4(2), FIA_USB.1) [NIAP PP_ESM_V.2.1, 2013] - O.AUDIT (FAU_GEN.1, FAU_SEL.1, FAU_STG_EXT.1, FPT_STM.1)
O.AUDIT_PROTECTION	The TOE shall provide the capability to protect audit information.	[NCIA TN-1485 v1.1, 2012] (FAU_SAR.2, FAU_STG.1, FAU_STG.3, FAU_STG.4(1), FAU_STG.4(2), FMT_MOF.1)
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.	[NCIA TN-1485 v1.1, 2012] (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))
O.CHANGE_MANAGEMENT	The configuration of, and all changes to, the TOE and its development evidence will be analysed, tracked, and controlled throughout the TOE's development.	[NCIA TN-1485 v1.1, 2012]
O.CORRECT_TSF_OPERATION	The TOE will provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.	[NCIA TN-1485 v1.1, 2012] (FPT_TST.1)
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.	[NCIA TN-1485 v1.1, 2012] (FTA_TAB.1) [NIAP PP_ESM_V.2.1, 2013] – O.BANNER (FTA_TAB.1)
O.MAINT_MODE	The TOE shall provide a mode from which recovery or initial start-up procedures can be performed.	[NCIA TN-1485 v1.1, 2012] (FPT_RCV.2)
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	[NCIA TN-1485 v1.1, 2012] (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))

			[NIAP PP_OS_V.4.1, 2016] - O.MANAGEMENT *(FMT_MOF_EXT.1, FTP_TRP.1)* [NIAP PP_NDCP_IPP_EP_V.2.1, 2016] - O.TOE_ADMINISTRATION *(FMT_MOF.1/IPS, FMT_MTD.1/IPS, FMT_SMF.1/IPS, FMT_SMR.2/IPS)* [NIAP PP_ESM_V.2.1, 2013] *(FAU_SEL_EXT.1, FMT_MOF.1, FMT_MOF_EXT.1, FMT_MTD.1, FMT_SMF.1)*
O.MEDIATE_FLOW	The TOE shall mediate the flow of information between the high network interface and the low network interface in accordance with the information flow policy.		[NCIA TN-1485 v1.1, 2012] *(FMT_REV.1(1), FMT_REV.1(2))*
O.MESSAGE_VETTING	The TOE shall control the flow of information from the low network interface to the high network interface and vice versa by only relaying messages that are allowed as part of the TOE security policy.		[NCIA TN-1485 v1.1, 2012] modified
O.MINIMAL_PROXY	The TOE shall provide mechanisms that can be used to limit the amount of information, which is transmitted from the high to the low network enclave in the header or envelope of a transport protocol message.		[NCIA TN-1485 v1.1, 2012] modified
O.REPLAY_DETECTION	The TOE will provide a means to detect and reject the replay of authentication data as well as other TSF data and security attributes.		[NCIA TN-1485 v1.1, 2012] *(FPT_RPL.1)*
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated; this includes that no residual information from a previously relayed message is transmitted.		[NCIA TN-1485 v1.1, 2012] *(FDP_RIP.2)*
O.RESOURCE_SHARING	The TOE shall provide mechanisms that mitigate attempts to exhaust resources provided by the TOE (e.g., resulting in denying access to high network resources).		[NCIA TN-1485 v1.1, 2012] modified *(FMT_MOF.1(5), FMT_MTD.2(2), FMT_MTD.2(3), FRU_RSA.1(1), FRU_RSA.1(2))*
O.REVERSE_PROXY	The TOE shall provide capability to hide unauthorised information attributes like type, address and name of resources of the high network enclave from the low network enclave.		[NCIA TN-1485 v1.1, 2012] modified
O.ROBUST_ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure delivery and management [NAC AC/35-D/1014-REV2, 2006].		[NCIA TN-1485 v1.1, 2012]

O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	[NCIA TN-1485 v1.1, 2012] *(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3, FTA_TSE.1)* [NIAP PP_ESM_V.2.1, 2013] – O.ROBUST *(FIA_AFL.1, FIA_SOS.1, FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, FTA_TSE.1)*
O.SELF_PROTECTION	The TSF shall maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure.	[NCIA TN-1485 v1.1, 2012] *(FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1(1), FTP_TRP.1(2))*
O.SOUND_DESIGN	The TOE will be designed using sound design principles and techniques. The TOE design, design principles and design techniques will be adequately and accurately documented.	[NCIA TN-1485 v1.1, 2012]
O.SOUND_IMPLEMENTATION	The implementation of the TOE will be an accurate instantiation of its design, and is adequately and accurately documented.	[NCIA TN-1485 v1.1, 2012]
O.THOROUGH_FUNCTIONAL_TESTING	The TOE will undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.	[NCIA TN-1485 v1.1, 2012]
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	[NCIA TN-1485 v1.1, 2012] *(FMT_MTD.1, FPT_STM.1)*
O.TRUSTED_PATH	The TOE will provide a means to ensure that administrators are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.	[NCIA TN-1485 v1.1, 2012] *(FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1(1), FTP_TRP.1(2))*
O.VALID_LABEL	The TOE shall validate the origin, integrity and binding [STANAG 4778] of a security label [STANAG 4774] to a data object before it is used.	[NCIA TN-1485 v1.1, 2012] *(FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3))*
O.VULNERABILITY_ANALYSIS	The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE does not allow attackers with medium attack potential to violate the TOE's security policies.	[NCIA TN-1485 v1.1, 2012]
O.ACCOUNTABILITY	An IEG shall ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.	[NIAP PP_OS_V.4.1, 2016] modified *(FAU_GEN.1)*
O.INTEGRITY	An IEG shall ensure the integrity of their update packages. OSs are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant IEGs provide execution environment-based	[NIAP PP_OS_V.4.1, 2016] modified *(FPT_SBOP_EXT.1,*

	mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. The TOE will contain the ability to assert the integrity of policy data. The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.	*FPT_ASLR_EXT.1,* *FPT_TUD_EXT.1,* *FPT_TUD_EXT.2,* *FCS_COP.1.1(2),* *FCS_COP.1.1(3),* *FCS_COP.1.1(4),* *FPT_ACF_EXT.1,* *FPT_SRP_EXT.1,* *FIA_X509_EXT.2,* *FPT_TST_EXT.1,* *FTP_ITC_EXT.1,* *FPT_W^X_EXT.1.1, FIA_AFL.1, FIA_UAU.5)* [NIAP PP_ESM_V.2.1, 2013] *(FTP_ITC.1)* [NIAP PP_ESM_AC_V.2.1, 2013] *(FTP_ITC.1)*
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant IEGs provide data-at-rest protection for credentials. Conformant IEGs also provide access controls which allow users to keep their files private from other users of the same system.	[NIAP PP_OS_V.4.1, 2016] modified *(FCS_STO_EXT.1,* *FCS_RBG_EXT.1,* *FCS_COP.1.1(1),* *FDP_ACF_EXT.1)*
O.SYSTEM_MONITORING	The IEG must collect and store information about all events that may indicate a policy violation related to misuse, inappropriate access, or malicious activity on monitored networks. For an IEG implemented in the static environment the TOE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016] modified *(FAU_ARP.1,* *FAU_GEN.1/IPS, FAU_SAR.1,* *FAU_SAR.2,* *FAU_SAR.3,* *FAU_STG.1,* *FAU_STG.4,* *FRU_RSA)* [NIAP PP_ESM_AC_V.2.1, 2013] – O.MONITOR *(FAU_GEN.1,* *FAU_SEL.1,* *FAU_STG.1,* *FAU_STG_EXT.1)*

		[NCIA TN-1485 v1.1, 2012] modified – OE.MALWARE_ SCANNER
O.IPS_ANAL YZE	The IEG must apply analytical processes to network traffic data collected from monitored networks and derive conclusions about potential intrusions or network traffic policy violations. For an IEG implemented in the static environment the TOE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NIAP PP_NDCP_IPP_ EP_V.2.1, 2016] modified *(IPS_ABD_EXT. 1, IPS_IPB_EXT.1, IPS_NTA_EXT. 1, IPS_SBD_EXT. 1, IPS_SBD_EXT. 2)* [NCIA TN-1485 v1.1, 2012] modified – OE.MALWARE_ SCANNER
O.IPS_REA CT	The IEG must respond appropriately to its analytical conclusions about policy violations. For an IEG implemented in the static environment the TOE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NIAP PP_NDCP_IPP_ EP_V.2.1, 2016] modified *(FAU_ARP.1, IPS_ABD_EXT. 1)* [NCIA TN-1485 v1.1, 2012] modified – OE.MALWARE_ SCANNER
O.TRUSTED _COMMUNI CATIONS	The IEG will ensure that communications between distributed components of the TOE are not subject to unauthorized modification or disclosure.	[NIAP PP_NDCP_IPP_ EP_V.2.1, 2016] modified *(FPT_ITT.1)* [NIAP PP_OS_V.4.1, 2016] modified – O.PROTECTED _COMMS *(FCS_TLSC_EX T.1, FCS_TLSC_EX T.2, FCS_TLSC_EX T.3, FCS_TLSC_EX T.4, FCS_DTLS_EX T.1, FCS_RBG_EXT .1, FCS_CKM.1(1), FCS_CKM.2(1), FCS_COP.1.1(1), FDP_IFC_EXT. 1, FIA_X509_EXT. 1, FIA_X509_EXT.*

			2, FTP_ITC_EXT.1) [NIAP PP_ESM_V.2.1, 2013] – O.PROTCOMM S *(FCS_HTTPS_E XT.1, FCS_IPSEC_EX T.1, FCS_SSH_EXT. 1, FCS_TLS_EXT. 1, FPT_SKP_EXT. 1, FTP_ITC.1, FTP_TRP.1)* [NIAP PP_ESM_AC_V .2.1, 2013] modified *(ESM_DSC.1, ESM_EID.2, FDP_ACC.1, FDP_ACF.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FTA_TSE.1)*
O.ACCESSI D	The TOE will contain the ability to validate the identity of other IEG-C components prior to distributing data to them.		[NIAP PP_ESM_V.2.1, 2013] modified
O.AUTH	The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.		[NIAP PP_ESM_V.2.1, 2013] *(ESM_EAU.2, ESM_EID.2, FIA_USB.1, FMT_MOF.1, FMT_SMR.1, FPT_APW_EXT .1, FTP_TRP.1)*
O.CONSIST ENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.		[NIAP PP_ESM_V.2.1, 2013]
O.CRYPTO_ NATO_APP ROVED	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications. The TOE provides 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). Ref: [NAC AC/322-D(2007)0002-REV1, 2015]		[NIAP PP_ESM_V.2.1, 2013] modified – O.CRYPTO *(FCS_CKM.1, FCS_CKM_EXT .4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT .1)*

		[NIAP PP_ESM_AC_V.2.1, 2013] modified – O.CRYPTO *(FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1)*
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.	[NIAP PP_ESM_V.2.1, 2013] *(ESM_ACT.1, FTP_ITC.1)*
O.MAINTAIN		[NIAP PP_ESM_AC_V.2.1, 2013] modified *(FPT_FLS_EXT.1, FRU_FLT.1)*
O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.	[NIAP PP_ESM_AC_V.2.1, 2013]
O.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	[NIAP CPP_FW_V.1.0, 2015] – OE.UPDATES [NIAP CPP_ND_V.1.0, 2015] - OE.UPDATES

C.2.2 Security Objectives for the Operational Environment

Security Objective	Description	Source
OE.ADMIN_NO_EVIL	Sites using the TOE will ensure that administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.	[NCIA TN-1485 v1.1, 2012]
OE.MALWARE_SCANNER	For an IEG implemented in the deployed environment the OE provides a NATO approved malware scanning capability. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]	[NCIA TN-1485 v1.1, 2012] modified
OE.NO_TOE_BYPASS	Information cannot flow between the high network enclave and the low network enclave without passing through the TOE. Ref: [NAC AC/322-D/0030-REV5]	[NCIA TN-1485 v1.1, 2012]
OE.PHYSICAL_ACCESS_MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2001-REV2, 2008], [NAC AC/35-D/1030, 2005].	[NCIA TN-1485 v1.1, 2012]
OE.TRUSTED_LABELLER	A labeller is trusted to only create security labels in accordance with the NATO policy and respective directives and guidelines. The assurance of the label creation process must be commensurate with the value of the information that the labels are created for. Ref: [NAC C-M(2002)49-COR12, 2015], [NAC AC/35-D/2002-REV4, 2012], [NAC AC/35-D/1032, 2005], [NAC AC/322-D(2004)0021 (INV) 2004], [NAC AC/322-D(2004)0022 (INV), 2004].	[NCIA TN-1485 v1.1, 2012]

OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE. The OS relies on being installed on trusted hardware.	[NIAP PP_APP_V.1.2, 2016] [NIAP PP_OS_V.4.1, 2016]
OE.PROPER_USER	The user of the IEG is not wilfully negligent or hostile, and uses the software within compliance of the applied NATO policy.	[NIAP PP_APP_V.1.2, 2016] modified [NIAP PP_OS_V.4.1, 2016] modified
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the operational environment.	[NIAP CPP_FW_V.1.0, 2015] modified [NIAP CPP_ND_V.1.0, 2015] modified
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015] [NIAP PP_ESM_V.2.1, 2013]
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015]
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	[NIAP CPP_FW_V.1.0, 2015] [NIAP CPP_ND_V.1.0, 2015]
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network and application traffic of monitored networks.	[NIAP PP_NDCP_IPP_EP_V.2.1, 2016] modified
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.	[NIAP PP_ESM_V.2.1, 2013]
OE.PROTECT	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.	[NIAP PP_ESM_V.2.1, 2013] [NIAP PP_ESM_AC_V.2.1, 2013]
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	[NIAP PP_ESM_V.2.1, 2013]
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.	[NIAP PP_ESM_V.2.1, 2013] [NIAP PP_ESM_AC_V.2.1, 2013]

APPENDIX D: Component Detailed Specifications

D.1   Firewalls

D.1.1 Palo Alto Networks PA-3260 with redundant AC power supplies

#	Part Number	Specification	Quantity
1.	PAN-PA-3260	Palo Alto Networks PA-3260 with redundant AC power supplies	1
2.	PAN-SVC-PREM-3260	Premium support year 1, PA-3260	1

D.2 Network Switches

D.2.1 Dell Networking N1124T Switch

#	Item	Specification	Quantity
1.	Configuration	• DELL N1124T-ON Switch • 24x 10/100/1000Mbps half/full duplex RJ45 ports • 4x SFP/SFP+ 1/10GbE ports • 1 RU switch form factor • User Guide • Power cord 250V, 2 M, C13/14	1
2.	Support	• 5 Years Basic Hardware Warranty Repair	1

D.2.2 Dell Networking S3048 Switch

#	Item	Specification	Quantity
1.	Configuration	• DELL S3048 Switch • 48x 1GbE, 4x SFP+ 10GbE, 1x AC PSU • User Guide • Power Supply, 200w, PSU S3048-ON • Jumper cord 250V, 12A, 2 M, C13/C14	1
2.	Support	• Lifetime limited Warranty NBD 5 Year • ProSupport NBD Onsite 5 Year • ProSupport 7X24 HW/SW Tech Support 5 Year	1

D.2.3 Dell Networking S3124F Switch

#	Item	Specification	Quantity
1	210-AIMS	Dell Networking S3124F, L3, 24x 1GbE SFP, 2xCombo, 2x 10GbE SFP+ fixed ports, Stacking, IO to PSU air, 1x AC PSU	2
2	407-BBDB	Dell Networking, Transceiver, SFP, 1000BASE-SX, 850nm Wavelength, 550m Reach	6
3	450-AART	Rack Power Cord 2M, C13/C14, 12A	2
4	470-AAPT	Stacking Cable, for Dell Networking N2000/N3000/S3100 series switches (no cross-series stack), 1m	2
5	709-14075	S3124P,S3124F,S3124 Base Warranty	2
6	709-14076	S3124P,S3124F,S3124 Limited Lifetime Hardware Warranty Minimum Warranty	2

| 7 | 709-14077 | S3124P,S3124F,S3124 90 Days Software Support (Bug Fixes), Software Media Replacement | 2 |
| 8 | 865-11154 | S3124P,S3124F,S3124 3Yr ProSupport and 4hr Mission Critical | 2 |

D.2.4 Dell Networking S3148P Switch

#	Item	Specification	Quantity
1	210-AIMP	Dell Networking S3148P, L3, PoE+, 48x 1GbE, 2x Combo, 2x 10GbE SFP+ fixed ports, Stacking, IO to PSU air, 1x 1100w AC PS	2
2	450-ADXF	European 250V C15 Power Cord for N20xxP/N30xxP	2
3	450-AFHX	Power Supply, 1100w, S3148P, Required for more than 900 watts of POE+, or for redundancy	2
4	470-AAPT	Stacking Cable, for Dell Networking N2000/N3000/S3100 series switches (no cross-series stack), 1m	2
5	709-14107	S3148,S3148P Base Warranty	2
6	709-14108	S3148P Limited Lifetime Hardware Warranty - Minimum Warranty	2
7	709-14109	S3148P 90 Days Software Support (Bug Fixes), Software Media Replacement	2
8	865-11486	S3148,S3148P 3Yr ProSupport and 4hr Mission Critical	2

D.3   Rack

D.3.1 Server Equipment Cabinet

#	Item	Specification	Quantity
1.	5500009 / MODNL	Network rack 800x2000x1200mm	1
2.		Cabinet based on TS-IT	1
3.		Size 800x2000x1200mm (WxHxD) 42HE	1
4.		Color RAL 7035 (light gray) cabinet frame and plate parts Color RAL 9005 (black) interior design	1
5.		Cabinet will be provided with:	
6.		Perforated, vertically divided, front door,	1
7.		(vented surface area approx. 85% perforated)	1
8.		Doors equipped with single-cylinder comfort handle with cylinder locks 3524E and 180 ° hinges	1
9.		Perforated, vertically divided, rear door, (vented surface area approx. 85% perforated)	1
10.		Doors equipped with single-cylinder comfort handle with cylinder locks 3524E and 180 ° hinges	1
11.		Base open	1
12.		Two 482.6 mm (19") mounting sections front and rear, variably mounted on support strips with quick-release fasteners, HE coding on all 19"	1
13.		profiles, statically loadable up to 1500kg	1
14.		Air baffle plates around the 19 inch as a partition between the hot and cold sides, including 6x 1HE blanking panel	1
15.		Roof plate, multi-piece, removable, with side cable entry in the depth	1
16.		and covered cut-out for fan mounting plate	1
17.		shipped on pallet.	1
18.		Loose provided in the cabinet:	
19.		component shelf DK 5501685, depth adjustable 600-900mm (loadable up to 50kg)	1

D.3.2 UPS

#	Item	Specification	Quantity
1	SMC1500I-2U	UPS SMC1500I-2U APC Smart-UPS C 1500VA 2U Rack mountable LCD 230V	1

D.3.3 Power Distribution Unit

#	Item	Specification	Quantity
1	IP-BA-C09SH00010	Powerstrip Conteg 19" 1U Basic PDU, plug IEC 320 C14, power cord 2.8m, Outlets - 9x Schuko, power rating 10A	2

D.5   Management Workstation

D.5.1 Hardware

D.5.1.1   Dell Optiplex 5070 SFF

#	Item	Minimum Requirements
1.	Form Factor	SFF
2.	Microsoft Licences	MS Windows 10 Pro OEM 64bit no-media
3.	Performance	i5- 9500, office productivity of 1073
4.	Processor	6 cores
5.	Graphics	Intel UHD Graphics 630, Performance: at least 917@ 1024x600 in ComputeMark v2.14, Triple Display Capable (1920x1200@60Hz on each display minimum); Compatible with DirectX 12 (Feature Level 12.0) and OpenGL 4.5; HDMI 1.4 and Displayport
6.	Memory	8GB
7.	Storage	Size: min. 240GB, Speed: min. 450MB/sec sequential read and min. 250MB/sec sequential write durability: 72TBW, supported functions: TCG Opal, IEEE-1667, FDE AES-256
8.	I/O Ports	10x USB (5x 3.1 & 5x 2.0) 2x DP 1.2 1x UAJ front incl. audio jack split adapter
9.	Network	On-board Gigabit Ethernet controller 1000BASE-T (RJ-45 interface port)
10.	Network	100Base-FX or 1000BASE-SX, LC connector, Wake-On-LAN, PXE
11.	Drive Bays	1x slim line external bay
12.	Expansion Slots	1x PCIe x16 & 1x PCIe x4, both low profile
13.	Security	Trusted Platform Module (TPM) 2.0 chip on the motherboard; AES New Instructions (AES-NI), SecureKey, BIOS Guard, OS Guard or equivalent; PnP and BIOS setup/boot password/system configuration protection
14.	Lock	Kensington supervisor lock included
15.	HDD cage	Optional Hard Disk Cage with Lock for 2,5" SATA Disk

D.5.1.2 Dell P2419H Monitor

#	Item	Minimum Requirements
1.	Size – diagonal	23.8" screen with ultrathin bezel
2.	Contrast	1000:1
3.	Brightness	250 nits
4.	Standards	TCO certified Displays 7.0
5.	Connections	Yes, 1 x VGA, 1 x HDMI, 1 x DP 1.2 standard ports
6.	Native refresh rate	60Hz
7.	Horizontal/vertical viewing angle	178 degrees horizontally and vertically
8.	Native resolution	FHD resolution 1920 x 1080 with 82% sRGB coverage or CIE 1931 value of >= 72%
9.	Speakers	Dell AC 511M Soundbar with 2x1,25 W speakers included
10.	Tilt and Swivel	Tilt: +21deg/-5deg Swivel: 90deg
11.	Appearance	Black colour
12.	Power supply and cords	1x Power cord included
13.	Cabling	1x DisplayPort cable (cable length 1.8m) included
14.	Lock	Kensington lock slot included

D.5.1.3 Dell KB216 Multimedia Keyboard

#	Item	Minimum Requirements
1.	Device	US QWERTY keyboard

NATO UNCLASSIFIED

2.	Compatibility	Microsoft Windows 10 Enterprise
3.	Connectors	USB
4.	Additional Features	Low profile keys
5.	Cabling	Length: 1.5m

D.5.1.4 Dell 6 Button Laser Mouse

#	Item	Minimum Requirements
1.	Device	Ergonomic keyboard US QWERTY
2.	Compatibility	Microsoft Windows 10
3.	Connectors	USB
4.	Additional Features	Low profile keys
5.	Cabling	Length: 1.0m

APPENDIX E: Named Elements

Common components acronyms used within the named elements

ACRONYM	DESCRIPTION
AV	Attachment Validation
BS	Business support
CIP	Content Inspection Policy
CIPE	Content Inspection Policy Enforcement
CIS	Content Inspection Services
COI	Community of Interest
DEX	Data Exchange services
EV	Envelope Validation
FLOT	First Line Of Text
HL	High-to-Low
IEG-FS	Information Exchange Gateway Functional Services
IFCPE	Information Flow Control Policy Enforcement
IFP	Information Flow control Policy
LH	Low-to-High
LV	Label Validation
MG	Mail guard component
PKCS	Public Key Cryptographic Services
SOA	Service Oriented Architecture
SV	Schema Validation
WG	Web guard component

Interfaces can be identified by the use of the "IF_" component. This component is generally prefixed by the related component, Web Guard (WG) or Mail Guard (MG).

NAME	DESCRITPION
IEG-C_IF_MGMT	Overall IEG-C Management Network Interface
IEG-C_IF_NET_HIGH	Overall IEG-C High Domain Network Interface
IEG-C_IF_NET_LOW	Overall IEG-C Low Domain Network Interface
MG_IF_LOCAL_MGMT	Mail Guard Local Management Interface
MG_IF_MGMT	Mail Guard (Remote) Management Network Interface
MG_IF_NET_HIGH	Mail Guard High Domain Network Interface
MG_IF_NET_LOW	Mail Guard Low Domain Network Interface
WG_IF_LOCAL_MGMT	Web Guard Local Management Interface
WG_IF_MGMT	Web Guard (Remote) Management Network Interface
WG_IF_NET_HIGH	Web Guard High Domain Network Interface
WG_IF_NET_LOW	Web Guard Low Domain Network Interface

Rulesets are prefixed with ''RULESET_"

NAME	DESCRIPTION
RULESET_MG_IFCPE-CA_HL_IN	Mail Guard Communications Access High to Low Inbound
RULESET_MG_IFCPE-CA_HL_OUT	Mail Guard Communications Access High to Low Outbound
RULESET_MG_IFCPE-CA_LH_IN	Mail Guard Communications Access Low to High Inbound
RULESET_MG_IFCPE-CA_LH_OUT	Mail Guard Communications Access Low to High Outbound
RULESET_MG_IFCPE-MGMT_IN	Mail Guard Management Inbound
RULESET_MG_IFCPE-MGMT_OUT	Mail Guard Management Outbound
RULESET_WG_CIS_HV-HL	Web Guard Header Validation High to Low
RULESET_WG_CIS_HV-LH	Web Guard Header Validation Low to Hugh
RULESET_WG_CIS_LV	Web Guard Label Validation
RULESET_WG_CIS_HV	Web Guard Header Validation
RULESET_WG_CIS_SV	Web Guard Schema Validation
RULESET_WG_CIS_MD	Web Guard Malware Detection
RULESET_WG_IFCPE-CA_HL_IN	Web Guard Communications Access High to Low Inbound
RULESET_WG_IFCPE-CA_HL_OUT	Web Guard Communications Access High to Low Outbound
RULESET_WG_IFCPE-CA_LH_IN	Web Guard Communications Access Low to High Inbound
RULESET_WG_IFCPE-CA_LH_OUT	Web Guard Communications Access Low to High Outbound
RULESET_WG_IFCPE-MGMT_IN	Web Guard Management Inbound
RULESET_WG_IFCPE-MGMT_OUT	Web Guard Management Outbound

Variables are prefixed with a keyword representing the type of data they are to hold:

- ACTIONS_: A set of actions.
- BOOL_: A boolean.
- LIST_ : A list of values.
- NUM_ : An integer
- STR_ : An array of characters

NAME	COMMENT
BOOL_MG_CIS_LV_CB	Indicates whether a Cryptographic Binding is required
LIST_MG_CIS_AV_DIRTYWORDS	Mail Guard Dirty Words (Attachment Validation)

NAME	COMMENT
LIST_MG_CIS_AV_MALWARE_DEFINITIONS	list of definitions/signatures of currently known malware
LIST_MG_CIS_AV_TYPES	Mail Guard Attachment Types (Attachment Validation)
LIST_MG_CIS_EV_ORIG	List of allowable SMTP originator
LIST_MG_CIS_EV_RECIPS	List of allowable SMTP recipients
LIST_MG_CIS_LV_FLOT	List of valid FLOT markings;
LIST_MG_CIS_LV_KEYWORDS	List of valid keywords.
LIST_MG_CIS_LV_TP	List of trust points (e.g. trusted root certificates).
LIST_MG_CIS_LV-CRL	List of certificate revocation lists
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-SPIF	List of allowable security policies (including classifications and categories)
LIST_WG_CIS_LV-CM	List of Canonicalization Methods.
LIST_WG_CIS_LV-CRL	List of certificate revocation lists
LIST_WG_CIS_LV-TP	List of trust points (e.g. trusted root certificates).
LIST_WG_CIS_LV-XS	List of XML Schemas (Label Validation)
LIST_WG_CIS_SV-NS	List of valid namespaces
LIST_WG_CIS_SV-XS	List of XML schemas (Schema Validation)
NUM_MG_CIS_AV_ATTACHMENTS	The maximum number of attachments
STR_MG_CIS_LV_FLOT_PREFIX	Prefix to identify a FLOT in a message
STR_MG_CIS_LV_KEYWORD_HEADER	SMTP header field which contains keywords
LIST_WG_CIS_LV-DM	List of Digest Methods
LIST_WG_CIS_LV-SM_HMAC	List of HMAC Signature Methods
LIST_WG_CIS_LV-SM_PKI	List of PKI Signature Methods

Outcomes are prefixed with "O_".

NAME	COMMENT
O_MG_CIS_AV	Outcome of Mail Guard attachment validation
O_MG_CIS_EV	Outcome of Mail Guard envelope validation
O_MG_CIS_LV	Outcome of Mail Guard label validation
O_MG_CIPE_HL	Outcome of Mail Guard Content Inspection High to Low
O_MG_CIPE_LH	Outcome of Mail Guard Content Inspection Low to High
O_MG_CIS	Outcome of Mail Guard Content Inspection Service
O_MG_IFCPE	Outcome of Mail Guard Information Flow Control Policy
O_WG_CIPE_HL	Outcome of Web Guard Content Inspection High to Low
O_WG_CIPE_LH	Outcome of Web Guard Content Inspection Low to High
O_WG_CIS	Outcome of Web Guard Content Inspection Service
O_WG_IFCPE	Outcome of Web Guard Information Flow Control Policy