Thales Communications & Security
4, Avenue des Louvresses
92622 Gennevilliers Cedex
France
Tel.: +33 (0)1 41 30 30 00
Fax: +33 (0)1 41 30 33 57
www.thalesgroup.com

SECURITY TARGET FOR MISTRAL VS9.0 GATEWAY SOFTWARE (CDS)

MISTRAL VS9.0 GATEWAY SOFTWARE

TABLE OF CONTENT

TABLE OF FIGURE

TABLE OF TABLE

1. INTRODUCTION

1.1. DOCUMENT IDENTIFICATION AND SUMMARY

Document reference: 63535113-306

Document version: -L lite

Evaluation Level: EAL3+ (EAL3 augmented with ALC_FLR.3 and AVA_VAN.3)

The security target is based on the Security Requirements of the collaborative Protection Profile for Network Devices [c_PP].

1.2. TOE IDENTIFICATION

TOE is Mistral gateway software V9.0.7.2 for Mistral system version 9.0. The same Mistral gateway software is embedded in Mistral gateway devices TRC7540-2.

The group formed by the Mistral gateway software embedded in Mistral gateway device, is called SS_IPSEC_GW. The relative commercial name is “IP9001” for TRC7540-2.

TOE, Mistral gateway, version's format is as follow: V9.x.y.z

x is the system version

y identifies major functional version

z is an optional free field and indicates test version, debug version (if it includes a d) or a version with minor evolutions on a same functional boundary

1.3. ABBREVIATION AND ACRONYMS

1.3.1. Administrative acronyms

Acronym	Meaning
ANSSI	National Agency for Information System Security
CC	Common Criteria
COTS	Component Off The Shelves
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Function Requirement
SFT	Security Function of the TOE
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Table 1: Administrative acronyms

1.3.2. Technical acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
AH	Authentication Header
ARP	Address Resolution Protocol
CBC	Cipher Block Chain
CLI	Command Line Interface
CRL	Certificate Revocation List
DR	Diffusion Restreinte
DRGB	Deterministic Random Bit Generator
ECDH (E)	Elliptic Curve Diffie-Hellman (Ephemeral)
ECDSA	Elliptic Curve Digital Signature Algorithm
ESN	Extended Serial Number

Acronym	Meaning
ESP	Encapsulating Security Payload
GCM	Galois Counter Mode
HMAC	Hash-based Message Authentication Code
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IGL	Local Management Interface (Interface de Gestion Locale)
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
LED	Light-Emitting Diode
MAC	Message Authentication Code
MMC	Mistral Management Center
MTU	Maximum Transmission Unit
NAT	Network Address Translation
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
OS	Operating System
RFC	Request For Comments
PFS	Perfect Forward Secrecy
PRF	Pseudo-Random Function
RSA	Rivest–Shamir–Adelman (public-key cryptosystem)
SA	Security Association
SHA	Secure Hash Algorithm
SP	Security Policy
SPI	Security Parameter Index
SSH	Secure Shell
TBD	To Be Defined
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network

Table 2 : Technical acronyms

1.3.3. Nomenclature rules

- A.: Assumption prefix
- F.: Security Function prefix
- O.: Security Objective prefix
- OE.: Security Objective for the TOE Environment
- P.: Organizational Security Policy prefix
- S_: System object of the solution prefix
- SS_: SubSystem of the system prefix
- CS_: Cooperative System prefix
- CSS_: SubSystem of the systems Cooperative prefix
- T.: Threat prefix
- ST_: State prefix
- U.: User prefix
- OP.: Operation

1.4. REFERENCES DOCUMENTS

	Title	References	version
RGS_B	Rules and recommendations regarding the management of cryptographic mechanisms Annex B1, B2 and B3 of « Référentiel Général de Sécurité »	N/A	**2.0**
CC-01	Common Criteria for Information Technology Security Evaluation: Introduction and general model	CCMB-2017-04-001	**3.1** Revision 5 - Part 1 - April 2017.
CC-02	Common Criteria for Information Technology Security Evaluation: Security functional components	CCMB-2017-04-002	**3.1** Revision 5 - Part 2 - April 2017.
CC-03	Common Criteria for Information Technology Security Evaluation: Security assurance components	CCMB-2017-04-003	**3.1** Revision 5 - Part 3 - April 2017.
CEM	Common Criteria for Information Technology Security Evaluation: Evaluation methodology	CCMB-2017-04-004	**3.1** Revision 5 - April 2017.
c_PP	collaborative Protection Profile for Network Devices	N/A	**2.1** – 24-Sep-2018
DR PROFILE	Note Crypto Référentiel IPSec DR	N°2765/ANSSI/DR	5-May-2017

Table 3: Reference documents

1.5. APPLICABLE DOCUMENTS

	Title	References	version
LINUX_ANSSI	Recommandations de configuration d'un système GNU/Linux	ANSSI/BP-028	**1.2 –** Mar. 2019
PARTIONNING _ANSSI	Recommandations pour la mise en place de cloisonnement système.	ANSSI-PG-040	**1 –** 14 Dec. 2017

Table 4: Applicable documents

2. TOE OVERVIEW

2.1. MISTRAL SYSTEM OVERVIEW

2.1.1. Architecture of the Mistral system

Mistral system (S_MISTRAL) is provided by **ROLE_PROVIDER** to **ROLE_ORGANISATION** (customer organisation) to protect the dataflow between ROLE_ORGANISATION stations for unique equipment as well as for a complex network with multiple site accesses.

Mistral system (S_MISTRAL) is composed with:

- IPv4 gateway (**SS_IPSEC_GW**) following DR profile (IPSec tunnel mode only, ESN etc.)
- Mistral Management Center (**SS_MMC**),
- Factory SECret OPerationS sub-system (**SS_FACTORY_SEC_OPS**) used by ROLE_PROVIDER to protect software before delivery,
- Production sub-system (**SS_PRODUCTION**) used by ROLE_PROVIDER to produce and check SS_IPSEC_GW before delivery,
- Soft delivery system (**SS_SW_DELIVERY**)

Nota: SS_IPSEC_GW is connected to the plaintext data network (i.e. the trusted network called CSS_RED_NETWORK), and to the ciphered data network (i.e. the untrusted network called CS_BLACK_NETWORK) with different interfaces.

Only **SS_IPSEC_GW** and **SS_MMC** are delivered by ROLE_PROVIDER to the ROLE_ORGANISATION**.**

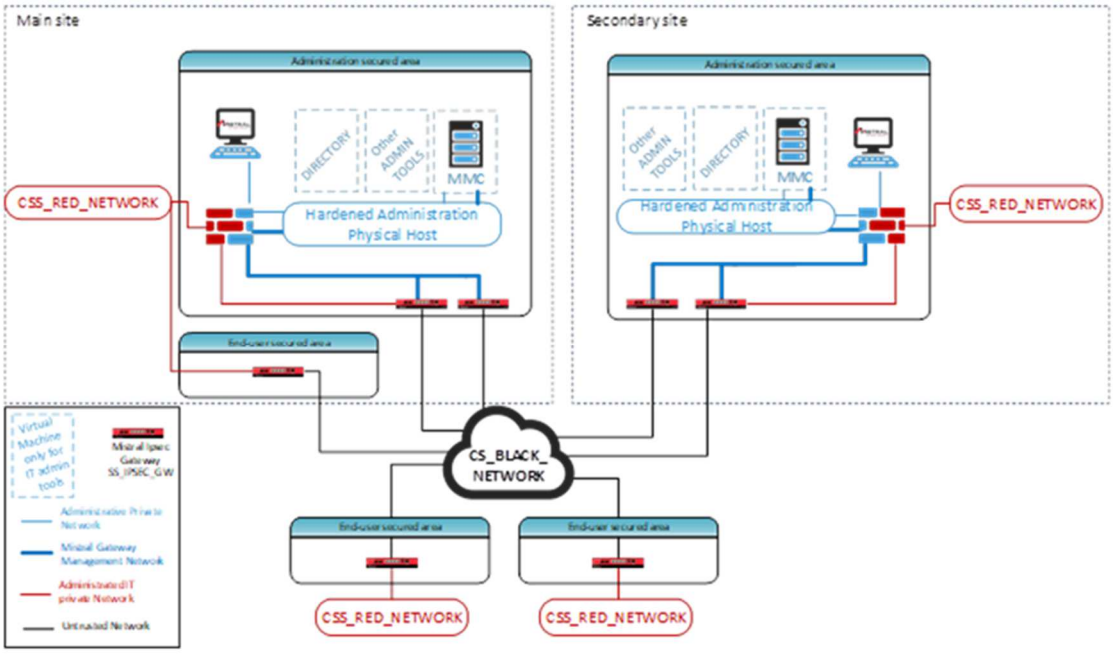

Figure 1: Example of MISTRAL System architecture with admin network

The cooperating systems and sub-systems are:

- Untrusted network (**CS_BLACK_NETWORK**)
- Trusted network (**CSS_RED_NETWORK**)
- Customer facilities (**CS_ORGANIZATION**)
- Sub-system providing the certification authority and certificates (**CSS_PKI**)
- Supervision center (**CSS_SOC**)
- Physical USB support used for data (configuration file, certificates and logs) transportation (**CSS_USB_MEDIA**)
- IPSec peers (**CSS_IPSEC_PEER**) other gateway than **SS_IPSEC_GW** which may connect to **SS_IPSEC_GW** using the same protocols and certificates.

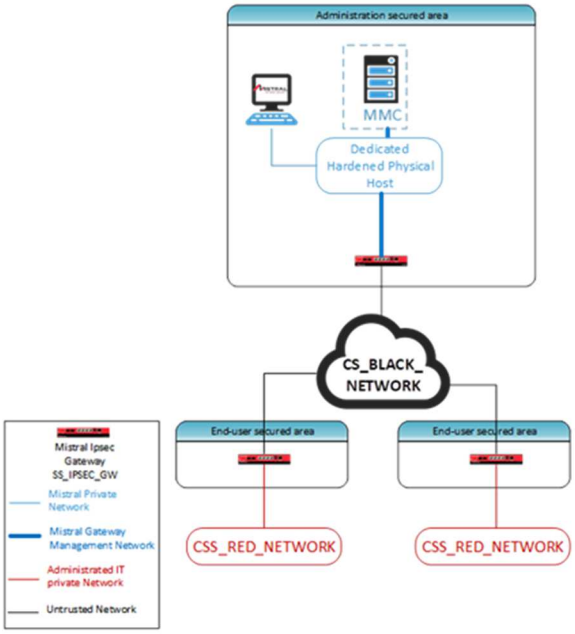

Figure 2: Example of MISTRAL System architecture without admin network

2.1.2. SS_IPSEC_GW

SS_IPSEC_GW provides data exchanges protection based on VPN (« Virtual Private Network ») technology across untrusted path. It secures data communication links inside network handling data at restricted level of classification (DIFFUSION RESTREINTE, NATO RESTRICTED, and RESTREINT UE/EU RESTRICTED).

2.1.3. Administration center

The elements of the administration center are used for the SS_IPSEC_GW configuration and certificates management and for monitoring:

- CSS_PKI is the element providing the certificates generated with SS_ IPSEC_GW public key.
- SS_MMC is the element of Mistral Management Center (MMC). It is composed of software located on a web server (virtual machine on Linux). SS_MMC must be authenticated by SS_IPSEC_GW and use a secured link (with parameters defined in the SS_IPSEC_GW) in order to remotely configure the SS_IPSEC_GW (see Figure 1: Example of MISTRAL System architecture) with configuration file and commands.

*Nota: **CSS_PKI** is required for the system but it can be an external service*

2.2. TOE DESCRIPTION

2.2.1. TOE definition

TOE is the software of the SS_IPSEC_GW, a network device providing IP datagram protection based on VPN (« Virtual Private Network ») technology. It secures data communication links.

2.2.2. TOE boundary

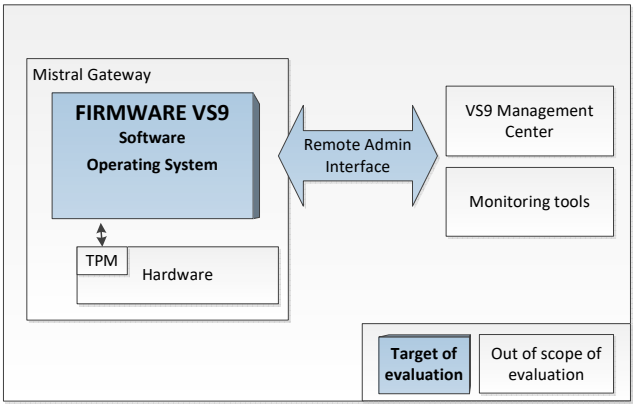

Figure 3 : TOE Boundary

The TOE is the **Mistral software** running on the SS_IPSEC_GW **with IPSec DR profile** in IPv4 environment. It is composed of a Linux OS and the Mistral applications.

The Linux OS is hardened and complies with guidance from French administration to secure Linux OS [LINUX_ANSSI] and [PARTIONNING_ANSSI].

All other components of the Mistral system are considered as part of the operational environment.

Hardware equipment is out of scope of the Target of Evaluation described in this Security Target. Following enabling elements, the Mistral Management Center device (SS_MMC), the Public Key Infrastructure device (CSS_PKI) are outside the TOE. SS_MMC may be replaced by any third party management system compliant with IF_REMOTE_MGT and IF_LOG_EXPORT.

2.2.3. TOE functionalities

The TOE's main functionalities are:

Dataflow protection (Control and filtering) from Ethernet interfaces, with Security Policies configuration allowing:

- IPv4 Data flow protection (against disclosure, modification, insertion and replay) with IPSec ESP Tunnel encapsulation mode, which provides datagram payload data and topology data encryption, integrity and anti-replay following only the cryptographic algorithms described in the IPSec DR profile.
- Data flow discard if no protection policy has been found for the flow.

Management flow control and protection:

- Management flow protection (against disclosure, modification, insertion and replay) with TLS VPN

TOE security management:

- Certificate and Key management
- Secure sensitive data storage with partition of red and black networks
- Secure boot
- Secure erasure
- Secure software update
- Self-tests (PBIT at start-up and IBIT on request)
- Supervision
- Audit generation

2.2.4. TOE Interfaces

TSFI identifier	Description
IF_GW_LOCAL_MGT	**Interface man-machine for command on line (CLI)** Local interface on SS_IPSEC_GW serial port used by ROLE_GW_OPERATOR (cf. § **Erreur ! Source du renvoi introuvable.**).
IF_REMOTE_MGT	**Remote management Interface** Interface between SS_IPSEC_GW and SS_MMC via IF_ETHERNET_RED or IF_VPN_ADMIN used by ROLE_SYS_ADMIN (cf. § **Erreur ! Source du renvoi introuvable.**).
IF_USB_MEDIA	**Interface of data import / export via CSS_USB_MEDIA**
IF_GW_VISU	**Visual interface** Interface allowing to check TOE status, network connection status and DR profile activation
IF_GW_WIPE_BTN	**Secure erasure button interface** Physical button triggering secure erasure.
IF_PKI	**CSS_PKI interface** Interface with CSS_PKI via IF_USB_MEDIA (using commands on IF_GW_LOCAL_MGT) or via IF_REMOTE_MGT for certificate import / export.
IF_GW_LOG_EXPORT	**Log files export interface** Interface used to export log files via IF_USB_MEDIA using commands on IF_GW_LOCAL_MGT.
IF_LOG_EXPORT	**Events transmission interface** Interface used to transmit events to SS_MMC via IF_ETHERNET_RED or IF_VPN_ADMIN.
IF_DOWNLOAD	**Software update interface** Interface used to get update software from SS_MMC via IF_RED_NETWORK or IF_VPN_ADMIN.
IF_SW_UPDATE	**Software update protection interface** Interface used to protect update software with SS_FACTORY_SEC_OPS
IF_VPN	**CS_BLACK_NETWORK interface for traffic** Virtual Private Network interface with IPSec gateway
IF_VPN_ADMIN	**CS_BLACK_NETWORK interface for TOE management** Virtual Private Network interface with IPSec gateway

Table 5: TSFI list

Supporting interface identifier	Description
IF_BLACK_NETWORK	**CS_BLACK_NETWORK interface** Interface for interactions with CS_BLACK_NETWORK concerning user data flow and network services with other sub-systems of S_MISTRAL on untrusted side.
IF_RED_NETWORK	**CSS_RED_NETWORK interface** Interface for interactions with CSS_RED_NETWORK concerning user data flow and network services with other sub-systems of S_MISTRAL on trusted side

Table 6: Network interfaces supporting TSFI

2.2.5. TOE states

2.2.5.1. TOE configuration state

State	Description
ST_GW_FACTORY	TOE software is loaded on the hardware. The local Operator account is created with default parameters. Provider asset are loaded without any customer parameters. It is also the final state of the TOE when a secure erasure is launched.
ST_GW_PERSONALIZED	The local operator password has been set up, the TOE encryption data have been loaded and the TOE has been customized.
ST_GW_CONFIGURED	Time has been configured and a configuration file has been loaded. TOE is ready to connect SS_MMC (if exists) and to create VPN IPSec with other TOE instances for user traffic depending of the configuration file loaded.

Table 7: Configuration state description

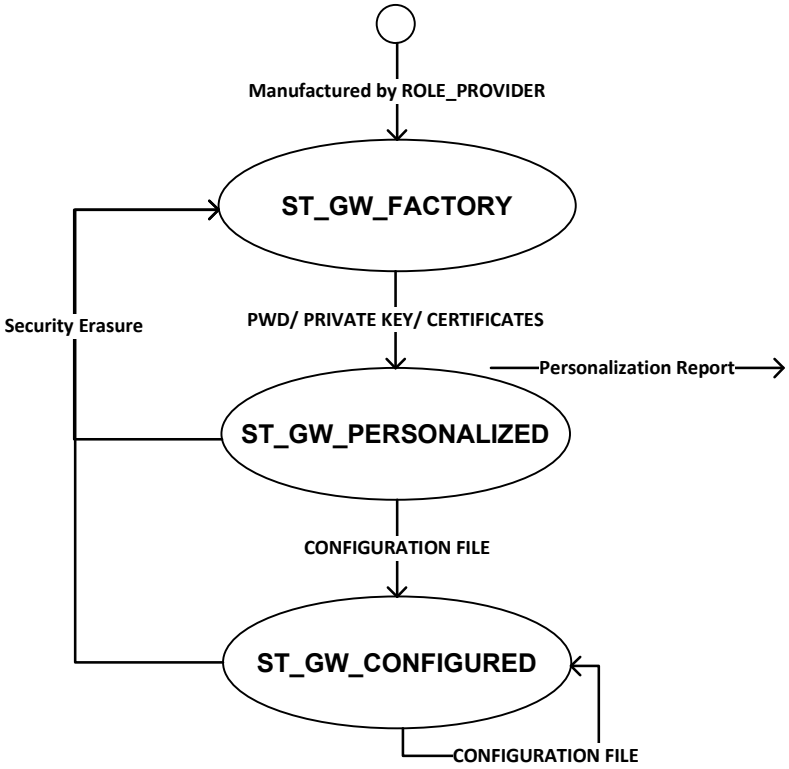

Figure 4: Configuration state diagram

2.2.5.2. TOE functional state

- ST_FAILURE: TOE enters this state when a failure is detected. It requires a system fix or be sent back to the provider.
- ST_OPERATIONAL: TOE provides its services depending of its configuration state.

2.2.6. TOE lifecycle

The TOE lifecycle is illustrated below:

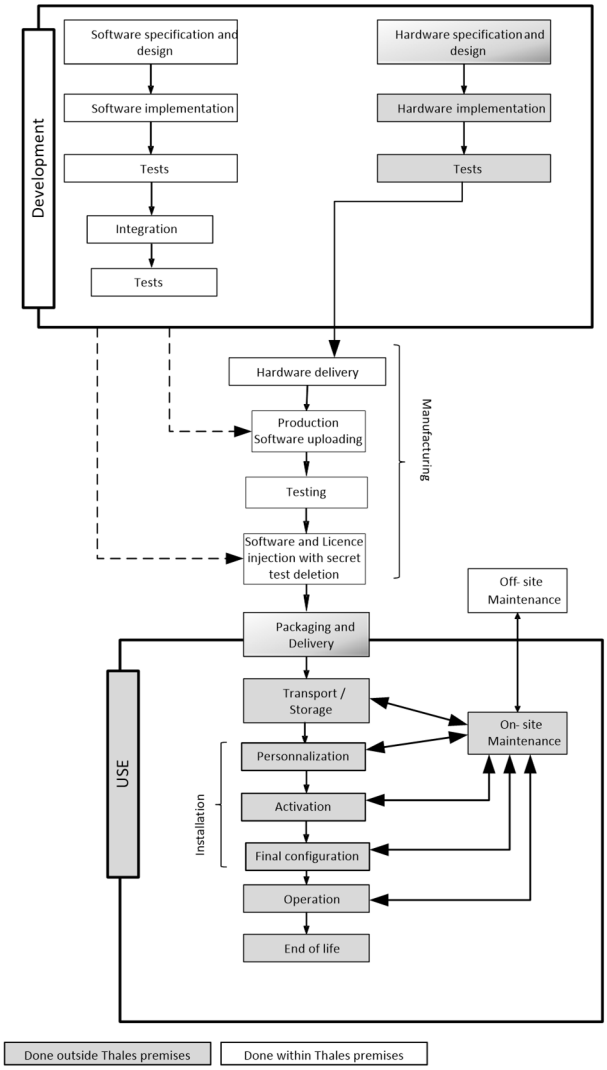

Figure 5: TOE Lifecycle

2.2.7. TOE update

TOE update consists in 3 steps.

- Software provider delivers software update to SS_MMC that informs the TOE that a software update is available.
- Then, TOE:
  - Downloads firmware update from SS_MMC through VPN,
  - Checks authenticity,
  - Decrypts firmware update and
  - Checks version number of firmware update.
- SS_MMC informs TOE to activate the software uploaded. TOE

- Installs firmware update when the firmware update has been accepted,
- Restarts TOE (self-test are automatically launched).
- In case of update failure, previous version can be reactivated by SS_MMC.

In case of any error, TOE stops process and continue its nominal activity. SS_MMC is aware about TOE state and its software version, it is in charge to launch again the procedure if necessary.

3. CONFORMANCE CLAIM

3.1. CC CONFORMANCE CLAIM

This security target is conformant to Common Criteria 3.1 revision 5 of April 2017:

- [CC-02] extended
- [CC-03] conformant

Here is the list of the Security Functional Requirement refined:

Object Name	Comment
FAU_GEN.1	
FAU_GEN.2	Precision about network device
FDP_UCT.1	Precision about use of the SFP
FDP_UIT.1	Precision about use of the SFP
FDP_ITC.2/VPN	VPN SFP enforcing
FDP_ETC.2/VPN	VPN SFP enforcing
FDP_ITC.2/CRYPTOINJECTION	Certificate injection enforcing
FMT_MSA.3	Precision of default value
FIA_UID.2	MMC limitation
FIA_UAU.6	Precision of the user U.ROLE_GW_OPERATOR
FIA_UAU.7	Precision of the user U.ROLE_GW_OPERATOR
FCS_CKM.1	For asymmetric cryptographic keys
FCS_CKM.2	For Key establishment
FCS_COP.1/Hash256	
FCS_COP.1/Hash384	
FCS_COP.1/KeyedHash256	
FCS_COP.1/KeyedHash384	
FTA_SSL.3	For remote session
FTA_SSL.4	Precision of the user U.ROLE_GW_OPERATOR
FTP_ITC.1	
FTP_TRP.1	

Table 8: Refined SFR

3.2. C_PP CONFORMANCE CLAIM

This security target is based on (but not conformant to) collaborative Protection Profile for Network Devices [c_PP].

Threats, Organizational Security Policies and Security Objective depicted in [c_PP] are all drawn to this ST.

Here is the list of the extended Security Functional Requirement part with the adaptation:

Object Name	Comment
FAU_STG_EXT.1	
FAU_STG_EXT.2/LocSpace	
FCS_RBG_EXT.1	
FCS_CKM_EXT.5/CERTIFICATE	SFR added to cover security objective

Object Name	Comment
FCS_CKM_EXT.5/IKEV2SA	
FCS_CKM_EXT.5/IKEV2CHILDSA	
FIA_X509_EXT.1	
FIA_X509_EXT.2	
FIA_X509_EXT.3	
FCS_IPSEC_EXT.1	
FCS_TLSC_EXT.2	
FCS_TLSS_EXT.2	
FCO_CPC_EXT.1	
FIA_PMG_EXT.1	
FIA_UIA_EXT.1	
FIA_UAU_EXT.2	
FTA_SSL_EXT.1	
FPT_SKP_EXT.1	
FPT_TUD_EXT.1	
FPT_APW_EXT.1	
FPT_TST_EXT.1	
FPT_STM_EXT.1	
FPT_SDP_EXT.2	SFR added to cover security objective

Table 9: Extended SFR

Note: These SFR are inspired from extended SFR proposed in cPP. The numbering used here respects the numbering used for the SFR of this document. For example, FCS_TLSC_EXT.1 is not used here, but the title of SFR FCS_TLSC_EXT.2 remains even if it is the first SFR FCS_TLSC_EXT of the ST.

3.3. PACKAGE CONFORMANCE CLAIM

This security target is conformant to EAL3+ consisting to EAL3 package augmented with ALC_FLR.3 and AVA_VAN.3.

4. SECURITY PROBLEM DEFINITION

The TOE is to be set up between a local network and a remote one, connected to its remote peer on the remote network. It creates a protected channel (IPSec tunnel) for confidentiality, authenticity and no reply between the local and remote networks. The tunnel is used to send (OP.Sending) and receive (OP.Receiving) trusted traffic over an untrusted network. The mutual authentication is performed with X509 certificates previously injected in the TOE (OP.Injection).

The TOE aims to protect all assets which are (typically) placed in the internal network and therefore shall be protected appropriately. The TOE protects the integrity of the software with secure boot and regular self-test using cryptographic mechanism. Software delivery is also protected by being ciphered and signed by THALES.

The TOE is intended to be used in a physically protected environment. It is assumed that no unauthorized personnel have physical access to the TOE. Therefore all attacks to the TOE have to be performed over the network connections of the TOE.

The TOE is assumed to operate in an environment where interception of radiation is covered by other environmental measures. The evaluation will therefore not address vulnerabilities caused by emanation from the TOE. Remote administrators and operators of the TOE authenticated with a TLS certificate are considered to be trustworthy.

It is also assumed that administrators are well trained, reducing the risk that they accidentally make security critical administration mistakes.

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- All assets including the protection they required (confidentiality, Integrity or/and Availability)
- All different users
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used

4.1. ASSETS

This section lists sensitive assets. For each of them, it associates a "security needs" attribute indicating what protection the asset needs.

Default values of parameters are specified within the requirement FMT_MSA.3.

4.1.1. Assets protected with the TOE (User Data)

User data are external data protected by the TOE:

- Applicative data are the sensitive data transmitted from a sensitive trusted sub-network to another sensitive trusted sub-network across an untrusted network,
- Red topology information is available from the trusted networks; it consists in IP address of customer, remote administration IP address.

Security needs of such data are: Confidentiality, Authenticity and Integrity.

4.1.2. Assets belonging to the TOE (TSF Data)

TSF data are internal data belonging to the TOE:

- Configuration parameters such as time, gateway range, software version, certificates and cryptographic data
- Master and session cryptographic keys used for VPN IPSec or TLS establishment
- Cryptographic keys, certificates and credentials used for the self-protection of the TOE in all states (in-rest or in-use)
- Security Associations (SAs) and Security Policies (SPs) configured within the TOE

  Security Associations are characterized at least by following parameters:

  - SPI: unique identifier of the SA
  - Protection mode : IPSec_Tunnel using ESP
  - Key management mode: negotiated mode (that is use of IKE protocol)
  - Certificates and associated Public keys
  - Peer IP address: IP address of a remote instance of the TOE
  - Lifetime of negotiated keys

  Security Policies are characterized at least by following parameters:

  - Action
  - Source IP address
  - Destination IP address
  - SA Identifier (link between SP and SA)
  - Authorized protocol and ports (for TCP and UDP)

- TOE supervision data (TOE state and audit record generated by the TOE).
  The format identified is SYSLOG protected with secure protocol (integrity protection) when the events are sent to remote devices
- The applicative software of the TOE
- The operating system of the TOE

Security needs of such data are: Confidentiality, Authenticity and Integrity.

4.2. USERS, SYSTEM AND SUB-SYSTEM

4.2.1. U.ROLE_GW_OPERATOR

TOE local operator interacts with the TOE through the CSS_LMGT and IF_GW_WIPE_BTN. He can at least

- Start the TOE
- Personalize the TOE
- Manage certificates on the TOE
- Load the TOE configuration file
- Check events on the TOE
- Launch secure erasure.

4.2.2. U.ROLE_SYS_ADMIN

TOE central administrator interacting with the TOE through the remote management service on SS_MMC.

4.2.3. SS_IPSEC_GW

Main TOE component composed of Mistral software embedded in Mistral gateway.

4.2.4. SS_MMC

TOE management center device, it is a device where remote management service is installed and interacts remotely with the TOE.

4.2.5. CSS_LMGT

TOE local management device, it interacts with the TOE through the Local Management Interface.

4.2.6. CSS_PKI

Public Key Infrastructure device, it is used for certificates generation.

4.3. ASSUMPTIONS

4.3.1. Securing the TOE

4.3.1.1. A.LIMITED_FUNCTIONALITY

The devices are assumed to provide networking functionality as their core function and not provide functionality/services that could be deemed as general purpose computing. For example the devices should not provide computing platform for general purpose applications (unrelated to networking functionality).

4.3.1.2. A.PHYSICAL_PROTECTION

The network device 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 device's physical interconnections and correct operation. SS_IPSEC_GW are installed and stored according to the state of the art regarding sensitive security devices and no unauthorized entities are able to interact physically with it. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, there is no requirement on physical tamper protection or other physical attack mitigations. It is not expected to defend the SS_IPSEC_GW against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device but SS_IPSEC_GW includes a way to detect physical intrusion (seals …).

4.3.1.3. A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an administrator **(Refinement) (U.ROLE_SYS_ADMIN)** on a regular basis in response to the release of product updates due to known vulnerabilities or software error.

4.3.1.4. A.TOE_ERASURE

The network device is assumed to be securely erased (security wipe button or commands) before any transportation outside protected premises or long storage.

4.3.1.5. A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the TOE requirements. It is assumed that this protection will be covered by requirements for particular types of network devices (e.g., firewall).

4.3.2. Administration

4.3.2.1. A.TRUSTED_ADMINISTRATOR

The **(Refinement) Administrators (U.ROLE_GW_OPERATOR and U.ROLE_SYS_ADMIN)** for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. They are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

4.3.2.2. A.ALARM

It is assumed that critical security audit data generated and forwarded by the TOE are remotely analyzed and processed after reception when remote administration is activated.

It is assumed that the TOE local operator (U.ROLE_GW_OPERATOR) may analyze and process alarms after their generation.

4.3.2.3. A.POLICIES_CONTINUITY

The system shall make sure that the information security policies of the two networks interconnected through the TOE are consistent between each other.

4.3.2.4. A.ADMINISTRATION_NETWORK

It is assumed that the administration network is a trusted network, dedicated to administration devices and isolated from other networks by boundary devices.

4.3.2.5. A.ADMIN_CREDENTIALS_SECURE

The administrator's credentials (refinement**: password and** private key) used to access the network device are protected by the platform on which they reside.

4.3.3. Assumptions about management devices

4.3.3.1. A.SECURED_MANAGEMENT_DEVICES

It is assumed that administration devices (the TOE management center device SS_MMC, the TOE local management device CSS_LMGT, the Public Key Infrastructure device CSS_PKI, the device delivering TOE software update, which belongs to SS_SW_DELIVERY etc) are properly and securely configured, according the sensitivity of assets they handle and generate events on each application access and application configuration operation
It is also assumed that these devices are regularly updated. For the SS_MMC in particular, an authorized administrator is in charge to update the software and/or the OS with deliveries provided by ROLE_PROVIDER.

4.3.3.2. A.ACCESS_CONTROL_MANAGEMENT_DEVICES

It is assumed that the access to administration devices (the TOE management center device SS_MMC, the TOE local management device CSS_LMGT, the Public Key Infrastructure device CSS_PKI, the device delivering TOE software update, which belongs to SS_SW_DELIVERY etc) is controlled and that these devices are managed by authorized administrator only.
The overall solution shall allow individual accounting. It can be physical (e.g. physical access restriction to the device hosting the software) and/or logical (e.g. user authentication by the operating system).

4.3.3.3. A.PHYSICAL_ENV_MANAGEMENT_DEVICES

It is assumed that physical security of the administration devices (the TOE management center device SS_MMC, the TOE local management device CSS_LMGT, the Public Key Infrastructure device CSS_PKI, the device delivering TOE software update, which belongs to SS_SW_DELIVERY etc) is commensurate with the value of the data concerning the TOE they contain and is provided by the environment.

4.3.3.4. A.AUDIT

It is assumed that the auditor regularly reviews audit events generated by the TOE.
It is also assumed that the memory units storing audit events are managed so that the auditor does not lose events too quickly.

4.3.3.5. A.SS_MMC_TO_TOE

It is assumed that the TOE management center device (SS_MMC) connects TOE:

- through trusted network (red side) or
- through untrusted network (black side) protected with IPSEC VPN managed by Mistral system.

4.3.3.6. A.DATA_TRANSPORTATION

It is assumed that physical devices used to transport sensitive data are manipulated in secure way during their transportation.

4.4. ORGANIZATIONAL SECURITY POLICIES (OSP)

4.4.1. Services

4.4.1.1. P.PROVIDED_SERVICES

The TOE shall enforce VPN security policies loaded by the TOE administrators (U.ROLE_GW_OPERATOR and U.ROLE_SYS_ADMIN).

It shall provide all related security services necessary to perform protections specified in these policies:

- datagram filtering,
- confidentiality protection of applicative data,
- integrity and authenticity protection of applicative data,
- protection against replay of applicative data,
- confidentiality protection of red topologic data on the untrusted network

4.4.1.2. P.AUDIT

The TOE shall record events concerning security functions and provide the possibility to send the records to remote center. Some of events are considered as alarm when an external action is required.

4.4.1.3. P.SUPERVISION

The TOE shall enable U.ROLE_SYS_ADMIN to review the operational status of the TOE and the VPN connections state.

4.4.2. Miscellaneous

4.4.2.1. P.CRYPTO_RGS

The TOE shall implement cryptographic mechanisms compliant with ANSSI guidance [RGS_B].

4.4.2.2. 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 Mistral application.

4.4.2.3. P.SA_SP_PROTECTION

The TOE shall protect the integrity and confidentiality of the SP and SA configuration while persistently stored.

4.4.2.4. P.TOE_PRODUCTION

The TOE shall be produced following the rules described below:

- Development is located in THALES secured premises
- Development is performed on dedicated network
- Private keys receive a special care in secured premises
- Hardware hosting the TOE is tested (bypass)
- Hardware hosting the private keys is authenticated

4.5. THREATS

The various threat agents are:

- internal attackers: entities belonging to the trusted network, they are users known to the TOE and its runtime environment. For these attackers, the only way to access the TOE is logical access via *CSS_RED_NETWORK*, no physical access to the TOE is to be considered.
- external attackers: entities not belonging to the trusted network, they are unauthorized third party and don't belong to the organization for which the TOE is used. For these attackers, the only way to access the TOE is logical access via *CS_BLACK_NETWORK*, no physical access to the TOE is to be considered

Administrators and operators are not considered as hackers neither threat agents.

4.5.1. T.SECURITY_FUNCTIONALITY_FAILURE

A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

4.5.2. T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the network device 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.

4.5.3. T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device 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 network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

This could lead either to:

- Modification or retrieval of TOE data (that is TSF Data and User Data stored within the TOE)
- Usurpation of the administrator identity in order to perform administration operations on the TOE (in TOE case, administrators are U.ROLE_GW_OPERATOR and U.ROLE_SYS_ADMIN)
- Modification, insertion or deletion of audit data recorded on the TOE or while they are transmitted by the TOE to the TOE management center (SS_MMC).

4.5.4. T.UPDATE_COMPROMISE

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.

4.5.5. T.USER_DATA_REUSE

User data may be inadvertently sent to a destination not intended by the original sender.

4.5.6. T.MISUSE

Misuse of the TOE due to TOE administrator error (bad configuration design …) the VPN rules are no longer compliant with system MISTRAL security policy.

4.5.7. T.TIME_BASE

A malicious party disturbs or tampers with the TOE time base with the aim of falsifying audit data.

4.5.8. T.RESIDUAL_DATA

A malicious party acquires knowledge, by direct access to the TOE, of old value of TOE data (keys, VPN security policies…) during a change of operational context (assignment of the TOE in a new premise, maintenance…). The access can be done after TOE theft.

4.5.9. T.WEAK_CRYPTOGRAPHY

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.

4.5.10. T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target network devices that do not use standardized secure tunneling 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 network device itself.

4.5.11. T.WEAK_AUTHENTICATION_ENDPOINTS

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 network device itself could be compromised.

4.5.12. T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

4.5.13. T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the network device 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 device credentials for use by the attacker.

4.5.14. T.TOE_CAPTURE

Threat agents may capture the TOE during transportation, compromise sensitive data and insert traps.

5. SECURITY OBJECTIVES

5.1. SECURITY OBJECTIVES FOR THE TOE

5.1.1. Communication protection

5.1.1.1. O.PROTECTED_COMMUNICATIONS

The TOE shall provide protected communication channels on

- Administration interface
- Interfaces connected to the untrusted network (to remote instances of the TOE).

This protection shall prevent (when it is used) disclosure, modification, insertion and replay of IP datagrams (payload and datagram header).

5.1.1.2. O.POL_FILTERING

The TOE shall provide information flow control policies coming in and out its external interfaces, in particular VPN security policies.

The TOE shall authorize only U.ROLE_GW_OPERATOR and U.ROLE_SYS_ADMIN to modify the filtering configuration of the flow control policies.

5.1.1.3. O.POL_DEFAULT

The TOE shall transmit no network flow if the TOE (SS_IPSEC_GW) is not in ST_OPERATIONAL state or if no VPN SP has been explicitly defined for the given IP addresses (source & destination).

5.1.2. Audit

5.1.2.1. O.AUDIT

The TOE shall generate audit data:

- For all security-relevant operations performed by the TOE or concerning protected communication channels
- For all security-relevant operations (including viewing operations on TOE sensitive assets) performed by U.ROLE_GW_OPERATOR or U.ROLE_SYS_ADMIN.

The TOE shall associate to generated audit data:

- A number (an incremental counter), offering a mean to detect audit data loss.
- A severity, offering a mean to discriminate informational, warning and critical audit data.
- A data offering the information if it is an alarm or not.

All the data included in the audit are under control and they are not sensitive data.

The TOE shall transmit continuously stored audit data from SS_IPSEC_GW database to the MMC interface.

After generation, the TOE shall send any ALARM-type audit data to the TOE management center device (SS_MMC).

Application note: Refer to FAU_GEN.1 for the list of audited security events.

5.1.2.2. O.TIME_BASE

The TOE shall provide a time base upon which the audit records are based.

5.1.2.3. O.AUDIT_PROTECTION

The TOE shall ensure the integrity of recorded audit data while being forwarded to the TOE management center device (SS_MMC).

The TOE shall ensure the authentication of recorded audit data forwarded to the TOE management center device (SS_MMC).

5.1.2.4. O.SUPERVISION

The TOE shall authorize the local administrator (U.ROLE_GW_OPERATOR on CSS_LMGT) and the TOE management center device (U.ROLE_SYS_ADMIN on SS_MMC) to supervise operational state and VPN connections state.

5.1.2.5. O.SUPERVISION_IMPACT

The TOE shall ensure that the supervision service does not endanger its sensitive assets.

5.1.3. TOE management

5.1.3.1. O.ROLES

The TOE shall implement access control and security policy enforcement for the following roles:

- Operator, which is the role corresponding to U.ROLE_GW_OPERATOR on CSS_LMGT
- TOE management center device, which is the role corresponding to U.ROLE_SYS_ADMIN on SS_MMC

5.1.3.2. O.I&A

The TOE shall require the identification of the TOE management center device before granting it with the TOE management center device access rights. The access rights for TOE on SS_MMC are controlled by profile definition on SS_MMC.

The TOE shall require the authentication of the local user before granting him with the operator access rights.

The authentication mechanism shall be compliant with ANSSI guidance [RGS_B].

5.1.3.3. O.AUTHENTICATION_FAILURE

The TOE shall temporarily lock the authentication mechanism after too many unsuccessful authentication attempts.

5.1.3.4. O.DISPLAY_BANNER

The TOE shall send to the local interface (CSS_LMGT) from which the user is connected to the TOE an advisory warning regarding use of the TOE, after its successful identification.

5.1.3.5. O.SESSION_LOCK

The TOE shall lock any local user session after a defined period of inactivity. The TOE shall provide the local user the reason for the session ending.

5.1.3.6. O.MANAGEMENT

The TOE shall allow modification of TSF data to only authorized entities which are the local operator (U.ROLE_GW_OPERATOR) or/and to TOE management center device (U.ROLE_SYS_ADMIN).

5.1.3.7. O.VIEW_RULES

The TOE shall authorize viewing of accessible TSF data to the administrator (U.ROLE_GW_OPERATOR) and/or to the TOE management center device administrator (U.ROLE_SYS_ADMIN) only:

- Security associations and policies
- Configuration parameters such as time data
- Supervision data such as audit event logs

The TOE shall authorize viewing of User data and TSF data (except those listed above), in plain text to no one.

5.1.4. Data protection

5.1.4.1. O.RESIDUAL_INFORMATION_CLEAR

The TOE shall ensure that any data contained in a protected resource is not available when the resource is deallocated or reallocated.

5.1.4.2. O.DATA_ERASURE

The TOE shall provide a secure data erasure mechanism which cause sensitive data (both persistently stored and in volatile memory) to be made unavailable.

5.1.4.3. O.LOCAL_DATA_PROTECTION

The TOE shall protect at least TSF Data and User Data that are persistently stored from disclosure (in regards to their security needs).

The TOE shall allow detecting modification of at least TSF Data and User Data (in regards to their security needs) that are persistently stored.

5.1.4.4. O.SELF_TEST

The TOE shall run a suite of tests at start-up concerning:

- Logs integrity
- Security functionalities for cryptographic primitives.

The TOE shall also provide the capability to the administrators (U.ROLE_SYS_ADMIN and U.ROLE_GW_OPERATOR) to request such tests during TOE running.

The result of a self-test can be OK or NOK. If all self-tests results are OK, then the TOE stay in ST_OPERATIONAL functional state. Otherwise, at the first self-test failure (that is a result is NOK), the TOE shall go in ST_FAILURE functional state.

5.1.5. Software

5.1.5.1. O.SOFTWARE_UPDATES

When a software update is requested, the TOE shall control the version, integrity and authenticity (done through a digital signature) of the software, before accepting and installing it.

5.1.5.2. O.BOOT_CONTROL

When the TOE reboots, it shall control the integrity and authenticity (done through a digital signature) of the software, before launching it.

5.1.6. Cryptography

5.1.6.1. O.CERTIFICATE_INJECTION

When certificate is injected via the Local and Remote Management Interface, the TOE shall control its authenticity before accepting and persistently storing it.

5.1.6.2. O.CRYPTO_PERIOD

The TOE shall manage a crypto-period for any cryptographic DATA used to protect communication channels (refer to O.PROTECTED_COMMUNICATIONS).

For IKEv2 protocols negotiated keys, at the end of a key lifetime, the TOE shall renew the key through SA renewal mechanism.

For IKEv2 protocols authentication with certificates, at the end of the certificate validity, the TOE shall generate an audit data while it continues to proceed the network traffic. In this case new communication channels for SAs using this certificate are refused till a new certificate can be used.

5.1.6.3. O.CRYPTO_REGULATION

The TOE shall implement cryptographic mechanisms compliant with ANSSI guidance [RGS_B].

5.2. SECURITY OBJECTIVES FOR THE TOE ENVIRONMENT

5.2.1. The management

5.2.1.1. OE.TRUSTED_ADMIN

The environment of the TOE shall provide trusted administrators (U.ROLE_SYS_ADMIN and U.ROLE_GW_OPERATOR) to follow and apply all administrator guidance documentation in a trusted manner.

5.2.1.2. OE.AUDIT

The environment of the TOE shall regularly analyses audit events generated by the TOE and react accordingly

The environment of the TOE shall manage the memory units storing audit events so that the TOE management center device does not lose events.

5.2.1.3. OE.ALARM

The environment of the TOE shall analyze and process critical security audit data generated and forwarded by the TOE, by administrators (U.ROLE_SYS_ADMIN and U.ROLE_GW_OPERATOR) immediately after reception.

5.2.1.4. OE.POLICIES_CONTINUITY

The environment of the TOE shall make sure that the information security policies of the two networks interconnected through the TOE are consistent between each other.

5.2.1.5. OE.ADMIN_CREDENTIALS_SECURE

The environment of the TOE shall protect the administrator's credentials (**refinement: private key, password**) used to access the network device, with the platform on which they reside.

5.2.2. The TOE

5.2.2.1. OE.PHYSICAL

The environment of the TOE shall provide physical security, commensurate with the value of the TOE and the data it contains.

5.2.2.2. OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

5.2.2.3. OE.TOE_INTEGRITY

The TOE environment shall provide the capability to check the integrity of the TOE hardware and software configuration. Seal applied on the hardware hosting the TOE is an output indication of possible intrusion attempt.

5.2.2.4. OE.TIME_TOE

The environment of the TOE shall locally enter right date and time in the TOE and ensures its reliability.

5.2.2.5. OE.TOE_ERASURE

The TOE environment shall erase TOE before any transportation outside protected premises or long storage.

5.2.2.6. OE.TOE_PRODUCTION

THALES shall produce the TOE following the rules described below:

- Development is located in THALES secured premises
- Development is performed on dedicated network
- Private keys receive a special the care in secured premises.
- Hardware hosting the TOE is tested (bypass)
- Hardware hosting the private keys is authenticated

5.2.2.7. OE.NO_THRU_TRAFFIC_PROTECTION

The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

5.2.3. The management devices

Management devices are composed of the following item:

- The TOE management center device (SS_MMC)

- The TOE local management device (CSS_LMGT)
- The Public Key Infrastructure device (CSS_PKI)

5.2.3.1. OE.SECURED_MANAGEMENT_DEVICES

The environment of the TOE shall securely configure and use the management devices listed above.

5.2.3.2. OE.ACCESS_CONTROL_MANAGEMENT_DEVICES

The environment of the TOE shall control the access to management devices and software listed above. The overall solution shall allow individual accounting. It can be physical (e.g. physical access restriction to the device) and/or logical (e.g. user authentication by the operating system or by the software itself).

5.2.3.3. OE.PHYSICAL_ENV_MANAGEMENT_DEVICES

The environment of the TOE shall provide physical security to management devices listed above commensurate with the value of the data concerning the TOE it contains.

The environment provides also physical security to all network devices connected to the SS_MMC and communicating with it, commensurate with the value of the data concerning the TOE they contain.

5.2.3.4. OE.AUDIT_RECORD

The environment of the TOE shall store any audit data received from the TOE as long as law required.

5.2.3.5. OE.LMGT_CONNECTION

The environment of the TOE shall provide a trustworthy link between the TOE and the TOE local management device (CSS_LMGT).

5.2.3.6. OE.SS_MMC_TO_TOE

The environment of the TOE shall provide a way to connect with management center device (SS_MMC):

- Directly through a trusted network (red side)
- Remotely through a protected path (VPN).

5.2.3.7. OE.DATA_TRANSPORTATION

The environment of the TOE shall manipulate physical devices used to transport sensitive data in secure way.

5.2.4. Software updates

5.2.4.1. OE.UPDATES

The environment of the TOE shall update the TOE firmware and software by **(refinement) U.ROLE_SYS_ADMIN only** on a regular basis in response to the release of product updates due to known vulnerabilities.

5.3. RATIONALE FOR THE SECURITY OBJECTIVES

5.3.1. Threats

	T.SECURITY_FUNCTIONALITY_FAILURE	T.UNDETECTED_ACTIVITY	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	T.UPDATE_COMPROMISE	T.USER_DATA_REUSE	T.MISUSE	T.TIME_BASE	T.RESIDUAL_DATA	T.WEAK_CRYPTOGRAPHY	T.UNTRUSTED_COMMUNICATION_CHANNELS	T.WEAK_AUTHENTICATION_ENDPOINTS	T.PASSWORD_CRACKING	T.SECURITY_FUNCTIONALITY_COMPROMISE	T.TOE_CAPTURE
O.AUDIT		X	X											X
O.AUTHENTICATION_FAILURE			X									X		
O.AUDIT_PROTECTION			X											
O.BOOT_CONTROL				X										X
O.DISPLAY_BANNER			X											
O.CRYPTO_REGULATION			X						X					
O.DATA_ERASURE								X						
O.I&A			X			X					X	X		
O.LOCAL_DATA_PROTECTION			X					X					X	X
O.MANAGEMENT			X			X								X
O.POL_DEFAULT	X				X					X				
O.POL_FILTERING			X		X					X				
O.PROTECTED_COMMUNICATIONS			X			X				X				
O.SELF_TEST	X													X
O.SESSION_LOCK			X											
O.SOFTWARE_UPDATES				X										
O.SUPERVISION						X								

	T.SECURITY_FUNCTIONALITY_FAILURE	T.UNDETECTED_ACTIVITY	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	T.UPDATE_COMPROMISE	T.USER_DATA_REUSE	T.MISUSE	T.TIME_BASE	T.RESIDUAL_DATA	T.WEAK_CRYPTOGRAPHY	T.UNTRUSTED_COMMUNICATION_CHANNELS	T.WEAK_AUTHENTICATION_ENDPOINTS	T.PASSWORD_CRACKING	T.SECURITY_FUNCTIONALITY_COMPROMISE	T.TOE_CAPTURE
O.SUPERVISION_IMPACT			X											
O.VIEW_RULES			X			X								
O.RESIDUAL_INFORMATION_CLEAR					X			X						
O.ROLES			X			X					X			
O.TIME_BASE							X							
O.CERTIFICATE_INJECTION													X	
OE.TRUSTED_ADMIN			X											
OE.ALARM			X											
OE.TOE_INTEGRITY	X		X											
OE.TIME_TOE							X							
OE.TOE_ERASURE								X						X
OE.LMGT_CONNECTION			X							X				
OE.SS_MMC_TO_TOE			X							X				
OE.SECURED_MANAGEMENT_DEVICES			X			X					X			
OE.ACCESS_CONTROL_MANAGEMENT_DEVICES			X								X		X	X
OE.PHYSICAL_ENV_MANAGEMENT_DEVICES			X								X			
OE.DATA_TRANSPORTATION													X	
OE.ADMIN_CREDENTIALS_SECURE			X										X	
OE.UPDATES				X										

Table 10 : Threat coverage

5.3.1.1. T.SECURITY_FUNCTIONALITY_FAILURE

This threat is countered by **O.SELF_TEST** because it ensures that cryptographic operations (base of Security Functions) are checked when the TOE starts. **O.POL_DEFAULT** and **OE.TOE_INTEGRITY**, limit the impacts of TSF failure by ensuring that no traffic can be transmitted during TOE reboot and that none can add or replace a component with a malicious or weak one.

5.3.1.2. T.UNDETECTED_ACTIVITY

This threat is covered by **O.AUDIT**, which requires the TOE to generate audit for security-relevant operations performed by the TOE or concerning protected communication channels, and for actions performed by users.

5.3.1.3. T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Regarding the threat concerning modification, it is countered:

- For accessible TSF Data:
  - by **O.MANAGEMENT** which requires that they can be modified by authorized entities only.
  - when persistently stored, by **O.LOCAL_DATA_PROTECTION** which requires that they are protected against disclosure when they are persistently stored and that any attempt to modify this data shall be detected.
- For event logs data:
  - by **O.AUDIT** and **O.AUDIT_PROTECTION** which ensure that audit data modification (enforced by **O.AUDIT_PROTECTION**) and audit data loss (enforced by **O.AUDIT**) can be detected by the receiver, associated to **OE.LMGT_CONNECTION** (for communications to LMGT), OE.SS_MMC_TO_TOE and **O.PROTECTED_COMMUNICATIONS** (for communications to SS_MMC).
- For the other data
  - **O.MANAGEMENT** which requires that they can't be modified by anyone
  - when persistently stored, by **O.LOCAL_DATA_PROTECTION** which requires that they are protected against disclosure when they are persistently stored and that any attempt to modify this data shall be detected.

Regarding the threat concerning disclosure, it is countered:

- For SA and SP configuration, by **O.VIEW_RULES** which requires that VPN security policies and their contexts can be viewed by authorized entities only, which are U.ROLE_SYS_ADMIN and U.ROLE_GW_OPERATOR.
- For accessible TSF Data, by **O.VIEW_RULES** which requires that such data can be viewed by authorized entities only, which are U.ROLE_SYS_ADMIN and U.ROLE_GW_OPERATOR.
- For the other data requiring confidentiality, by **O.VIEW_RULES** which requires that they can't be seen by anyone

All those countermeasures rely upon the Identification & Authentication security objectives which are:

- **O.I&A** which requires the management center device and U.ROLE_GW_OPERATOR to be authenticated before performing any management functions. Protection of TOE local management communication is ensured through **OE.LMGT_CONNECTION**. **O.AUTHENTICATION_FAILURE** prevents brute force attacks on the authentication mechanism and **O.SESSION_LOCK** prevents theft of user session.
- **O.I&A** and **O.PROTECTED_COMMUNICATIONS** which require the SS_MMC to be identified before performing any management functions and the communication between SS_MMC and the TOE to be a protected communication channel (ensuring authentication and encryption) implemented between the TOE and another instance of the TOE.

- And **O.ROLES** which requires the TOE to distinguish two roles to implement the Identification & Authentication security objective (**O.I&A**): the U.ROLE_GW_OPERATOR and the TOE management center device.

Nota: The SS_MMC is part of the management center and it is authenticated to the TOE through a protected communication channel (i.e. a dedicated tunnel going through a VPN as for user traffic when needed) using certificates.

The following objectives also contribute to the threat coverage:

- **O.SUPERVISION_IMPACT** ensures that the TOE supervision service does not question sensitive assets security.
- **O.AUDIT** ensures that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that critical security events are generated to indicate TOE operational failures. Therefore, they provide the capability to detect and process errors or attacks after an analysis of audit events and security alarms.
- **OE.TOE_INTEGRITY** ensures the integrity check of the TOE hardware and software configuration.
- **O.CRYPTO_REGULATION** ensures that the TOE implements robust cryptographic mechanisms.
- **O.POL_FILTERING** requires filtering of data flow coming into the TOE network interfaces. It hardens attacks exploiting protocol vulnerabilities.
- **O.DISPLAY_BANNER** requires that the TOE sends to the local interface (CSS_LMGT) from which the user is connected to the TOE an advisory warning regarding a wrong use of the TOE.

5.3.1.4. T.UPDATE_COMPROMISE

This threat is countered by:

- **O.SOFTWARE_UPDATES** counters this threat by providing a cryptographic authentication mechanism during updates.
- **O.BOOT_CONTROL** counters this threat by providing a cryptographic authentication mechanism on TOE boots.
- **OE.UPDATES** contributes to the threat's coverage by requiring that software is updating by U.ROLE_SYS_ADMIN only.

5.3.1.5. T.USER_DATA_REUSE

This threat is countered by **O.RESIDUAL_INFORMATION_CLEAR** to ensure that no unused user data remains in TOE's volatile memory and so can be sent to an unexpected receiver.

It is also countered by **O.POL_FILTERING** which requires the TOE to systematically apply the VPN policies when treating user data flow and O.POL_DEFAULT which requires that the TOE must be operational before to start traffic transmission.

5.3.1.6. T.MISUSE

This threat is countered by:

- **O.I&A, O.MANAGEMENT, O.ROLES** and **OE.SECURED_MANAGEMENT_DEVICES** which limit the impact of user to authenticated local or remote users with control access and has the opportunity to reconfigure correctly the TOE in case of security weakness detection.
- **O.PROTECTED_COMMUNICATION** which ensure that communications security can't be degraded,
- **O.SUPERVISION** and **O.VIEW_RULES** which ensure that any issue on VPN connection is detected remotely.

5.3.1.7. T.TIME_BASE

This threat is covered by the security objective **O.TIME_BASE** and **OE.TIME_TOE** which ensure the time base reliability.

5.3.1.8. T.RESIDUAL_DATA

This threat is countered by:

- **O.DATA_ERASURE** which requires the TOE to provide a mechanism to securely erase stored data.
- **O.LOCAL_DATA_PROTECTION** which requires the TOE to protect persistently stored sensitive data.
- **O.RESIDUAL_INFORMATION_CLEAR** contributes to the threat's coverage by requiring that no unused user data remains in TOE's volatile memory.
- **OE.TOE_ERASURE** contributes to the threat's coverage by requiring a secure erasure before any transportation outside protected premises.

5.3.1.9. T.WEAK_CRYPTOGRAPHY

This threat is countered by **O.CRYPTO_REGULATION** which requires the TOE to implement cryptographic mechanisms compliant with ANSSI guidance [RGS_B].

5.3.1.10. T.UNTRUSTED_COMMUNICATION_CHANNELS

This threat is countered by

- **O.PROTECTED_COMMUNICATION** which requires the TOE to protect communication between itself and a remote instance of the TOE or remote SS_MMC.
- **O.POL_FILTERING** which requires the TOE to systematically apply the VPN policies when treating user data flow.
- **O.POL_DEFAULT** which requires that the TOE must be operational before to start traffic transmission and define a default policy to discard flow that doesn't match with any SP.
- **OE.LMGT_CONNECTION** which requires the environment to protect communication between the TOE and the TOE local management device (CSS_LMGT)

- **OE.SS_MMC_TO_TOE** which requires the environment to protect communication between TOE and the SS_MMC

5.3.1.11. T.WEAK_AUTHENTICATION_ENDPOINTS

This threat is countered by

- **O.ROLES** which requires the TOE to implement roles to access to the TOE itself.
- **O.I&A** which requires the TOE to implement authentication mechanism compliant with ANSSI guidance [RGS_B].

The following security objectives for the TOE environment:

- **OE.SECURED_MANAGEMENT_DEVICES** which requires that management devices are securely configured and used**,**
- **OE.ACCESS_CONTROL_MANAGEMENT_DEVICES** which requires that the management devices access are physically and logically controlled.
- **OE.PHYSICAL_ENV_MANAGEMENT_DEVICES** which requires that the environment provides also physical security to all network devices connected to the SS_MMC and communicating with it, commensurate with the value of the data concerning the TOE they contain, contributes to the threat's coverage by requiring particular protection on devices connected to the TOE.

5.3.1.12. T.PASSWORD_CRACKING

This threat is countered by **O.I&A** which requires the TOE to implement authentication mechanism compliant with ANSSI guidance [RGS_B] annex B3.

O.AUTHENTICATION_FAILURE contributes to the threat coverage by minimizing the number of attempts before locking temporarily the authentication mechanism.

5.3.1.13. T.SECURITY_FUNCTIONALITY_COMPROMISE

This threat is countered by

- **O.LOCAL_DATA_PROTECTION** which requires the TOE to protect TSF DATA as credentials and to detect modification.
- **O.CERTIFICATE_INJECTION** which requires the TOE to control the integrity and the authenticity of the certificates injected.

OE.ACCESS_CONTROL_MANAGEMENT_DEVICE, OE.PHYSICAL_ENV_MANAGEMENT_DEVICES and OE.DATA_TRANSPORTATION contribute to the threat coverage by ensuring the credentials protection from the source on administration interface.

The threat coverage is completed by **OE.ADMIN_CREDENTIALS_SECURE** which ensures the administrator credentials protection by the platform.

5.3.1.14. T.TOE_CAPTURE

This threat is countered by

- **O.LOCAL_DATA_PROTECTION** which requires the TOE to protect TSF DATA as credentials and to detect modification and **O.MANAGEMENT** which limits the rights and access to TSF DATA.
- **O.AUDIT** and **O.SELF_TEST** which participates to analyze traps injections on the TOE.
- **O.BOOT_CONTROL** participates to counter this threat by providing a cryptographic authentication mechanism on TOE boots avoiding boot with trap.

OE.ACCESS_CONTROL_MANAGEMENT_DEVICE contributes to the threat coverage by ensuring the logical access protection.

OE.TOE_ERASURE contributes to the threat's coverage by requiring a secure erasure before any transportation outside protected premises (avoiding disclosure).

5.3.2. Organizational Security Policies (OSP)

	P.CRYPTO_RGS	P.PROVIDED_SERVICES	P.AUDIT	P.SUPERVISION	P.ACCESS_BANNER	P.SA_SP_PROTECTION	P.TOE_PRODUCTION
O.CRYPTO_PERIOD	X						
O.PROTECTED_COMMUNICATIONS		X					
O.POL_DEFAULT		X					
O.POL_FILTERING		X					
O.AUDIT			X				
O.SELF_TEST		X					
O.SUPERVISION				X			
O.DISPLAY_BANNER					X		
O.LOCAL_DATA_PROTECTION						X	
O.CRYPTO_REGULATION	X						
OE.AUDIT_RECORD		X	X				
OE.TOE_INTEGRITY		X					
OE.TOE_PRODUCTION							X

Table 11: Organizational Security Policy coverage

5.3.2.1. P.CRYPTO_RGS

The OSP is entirely covered through the implementation of the security objective **O.CRYPTO_REGULATION**, which uses the same words as the OSP.

O.CRYPTO_PERIOD contributes to the coverage of the OSP by requiring the TOE to manage key lifetimes.

5.3.2.2. P.PROVIDED_SERVICES

This OSP is covered by **O.PROTECTED_COMMUNICATIONS** which requires that the TOE provides security services.

It is also covered by

- **O.POL_FILTERING** which requires the TOE to systematically apply the VPN policies when treating user data flow.
- **O.POL_DEFAULT** which requires that the TOE must be operational before to start traffic transmission and define a default policy to discard flow that doesn't match with any SP

This OSP is covered by **O.SELF_TEST** and **OE.TOE_INTEGRITY**, because they ensure that security function including cryptographic operations work and that none can add or replace a component with a malicious or weak one.

5.3.2.3. P.AUDIT

This OSP is entirely covered **by O.AUDIT**, because they ensure that operations concerning VPN links are logged and that security critical events are generated to indicate operational failures. **OE.AUDIT_RECORD** completes the cover assuring that SS_MMC stores the events generated by the TOE.

5.3.2.4. P.SUPERVISION

This OSP is entirely covered through the implementation of the security objective **O.SUPERVISION**, which uses the same words as the OSP.

5.3.2.5. P.ACCESS_BANNERS

This OSP is covered through the implementation of the sending to the local interface of a banner describing restrictions of use, legal agreements, or any other appropriate information just after its connection establishment (**O.DISPLAY_BANNER**).

5.3.2.6. P.SA_SP_PROTECTION

This OSP is covered by **O.LOCAL_DATA_PROTECTION** which requires the TOE to be able to detect modification of TSF Data, in particular of SA and SP configuration.

5.3.2.7. P.TOE_PRODUCTION

This OSP is entirely covered through the implementation of the security objective **OE.TOE_PRODUCTION**, which uses the same words as the OSP.

5.3.3. Assumptions

	A.LIMITED_FUNCTIONALITY	A.PHYSICAL_PROTECTION	A.REGULAR_UPDATES	A.TOE_ERASURE	A.NO_TRU_TRAFFIC_PROTECTION	A.TRUSTED_ADMINISTRATOR	A.ALARM	A.POLICIES_CONTINUITY	A.ADMIN_CREDENTIALS_SECURE	A.SECURED_MANAGEMENT_DEVICES	A.ACCESS_CONTROL_MANAGEMENT_DEVICES	A.PHYSICAL_ENV_MANAGEMENT_DEVICES	A.AUDIT	A.SS_MMC_TO_TOE	A.DATA_TRANSPORTATION
OE.NO_GENERAL_PURPOSE	X														
OE.PHYSICAL		X													
OE.TOE_ERASURE				X											
OE.TRUSTED_ADMIN						X									
OE.TOE_INTEGRITY.		X													
OE.ALARM							X								
OE.POLICIES_CONTINUITY								X							
OE.SECURED_MANAGEMENT_DEVICES										X					
OE.ACCESS_CONTROL_MANAGEMENT_DEVICES											X				
OE.PHYSICAL_ENV_MANAGEMENT_DEVICES												X			
OE.NO_THRU_TRAFFIC_PROTECTION					X										
OE.UPDATES			X												
OE.ADMIN_CREDENTIALS_SECURE									X						
OE.AUDIT													X		
OE.SS_MMC_TO_TOE														X	
OE.DATA_TRANSPORTATION															X

Table 12: Assumptions coverage

All assumptions are covered with Security Objectives for the TOE Environment as described above.

6. EXTENDED SECURITY REQUIREMENTS

This chapter contains the definitions for the extended requirements that are used in this document.

6.1. SECURITY AUDIT (FAU)

6.1.1. Protected audit event storage (FAU_STG_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to securely transmit audit data between the TOE and an external IT entity.

Component levelling

FAU_STG_EXT.1 Protected audit event storage requires the TSF to use a trusted channel implementing a secure protocol.

FAU_STG_EXT.2/LocSpace Counting lost audit data requires the TSF to provide information about audit records affected when the audit log becomes full.

FAU_STG_EXT.3/LocSpace Protected Local audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.

FAU_STG_EXT.4 Protected Remote audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.

Management: FAU_STG_EXT.1, FAU_STG_EXT.2/LocSpace, FAU_STG_EXT.3/LocSpace, FAU_STG_EXT.4

The following actions could be considered for the management functions in FMT:

a) The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_STG_EXT.1, FAU_STG_EXT.2/LocSpace, FAU_STG_EXT.3/LocSpace, FAU_STG_EXT.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) No audit necessary.

6.1.1.1. FAU_ STG_EXT.1 Protected Audit Event Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation, FTP_ITC.1 Inter-TSF Trusted Channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. [selection:

- TOE shall consist of a single standalone component that stores audit data locally
- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components],
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [assignment: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data].

FAU_STG_EXT.1.3 The TSF shall [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]] when the local storage space for audit data is full.

6.1.1.2. FAU_ STG_EXT.2/LocSpace Counting lost audit data

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation, FAU_STG_EXT.1 External Audit Trail Storage,

FAU_STG_EXT.2.1/LocSpace The TSF shall provide information about the number of [selection: dropped, overwritten, [assignment: other information]] audit records in the case where the local storage has been filled and the TSF takes one of the actions defined in FAU_STG_EXT.1.3.

6.2. CRYPTOGRAPHIC SUPPORT (FCS)

6.2.1. Random Bit Generation (FCS_RBG_EXT)

Family Behaviour

Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

Component levelling

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: failure of the randomization process

FCS_RBG_EXT.1 - RANDOM BIT GENERATION

Hierarchical to: No other components

Dependencies: No other components

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of hardware-based sources] hardware-based noise source] with a minimum of [selection: 128 bits, 192 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.2.2. Cryptographic Protocols (FCS_IPSEC_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

6.2.2.1. FCS_IPSEC_EXT.1 IPsec Protocol

Family Behaviour

Components in this family address the requirements for protecting communications using IPsec.

Component levelling

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management: FCS_IPSEC_EXT.1

The following actions could be considered for the management functions in FMT:

a) Maintenance of SA lifetime configuration

Audit: FCS_IPSEC_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Decisions to DISCARD, BYPASS, PROTECT network packets processed by the TOE.
b) Failure to establish an IPsec SA
c) IPsec SA establishment
d) IPsec SA termination
e) Negotiation “down” from an IKEv2 to IKEv1 exchange.

FCS_IPSEC_EXT.1 - INTERNET PROTOCOL SECURITY (IPSEC) COMMUNICATIONS

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic Key Generation, FCS_CKM.2 Cryptographic Key Establishment, FCS_COP.1/DataEncryptionGCM or FCS_COP.1/DataEncryptionCTRCryptographic operation (AES Data encryption/decryption), FCS_COP.1/SigGenECDSA Cryptographic operation (Signature Generation and Verification), FCS_COP.1/Hash256 Cryptographic operation (Hash Algorithm), FCS_COP.1/KeyedHash256 Cryptographic operation (Keyed Hash Algorithm), FCS_RBG_EXT.1 Random Bit Generation

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: tunnel mode, transport mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms

- AES-GCM with 256 bits key and 16 bytes ICV *(specified in RFC 4106)*

- AES-CTR with 256 bits key

together with secure Hash Algorithm) AUTH_HMAC_SHA2_256_128 (truncated)

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection:

- IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], and [selection: no other RFCs for hash functions, RFC 4868 for hash functions];
- IKEv2 as defined in RFCs 7296 [selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in RFC 7296, section 2.23)], and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the IKEv2 protocol uses the cryptographic algorithms:

- AES-GCM with 256 bits key and 16 bytes ICV *(specified in RFC 5282)*
- AES-CTR with 256 bits key and HMAC-SHA256 with 32 bytes Key and 16 bytes MAC

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

- IKEv1 Phase 1 SA lifetimes can be configured by an Administrator based on [selection:
  - number of bytes;
  - length of time, where the time values can be configured within [assignment: integer range including 24] hours;];
- IKEv2 SA lifetimes can be configured by an Administrator based on [selection:
  - number of bytes;
  - length of time, where the time values can be configured within [assignment: integer range including 24] hours]].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

- IKEv1 Phase 2 SA lifetimes can be configured by an Administrator based on [selection:
  - number of bytes;
  - length of time, where the time values can be configured within [assignment: integer range including 8] hours;];
- IKEv2 Child SA lifetimes can be configured by an Administrator based on [selection:
  - number of bytes;
  - length of time, where the time values can be configured within [assignment: integer range including 8] hours;]].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in x.G mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment: (one or more) number(s) of bits that is at least twice the security strength of the negotiated Diffie-Hellman group] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [selection: IKEv1, IKEv2] exchanges of length [selection:

- according to the security strength associated with the negotiated Diffie-Hellman group;
- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection: 14 (2048-bit MODP), 19 (secp256r1), 20 (384-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 28 (BrainpoolP256r1)].

FCS_IPSEC_EXT.1.12 The TSF shall ensure that all IKE protocols perform peer authentication using [selection: RSA, ECDSA] that use X.509v3 certificates that conform to RFC 4945 and [selection: Pre-shared Keys, no other method].

FCS_IPSEC_EXT.1.13 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [selection: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, CN: IP address, CN: Fully Qualified Domain Name (FQDN), CN: user FQDN, Distinguished Name (DN)] and [selection: no other reference identifier type, [assignment: other supported reference identifier types]].

Note: FCS_IPSEC_EXT.1.4 and 1.6 are a DR profile adaptation.

6.2.2.2. FCS_TLSC_EXT TLS Client Protocol

Family Behaviour

The component in this family addresses the ability for a client to use TLS to protect data between the client and a server using the TLS protocol.

Component levelling

FCS_TLSC_EXT.2 TLS Client requires that the client side of the TLS implementation include mutual authentication.

Management: FCS_TLSC_EXT.2

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_TLSC_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of TLS session establishment

b) TLS session establishment

c) TLS session termination

FCS_TLSC_EXT.2 - TLS CLIENT PROTOCOL WITH AUTHENTICATION

Hierarchical to: No other components

Dependencies: FCS_CKM.1Cryptographic Key Generation, FCS_CKM.2 Cryptographic Key Establishment, FCS_COP.1/DataEncryptionGCM Cryptographic operation (AES Data encryption/decryption), FCS_COP.1/SigGenECDSA Cryptographic operation (Signature Generation and Verification), FCS_COP.1/Hash384

Cryptographic operation (Hash Algorithm), FCS_COP.1/KeyedHash384 Cryptographic operation (Keyed Hash Algorithm), FCS_RBG_EXT.1 Random Bit Generation

FCS_TLSC_EXT.2.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following cipher suites:

- [assignment: list of optional cipher suites and reference to RFC in which each is defined].

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

FCS_TLSC_EXT.2.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [selection:

- Not implement any administrator override mechanism
- require administrator authorization to establish the connection if the TSF fails to [selection: match the reference identifier, validate certificate path, validate expiration date, determine the revocation status] of the presented server certificate].

FCS_TLSC_EXT.2.4 The TSF shall [selection: not present the Supported Elliptic Curves Extension, present the Supported Elliptic Curves Extension with the following NIST curves: [selection: secp256r1, secp384r1, secp521r1, braipool256r1, braipool384r1, braipool521r1] and no other curves] in the Client Hello.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates

6.2.2.3. FCS_TLSS_EXT TLS Server Protocol

Family Behaviour

The component in this family addresses the ability for a server to use TLS to protect data between a client and the server using the TLS protocol.

Component levelling

FCS_TLSS_EXT.2: TLS Server requires the mutual authentication be included in the TLS implementation.

Management:FCS_TLSS_EXT.2

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FCS_TLSS_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of TLS session establishment

b) TLS session establishment

c) TLS session termination

FCS_TLSS_EXT.2 - TLS SERVER PROTOCOL WITH MUTUAL AUTHENTICATION

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic Key Generation, FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryptionGCM Cryptographic operation (AES Data encryption/decryption), FCS_COP.1/SigGenECDSA Cryptographic operation (Signature Generation and Verification),FCS_COP.1/Hash384 Cryptographic operation (Hash Algorithm), FCS_COP.1/KeyedHash384 Cryptographic operation (Keyed Hash Algorithm), FCS_RBG_EXT.1 Random Bit Generation.

FCS_TLSS_EXT.2.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following cipher suites:

- [assignment: list of optional cipher suites and reference to RFC in which each is defined].

FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [selection: TLS 1.1, TLS 1.2, none].

FCS_TLSS_EXT.2.3 The TSF shall [selection: perform ECDSA key establishment with key size [selection: 256 bits, 384 bits, 512 bits]; generate EC Diffie-Hellman parameters over NIST curves [selection: secp256r1, secp384r1, secp521r1, braipool256r1, braipool384r1, braipool521r1] and no other curves; generate Diffie-Hellman parameters of size [selection: 256 bits, 384 bits, 512 bits]].

FCS_TLSS_EXT.2.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [selection:

- Not implement any administrator override mechanism
- require administrator authorization to establish the connection if the TSF fails to [selection: match the reference identifier, validate certificate path, validate expiration date, determine the revocation status] of the presented client certificate].

FCS_TLSS_EXT.2.6 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

6.2.3. Cryptographic Key Lifetime (FCS_CKM_EXT.5)

Family Behaviour

Cf. part 2 [CC].

The family FCS_CKM is extended with the new component FCS_CKM_EXT.5 which provides the capability to the TSF to manage and monitor key lifetime.

Component levelling

FCS_CKM_EXT.5 Cryptographic key lifetime, requires specifying and monitoring cryptographic key lifetime.

Management: FCS_CKM_EXT.5

The following actions could be considered for the management functions in FMT:

a) Managing key lifetime value.

Audit: FCS_CKM_EXT.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: expiration of a cryptographic key.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM_EXT.5 KEY CRYPTOPERIOD

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1 Cryptographic key generation or FDP_ITC.1 Import of User Data without Security Attributes or FDP_ITC.2 Import of User Data With Security Attributes], FCS_CKM.4 Cryptographic key destruction, FPT_STM_EXT.1 Reliable time stamps

FCS_CKM_EXT.5.1 The TSF shall manage [selection: *an expiration date and time, a cryptoperiod, other*] for [assignment: *list of cryptographic keys or certificates*].

FCS_CKM_EXT.5.2 The TSF shall calculate the [selection: *key(s) lifetime, validity*] from [selection: *key generation, key first use*, *other*].

FCS_CKM_EXT.5.3 The TSF shall [assignment: *list of actions*] after the [selection: *key(s), certificate(s)*] has(have) expired.

Rationale

This component was defined because part 2 of [CC] does not contain any SFR which allows specifying a lifetime for cryptographic keys. For the TOE described in this ST it was necessary to provide such capability.

6.3. IDENTIFICATION AND AUTHENTICATION (FIA)

6.3.1. Password Management (FIA_PMG_EXT)

Family Behaviour

The TOE defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component levelling

FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

No management functions.

Audit: FIA_PMG_EXT.1

No specific audit requirements.

FIA_PMG_EXT.1 - PASSWORD MANAGEMENT

Hierarchical to: No other components.

Dependencies: No other components.

FIA_PMG_EXT.1.1 The TSF shall provide a password management capabilities for administrative passwords.

6.3.2. User Identification and Authentication (FIA_UIA_EXT)

Family Behaviour

The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process.

Component levelling

FIA_UIA_EXT.1 User Identification and Authentication requires Administrators (including remote Administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions

Management: FIA_UIA_EXT.1

The following actions could be considered for the management functions in FMT:

a) Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.N

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) All use of the identification and authentication mechanism

b) Provided user identity, origin of the attempt (e.g. IP address)

FIA_UIA_EXT.1 - USER IDENTIFICATION AND AUTHENTICATION

Hierarchical to: No other components.

Dependencies: FTA_TAB.1 Default TOE Access Banners,

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the authentication process:

- [selection: no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

6.3.3. User authentication (FIA_UAU_EXT)

Family Behaviour

Provides for a locally based administrative user authentication mechanism

Component levelling

FIA_UAU_EXT.2 The password-based authentication mechanism provides administrative users a locally based authentication mechanism.

Management: FIA_UAU_EXT.2

The following actions could be considered for the management functions in FMT:

a) None

Audit: FIA_UAU_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All use of the authentication mechanism

FIA_UAU_EXT.2 - PASSWORD-BASED AUTHENTICATION MECHANISM

Hierarchical to: No other components.

Dependencies: No other components.

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [selection: [assignment: other authentication mechanism(s)], no other authentication mechanism] to perform local administrative user authentication.

6.3.4. Authentication using X.509 certificates (FIA_X509_EXT)

Family Behaviour

This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules, use of certificates for authentication for protocols and integrity verification, and the generation of certificate requests.

Component levelling

FIA_X509_EXT.1 X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the RFCs and rules specified in the component.

FIA_X509_EXT.2 X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates, as well as for integrity verification and potentially other functions that require certificates.

FIA_X509_EXT.3 X509 Certificate Requests, requires the TSF to be able to generate Certificate Request Messages and validate responses.

Management: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions could be considered for the management functions in FMT:

a) Remove imported X.509v3 certificates

b) Approve import and removal of X.509v3 certificates

c) Initiate certificate requests

Audit: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: No specific audit requirements are specified.

FIA_X509_EXT.1 - X.509 CERTIFICATE VALIDATION

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.2 X.509 Certificate Authentication,

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, no revocation method]

- The TSF shall validate the extendedKeyUsage field according to the following rules: [assignment: rules that govern contents of the extendedKeyUsage field that need to be verified].
- The TSF shall validate the Certificates presented for IPSec Authentication shall have the algorithm id ECDSA-SHA256 with :
    - Secp256r1 as curve associated or
    - Brainpool256r1 as curve associated

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 - X.509 CERTIFICATE AUTHENTICATION

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: DTLS, HTTPS, IPsec, TLS, SSH, [assignment: other protocols], no protocols], and [selection: code signing for system software updates, code signing for integrity verification, [assignment: other uses], no additional uses].

FIA_X509_EXT.3 - X.509 CERTIFICATE REQUESTS

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic Key Generation, FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: device-specific information, Common Name, Organization, Organizational Unit, Country, [assignment: other information]].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.4. PROTECTION OF THE TSF (FPT)

6.4.1. Protection of TSF Data (FPT_SKP_EXT)

Family Behaviour

Components in this family address the requirements for managing and protecting TSF data, such as cryptographic keys. This is a new family modelled after the FPT_PTD Class.

Component levelling

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

The following actions could be considered for the management functions in FMT:

a) There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

FPT_SKP_EXT.1 PROTECTION OF TSF DATA (FOR READING OF ALL SYMMETRIC KEYS)

Hierarchical to: No other components.

Dependencies: No other components.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys that is [assignment: list of keys].

6.4.2. Protection of Administrator Passwords (FPT_APW_EXT)

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure.

Component levelling

FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

The following actions could be considered for the management functions in FMT:

a) No management functions.

Audit: FPT_APW_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) No audit necessary.

FPT_APW_EXT.1 PROTECTION OF ADMINISTRATOR PASSWORDS

Hierarchical to: No other components

Dependencies: No other components.

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

6.4.3. TSF Self-Test (FPT_TST_EXT)

Family Behaviour

Components in this family address the requirements for self-testing the TSF for selected correct operation.

Component levelling

FPT_TST_EXT.1 TSF Self-Test requires a suite of self-tests to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management: FPT_TST_EXT.1

The following actions could be considered for the management functions in FMT:

a) No management functions.

Audit: FPT_TST_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Indication that TSF self-test was completed

b) Failure of self-test

FPT_TST_EXT.1 TSF TESTING

Hierarchical to: No other components.

Dependencies: No other components.

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [selection: during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]] to demonstrate the correct operation of the TSF: [assignment: list of self-tests run by the TSF].

6.4.4. Trusted Update (FPT_TUD_EXT)

Family Behaviour

Components in this family address the requirements for updating the TOE firmware and/or software.

Component levelling

FPT_TUD_EXT.1 Trusted Update requires management tools be provided to update the TOE firmware and software, including the ability to verify the updates prior to installation.

Management: FPT_TUD_EXT.1

The following actions could be considered for the management functions in FMT:

a) Ability to update the TOE and to verify the updates

b) Ability to update the TOE and to verify the updates using the digital signature capability (FCS_COP.1/SigGenECDSA) and [selection: no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]]

c) Ability to update the TOE, and to verify the updates using [selection: digital signature, published hash, no other mechanism] capability prior to installing those updates

Audit: FPT_TUD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Initiation of the update process.

b) Any failure to verify the integrity of the update

FPT_TUD_EXT.1 TRUSTED UPDATE

Hierarchical to: No other components

Dependencies: FCS_COP.1/SigGenRSA Cryptographic operation (for Cryptographic Signature and Verification), or FCS_COP.1/Hash256 Cryptographic operation (for cryptographic hashing)

FPT_TUD_EXT.1.1 The TSF shall provide [assignment: Administrators] the ability to query the currently executing version of the TOE firmware/software and [selection: the most recently installed version of the TOE firmware/software; no other TOE firmware/software version].

FPT_TUD_EXT.1.2 The TSF shall provide [assignment: Administrators] the ability to manually initiate updates to TOE firmware/software and [selection: support automatic checking for updates, support automatic updates, no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: digital signature mechanism, published hash] prior to installing those updates.

6.4.5. Time stamps (FPT_STM_EXT)

Family Behaviour

Components in this family extend FPT_STM requirements by describing the source of time used in timestamps.

Component levelling

FPT_STM_EXT.1 Reliable Time Stamps is hierarchic to FPT_STM.1: it requires that the TSF provide reliable time stamps for TSF and identifies the source of the time used in those timestamps.

Management: FPT_STM_EXT.1

The following actions could be considered for the management functions in FMT:

a) Management of the time

b) Administrator setting of the time.

Audit: FTA_SSL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Discontinuous changes to the time.

FPT_STM_EXT.1 RELIABLE TIME STAMPS

Hierarchical to: No other components

Dependencies: No other components.

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [selection: allow the Security Administrator to set the time, synchronise time with an NTP server].

6.4.6. FPT_SDP_EXT - STORED TSF DATA PROTECTION

Family Behaviour

This family FPT_SDP_EXT (Stored TSF Data Protection) extends the functional class FPT with the capability to protect TSF data in confidentiality and/or integrity while data are stored within containers controlled by the TSF.

Component levelling

FPT_SDP_EXT.2 Stored TSF Data protection capability and action, adds the additional capability to the first component by allowing for actions to be taken as a result of an error detection.

Management: FPT_SDP_EXT.2

There are no management activities foreseen.

Audit: FPT_SDP_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success or failure of integrity check of TSF data.

FPT_SDP_EXT.2 STORED TSF DATA PROTECTION CAPABILITY AND ACTION

Hierarchical to: No other components

Dependencies: No dependencies.

FPT_SDP_EXT.2.1 The TSF shall protect [assignment: list of TSF data] stored in containers controlled by the TSF from [selection: disclosure, none] and shall detect [selection: integrity errors, none] on those data.

FPT_SDP_EXT.2.2 the TSF shall [assignment: action to be taken], upon detection of a data integrity error.

Rationale

This family was defined because part 2 of [CC] does not contain any SFR which requires protection of TSF data stored within the TOE.

6.5. TOE ACCESS (FTA)

6.5.1. TSF-initiated Session Locking (FTA_SSL_EXT)

Family Behaviour

Components in this family address the requirements for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

The extended FTA_SSL_EXT family is based on the FTA_SSL family.

Component levelling

FTA_SSL_EXT.1 TSF-initiated session locking, requires system initiated locking of an interactive session after a specified period of inactivity. It is the only component of this family.

Management: FTA_SSL_EXT.1

The following actions could be considered for the management functions in FMT:

c) Specification of the time of user inactivity after which lock-out occurs for an individual user.

Audit: FTA_SSL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

b) Any attempts at unlocking an interactive session.

FTA_SSL_EXT.1 TSF-INITIATED SESSION LOCKING

Hierarchical to: No other components

Dependencies: FIA_UIA_EXT.1User Identification and Authentication

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection:

- lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator reauthenticate to the TSF prior to unlocking the session;
- terminate the session]

after three (3) minutes of user inactivity.

6.6. COMMUNICATION (FCO)

6.6.1. Communication Partner Control (FCO_CPC_EXT)

Family Behaviour

This family is used to define high-level constraints on the ways that partner IT entities communicate. For example, there may be constraints on when communication channels can be used, how they are established, and links to SFRs expressing lower-level security properties of the channels.

Component levelling

FCO_CPC_EXT.1 Component Registration Channel Definition, requires the TSF to support a registration channel for joining together components of a distributed TOE, and to ensure that the availability of this channel is under the control of an Administrator. It also requires statement of the type of channel used (allowing specification of further lower-level security requirements by reference to other SFRs).

Management: FCO_CPC_EXT.1

No separate management functions are required. Note that elements of the SFR already specify certain constraints on communication in order to ensure that the process of forming a distributed TOE is a controlled activity.

Audit: FCO_CPC_EXT.1

The following actions should be auditable if FCO_CPC_EXT.1 is included in the PP/ST:

a) Enabling communications between a pair of components as in FCO_CPC_EXT.1.1 (including identities of the endpoints).

b) Disabling communications between a pair of components as in FCO_CPC_EXT.1.3 (including identity of the endpoint that is disabled).

If the required types of channel in FCO_CPC_EXT.1.2 are specified by using other SFRs then the use of the registration channel may be sufficiently covered by the audit requirements on those SFRs: otherwise a separate audit requirement to audit the use of the channel should be identified for FCO_CPC_EXT.1.

FCO_CPC_EXT.1 Component Registration Channel Definition

Hierarchical to: No other components.

Dependencies: No other components.

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [assignment: list of different types of channel given in the form of a selection] for at least [assignment: type of data for which the channel must be used].

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

7. SECURITY REQUIREMENTS

7.1. SECURITY FUNCTIONAL REQUIREMENTS

7.1.1. Terms used within SFRs

7.1.1.1. External Entities

Almost any subjects used within SFRs are defined previously in section “Security Problem Definition”.

TOE is able to work with IPv4 only. All IP references in this document refer to IPv4.

Subjects that are not defined in that section are:

- Remote (instance of the) TOE: it is a remote instance of the TOE with the TOE communicates.
- Network Device on the WAN: it is any network device connected to the network which is neither the TOE nor a Remote TOE.

7.1.1.2. Security Attributes

Security attributes used within the SFRs are:

For IPv4 datagrams:

- Datagram protocol type
- Datagram protocol version
- Datagram topologic data (i.e. source and destination IPv4 addresses)
- Datagram IPSec protection mode

For the TOE plaintext and cipher interfaces:

- TOE IP addresses

For cryptographic keys:

- Key lifetime (for symmetric keys only),
- Key value

For certificate:

- Serial number,
- Issuer
- Subject
- Validity
- Digital signature

- Public key

7.1.1.3. Security Functional Policy

7.1.1.3.1. VPN SFP

The protection offered by IPsec is based on requirements defined by a Security Policy Database (SPD) established and maintained by a user or system administrator. IP packets are selected for one processing action based on IP and next layer header information ("Selectors"), matched against entries in the SPD. Each IP packet is either PROTECTed using IPsec security services or DISCARDed, based on the applicable SPD policies identified by the Selectors.

SS_IPSEC_GW allows only SP with unidirectional flows referencing one or several IPSec SA previously defined

IPSec SP are identified with ipsec_sp_id.

IPSec SP support following selectors:

- Local Address: IP address with a mask.
- Remote Address: IP address with a mask.
- Next Layer Protocol: IP protocol number (TCP, UDP etc.) or wildcard.
- Local Port: Range of ports TCP/UDP or wildcard.
- Remote Port : Range of ports TCP/UDP or wildcard

IPSec protection is done with:

- Tunnel mode
- ESP
- IKEv2
- ESP over UDP

TOE shall implement VPN SFP using TLS for remote administration security. Authentication is based on mutual authentication with X509 certificates.

7.1.1.3.2. Access control SFP

The TOE will implement the access control policy access control SFP.

The TSF shall enforce identification and authentication of remote administrators and operators before giving any administrative access to the TOE (i.e. giving any access to TSF data).

The SFP includes data control on data injection.

7.1.1.4. SFR presentation

For SFR presentation:

- Assignment are identified as normal text in square brackets
  - [text]
- Selections are identified as italic text in square brackets
  - [*text*]
- Assignment operation inside a selection operation is identified as bold italic text in square brackets
  - [*text, **text**, text*]
- Refinement is identified as underlined text for when new text has been inserted into the security functional requirement and strikethrough text when text has been deleted
  - Original_text, ~~removed_text~~
- Iterations are identified using a slash (“/”)
  - E.g. FCS_COP.1/DataEncryption

7.1.2. Audit

FAU_GEN.1 (REFINED) – AUDIT DATA GENERATION

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified*] level of audit; and

c) [All administrative actions comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Certificate and CRL import or deletion
- Passwords modification (name of related user account shall be logged).
- Unsuccessful login attempts
- Software download and activation
- Time change

d) Specifically defined auditable events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST Information specified in the table above,

FAU_GEN.2 (REFINED) - USER IDENTITY ASSOCIATION

FAU_GEN.2.1 For audit events resulting from actions of identified users and network devices, the TSF shall be able to associate each auditable event with the identity of the user or the network device that caused the event.

FAU_STG_EXT.1 (EXTENDED) - PROTECTED AUDIT EVENT STORAGE

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

[*TOE shall consist of a single standalone component that stores audit data locally*].

FAU_STG_EXT.1.3 The TSF shall [*overwrite previous audit records according to the following rule:* ***replace the audit records backup with the backup of the new audit records file using a rotation mechanism***] when the local storage space for audit data is full.

FAU_STG_EXT.2/LOCSPACE (EXTENDED) - COUNTING LOST AUDIT DATA

FAU_STG_EXT.2.1/LocSpace The TSF shall provide information about the number of [*overwritten*] audit records in the case where the local storage has been filled and the TSF takes one of the actions defined in FAU_STG_EXT.1.3.

Nota: The audit records are numbered with a counter which increases for each event.

FAU_STG.3/LOCSPACE - ACTION IN CASE OF POSSIBLE AUDIT DATA LOSS

FAU_STG.3.1/LocSpace The TSF shall [generate a warning] if the audit trail exceeds [the local audit trail storage capacity].

FPT_STM_EXT1 (EXTENDED) - RELIABLE TIME STAMPS

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [*allow the Security Administrator to set the time*].

7.1.3. Cryptography

7.1.3.1. Key management

FCS_RBG_EXT.1 (EXTENDED) - RANDOM BIT GENERATION

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [*CTR_DRBG (AES)*];

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [**2**] software-based noise source, [**2**] hardware-based noise source with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

FCS_CKM.1 (REFINED) - CRYPTOGRAPHIC KEY GENERATION

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [ECC schemes using curve P-256] that meet the following: [French National Cybersecurity Agency DR profile].

FCS_CKM.2 (REFINED) – CRYPTOGRAPHIC KEY ~~DISTRIBUTION~~ ESTABLISHMENT

FCS_CKM.2.1 The TSF shall perform ~~distribute~~ cryptographic key establishment in accordance with a specified cryptographic key establishment method **[**Elliptic curve-based key establishment schemes] that meets [French National Cybersecurity Agency DR profile].

FCS_CKM.4 - CRYPTOGRAPHIC KEY DESTRUCTION

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following: [no standard].

FCS_CKM_EXT.5/CERTIFICATE (EXTENDED) - CERTIFICATE CRYPTOPERIOD

FCS_CKM_EXT.5.1/Certificate The TSF shall manage [*the validity*] for [the authentication certificates].

FCS_CKM_EXT.5.2/Certificate The TSF shall calculate the [*validity*] from [*certificate first use*]**.**

FCS_CKM_EXT.5.3/Certificate The TSF shall [generate an audit data while it continues to proceed the network traffic] after the [*certificates*] have expired.

Note: In this case new communication channels for SAs using this certificate are refused till a new certificate can be used.

FCS_CKM_EXT.5/IKEV2SA (EXTENDED) - IKEV2 IKE SA KEY CRYPTO-PERIOD

FCS_CKM_EXT.5.1/ikeV2SA The TSF shall manage [*a crypto-period*] for [IKEv2 SAs keys].

FCS_CKM_EXT.5.2/ikeV2SA The TSF shall calculate the [*key lifetime*] from [*keys generation*].

FCS_CKM_EXT.5.3/ikeV2SA The TSF shall [renew the keys by establishing a new IKEv2 SA (i.e. rekeying)] after the [*key*] has expired.

FCS_CKM_EXT.5/IKEV2CHILDSA (EXTENDED) - IKEV2 CHILD SAS KEY CRYPTO-PERIOD

FCS_CKM_EXT.5.1/ikeV2childSA The TSF shall manage [*a crypto-period*] for [IKEv2 Child SAs keys].

FCS_CKM_EXT.5.2/ikeV2childSA The TSF shall calculate the [*key lifetime*] from [*keys generation*].

FCS_CKM_EXT.5.3/ikeV2childSA The TSF shall [renew the keys by establishing a new IKEv2 Child SA (i.e. rekeying)] after the [*key*] has expired.

7.1.3.2. Cryptographic Operations

FCS_COP.1/DATAENCRYPTIONGCM - CRYPTOGRAPHIC OPERATION (AES DATA ENCRYPTION/DECRYPTION)

FCS_COP.1.1/DataEncryptionGCM The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm [AES used in GCM mode] and cryptographic key sizes [256 bits], that meet the following: [AES as specified in ISO 18033-3, GCM as specified in ISO 19772].

FCS_COP.1/DATAENCRYPTIONCTR - CRYPTOGRAPHIC OPERATION (AES DATA ENCRYPTION/DECRYPTION)

FCS_COP.1.1/DataEncryptionCTR The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm [AES used in CTR mode] and cryptographic key sizes [256 bits] that meet the following: [AES as specified in ISO 18033-3, CTR as specified in ISO 10116].

FCS_COP.1/DATAENCRYPTIONCBC - CRYPTOGRAPHIC OPERATION (AES DATA ENCRYPTION/DECRYPTION)

FCS_COP.1.1/DataEncryptionCBC The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm [AES used in CBC mode] and cryptographic key sizes [256 bits], that meet the following: [AES as specified in ISO 18033-3, CBC as specified in ISO 10116].

FCS_COP.1/DATAENCRYPTIONXTS - CRYPTOGRAPHIC OPERATION (AES DATA ENCRYPTION/DECRYPTION)

FCS_COP.1.1/DataEncryptionXTS The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm [AES used in XTS mode] and cryptographic key sizes [256 bits] that meet the following: [AES as specified in ISO 18033-3, XTS as specified in IEEE P1619/DM].

FCS_COP.1/SIGNGENRSA - CRYPTOGRAPHIC OPERATION (SIGNATURE GENERATION AND VERIFICATION)

FCS_COP.1.1/SignGenRSA The TSF shall perform [cryptographic signature services (generation and verification)] in accordance with a specified cryptographic algorithm: [RSA Digital Signature Algorithm] and cryptographic key sizes [4096 bits] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5;ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3].

FCS_COP.1/SIGNGENECDSA - CRYPTOGRAPHIC OPERATION (SIGNATURE GENERATION AND VERIFICATION)

FCS_COP.1.1/SignGenECDSA The TSF shall perform [cryptographic signature services (generation and verification)] in accordance with a specified cryptographic algorithm: [Elliptic Curve Digital Signature Algorithm] and cryptographic key sizes [256 bits] that meet the following: [ECDSA schemes defined for French National Cybersecurity Agency DR profile and no other curves].

FCS_COP.1/HASH256 (REFINED) - CRYPTOGRAPHIC OPERATION (HASH ALGORITHM)

FCS_COP.1.1/Hash256 The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [SHA-256] and ~~cryptographic key~~ message digest sizes [256 bits] that meet the following: [ISO/IEC 10118-3:2004].

FCS_COP.1/HASH384 (REFINED) - CRYPTOGRAPHIC OPERATION (HASH ALGORITHM)

FCS_COP.1.1/Hash384 The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [SHA-384] and ~~cryptographic key~~ message digest sizes [384 bits] that meet the following: [ISO/IEC 10118-3:2004].

FCS_COP.1/KEYEDHASH256 (REFINED) - CRYPTOGRAPHIC OPERATION (KEYED HASH ALGORITHM)

FCS_COP.1.1/KeyedHash256 The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA-256], and cryptographic key sizes [256 bits] used in HMAC and message digest sizes [256 bits] that meet the following: [ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”].

FCS_COP.1/KEYEDHASH384 (REFINED) - CRYPTOGRAPHIC OPERATION (KEYED HASH ALGORITHM)

FCS_COP.1.1/KeyedHash384 The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA-384], and cryptographic key sizes [384 bits] used in HMAC and message digest sizes [384 bits] that meet the following: [ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”].

7.1.4. Communications Protection and Flow Controls

7.1.4.1. Authentication

FIA_X509_EXT.1 (EXTENDED) - X509 CERTIFICATION VALIDATION

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension and that the CA flag set to TRUE.

- The TSF shall validate the revocation status of the certificate using [*a Certificate Revocation List (CRL) as specified in RFC 5759 section 5*].
- The TSF shall validate the extendedKeyUsage field according to the following rules**:**

  [
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.]
- The TSF shall validate the Certificates presented for IPSec Authentication shall have the algorithm id ECDSA-SHA256 with :
  - Secp256r1 as curve associated or
  - Brainpool256r1 as curve associated

*Nota: no OCSP used**.***

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 (EXTENDED) - X.509 CERTIFICATE AUTHENTICATION

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*IPsec, TLS*] and [*no additional use*].

FIA_X509_EXT.3 (EXTENDED) - X.509 CERTIFICATE REQUESTS

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [*CN, **pseudonym, CountryName and OrganisationName***].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

7.1.4.2. Communication Protection

7.1.4.2.1. Inter-TOE Communications Protection

FTP_ITC.1 (REFINED) - INTER-TSF TRUSTED CHANNEL

FTP_ITC.1.1 The TSF shall be capable of using [TLS or IPSec] to provide a trusted communication channel between itself and ~~another IT product~~ authorized IT entities supporting the following capabilities: audit server (TLS) and a remote instance of the TOE (IPSec) that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit [*the TSF or the authorized IT entities*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [VPN service (communication with a remote instance of the TOE and audit server)].

FDP_UCT.1 (REFINED) - INTER-TSF BASIC DATA EXCHANGE CONFIDENTIALITY

FDP_UCT.1.1 The TSF shall enforce the [access control SFP and VPN SFP(s)] to [*transmit and receive*] user data in a manner protected from unauthorized disclosure between itself and a remote instance of the TOE.

FDP_UIT.1 (REFINED) - INTER-TSF DATA EXCHANGE INTEGRITY

FDP_UIT.1.1 The TSF shall enforce the [VPN SFP] to [*transmit and receive*] user data in a manner protected from [*modification, insertion and replay*] errors between itself and a remote instance of the TOE.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [*modification, insertion and replay*] has occurred.

FCS_IPSEC_EXT.1 (EXTENDED) – INTERNET PROTOCOL SECURITY (IPSEC) COMMUNICATIONS

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as defined by RFC 4301

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [*tunnel mode*].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms

- AES-GCM with 256 bits key and 16 bytes ICV (specified in RFC 4106)
- AES-CTR with 256 bits key

together with secure Hash Algorithm) AUTH_HMAC_SHA2_256_128 (truncated)

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [*IKEv2 as defined in RFC 7296 with mandatory support for NAT traversal as specified in RFC 7296, section 2.23) and RFC 4868 for hash functions*].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the IKEv2 protocol uses the cryptographic algorithms**:**

- AES-GCM with 256 bits key and 16 bytes ICV (specified in RFC 5282)

- AES-CTR with 256 bits key and HMAC-SHA256 with 32 bytes Key and 16 bytes MAC

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [*IKEv2 SA lifetimes can be configured by an Administrator based on length of time, where the time values can be configured within **72 hours***].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [*IKEv2 Child SA lifetimes can be configured by an Administrator based on length of time, where the time values can be configured within **72 hours***].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in x.G mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [256] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [*IKEv2*] exchanges of length [*at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash*].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups [*28 (BrainpoolP256r1) and 19 (secp256r1)*]**.**

FCS_IPSEC_EXT.1.12 The TSF shall ensure that all IKE protocols perform peer authentication using [*ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [*no other method*].

FCS_IPSEC_EXT.1.13 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types**:** [*Distinguished Name (DN), **Country Name and Organisation Name***].

Note for **FCS_IPSEC_EXT.1.9** : "x" here is a 256-bit (random) ephemeral key and the shared secret "Y = x.G" is a point in the 512-bit size elliptical curve

7.1.4.2.2. Management Center Communication Protection

The management center of the TOE is performed through a secured communication link based on TLS.

FTP_TRP.1 (REFINED) - TRUSTED PATH

FTP_TRP.1.1 The TSF shall <u>be capable of using TLS to</u> provide a communication path between itself and <u>authorized remote administrators</u> ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*disclosure*] <u>and provides detection of modification of the channel data</u>.

Note : When remote administrator is located in remote network, the communication path uses inter-TOE VPN IPSEC (see FTP_ITC.1).

FTP_TRP.1.2 The TSF shall permit <u>remote Administrators</u> to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for <u>initial administrator authentication and all remote administration actions</u>.

FCS_TLSC_EXT.2 (EXTENDED) - TLS Client Protocol with Authentication

FCS_TLSC_EXT.2.1 The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions**.** The TLS implementation will support the following cipher suites:

[TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (RFC5289)]

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6**.**

FCS_TLSC_EXT.2.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [*Not implement any administrator override mechanism*]

FCS_TLSC_EXT.2.4 The TSF shall [*present the Supported Elliptic Curves Extension with the following NIST curves: secp256r1 or brainpool256r1 and no other curves*] in the Client Hello.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates

FCS_TLSS_EXT.2 (EXTENDED) - TLS Server Protocol with mutual authentication

FCS_TLSS_EXT.2.1 The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions**.** The TLS implementation will support the following cipher suites:

[TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (RFC5289)]

FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL2.0, SSL 3.0, TLS 1.0, and [*TLS 1.1*].

FCS_TLSS_EXT.2.3 The TSF shall [*perform ECDSA key establishment with key size 256 bits*], generate EC Diffie-Hellman parameters over NIST curves [*secp256r1 or brainpool256r1 and no other curves*];

FCS_TLSS_EXT.2.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [*not implement any administrator override mechanism*]

FCS_TLSS_EXT.2.6 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

7.1.4.3. Flows Controls

7.1.4.3.1. Communication partner control

FCO_CPC_EXT.1 (EXTENDED) - COMMUNICATION PARTNER CONTROL

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses: [TLS channel]

For at least: [

- Configuration data including network topology
- Update firmware
- Firmware activation]

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

7.1.4.3.2. VPN Policy flow control

FDP_ITC.2/VPN (REFINED) - VPN IMPORT OF USER DATA WITH SECURITY ATTRIBUTES

FDP_ITC.2.1/VPN The TSF shall enforce [the VPN SFP] when importing user data to send to a remote private network or IPSec frame, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/VPN The TSF shall use the ~~security attributes~~ IP protocol and topologic data associated with the imported ~~user data~~ IP frame.

FDP_ITC.2.3/VPN The TSF shall ensure that the protocol used provides for the unambiguous association between the security attribute and the ~~user data~~ IP frame received.

FDP_ITC.2.4/VPN The TSF shall ensure that interpretation of the ~~security attributes~~ IP protocol and topologic data of the imported ~~user data~~ IP frame is as intended by the source of the ~~user data~~ IP frame**.**

FDP_ITC.2.5/VPN The TSF shall enforce the following rules when importing ~~user data~~ IP frame controlled under the SFP from outside the TOE: [no additional import control rules].

FDP_ETC.2/VPN (REFINED)- VPN EXPORT OF USER DATA WITH SECURITY ATTRIBUTES

FDP_ETC.2.1/VPN The TSF shall enforce the [VPN SFP] when exporting ~~user data~~ IP frame controlled under the SFP, outside of the TOE.

FDP_ETC.2.2/VPN The TSF shall export the ~~user data~~ IP datagrams payload and topologic data with the ~~user data's~~ IP datagrams protocol and topologic data associated security attributes.

FDP_ETC.2.3/VPN The TSF shall ensure that the ~~security attributes~~ IP datagrams protocol and topologic data, when exported outside the TOE, are unambiguously associated with the exported ~~user data~~ IP datagrams payload and topologic data.

FDP_ETC.2.4/VPN The TSF shall enforce the following rules when ~~user data~~ IP datagrams and topologic data are exported from the TOE: [no additional exportation control rules].

FDP_IFC.1/VPN - VPN SUBSET INFORMATION FLOW CONTROL

FDP_IFC.1.1/VPN The TSF shall enforce the [VPN SFP with IPSec] on: [

- Subjects:
  - Encrypted Data Interface
  - Plain Text Data Interface
  - IP source and destination ports
- Information:
  - IP frame
- Operations:

- OP.Receiving: Processing of information coming from the Subject according data flow selectors.
- OP.Sending: Emission of information to the Subject according data flow selectors.

]

FDP_IFF.1/VPN - VPN SIMPLE SECURITY ATTRIBUTES

FDP_IFF.1.1/VPN The TSF shall enforce the [VPN SFP with TLS] based on the following types of subject and information security attributes: [

- Subjects:
  - Encrypted Data Interface
  - Plain Text Data Interface
- Information:
  - TOE administration flow.

]

FDP_IFF.1.2/VPN The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold

- [For the operation OP.Receving (from Encrypted Data Interface):
  - If the IP datagram contains a SPI
    - The TSF can find an associated SA using the SPI within the IP datagram
    - The IPSec protection mode contained within the IP datagram is the same as the one specified within the SA
    - The IP frame has not been inserted maliciously in the traffic (refer to FDP_UIT.1)
    - The IP frame has not been modified (refer to FDP_UIT.1)
    - The IP datagram has not been replayed (refer to FDP_UIT.1)
    - The TSF can find an associated SP
- For the operation OP.Receiving (from Plaintext Data Interface):
  - The TSF can find an associated SP using the source and destination IP addresses of the IP datagram and protocol used
- For the operation OP.Sending (to Encrypted Data Interface):
  - The datagram has been properly protected according to the SA referred by the associated SA and SP
- For the operation OP.Sending (to Plaintext Data Interface):
  - The datagram has been properly checked and unprotected according to the associated SA and SP]

FDP_IFF.1.3/VPN The TSF shall enforce [none].

FDP_IFF.1.4/VPN The TSF shall explicitly authorize an information flow based on the following rules: [that explicitly authorise information flows].

FDP_IFF.1.5/VPN The TSF shall explicitly deny an information flow based on the following rules [

- When no VPN SP has been explicitly defined for the given IP datagram (no match with the given source and destination IP addresses, port and protocols).
- When the given VPN SP specifies that sending IP packets to the destination address and ports (specific to a subnetwork) or protocol is forbidden,
- When an error occurs during the application or verification of security protections
- When datagram is not IP datagram
- When the TOE is not in its final operational state]

7.1.4.3.3. Import of Certificate

FDP_ITC.2/CRYPTOINJECTION (REFINED)- CERTIFICATE IMPORT OF USER DATA WITH SECURITY ATTRIBUTES

FDP_ITC.2.1/CryptoInjection The TSF shall enforce the [access control SFP] when importing ~~user data~~ certificate, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/CryptoInjection The TSF shall use the security attributes associated with the imported ~~user data~~ certificate.

FDP_ITC.2.3/CryptoInjection The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the ~~user data~~ certificate received.

FDP_ITC.2.4/CryptoInjection The TSF shall ensure that interpretation of the security attributes of the imported ~~user data~~ certificate is as intended by the source of the ~~user data~~ certificate.

FDP_ITC.2.5/CryptoInjection The TSF shall enforce the following rules when importing ~~user data~~ the certificate controlled under the SFP from outside the TOE: [no additional control rules].

FDP_IFC.1/CRYPTOINJECTION - SECURITY DATA INJECTION SUBSET INFORMATION FLOW CONTROL

FDP_IFC.1.1/CryptoInjection The TSF shall enforce the [access control SFP] on [:

- Subjects:
  - USB Interface
  - Remote management interface
- Information:
  - Certificates
- Operations:
  - OP.Injection: Processing of information coming from the Subject]

FDP_IFF.1/CRYPTOINJECTION - SECURITY DATA INJECTION SIMPLE SECURITY ATTRIBUTES

FDP_IFF.1.1/CryptoInjection The TSF shall enforce the [access control SFP] based on the following types of subject and information security attributes: [

- Subjects and their security attributes:
  - USB Interface
  - Remote management interface

- Information and their security attributes:
    - Certificates: Serial number, signature, issuer, validity, subject, subject public key info, unique identifiers issuer & subjects, key usage]

FDP_IFF.1.2/CryptoInjection The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

For the operation OP.Injection (from Encrypted Data Interface):

- The certificate and the corresponding security attributes are consistent

For the operation OP.Injection (from Plaintext Data Interface):

- The certificate and the corresponding security attributes are consistent

For the operation OP.Injection (from USB Interface):

- U.ROLE_GW_OPERATOR is successfully authenticated for local injection
- The certificate and the corresponding security attributes are consistent

]

FDP_IFF.1.3/CryptoInjection The TSF shall enforce [none].

FDP_IFF.1.4/CryptoInjection The TSF shall explicitly authorize an information flow based on the following rules: [none]**.**

FDP_IFF.1.5/CryptoInjection The TSF shall explicitly deny an information flow based on the following rules: [none].

FPT_TDC.1/CRYPTOINJECTION - INTER-TSF BASIC TSF DATA CONSISTENCY

FPT_TDC.1.1/CryptoInjection The TSF shall provide the capability to consistently interpret [the certificate and CRL] when shared between the TSF and another trusted IT product**.**

FPT_TDC.1.2/CryptoInjection The TSF shall use [common certificates and CRLs standards] when interpreting the TSF data from another trusted IT product.

FPT_TDC.1/VPN - INTER-TSF BASIC TSF DATA CONSISTENCY

FPT_TDC.1.1/VPN The TSF shall provide the capability to consistently interpret [the IKE parameters] when shared between the TSF and another trusted IT product**.**

FPT_TDC.1.2/VPN The TSF shall use [common certificates and CRLs standards] when interpreting the TSF data from another trusted IT product.

7.1.4.3.4. TSF Data Default Values

FMT_MSA.3 (REFINED) - STATIC ATTRIBUTE INITIALIZATION

FMT_MSA.3.1 The TSF shall enforce the [VPN SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP that is:

- Protection mode: IPSec Tunnel

- Key management mode: IKEv2
- Lifetime of IKE SAs keys: 86400 seconds (24 hours)
- Lifetime of IKE Child SAs keys: 14400 seconds (4 hours)
- Perfect Secrecy (PFS) mode (for IKE protocol): activated
- List of authorized TOE Management Center Devices (SS_MMC) IP address: 0.0.0.0 / none

FMT_MSA.3.2 The TSF shall allow [U.ROLE_GW_OPERATOR and U.ROLE_SYS_ADMIN] to specify alternative initial values to override the default values when an object or information is created.

Note: The modification are allowed only with configuration file injection

7.1.5. Users and Devices

7.1.5.1. Roles

FMT_SMR.2 – RESTRICTION ON SECURITY ROLES

FMT_SMR.2.1 The TSF shall maintain the role: [

- Authorised local Administrator (corresponding to a human user U.ROLE_GW_OPERATOR))
- Authorised TOE Management Center Device (corresponding to U.ROLE_SYS_ADMIN)]

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [the operator role shall be able to administer the TOE locally and the Administrator role shall be able to administer the TOE remotely] are satisfied

7.1.5.2. Identification and Authentication

7.1.5.2.1. TOE Management Center Device

FIA_UID.2 (REFINED) – SS_MMC IDENTIFICATION BEFORE ANY ACTION

FIA_UID.2.1 The TSF shall require each ~~user~~ TOE Management Center Device to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ TOE Management Center Device.

7.1.5.2.2. Users

FIA_UIA_EXT.1 (EXTENDED) - USER IDENTIFICATION AND AUTHENTICATION

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the authentication process**:** [

- *automated generation of cryptographic keys*
- ***TOE Start-up***
- ***TOE Shutdown***
- ***Secure erasure***
- ***Enter logging password of the local account***]

Nota: Display the warning banner in accordance with FTA_TAB.1 is performed after authentication

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF- mediated actions on behalf of that administrative user.

FIA_UAU_EXT.2 (EXTENDED) - PASSWORD-BASED AUTHENTICATION MECHANISM

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism and [*no other authentication mechanism*] to perform local administrative user authentication.

FIA_UAU.6 (REFINED) - RE-AUTHENTICATING

FIA_UAU.6.1 The TSF shall re-authenticate the ~~user~~ U.ROLE_GW_OPERATOR under the conditions [when he changes his password or when the initial session is expired].

FIA_UAU.7 (REFINED) - PROTECTED AUTHENTICATION FEEDBACK

FIA_UAU.7.1 The TSF shall provide only [obscured feedback] to the ~~user~~ U.ROLE_GW_OPERATOR while the authentication is in progress at the local console.

FIA_AFL.1 - AUTHENTICATION FAILURE MANAGEMENT

FIA_AFL.1.1 The TSF shall detect when [*an Administrator configurable positive integer*] unsuccessful successive authentication attempts occur related to [Administrators attempting to authenticate remotely].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall: [prevent the offending Administrator from successfully authenticating until a defined time period has elapsed].

FIA_PMG_EXT.1 (EXTENDED) - PASSWORD MANAGEMENT

FIA_PMG_EXT.1.1 The TSF shall provide a password management capabilities for administrative passwords.

7.1.5.3. Sessions management

FTA_SSL_EXT.1 (EXTENDED) - TSF-INITIATED SESSION LOCKING

FTA_SSL_EXT.1.1 The TSF shall, for local interactive session [*terminate the session*] after a defined period of user inactivity**.**

FTA_SSL.3 (REFINED) - TSF-INITIATED TERMINATION

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after a [Security Administrator time interval of session inactivity].

FTA_SSL.4 (REFINED) - USER-INITIATED TERMINATION

FTA_SSL.4.1 The TSF shall allow ~~user~~ U.ROLE_GW_OPERATOR or remote Administrator -initiated termination of the ~~user~~ U.ROLE_GW_OPERATOR's or Administrator's own interactive session.

FTA_TAB.1 - DEFAULT TOE ACCESS BANNERS

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

7.1.6. TSF Management

FMT_SMF.1 - SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- Ability to administer the TOE locally and remotely
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Ability to start and stop services
- Ability to configure the cryptographic functionality]

FMT_MOF.1/AUTOUPDATE - MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

FMT_MOF.1.1/AutoUpdate The TSF shall restrict the ability to [*enable*] the functions [automatic update] to [remote Administrator (U.ROLE_SYS_ADMIN)].

FMT_MOF.1/FUNCTIONS - MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [*modify*] the functions [transmission of audit data to an external IT entity] to [Administrators (U.ROLE_SYS_ADMIN and U.ROLE_GW_OPERATOR)].

FPT_SKP_EXT.1 (EXTENDED) - PROTECTION OF TSF DATA (FOR READING OF SENSITIVE KEYS)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys and private keys.

FMT_MTD.1 - MANAGEMENT OF TSF DATA (CONFIGURATION MODIFICATION)

FMT_MTD.1.1 The TSF shall restrict the ability to [*query and modify*] the [TSF data as described in § 5.1.3.7 (query) and § 5.1.3.6 (modify)] to [the authorized identified roles].

FPT_TUD_EXT.1 (EXTENDED) - TRUSTED UPDATE

FPT_TUD_EXT.1.1 The TSF shall provide [U.ROLE_GW_OPERATOR and TOE Management Center Device] the ability to query the currently executing version of the TOE firmware/software and [*the most recently installed version of the TOE firmware/software*].

FPT_TUD_EXT.1.2 The TSF shall provide [TOE Management Center Device] the ability to initiate updates to TOE firmware/software and [*no other update mechanism*].

FPT_TUD_EXT.1.3 The TSF shall provide a means to authenticate firmware/software updates to the TOE using a [*digital signature mechanism*] prior to installing those updates.

FPT_APW_EXT.1 (EXTENDED) - PROTECTION OF ADMINISTRATOR PASSWORDS

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

7.1.7. Miscellaneous

FPT_RCV.1 – MANUAL RECOVERY

FPT_RCV.1.1 After [a service crash] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2 – AUTOMATED RECOVERY

FPT_RCV.2.1 When automated recovery from [switch on or reboot] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2 For [switch on or reboot], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_FLS.1 - FAIL WITH PRESERVATION OF SECURE STATE

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [self-test failure].

FPT_TST_EXT.1 (EXTENDED) - TSF TESTING

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [*during initial start-up and at the request of the authorized user*] to demonstrate the correct operation of the TSF: [

- All cryptographic operations (all FCS_COP.1 requirements)
- Audit log integrity]

FPT_SDP_EXT.2 (EXTENDED) - STORED TSF DATA PROTECTION CAPABILITY AND ACTION

FPT_SDP_EXT.2.1 The TSF shall protect: [

- **SP and SA definitions**
- **Configuration parameters of the TOE**
- **Credentials**
- **Self-protection cryptographic keys**]

stored in containers controlled by the TSF from [*disclosure*] and shall detect [*integrity errors*] on those data.

FPT_SDP_EXT.2.2 The TSF shall [generate an event and preserve a secure state (FPT_FLS.1)], upon detection of a data integrity error.

Note: Failure of integrity check in generated with FAU_GEN.1

FDP_RIP.2 - FULL RESIDUAL INFORMATION PROTECTION

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation and deallocation of the resource from*] all objects.

7.2. SECURITY ASSURANCE REQUIREMENTS

The security target claims an EAL3 security assurance level augmented with AVA_VAN.3 and ALC_FLR.3.

Assurance requirements for this level are:

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR3 Flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction

Assurance Class	**Assurance components**
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Vulnerability analysis

Table 13: Assurance requirements for EAL3+

7.3. RATIONALE FOR THE SECURITY REQUIREMENTS

7.3.1. Security objectives for the TOE

	O.AUDIT	O.AUDIT_PROTECTION	O.AUTHENTICATION_FAILURE	O.BOOT_CONTROL	O.CRYPTO_PERIOD	O.CRYPTO_REGULATION	O.DATA_ERASURE	O.DISPLAY_BANNER	O.I&A	O.LOCAL_DATA_PROTECTION	O.MANAGEMENT	O.POL_DEFAULT	O.POL_FILTERING	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEAR	O.ROLES	O._CERTIFICATE_INJECTION	O.SELF_TEST	O.SESSION_LOCK	O.SOFTWARE_UPDATES	O.SUPERVISION	O.SUPERVISION_IMPACT	O.TIME_BASE	O.VIEW_RULES
FAU_GEN.1	X																							
FAU_GEN.2	X																							
FAU_STG_EXT.1	X	X																						

	O.AUDIT	O.AUDIT_PROTECTION	O.AUTHENTICATION_FAILURE	O.BOOT_CONTROL	O.CRYPTO_PERIOD	O.CRYPTO_REGULATION	O.DATA_ERASURE	O.DISPLAY_BANNER	O.I&A	O.LOCAL_DATA_PROTECTION	O.MANAGEMENT	O.POL_DEFAULT	O.POL_FILTERING	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEAR	O.ROLES	O._CERTIFICATE_INJECTION	O.SELF_TEST	O.SESSION_LOCK	O.SOFTWARE_UPDATES	O.SUPERVISION	O.SUPERVISION_IMPACT	O.TIME_BASE	O.VIEW_RULES
FAU_STG_EXT.2/LocSpace	X																							
FAU_STG.3/LocSpace	X	X																						
FPT_STM_EXT.1																							X	
FCS_RBG_EXT.1						X																		
FCS_CKM.1						X																		
FCS_CKM.2						X																		
FCS_CKM.4						X	X			X														
FCS_CKM_EXT.5/certificate					X																			
FCS_CKM_EXT.5/ikeV2SA					X																			
FCS_CKM_EXT.5/ikeV2childSA					X																			
FCS_COP.1/DataEncryptionGCM						X								X										
FCS_COP.1/DataEncryptionCTR						X								X										
FCS_COP.1/DataEncryptionCBC						X														X				
FCS_COP.1/DataEncryptionXTS						X				X														
FCS_COP.1/SignGenRSA				X		X																		
FCS_COP.1/SignGenECDSA						X								X						X				
FCS_COP.1/Hash256						X								X										
FCS_COP.1/Hash384						X								X										
FCS_COP.1/KeyedHash256						X								X						X				
FCS_COP.1/KeyedHash384						X								X										
FIA_X509_EXT.1														X										
FIA_X509_EXT.2														X										
FIA_X509_EXT.3														X										
FTP_ITC.1		X												X										

	O.AUDIT	O.AUDIT_PROTECTION	O.AUTHENTICATION_FAILURE	O.BOOT_CONTROL	O.CRYPTO_PERIOD	O.CRYPTO_REGULATION	O.DATA_ERASURE	O.DISPLAY_BANNER	O.I&A	O.LOCAL_DATA_PROTECTION	O.MANAGEMENT	O.POL_DEFAULT	O.POL_FILTERING	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEAR	O.ROLES	O._CERTIFICATE_INJECTION	O.SELF_TEST	O.SESSION_LOCK	O.SOFTWARE_UPDATES	O.SUPERVISION	O.SUPERVISION_IMPACT	O.TIME_BASE	O.VIEW_RULES
FDP_UCT.1		X												X										
FDP_UIT.1		X												X										
FTP_TRP.1														X										
FCS_IPSEC_EXT.1		X										X		X										
FCS_TLSC_EXT.2														X										
FCS_TLSS_EXT.2														X										
FCO_CPC_EXT.1														X										
FDP_ITC.2/VPN													X											
FDP_ETC.2													X											
FDP_IFC.1/VPN													X									X		
FDP_IFF.1/VPN												X	X									X		
FDP_ITC.2/CryptoInjection																	X							
FDP_IFC.1/CryptoInjection																	X					X		
FDP_IFF.1/CryptoInjection																	X					X		
FPT_TDC.1/CryptoInjection																	X							
FPT_TDC.1/VPN														X										
FMT_MSA.3													X				X					X		
FMT_SMR.2																X								
FIA_UID.2									X															
FIA_UIA_EXT.1									X															
FIA_UAU_EXT.2									X															
FIA_UAU.6											X													
FIA_UAU.7									X															
FIA_AFL.1			X						X															

	O.AUDIT	O.AUDIT_PROTECTION	O.AUTHENTICATION_FAILURE	O.BOOT_CONTROL	O.CRYPTO_PERIOD	O.CRYPTO_REGULATION	O.DATA_ERASURE	O.DISPLAY_BANNER	O.I&A	O.LOCAL_DATA_PROTECTION	O.MANAGEMENT	O.POL_DEFAULT	O.POL_FILTERING	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEAR	O.ROLES	O._CERTIFICATE_INJECTION	O.SELF_TEST	O.SESSION_LOCK	O.SOFTWARE_UPDATES	O.SUPERVISION	O.SUPERVISION_IMPACT	O.TIME_BASE	O.VIEW_RULES
FIA_PMG_EXT.1									X															
FTA_SSL_EXT.1																			X					
FTA_SSL.3																			X					
FTA_SSL.4																			X					
FTA_TAB.1								X																
FMT_SMF.1											X													X
FMT_MOF.1/AutoUpdate											X													
FMT_MOF.1/Functions											X													
FMT_MTD.1											X										X	X		X
FPT_SKP_EXT.1.1																								X
FPT_TUD_EXT.1											X									X				
FPT_APW_EXT.1									X															
FPT_RCV.1				X																				
FPT_RCV.2				X																				
FPT_FLS.1																		X						
FPT_TST_EXT.1																		X						
FPT_SDP_EXT.2										X												X		
FDP_RIP.2															X									

Table 14: Objectives coverage

O.AUDIT

This security objective is covered by the capability of the TSF to generate audit records data (**FAU_GEN.1**). **FAU_GEN.2** requires the TSF to associate each audit data with the identity of the user or the network device that caused the event.

FAU_STG_EXT.1 ensures the audit data to be recorded (by the TOE and by an external device). **FAU_STG.3/LocSpace** requires the TSF to generate a security event in order to inform a local user before the local space to store audit data is used up and **FAU_STG_EXT.2/LocSpace** requires numbering events.

O.AUDIT_PROTECTION

This security objective is covered by **FAU_STG_EXT.1** which requires the TSF to send all audit records data to an external device since the TSF does not locally stores audit data.

The external device is the management center, the link between the TOE and the external device is therefore a protected management communication channel (i.e. an IPSec and TLS VPN). **FTP_ITC.1**, **FCS_IPSEC_EXT.1**, **FDP_UCT.1** and **FDP_UIT.1** provide the appropriate requirements (as for O.PROTECTED_COMMUNICATIONS).

FAU_STG.3/LocSpace requires the TSF to generate a security event in order to inform a local user before the local space to store audit data is used up (in order to export the audit log)

O.AUTHENTICATION_FAILURE

This security objective is covered by **FIA_AFL.1** which defines the number of possible tries to authenticate to TOE behavior in case of authentication failure.

O.BOOT_CONTROL

This security objective is covered by **FPT_RCV.1** and **FPT_RCV.2** with **FCS_COP.1.1/SignGenRSA** which require the TSF started up without protection compromise and can recover without protection compromise after discontinuity of operations.

O.CRYPTO_PERIOD

This security objective is covered by all instances of **FCS_CKM_EXT.5** security requirements which define certificate validity.

O.CRYPTO_REGULATION

This objective is covered by requirements concerning cryptographic keys and cryptographic operations: **FCS_RBG_EXT.1**, **FCS_CKM.1, FCS_CKM.2, FCS_CKM.4** and all instances of **FCS_COP.1**.

O.DATA_ERASURE

This security objective is covered by **FCS_CKM.4** which gives the method of erasure.

O.DISPLAY_BANNER

This security objective is covered by **FTA_TAB.1** which requires the banner display before the session establishment.

O.I&A

This security objective is covered by **FIA_UID.2** and **FIA_UIA_EXT.1** which require identification of devices and authentication of users before granting access to security functions. **FPT_APW_EXT.1** supports FIA_UIA by requiring password protection.

Authentication of users is password based (**FIA_UAU_EXT.2**).

Brute force attacks are countered by requiring specific rules for users' passwords (**FIA_PMG_EXT.1 and FIA_AFL.1**), and eavesdropping by requiring protected feedback (**FIA_UAU.7**).

O.LOCAL_DATA_PROTECTION

This security objective is covered by **FPT_SDP_EXT.2** which requires securing sensitive data in the TOE. Key destruction after use is covered with **FCS_CKM.4** and **FCS_COP.1/DataEncryptionXTS** for local data encryption.

O.MANAGEMENT

This security objective is covered by **FMT_SMF.1**. All instances of **FMT_MTD.1**, **FPT_TUD_EXT.1**, **FIA_UAU.6**, **FMT_MOF.1**/**AutoUpdate** and **FMT_MOF.1**/**Functions** provide details on management functionalities

O.POL_DEFAULT

This security objective is covered by the policies **FDP_IFF.1**/**VPN** and **FCS_IPSEC_EXT.1**, because it controls IP flows by providing default security policy and a TOE state to apply filtering.

O.POL_FILTERING

This security objective is covered by the VPN enforcement policy **FDP_IFC.1**/**VPN**, **FDP_IFF.1**/**VPN**, **FDP_ITC.2**/**VPN** and **FDP_ETC.2**, because it controls IP datagrams flows by enforcing them security rules and services.

FMT_MSA.3 supports FDP_IFF.1 by providing default values.

O.PROTECTED_COMMUNICATIONS

This security objective is covered in one hand by the security requirements

- **FTP_ITC.1**, **FDP_UCT.1 FDP_UIT.1** which require the TSF to provide a trusted communication channel between itself and a remote instance of the TOE that protect data from disclosure, modification, insertion and replay.
- **FTP_TRP.1**, **FDP_UCT.1** and **FDP_UIT.1** which require the TSF to provide a trusted communication path with SS_MMC that protect data from disclosure, modification, insertion and replay.

In another hand, the security objective is covered by:

- **FCS_IPSEC_EXT.1** which requires the trusted channel between TOE itself and a remote instance of the TOE to implement IPSec and IKE
- **FPT_TDC.1** which requires the consistency check for IKE parameter exchange
- **FCS_TLSC_EXT.2 and FCS_TLSS_EXT.2** which requires the trusted channel between TOE itself and SS_MMC to implement TLS with authentication.
- **FCO_CPC_EXT.1** which requires the TOE registration before to be allowed to start communication with the other network elements.

Finally the security objective is covered by

- **authentication operation used by IPSEC and TLS, that is: FIA_X509_EXT.2 enhanced with FIA_X509_EXT.1** which requires use of valid certificates for authentication and **FIA_X509_EXT.3** which requires certificates loaded on the TOE comes from TOE requests**.**
- all cryptographic operations used by IPSec and IKE, that is: **FCS_COP.1**/**DataEncryptionGCM** and **FCS_COP.1**/**DataEncryptionCTR, FCS_COP.1**/**SignGenECDSA**, **FCS_COP.1**/**Hash256** and **FCS_COP.1**/**KeyedHash256.**
- all cryptographic operations used by TLS, that is: **FCS_COP.1**/**DataEncryptionGCM, FCS_COP.1**/**SignGenECDSA**, **FCS_COP.1**/**Hash384** and **FCS_COP.1**/**KeyedHash384.**

O.RESIDUAL_INFORMATION_CLEAR

This security objective is covered by **FDP_RIP.2** which ensures residual information protection

O.ROLES

This security objective is covered by **FMT_SMR.2** which defines roles for users and roles for devices the TSF shall maintain.

O.CERTIFICATE_INJECTION

This objective is covered by the security data injection policy (**FDP_IFC.1**/**CryptoInjection**, **FDP_IFF.1**/**CryptoInjection** and **FDP_ITC.2**/**CryptoInjection**) which controls certificates flows of security data injection.

FMT_MSA.3 supports FDP_IFF.1/CryptoInjection, providing default values.

FPT_TDC.1/**CryptoInjection** supports FDP_ITC.2/CryptoInjection, providing data consistency check.

O.SELF_TEST

This security objective is covered by **FPT_TST_EXT.**1 which requires self-test capabilities. In case of self-test failure, the TSF shall preserve a secure state (**FPT_FLS.1**).

O.SESSION_LOCK

This security objective is covered by **FTA_SSL_EXT.1, FTA_SSL.3** and **FTA_SSL.4** which define session termination.

O.SOFTWARE_UPDATES

This security objective is covered by **FPT_TUD_EXT.1** and cryptography operation **FCS_COP.1.1**/**DataEncryptionCBC, FCS_COP.1.1**/**SignGenECDSA** for authentication and **FCS_COP.1.1**/**KeyedHash256** for integrity test**.**

O.SUPERVISION

This objective is covered by **FMT_MTD.1** to query relevant information on the TOE.

O.SUPERVISION_IMPACT

This objective is covered by all policies concerning TOE sensitive assets by restricting access to operations handling these assets: **FDP_IFC.1**/**VPN**, **FDP_IFF.1**/**VPN**, **FDP_IFC.1**/**CryptoInjection** and **FDP_IFF.1**/**CryptoInjection** and completed with **FPT_SDP_EXT.2** for data control in the containers.

FMT_MSA.3 supports FDP_IFF.1 by providing default values.

Furthermore, for the same reasons this objective is covered by all requirements concerning the TSF data management: **FMT_MTD.1**.

O.TIME_BASE

This objective is covered by the requirement **FPT_STM_EXT.1** which requires time reliability.

O.VIEW_RULES

This security objective is covered by the protection policy of TSF configuration and cryptographic keys (**FMT_SMF.1**, **FMT_MTD.1**, **and FPT_SKP_EXT.1**) by controlling their access to the action allowing review.

7.3.2. Rationale for the security assurance requirements

The TOE evaluation is performed through the ANSSI "Qualification" process, claiming a "Standard" assurance level. This level requires a CC EAL3 security assurance level augmented with ALC_FLR.3 and AVA_VAN.3.

7.3.2.1. AVA_VAN.3 Focused vulnerability analysis

This augmentation is required by the ANSSI "Qualification" process at "Standard" level.

7.3.2.2. ALC_FLR.3 Systematic flaw remediation

This augmentation is required by the ANSSI "Qualification" process at "Standard" level.

7.3.3. Dependencies

7.3.3.1. Dependencies for the Security Functional Requirements

SFR	CC dependencies	Satisfied dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM_EXT.1
FAU_GEN.2	(FAU_GEN.1) and (FIA_UID.1)	FAU_GEN.1 FIA_UID.2 (hierarchical to FIA_UID.1)
FAU_STG_EXT.1	(FAU_GEN.1) and (FTP_ITC.1)	FAU_GEN.1 FTP_ITC.1
FAU_STG_EXT.2/LocSpace	(FAU_GEN.1) and (FAU_STG_EXT.1)	(FAU_GEN.1) and (FAU_STG_EXT.1)
FAU_STG.3/LocSpace	FAU_STG.1	FAU_STG_EXT.1
FPT_RCV.1	AGD_OPE.1 Operational user guidance	AGD_OPE.1 Operational user guidance
FPT_RCV.2	AGD_OPE.1 Operational user guidance	AGD_OPE.1 Operational user guidance
FPT_STM_EXT.1	No dependencies.	
FCS_RBG_EXT.1	No dependencies.	
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_CKM.2 FCS_COP.1 FCS_CKM.4
FCS_CKM.2	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1
FCS_CKM_EXT.5/certificate	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) and (FPT_STM_EXT.1)	FCS_CKM.1 FCS_CKM.4 FPT_STM_EXT.1
FCS_CKM_EXT.5/ikeV2SA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) and (FPT_STM_EXT.1)	FCS_CKM.1 FCS_CKM.4 FPT_STM_EXT.1
FCS_CKM_EXT.5/ikeV2childSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) and (FPT_STM_EXT.1)	FCS_CKM.1 FCS_CKM.4 FPT_STM_EXT.1
FCS_COP.1/DataEncryptionGCM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/DataEncryptionCTR	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/DataEncryptionCBC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/DataEncryptionXTS	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/SignGenRSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/SignGenECDSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/Hash256 (3)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/Hash384 (3bis)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/KeyedHash256 (4)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4

SFR	CC dependencies	Satisfied dependencies
FCS_COP.1/KeyedHash384 (4bis)	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1 FCS_CKM.4
FIA_X509_EXT.1	(FIA_X509_EXT.2)	FIA_X509_EXT.2
FIA_X509_EXT.2	(FIA_X509_EXT.1)	FIA_X509_EXT.1
FIA_X509_EXT.3	(FCS_CKM.1) and (FIA_X509_EXT.1)	FCS_CKM.1 FIA_X509_EXT.1
FTP_ITC.1	No dependencies.	
FDP_UCT.1	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/VPN FTP_ITC.1 FTP_TRP.1
FDP_UIT.1	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/VPN FTP_ITC.1 FTP_TRP.1
FTP_TRP.1	No dependencies	
FCS_IPSEC_EXT.1	(FCS_CKM.1) and (FCS_CKM.2) and ((FCS_COP.1/DataEncryptionGCM) or (FCS_COP.1/DataEncryptionCTR)) and (FCS_COP.1/SignGenECDSA) and (FCS_COP.1/Hash256) and (FCS_COP.1/KeyedHash256) and (FCS_RBG_EXT.1)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryptionGCM FCS_COP.1/DataEncryptionCTR FCS_COP.1/ SignGenECDSA FCS_COP.1/Hash256 FCS_COP.1/KeyedHash256 FCS_RBG_EXT.1
FCS_TLSC_EXT.2	(FCS_CKM.1) and (FCS_CKM.2) and (FCS_COP.1/DataEncryptionGCM) and (FCS_COP.1/SignGenECDSA) and (FCS_COP.1/Hash384) and (FCS_COP.1/KeyedHash384) and (FCS_RBG_EXT.1)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryptionGCM FCS_COP.1/ SignGenECDSA FCS_COP.1/Hash384 FCS_COP.1/KeyedHash384 FCS_RBG_EXT.1
FCS_TLSS_EXT.2	((FCS_CKM.1) and (FCS_CKM.2) and (FCS_COP.1/DataEncryptionGCM) and (FCS_COP.1/SignGenECDSA) and (FCS_COP.1/Hash384) and (FCS_COP.1/KeyedHash384) and (FCS_RBG_EXT.1)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryptionGCM FCS_COP.1/ SignGenECDSA FCS_COP.1/Hash384 FCS_COP.1/KeyedHash384 FCS_RBG_EXT.1
FCO_CPC_EXT.1	No dependencies	
FDP_ITC.2/VPN	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1) and (FPT_TDC.1)	FDP_IFC.1/VPN FTP_TRP.1 FPT_TDC.1/VPN
FDP_ETC.2	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/VPN
FDP_IFC.1/VPN	(FDP_IFF.1)	FDP_IFF.1/VPN
FDP_IFF.1/VPN	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/VPN FMT_MSA.3
FDP_ITC.2/CryptoInjection	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1) and (FPT_TDC.1)	FDP_IFC.1/CryptoInjection FTP_ITC.1 FPT_TDC.1/CryptoInjection

SFR	CC dependencies	Satisfied dependencies
FDP_IFC.1/CryptoInjection	(FDP_IFF.1)	FDP_IFF.1/CryptoInjection
FDP_IFF.1/CryptoInjection	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/CryptoInjection FMT_MSA.3
FPT_TDC.1/CryptoInjection FPT_TDC.1/VPN	No dependencies.	
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.2 (hierarchical to SMR.1)
FMT_SMR.2	(FIA_UID.1)	FIA_UID.2 (hierarchical to FIA_UID.1)
FIA_UID.2	No dependencies.	
FIA_UIA_EXT.1	(FTA_TAB.1)	FTA_TAB.1
FIA_UAU_EXT.2	No dependencies.	
FIA_UAU.6	No dependencies.	
FIA_UAU.7	(FIA_UAU.1)	FIA_UIA_EXT.1
FIA_AFL.1	(FIA_UAU.1)	FIA_UIA_EXT.1
FIA_PMG_EXT.1	No dependencies.	
FTA_SSL_EXT.1	FIA_UIA_EXT.1	FIA_UIA_EXT.1
FTA_SSL.3	No dependencies.	
FTA_SSL.4	No dependencies.	
FTA_TAB.1	No dependencies.	
FMT_SMF.1	No dependencies.	
FMT_MOF.1/AutoUpdate	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.2
FMT_MOF.1/Functions	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.2
FMT_MTD.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.2
FPT_SKP_EXT.1	No dependencies.	
FPT_TUD_EXT.1	(FCS_COP.1/SignGenRSA) or (FCS_COP.1/Hash256)	FCS_COP.1/SignGenRSA FCS_COP.1/Hash256)
FPT_APW_EXT.1	No dependencies.	
FPT_FLS.1	No dependencies.	
FPT_TST_EXT.1	No dependencies.	
FPT_SDP_EXT.2	No dependencies.	
FDP_RIP.2	No dependencies.	

Table 15: SFR dependencies status

7.3.3.2. Rationale for the unsatisfied SFR dependencies

SFR	SFR unsatisfied dependencies
FMT_MSA.3	FMT_MSA.1 dependency is unsatisfied, because default settings values cannot be modified.
FMT_SMR.2	FIA_UID.1 dependency is unsatisfied because it has been replaced with FIA_UIA_EXT.1, which specifies the relevant Administrator identification (see [c_PP])
FIA_UAU.7	FIA_UAU.1 dependency is unsatisfied because it has been replaced with FIA_UIA_EXT.1, which specifies the relevant Administrator identification (see [c_PP])
FIA_AFL.1	FIA_UAU.1 dependency is unsatisfied because it has been replaced with FIA_UIA_EXT.1, which specifies the relevant Administrator identification (see [c_PP])

Table 16: Unsatisfied SFR dependencies

7.3.3.3. Dependencies for the Security Assurance Requirements

SAR	CC dependencies	Satisfied dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.3 ADV_TDS.2
ADV_FSP.3	(ADV_TDS.1)	ADV_TDS.2
ADV_TDS.2	(ADV_FSP.3)	ADV_FSP.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.3
AGD_PRE.1	No dependencies.	
ALC_CMC.3	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.3 ALC_DVS.1 ALC_LCD.1
ALC_CMS.3	No dependencies.	
ALC_DEL.1	No dependencies.	
ALC_DVS.1	No dependencies.	
ALC_FLR.3	No dependencies.	
ALC_LCD.1	No dependencies.	
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
ASE_ECD.1	No dependencies.	
ASE_INT.1	No dependencies.	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1 ASE_OBJ.2
ASE_SPD.1	No dependencies.	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.3 ASE_INT.1 ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.3 ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1 ADV_TDS.2 ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.3 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1

Table 17: SAR dependencies status

8. TOE SUMMARY SPECIFICATIONS

8.1. SECURITY FUNCTIONS

8.1.1. F.AUDIT_AND_EVENTS_LOGGING

An **event** is the result of known/specified action in the Mistral system. There is a special event kind named **alarm**. An alarm is an event with a severity level equal or superior to **Alert** described below.

8.1.1.1. Events storage

Events are written by the TOE itself in local files on the TOE to allow the viewing of past actions history and detected problems. Events stored contain:

- Sub-System name generating the event
- Sequence number (incremented of one unit on each new event)
- Date and time
- Event Occurrence
- Severity level
- Type of event
- Optional parameters
- Authenticated role when event occur
- Event type description

No sensitive data are contained in the events.

When current sequence number reaches its maximum value, it is reset to its original value. Some events concerning network are aggregated in order to not fill too quickly the event log.

TOE is able to store in a file a finite number of events. TOE creates a backup of the log file when the maximum number of records is reached. Log file backup is managed with a rotation mechanism. TOE raises an event before to delete the events. TOE notifies in its log file the automatic backup of the current file and recent backup files deletion.

Alarms are logged and sent to Management Center Devices. They can be displayed to the Local Management Interface.

Event log can be archived locally on external media; TOE shall record this action in the event log.

8.1.1.2. Events & Alarms

The events and alarms generated by the TOE are:

- Notice

- Warning
- Error
- Alert
- Emergency

Alert and emergency events are considered as alarms.

Events notified by the TOE as a notice or a warning are:

- Start-up of the TOE,
- Administrative login and logout,
- Security related configuration changes,
- Generating asymmetric cryptographic keys,
- Passwords modification,
- Log archive or deletion,
- VPN establishment (successful),
- Certificate or CRL injection/deletion (successful),
- Software Update,
- Configuration injection,
- Time change,
- Secure erasure (success).

Events notified as an error are:

- TOE in failure state,
- Passwords modification error,
- Unsuccessful login attempts,
- Certificate or CRL injection/deletion with error,
- Security related configuration changes error,
- VPN establishment error and link down,
- Software Update upload failure.

Events notified as an alarm or an emergency are:

- Self-test error,
- Integrity error,
- Secure erasure (failure),
- Authentication failure ,
- Certificates end of life,

- Software Update installation failure,
- Fast event log deletion,
- and some network events considered as errors.

8.1.2. F.STORAGE_AND_PROTECTION_FOR LOCAL_DATA

8.1.2.1. Data definition

Data can be gathered in 2 groups:

- **Permanent data**: saved in the non-volatile memory of the gateway between two starts.
- **Volatile data**: not saved after the shutdown or the restart of the equipment .

Permanent data are divided in the following groups:

- **Factory data**: default Local Management Interface user profiles. Not erasable, those data are written in concerned data containers during secure erasure.
- **Hardware data**: serial numbers and Ethernet addresses. Set once during the equipment manufacturing and not erasable after.
- Sensitives **Network data**: parameters of all network interfaces.
- **Security data for remote managemen**t: security rules (Security Association / Security Policies), keys, certificates, IKE parameters and keys, management centers IP addresses and other useful parameters for remote management.
- **Security data for user data flows**: security rules (Security Association / Security Policies)
- **Events log file**: storage of events/alarms detected by the equipment.

8.1.2.2. Data protection

Containers are protected in confidentiality and integrity. **Data erasing**

Erasing of plain-texted security data brings them confidentiality protection.

8.1.3. F.TRAFFIC_KEYS_AND_CERTIFICATES_MANAGEMENT

Keys and **X509 certificates** are used for network flows protection or authentication of counterpart equipment.

8.1.3.1. Keys description:

There are 2 key types in the Mistral system:

- **Negotiated keys**: dynamic negotiated keys by IKEv2. There are not saved between 2 starts.
- **Generated keys:** keys generated by cryptographic algorithms used to VPN keys establishment (IPSec and TLS)

8.1.3.2. Keys physical protection

Generated keys are **protected in the SS_IPSEC_GW** and don't go out from any interface. **Keys erasing**

On secure erasing, keys in Mistral partition are cleared.

Nota: If the read-verification of the overwritten data fails, the process shall be repeated again.

Generated keys and negotiated are cleared after use.

8.1.3.4. Certificates using

The TOE certificates provided by CSS_PKI are injected in the TOE before to become operational device. They are used for IKE authentication with remote instance of TOE (IPSEC) and with SS_MMC (TLS).

TOE checks certificates validity when they are loaded from USB media.

Nota: In case of certificate renewal, TOE checks that new certificate can be used before older certificate end or at the current date. During traffic establishment, certificates are used to authenticate TOE with SS_MMC (TLS) or another TOE instance (IPSec). TOE check if the certificate received is linked with a trusted CA (trusted anchor).

8.1.4. F.USERS_CONFIGURATION_AND_MONITORING

8.1.4.1. Local management

Mistral gateways are manageable with management centers and allowed stations through the network.

Some commands can be executed with the **Local Management Interface.**

Local Management Interface access is limited with the active user profile. Local Management Interface is accessible locally. Users do not have their own account but use a single administrator profile with limited granted commands. The TOE protects **U.ROLE_GW_OPERATOR** account with a password and freezes it for a moment when the number of authorized failure is reached.

When users are authenticated with a password, they are allowed to access to **U.ROLE_GW_OPERATOR** commands as restart, stop, status query, self-tests and configure the equipment. **U.ROLE_GW_OPERATOR** is an administrator for the TOE.

User session termination is done by the user, or automatically after a delay of inactivity.

Banner: at user session opening, a notice and consent warning message is displayed.

8.1.4.2. Remote management

TOE allows remote connection using TLS tunnel with X.509 certificates for authentication.
Remote session termination is done automatically after the command passed, or by TOE after a delay of inactivity.
Nota: Remote users do not have their own account on the TOE but use a user profile with limited allowed commands. Remote access profile gives the user access to all commands as restart, stop status query, self-tests, equipment configuration, audit log consulting and updates. It is an administrator for the TOE.

8.1.4.3. Configuration and monitoring

Local Management Interface lets configuration and monitoring of the Mistral gateway with restricted CLI commands. Parameters can be set individually or imported from a secured file containing all or part of the configuration following user profile:

The TOE shall authorize modification of data described in § 5.1.3.6 only to the authorized identified roles which are the local operator (U.ROLE_GW_OPERATOR) and the TOE management center device (U.ROLE_SYS_ADMIN). TOE shall receive a configuration file from management center device before starting user traffic handling.

8.1.4.4. Software update

In the Mistral system software, update can be performed through the remote management protocol. The update consists in the download of a single file protected in authentication, integrity and confidentiality called firmware. The firmware contains all software components (OS, main software …).

8.1.4.5. IKE data injection

Certificates are injected in the equipment locally (**U.ROLE_GW_OPERATOR** rights needed) or by a TOE Management Center. Certificates used are X509 certificates provided by CSS_PKI and signed by certificate authority.

Time management

TOE has to rely on current time (event log …). Time must have been configured on the TOE by **U.ROLE_GW_OPERATOR** before it starts to cipher/decipher. During all its lifetime, TOE allows **U.ROLE_GW_OPERATOR and U.ROLE_SYS_ADMIN** to change time locally.
The TOE has to hold date and time when it is turned off using a battery which guarantees this function during the whole life of the TOE.

8.1.5. F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS

8.1.5.1. Traffic policy

All incoming and outgoing network flows are analyzed and have a predefined handling. Possible actions allowed in SP for frames to be sent through untrusted network are:

- **Discard**: the frame is destroyed. This is the default security policy (in case no VPN SP has been explicitly defined)
- **Protect**: the frame must be encrypted/decrypted depending on the mode defined in the SA.

If no rule corresponds during the analysis a **default discard** action is applied on the frame.

8.1.5.2. User network flow filtering

Each incoming and outgoing frame from cipher or plain zone is systematically analyzed and filtered. Filtering is based on **IPSec** selectors and **SA** (Security Association) / **SP** (Security Policy).

TOE is a network gateway and isolate plain and ciphered network from ISO layer 2 messages.

The criteria of filter rules are:

- **The receiving or destination interface of IP packets covered by the rule;**
- **The source of the information flows covered by the rule;**
- **The IP protocol(s), TCP services or types of ICMP messages of information flows covered by the rule;**
- **The destination of information flows covered by the rule**;

Each filter rule must specify a control action and may logging action.

8.1.5.3. User network flow protection

When the filtering action is « protect », frames are encrypted (or decrypted) depending on the protection mode and keys specified in the SA: integrity, confidentiality encapsulated in tunnel mode using IKEv2 negotiated keys.

When frame protection is finished, the Commutation software component established the interface/outgoing zone to send the new packet.

The sensitive assets handled by uncontrolled component (used for VPN flow) must be ciphered first.

If the gateway receives an **ESP** frame on a cipher interface, it will first of all try to decrypt the frame with the SA identified by the SPI of the ESP header before filtering.

IKE and IPSec definition:

- Key exchange: EC-DH : BrainpoolP256r1 or secp256r1
- Authentication mode: ECDSA : BrainpoolP256r1 or secp256r1 with SHA256 using X.509v3 certificates
- Key derivation: PRF_HMAC_SHA2_256
- IKE protocol confidentiality algorithm: AES-GCM16 and AES-CTR (AUTH_HMAC_SHA2_256_128) with 256-bits long key
- IKE protocol integrity algorithm: HMAC-SHA- 256_128
- IKE SA childless creation method. No other algorithms or key length than described above are allowed

8.1.6. F.SECURE_BOOT

On TOE restarts (switch on or any reboot), TOE shall control:

- Boot chain integrity
- Secure boot certificates revocation
- Software integrity and authenticity

8.1.7. F.FAILURE_STATE

When one of the following errors occurs the equipment enters in a failure state:

- Memory access error
- Self-test failure
- Failure of a service start
- Writing memory error
- Event recording error
- Boot error

In a failure state all user network services are blocked but data are kept in memory for analysis.

8.1.8. F.SECURITY_ERASURE

TOE allows U.ROLE_GW_OPERATOR to perform security erasure.

On security erasure, TOE:

- Goes in ST_GW_FACTORY state

- Keeps the current software version
- Erase configuration data and data injected during installation (password, certificates) and keys generated
- Keeps the event log**F.SELF-TEST**

A cryptographic self-test is automatically performed at TOE start.

While the TOE is operational, a cryptographic self-test can be performed on user request.

8.2. SFR AND SECURITY FUNCTION MAPPING

SFR	SFT
FAU_GEN.1	F.AUDIT_AND_EVENTS_LOGGING F.SECURE_ERASURE
FAU_GEN.2	F.AUDIT_AND_EVENTS_LOGGING
FAU_STG_EXT.1	F.AUDIT_AND_EVENTS_LOGGING
FAU_STG_EXT.2/LocSpace	F.AUDIT_AND_EVENTS_LOGGING
FAU_STG.3/LocSpace	F.AUDIT_AND_EVENTS_LOGGING
FPT_STM_EXT.1	F.USERS_CONFIGURATION_AND_MONITORING
FCS_RBG_EXT.1	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FCS_CKM.1	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FCS_CKM.2	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FCS_CKM.4	F.SECURITY_ERASURE F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FCS_CKM_EXT.5/certificate	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FCS_CKM_EXT.5/ikeV2SA	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FCS_CKM_EXT.5/ikeV2childSA	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FCS_COP.1/DataEncryptionGCM	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FCS_COP.1/DataEncryptionCTR	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FCS_COP.1/DataEncryptionCBC	F.USERS_CONFIGURATION_AND_MONITORING
FCS_COP.1/DataEncryptionXTS	F.STORAGE_AND_PROTECTION_FOR_LOCAL_DATA
FCS_COP.1/SignGenRSA	F.USERS_CONFIGURATION_AND_MONITORING F.SECURE_BOOT
FCS_COP.1/SignGenECDSA	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FCS_COP.1/Hash256	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS F.STORAGE_AND_PROTECTION_FOR_LOCAL_DATA
FCS_COP.1/KeyedHash256	F.USERS_CONFIGURATION_AND_MONITORING F.STORAGE_AND_PROTECTION_FOR_LOCAL_DATA

FCS_COP.1/Hash384	F.USERS_CONFIGURATION_AND_MONITORING
FCS_COP.1/KeyedHash384	F.USERS_CONFIGURATION_AND_MONITORING
FIA_X509_EXT.1	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FIA_X509_EXT.2	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FIA_X509_EXT.3	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FTP_ITC.1	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FDP_UCT.1	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FDP_UIT.1	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FCS_IPSEC_EXT.1	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FTP_TRP.1	F.USERS_CONFIGURATION_AND_MONITORING
FCS_TLSC_EXT.2	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT F.USERS_CONFIGURATION_AND_MONITORING
FCS_TLSS_EXT.2	F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT F.USERS_CONFIGURATION_AND_MONITORING
FCO_CPC_EXT.1	F.USERS_CONFIGURATION_AND_MONITORING
FDP_ITC.2/VPN	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FDP_ETC.2	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FDP_IFC.1/VPN	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FDP_IFF.1/VPN	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FDP_ITC.2/CryptoInjection	F.USERS_CONFIGURATION_AND_MONITORING F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FDP_IFC.1/CryptoInjection	F.USERS_CONFIGURATION_AND_MONITORING F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FDP_IFF.1/CryptoInjection	F.USERS_CONFIGURATION_AND_MONITORING F.TRAFFIC_KEYS_AND_CERTIFICATES_ MANAGEMENT
FPT_TDC.1/CryptoInjection	F.USERS_CONFIGURATION_AND_MONITORING
FPT_TDC.1/VPN	F.FILTERING_AND_PROTECTION_NETWORK_DATA_FLOWS
FMT_MSA.3	F.USERS_CONFIGURATION_AND_MONITORING
FMT_SMR.2	F.USERS_CONFIGURATION_AND_MONITORING
FIA_UID.2	F.USERS_CONFIGURATION_AND_MONITORING
FIA_UIA_EXT.1	F.USERS_CONFIGURATION_AND_MONITORING
FIA_UAU_EXT.2	F.USERS_CONFIGURATION_AND_MONITORING
FIA_UAU.6	F.USERS_CONFIGURATION_AND_MONITORING
FIA_UAU.7	F.USERS_CONFIGURATION_AND_MONITORING
FIA_AFL.1	F.USERS_CONFIGURATION_AND_MONITORING

FIA_PMG_EXT.1	F.USERS_CONFIGURATION_AND_MONITORING
FTA_SSL_EXT.1	F.USERS_CONFIGURATION_AND_MONITORING
FTA_SSL.3	F.USERS_CONFIGURATION_AND_MONITORING
FTA_SSL.4	F.USERS_CONFIGURATION_AND_MONITORING
FTA_TAB.1	F.USERS_CONFIGURATION_AND_MONITORING
FMT_SMF.1	F.USERS_CONFIGURATION_AND_MONITORING
FMT_MOF.1/AutoUpdate	F.USERS_CONFIGURATION_AND_MONITORING
FMT_MOF.1/Functions	F.USERS_CONFIGURATION_AND_MONITORING
FMT_MTD.1	F.USERS_CONFIGURATION_AND_MONITORING
FPT_SKP_EXT.1	F.USERS_CONFIGURATION_AND_MONITORING
FPT_TUD_EXT.1	F.USERS_CONFIGURATION_AND_MONITORING
FPT_APW_EXT.1	F.STORAGE_AND_PROTECTION_FOR_LOCAL_DATA F.USERS_CONFIGURATION_AND_MONITORING
FPT_RCV.1	F.SECURE_BOOT F.FAILURE_STATE
FPT_RCV.2	F.SECURE_BOOT F.FAILURE_STATE
FPT_FLS.1	F.FAILURE_STATE
FPT_TST_EXT.1	F.SELF-TEST
FPT_SDP_EXT.2	F.STORAGE_AND_PROTECTION_FOR_LOCAL_DATA
FDP_RIP.2	F.STORAGE_AND_PROTECTION_FOR_LOCAL_DATA

Table 18 : SFR and SFT mapping