# SECURITY TARGET OF MISTRAL IP ENCRYPTION DEVICE


**Prepared by :**
**THALES Communications**
**4, rue des louvresses 92230 Gennevilliers - FRANCE**

**fr**

| THALES<br>THALES Communications & Security<br>**F0057** | NUMERO DOCUMENT / DOCUMENT NUMBER | REVISION | FORMAT / SIZE | PAGE |
|---|---|---|---|---|
| | **63 295 297 - 306** | -A Lite | **A4** | **1/128** |

# TABLE OF CONTENTS

# 1. INTRODUCTION

## 1.1. DOCUMENT IDENTIFICATION AND SUMMARY

Document reference: 63 295 297 - 306

Document version: -A

Evaluation Level: EAL3 augmented with ALC_FLR.3 and AVA_VAN.3

The security target is based on, but it is not conformant to, the Security Requirements for Network Devices Protection Profile [ND_PP].

## 1.2. TOE IDENTIFICATION

TOE : Mistral IP software v2.1.2 for Mistral IP system version 8

Nota : *The TOE is embedded in Mistral device v1.2.00 also known as V5M .*

*The group formed by the Mistral IP software embedded in Mistral device, is called Mistral IP device. The relative commercial name is "Mistral Net".*

TOE reference: TRC7546-I0 version 8.2.1.2

Mistral IP software version's format is as follow: x.y.z

– x is the system version

– y identifies major functional version

– z indicates minor functional evolution and flaws patchs

Mistral device release's format is as follow : x.y.z

– x identifies the equipment form factor

– y identifies the hardware architecture

– z indicates minor evolutions (e.g. a component change)

## 1.3. TOE OVERVIEW

### 1.3.1. MISTRAL IP DEVICE

Mistral IP is a network device providing IP datagram protection based on VPN (« Virtual Private Network ») technology. It secures data communication links (MAN or WAN, Radio communication link, Satcom link).

Mistral IP provides following data protection:

– Data encryption

– Data Integrity and Authentication

– Anti-Replay (only for IPSec)

– Remote TOE authentication

Those protections are provided through different modes which are:

– ENHANCED SIMPLE encryption mode, which provides data encryption and integrity without encapsulation,

– IPSEC ESP Tunnel encapsulation mode, which provides data and topology information encryption, integrity and anti-replay

Two cryptographic key management modes are available:

– Negotiated keys mode: in this case, VPN keys are negotiated (IKEv2 protocol) and the Mistral management center distributes peer authentication keys

– Distributed keys mode: in this case, the Mistral management center distributes the VPN keys

The TOE can be integrated within networks using the brigde mode. In bridge mode, the TOE is routing-transparent for the network. The TOE accepts any network datagram, even if the MAC (Ethernet) address is not its. The TOE authorised routing procotols (list of authorised protocols is configurable) to bypass the TOE.

The TOE support IPv4 and IPv6 protocols; In IPSEC ESP Tunnel mode, it could manage the following encapsulation modes IPv4 in IPv6, and IPv6 in IPv4.

### 1.3.2. ARCHITECTURE OF THE MISTRAL IP SYSTEM

Mistral IP system is composed of IP encryption devices (Mistral IP) and one or several CG (Mistral Management Center).

Nota : *When using terms “Mistral IP system” we refer to the system, that is a network architecture composed of many encryption devices, Mistral management centers, …*

*When using term “Mistral IP” we refer to the IP encryption device only.*

Mistral IP has an interface connected to the plaintext data network (i.e. the trusted network), another connected to the ciphered data network (i.e. the untrusted network).

Mistral IP VS8.X system is composed of following entities:

– IP encryption devices
  - Mistral One (20Mbps, 100 VPNs)
  - Mistral Net (100Mbps, 1000 VPNs)
  - Mistral Max (2Gbps, 10000 VPNs)

– A Mistral Management Center Software (LGC): application that allows to manage, configure and supervise those encryption devices. It is installed on the Mistral Management Center Device (SGC). It’s main functionalities are:
  - Smartcard and initialisation-files configuration
  - Security associations and security policies configuration
  - Cryptographic key distribution (for “Distributed keys” mode)
  - Audit records data retrieving
  - Encryption device supervision
  - Secured device’s software update
  - Devices supervision

– Key Generation Center (CEC): a stand-alone workstation, connected to a cryptographic resource device, with a specific software for Mistral system key generation.

The CEC generates keys using a HSM (Hardware Security Module). The CEC exports keys in plaintext mode or wrapped into an encrypted file (AES 128 bits). The encryption key for the file is derived from a passphrase that the administrator has to enter to unwrap keys at injection. This passphrase may either be randomly generated by the CEC or be entered by the user on the CEC (on that latter case, it is 16-chars minimum).

The HSM used by the CEC is a Mistral IP encryption device with a specific software.

– NTP Server: application that allows providing and maintaining date and time reference through synchronization process (NTPv4 protocol) to encryption devices.

Mistral IP VS8.X system can also be connected to external devices:

– External encryption device: any other Mistral-compatible encryption device or software.

– Supervision device (SE): any network supervision device

Any management data flow between a Mistral encryption device and the Mistral Management Center Device (SGC) is protected using a VPN between the encryption device and another Mistral configured as a “front-end”. Therefore, the Mistral IP device has two configurations:

– "classic", which is the common configuration

– "front-end", which is the configuration necessary for the Management Center Device

Mistral Management Center (CGM) is the group formed by a SGC and a front-end Mistral. Several CGM can be integrated in a system for redundancy purposes.

Mistral IP is able to operate in two different modes:

- with one or more connected CGM : the connected operation mode
- without any connected CGM : the autonomous operation mode

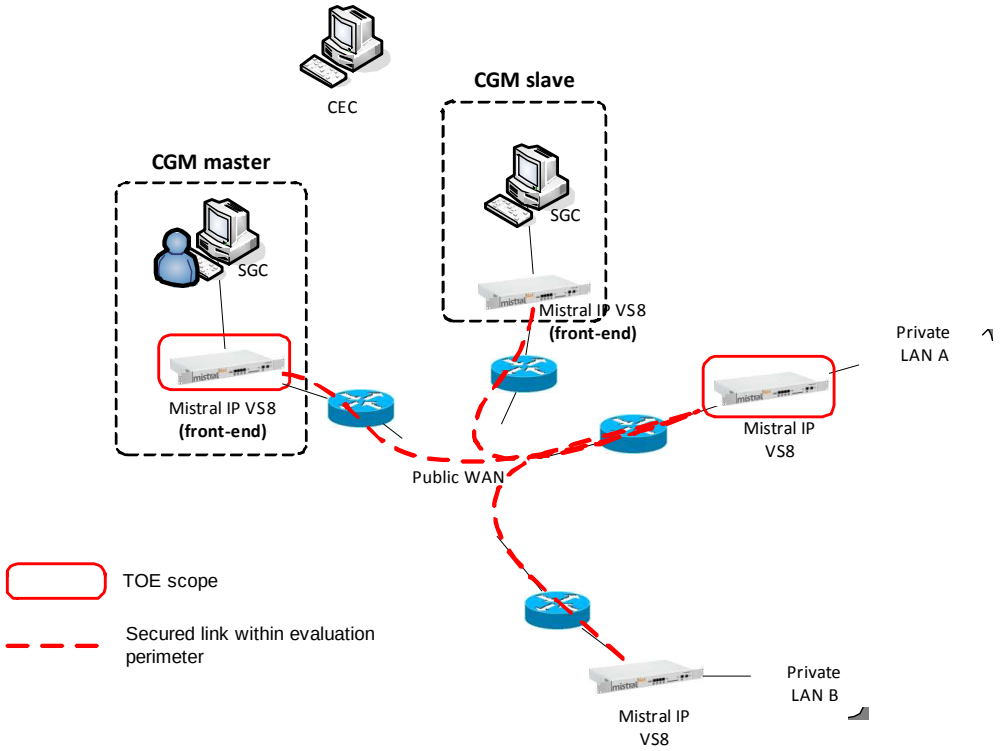


**Figure 1:Mistral IP VS8 System**

## 1.4. ABBREVIATIONS AND ACRONYMS

### 1.4.1. CC ACRONYMS

| | |
|---|---|
| CC | Common Criteria |
| EAL | Evaluation Assurance Level |
| IT | Information Technology |
| PP | Protection Profile |
| SF | Security Function |
| SFP | Security Function Policy |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Functions |
| TSFI | TSF Interface |
| TSP | TOE Security Policy |

### 1.4.2. TOE-SPECIFIC ACRONYM

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CEC | Key Generation Centre (Centre d'Élaboration des Clés) |
| CG | Management Centre (Centre de Gestion) |
| CH | Cipher Interface (Port Chiffre) |
| CL | Plain Interface (Port Clair) |
| CLI | Command Line Interface |
| COTS | Component Off The Shelves |
| FPD | Firmware Packaging Device |
| GC | Console Interface (Port Console) |
| GE | Management Interface (Port de Gestion) |
| IGL | Local Management Interface (Interface de Gestion Locale) |
| SGC | Station de Gestion Centrale |
| SNMP | Simple Network Management protocol |
| SSH | Secure Shell |

## 1.5. REFERENCES

| Reference | Title and version |
|---|---|
| [802.3-2000] | Local and metropolitan area networks, 2000 Edition (inclus Ethernet 10Mbps, 100Mbps, Full Duplex et autonégociation) |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>- Part 1: Introduction and general model, dated September 2012, version 3.1 R4<br>- Part 2: Security functional components, dated September 2012, version 3.1 R4<br>- Part 3: Security assurance components, dated September 2012, version 3.1 R4 |
| [CEM] | Common Evaluation Methodology for Information Technology Security – Evaluation Methodology, dated September 2012, version 3.1 R4 |
| [FIPS PUB 197] | Advanced Encryption Standard (AES) |
| [QS] | Référentiel général de sécurité<br>Processus de qualification d'un produit de sécurité - niveau standard<br>Version 1.2<br>ANSSI |
| [RFC 1042] | A Standard for the Transmission of IP Datagrams over IEEE 802 Networks |
| [RFC 1213] | Management Information Base for Network Management of TCP/IP-based internets : MIB II |
| [RFC 2408] | Internet Security Association and Key Management Protocol (ISAKMP) |
| [RFC 2409] | The Internet Key Exchange (IKE) |
| [RFC 5996] | Internet Key Exchange Protocol Version 2 (IKEv2) |
| [RFC 3566] | The AES-XCBC-MAC-96 Algorithm and Its Use With IPSec |
| [RFC 3602] | The AES-CBC Cipher Algorithm and Its Use with IPSec |
| [RFC 894] | A Standard for the Transmission of IP Datagrams over Ethernet Networks |
| [RGS_B] | Référentiel Général de Sécurité version 2.0 du 13 juin 2014 – Annexes B1 et B2 :<br>- Annexe B1 : Mécanismes cryptographiques - Version 2.03 du 21 février 2014<br>- Annexe B2 : Gestion des clés cryptographiques - Version 2.0 du 8 juin 2012 |
| [LINUX_DGA] | Recommandations pour la sécurisation des distributions GNU/Linux Redhat et Mandrake<br>Référence 2005/102317/CELAR/SSI/SSY/EA/51703616/NC<br>Version 2 |
| [LINUX_ANSSI] | Recommandations de sécurité relatives à un systèmeGNU/Linux<br>Référence DAT-NT-002/ANSSI/SDE/NP<br>Version1.1 |
| [ND_PP] | Protection Profile for Network Devices<br>version 1.1 |

## 1.6. TOE DESCRIPTION

### 1.6.1. TOE BOUNDARY

The TOE is the Mistral IP software (including its FPGA firmware) running on the Mistral device, in both configurations ("classic" and "front-end"). It is composed of a Linux OS, the Mistral IP application and the FPGA firmware (implementing cryptographic functions). The implementation of the TOE relies on COTS and open-source software (SNMP, ICMP, ARP). The list is provided below.

The Linux OS is hardened and complies with DGA/MI guidance to secure Linux OS [LINUX_DGA] and [LINUX_ANSSI].

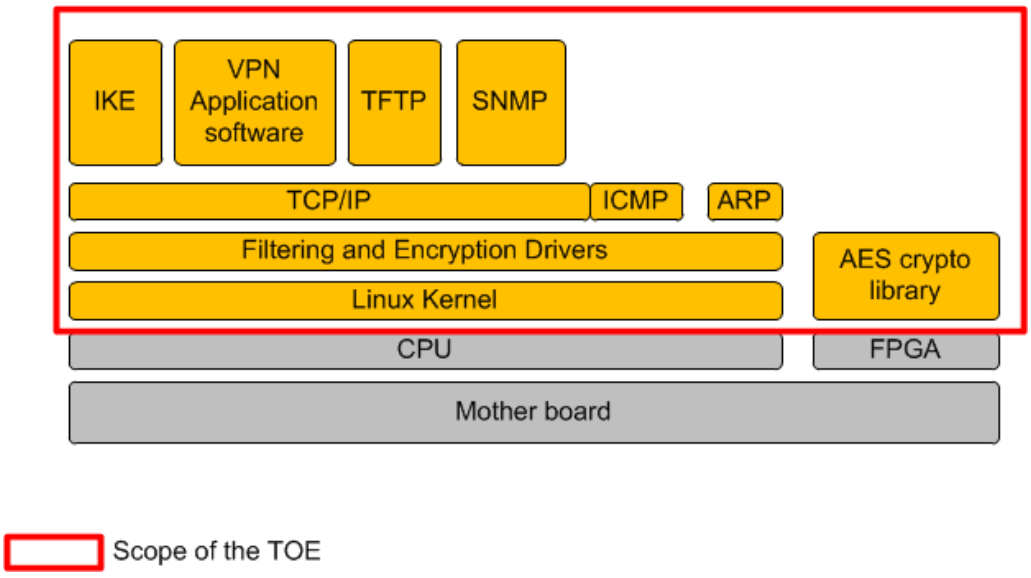


**Figure 2: Mistral IP block architecture**

COTS and open-source softwares used by the TOE are:

– Kernel Linux version 2.6.38

– UBoot version 1.3.4

– DBus version 1.2.20

– DBus-glib version 0.84

– NetSNMP version 5.5.1

– Ntpclient version 2013_194

– Strongswan version 5.1.0

– Busybox version 1.20.1

All other devices of the Mistral IP system are considered as part of the operational environment. Thus, those equipments are out of scope of the Target of Evaluation described in this Security Target. In particular, the Mistral Management Center Device (SGC), the Key Generation Center (CEC), the Firmware Packaging Device (FPD) and the NTP Server are outside the TOE.

### 1.6.2. MISTRAL IP PHYSICAL INTERFACES

The Mistral IP device has the following external interfaces:

– RJ45 interfaces for TCP/IP over Ethernet protocol:
  - 1 "Encrypted data" interface, connected to the untrusted network: CH
  - 1 "Plaintext data" interface, connected to the trusted network (the LAN): CL
  - The other Ethernet interfaces are not used
– RJ45 interface for RS232 protocol:
  - 1 Console interface (GC) providing an access to the IGL (via the CLI)
– And:
  - 1 secure erasure push-button
  - 1 USB interface (not used)
  - 1 Smartcard reader interface (for key and configuration files injection only)
  - 2 LEDS : the first indicating the device is powered on, the second indicating its status
  - 1 remote secure erasure interface. An erasure requested though this interface has the same effect as the push-button. It simply offers the possibility to remotely activate the erasure
  - 1 On / Off switch
  - 1 power input interface

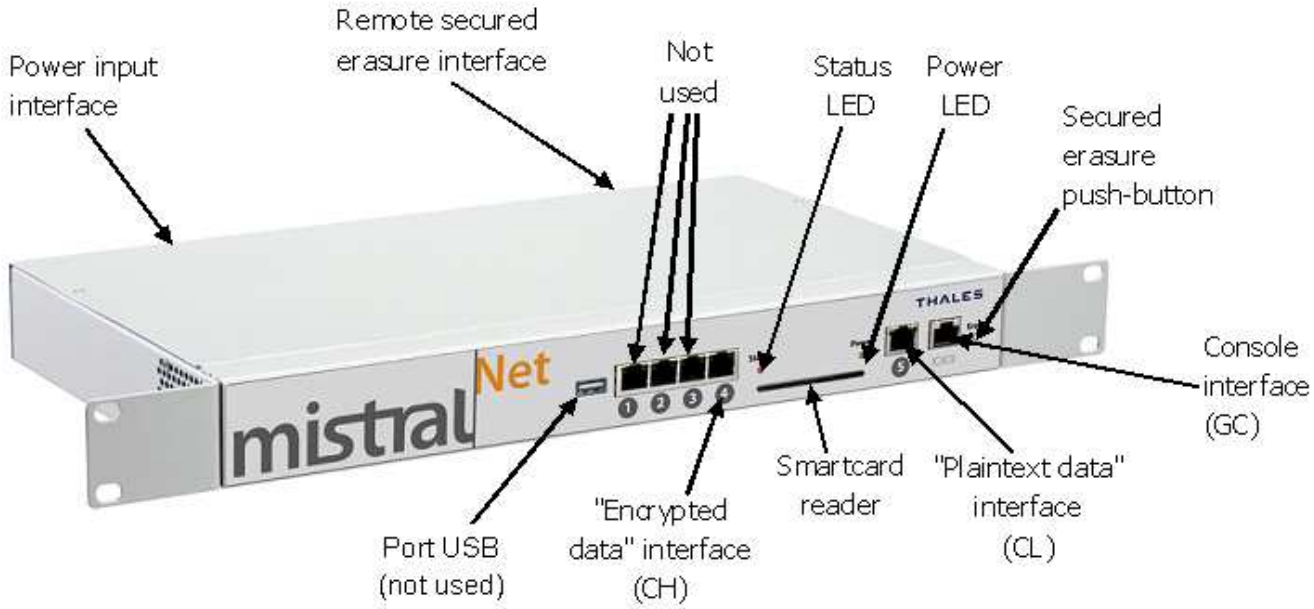


**Figure 3:Mistral IP device**

The IP encryption device owns one IP address and one MAC (Ethernet) address shared by network interfaces CH and CL.

The device accepts to be managed through:
– Its CL network interface (in “front-end” mode)

– Its CH network interface (in “classic” mode)
– Its GC console interface

### 1.6.3. MISTRAL IP LIFECYCLE

The Mistral IP lifecycle is illustrated below:

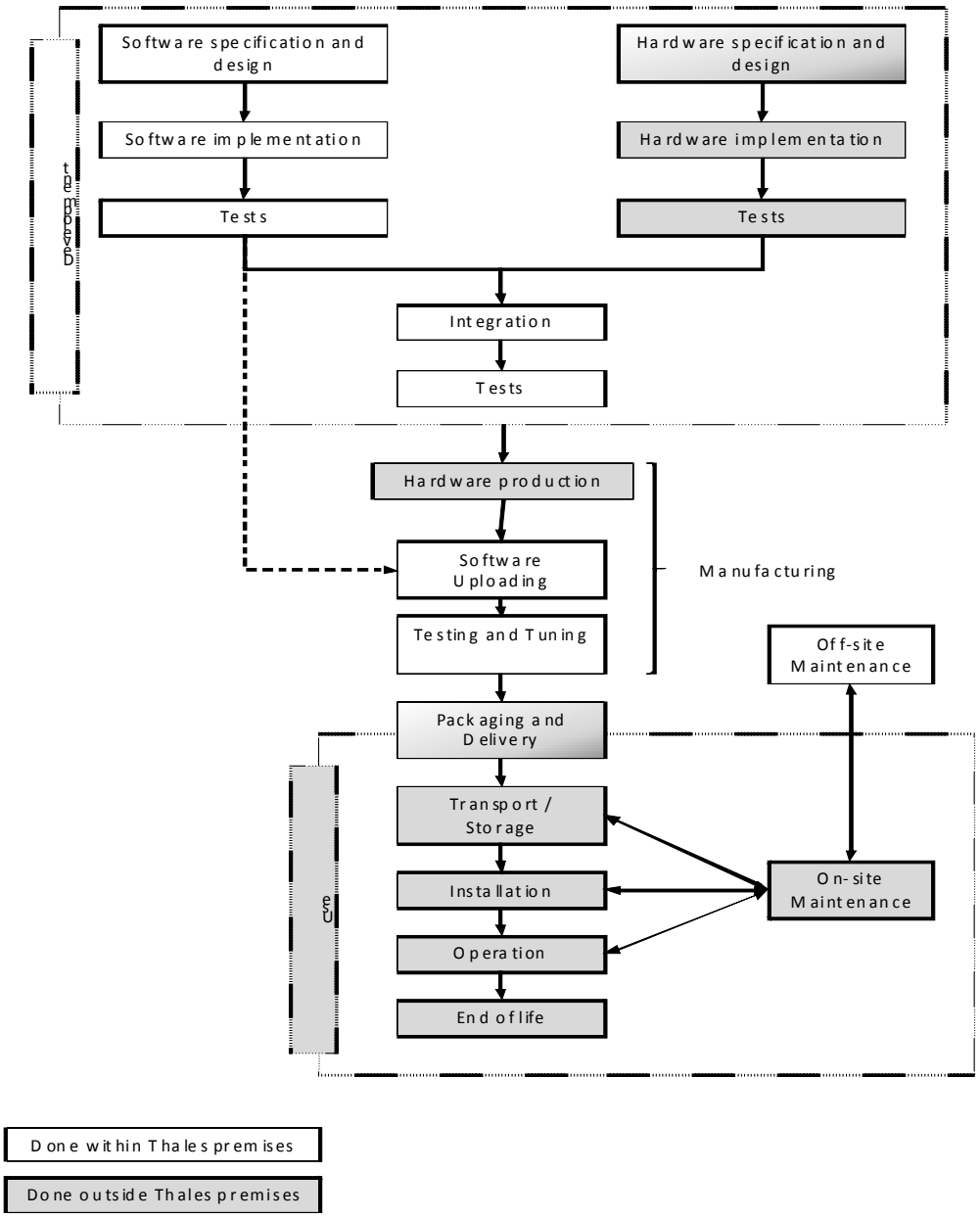


**Figure 4: Mistral IP Lifecycle**

Mistral IP is manufactured in two steps:

– The hardware is produced outside Thales premises,

– The software injection and the final configuration are performed inside Thales premises.

Note: Mistral software implementation binaries, generated by the development team are packaged into a “firmware” before to be uploaded inside the Mistral Hardware; this operation is realized inside Thales premises by the Firrmware Packaging Device (FPD). This resource allows dedicated development team members to protect and digitally sign the software implementation.

### 1.6.4. MISTRAL IP FUNCTIONAL STATE DIAGRAM

Mistral IP can hold different functional states. Those states are:

– "Booting": it is the functional state Mistral IP holds just after it has been switched on. It does hardware tests (not including FPGA self-tests) and launches softwares

– "Self-test": in this state, Mistral IP runs selftests : it checks software and data integrity, it checks FPGA security functions

– "Updating": Mistral IP is in this state when a software update is performed

– "Failure": Mistral IP enters this state when a failure occurs and is detected

– "Running": this state is the general state in which Mistral IP provides all its network services

### 1.6.5. OPERATIONAL CRYPTOGRAPHIC KEYS

The TOE keeps within its internal memory operational cryptographic keys used by Security Associations (SA) in order to protect network dataflow.

The TOE implements two kinds of key management scheme in the SAs:

– **Distributed mode**, in which keys are directly used by the TOE to protect network dataflow. Those keys are pre-shared by the TOE and a remote TOE. They are call “distributed mode PSK” and are symmetric keys.

In distributed mode, when an IPSec is opened, the SA’s distributed mode PSK is derivate into 2 keys, one used to cipher and decipher network datagrams, the other used to calculate and check integrity patterns of network datagrams.

The "distributed mode PSK" are generated by the Key Generation Center (CEC)

– **Negotiated mode**, in which keys are used by the TOE to authenticate itself and the remote TOE during a key exchange protocol. Those keys are called “IKE peer authentication keys” .

  These IKE peer authentication Pre-shared keys are symmetric keys shared by the TOE and a remote TOE. They are generated by the Key Generation Center (CEC).

In negotiated mode, 2 keys are exchanged, one used to cipher and decipher network datagrams, the other used to calculate and check integrity patterns of network datagrams.

The used key exchange protocol is IKE version 2.

### 1.6.6. KEY INJECTION

Operational cryptographic master keys are generated by the CEC; keys are stored in plaintext or secure file format.

Secure file format offer confidentiality and integrity protection by an AES-128 bits algorithms (confidentiality protection: AES-CBC-128; integrity protection: AES XCBC-MAC96). The protection keys used by these algorithms are derived from a passphrase determined at keys generation (at CEC).

The key files generated by the CEC can either be injected in MISTRAL IP through the following ways:

– Via a remote command from the Management Center: the key files are prior imported in the management center (secure or plaintext file format is allowed) ; Then the management center may either generate smartcard content (see below) or inject imported keys to the Mistral-IP devices via the management VPN (*remote management* Security Association used by the Mistral-IP devices to communicate with the Management Center). *Note : This second capability is not available for the very first configuration or after a secured-erasure, as the Mistral IP does not have the necessary configuration parameters to be connected to its Management Center.*

– Via a Smartcard generated by the Management center: key files are prior injected in the management center; then the management center is able to generate Smartcard content; thus, the operator insert the generated smartcard in reader interface of the Mistral IP device; the content of the smartcard is in plaintext.

– Via the Command Line Interface (CLI) offered by the console physical interface (GC); (only Secure File Format is allowed); the secured key file content (representing the keys) is manually copied on the CLI.

### 1.6.7. DATE AND TIME MANAGEMENT

The TOE does not hold date and time when it is turned off. It provides the time related to its last power on.

Therefore, the time is set at startup. Two methods are provided and can be used:

– A network synchronization through NTP v4 protocol

– A manual configuration of the TOE performed by the local administrator

### 1.6.8. LOCAL DATA PROTECTION

The TOE persistently stores sensitive data. Those data are securely stored by a cryptographic functionality preventing their disclosure and allowing detection of their modification.

The cryptographic functionality (which implements AES256-GCM16 for confidentiality and integrity) uses a local cryptographic key (called Local Protection Key, LPK).

### 1.6.9. TOE FUNCTIONALITIES

The TOE's main functionalities are :

– Dataflow control and filtering from all interfaces, with Security Policies configuration allowing:
  - Data flow protection (against disclosure, modification, insertion and replay).
    – IPSEC ESP Tunnel encapsulation mode, which provides datagram payload data and topology data encryption, integrity and anti-replay
  - Data flow forwarding (without protection).

– TOE configuration management (including key management and negotiation)
– Secure sensitive data storage
– Secure erasure
– Secure software update
– Auto-test (at startup and on request)
– SNMP supervision
– Audit generation

For details on those functionalities, refer to section *TOE Summary Specification*.

# 2. CONFORMANCE CLAIM

## 2.1. CC CONFORMANCE CLAIM

This security target is conformant to Common Criteria 3.1 revision 4 of September 2012 [CC]:

– CC Part 2 extended

– CC Part 3 conformant

## 2.2. PP CONFORMANCE CLAIM

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

### 2.2.1. [ND_PP] CONFORMANCE ANALYSIS

Here is the conformance analysis for the Security Problem Definition part:

| Object Name in [ND_PP] | Object Name in this ST | Rationale |
|---|---|---|
| T.ADMIN_ERROR | T.ADMIN_ERROR | The threat in this ST is drawn from the PP |
| T.TSF_FAILURE | T.TSF_FAILURE | The threat in this ST is drawn from the PP |
| T.UNDETECTED_ACTIONS | T.UNDETECTED_ACTIONS | The threat in this ST is drawn from the PP |
| T.UNAUTHORIZED_ACCESS | T.UNAUTHORISED_ACCESS | The threat in this ST is drawn from the PP |
| T.UNAUTHORIZED_UPDATE | T.UNAUTHORISED_UPDATE | The threat in this ST is drawn from the PP |
| T.USER_DATA_REUSE | T.USER_DATA_REUSE | The threat in this ST is drawn from the PP |
| P.ACCESS_BANNER | P.BANNER | The OSP in this ST is drawn from the PP |
| A.NO_GENERAL_PURPOSE | A.NO_GENERAL_PURPOSE | The assumption in this ST is drawn from the PP |
| A.PHYSICAL | A.PHYSICAL_ENVIRONMENT_TOE | The assumption in this ST is drawn from the PP |
| A.TRUSTED_ADMIN | A.TRUSTED_ADMIN | The assumption in this ST is drawn from the PP |
| A.TRUSTED_NETWORKS | A.TRUSTED_NETWORKS | The assumption in this ST is drawn from the PP |

Here is the conformance analysis for the Security Objectives part:

| Object Name in [ND_PP] | Object Name in this ST | Rationale |
|---|---|---|
| O.PROTECTED_COMMUNICATIONS | O.PROTECTED_COMMUNICATIONS | The security objective in this ST is equivalent to the one in [ND_PP], taking into account the TOE operation. |
| O.VERIFIABLE_UPDATES | O.SOFTWARE_UPDATES | The security objective in this ST is equivalent to the one in [ND_PP], taking into account the TOE operation. |
| O.SYSTEM_MONITORING | O.AUDIT | The security objective in this ST is equivalent to the one in [ND_PP], taking into account the TOE operation. |

| Object Name in [ND_PP] | Object Name in this ST | Rationale |
|---|---|---|
| O.DISPLAY_BANNER | O.DISPLAY_BANNER | The security objective in this ST is equivalent to the one in [ND_PP], taking into account the TOE operation. |
| O.TOE_ADMINISTRATION | O.I&A<br>O.MANAGEMENT | The [ND_PP] security objective is splitted into 2 security objectives within this ST in order to be more explicit and to take into account TOE operation. |
| O.RESIDUAL_INFORMATION_CLEAR | O.RESIDUAL_INFORMATION_CLEAR | The security objective in this ST is drawn from the PP. |
| O.SESSION_LOCK | O.SESSION_LOCK | The security objective in this ST is equivalent to the one in [ND_PP], taking into account the TOE operation. |
| O.TSF_SELF_TEST | O.SELF_TEST | The security objective in this ST is equivalent to the one in [ND_PP], taking into account the TOE operation. |
| OE.NO_GENERAL_PURPOSE | OE.LINUX_GUIDANCE | The security objective in this ST is an intanciation (being more restrictive) of the one in [ND_PP]. |
| OE.PHYSICAL | OE.PHYSICAL_ENVIRONMENT_TOE | The security objective in this ST is drawn from the PP. |
| OE.TRUSTED_ADMIN | OE.TRUSTED_ADMIN | The security objective in this ST is drawn from the PP. |
| OE.TRUSTED_NETWORKS | OE.TRUSTED_NETWORKS | The security objective in this ST is drawn from the PP. |

Here is the conformance analysis for the Security Functional Requirement part:

| Object Name in [ND_PP] | Object Name in this ST | Rationale |
|---|---|---|
| FAU_GEN.1.1 | FAU_GEN.1.1 | The SFR in this ST is drawn from [ND_PP] taking into account the TOE operation. At least any audit events required in [ND_PP] are generated. |
| FAU_GEN.1.2 | FAU_GEN.1.2 | The SFR in this ST is drawn from [ND_PP] taking into account the TOE operation. At least the required information in [ND_PP] are recorded. (with a refinement on subject identity) |
| FAU_GEN.2.1 | FAU_GEN.2.1 | The SFR in this ST is drawn from [ND_PP] taking into account the TOE operation. |
| FAU_STG_EXT.1.1 | FAU_STG_EXT.1.1 | The SFR in this ST is drawn from [ND_PP] taking into account the TOE operation. |
| FCS_CKM.1.1 (for asymmetric keys) | | The TOE does not generated asymmetric keys.<br>(but it generates symmetric session keys using IKE protocol) |
| FCS_CKM_EXT.4.1 | FCS_CKM_EXT.4.1/anyPlainTextData | The SFR in this ST is drawn from [ND_PP]. However it instantiates the SFR to be more precise. |
| FCS_COP.1.1(1) (data encryption / decryption) | FCS_COP.1.1/aes-cbc<br>FCS_COP.1.1/aes-gcm | The SFRs in this ST are instantiations of FCS_COP.1(1) |
| FCS_COP.1.1(2) (crypto signature) | FCS_COP.1.1/ecdsaSw | The ECDSA instantiation regarding the software signature does not need all "NIST curves" but only one, that why only one curve is specified.<br><br>The ECDSA and DSA instantiations are not claimed in this ST : the TOE does not perform IKE authentication through certificates but only through PSK. |
| FCS_COP.1.1(3) (crypto hashing) | FCS_COP.1.1/sha | The SFR in this ST instantiates the one in the PP. |
| FCS_COP.1.1(4) (keyed-hash message auth.) | FCS_COP.1.1/hmac | The requirement in this ST instantiates the one in the PP. |
| FCS_RBG_EXT.1.1 | FCS_RBG_EXT.1.1 | The requirement in this ST instantiates the one in the PP. |
| FCS_RBG_EXT.1.2 | FCS_RBG_EXT.1.2 | The requirement in this ST instantiates the one in the PP. |
| FDP_RIP.2.1 | FDP_RIP.2.1 | The requirement in this ST instantiates the one in the PP. |

| Object Name in [ND_PP] | Object Name in this ST | Rationale |
|---|---|---|
| FIA_PMG_EXT.1.1 | FIA_PMG_EXT.1.1/localMngt | The SFR as been instantiated for the human user.<br>Refinements have been performed to take into account the TOE operation : minimum password length is not settable and set to 8 characters. |
| FIA_UIA_EXT.1.1 | FIA_UIA_EXT.1.1/localMngt | The requirement is drawn from the PP.<br>A refinement has been performed as the TOE does not identify users: it recognizes 2 roles without user identification. |
| FIA_UIA_EXT.1.2 | FIA_UIA_EXT.1.2/localMngt | The requirement is drawn from the PP.<br>A refinement has been performed to precise human user roles. |
| FIA_UAU_EXT.2.1 | FIA_UAU_EXT.2.1/localMngt | The requirement is drawn from the PP.<br>A refinement has been performed to precise human user roles. |
| FIA_UAU.7.1 | FIA_UAU.7.1/localMngt | The requirement is drawn from the PP.<br>A refinement has been performed to precise human user roles. |
| FMT_MTD.1.1 | FMT_MTD.1.1/configuration<br>FMT_MTD.1.1/keys<br>FMT_MTD.1.1/dateTime | The requirement into [ND_PP] is divided into two parts in the ST.<br>The first part concerns general TSF data that can be manage from the local management (administrator role only) and from the management center.<br>The second part concerns crypto keys which can only be managed by the local management (administrator role only) |
| FMT_SMF.1.1 | FMT_SMF.1.1 | The requirement is drawn from the PP.<br>A capability has been added regarding TOE supervision (SNMP). |
| FMT_SMR.2.1 | FMT_SMR.1.1/user | The requirement is drawn from the PP.<br>An "operator" role has been added regarding the [ND_PP] in order to provide a minimal on-site configuration supervision capabilities. |
| FMT_SMR.2.2 | FMT_SMR.1.2/user | The requirement is drawn from the PP. |
| FMT_SMR.2.3 | | This requirement is not taken into this security target as per the TOE operation. Indeed, the TOE can be locally and remotely administered, however the authentication mechanism is different. Local management is performed by a human user who has to authenticate himself onto the TOE.<br>Remote management is performed by a human user who has to authenticate himself on the management center device (but not on the TOE). From the TOE point of view, it is the trusted path between the management center and the TOE (done through a TOE in "front-end" configuration) which authenticates the management center. |
| FPT_SKP_EXT.1.1 | FPT_SKP_EXT.1.1 | The requirement is drawn from the PP.<br>A refinement has been performed to be more precise. |
| FPT_APW_EXT.1.1 | FPT_APW_EXT.1.1 | The requirement is drawn from the PP. |
| FPT_APW_EXT.1.2 | FPT_APW_EXT.1.2 | The requirement is drawn from the PP. |
| FPT_STM.1.1 | FPT_STM.1.1 | The requirement is drawn from the PP. |
| FPT_TUD_EXT.1.1 | FPT_TUD_EXT.1.1/software | The requirement is drawn from the PP.<br>A refinement has been performed to be more precise about the "administrators". |
| FPT_TUD_EXT.1.2 | FPT_TUD_EXT.1.2/software | The requirement is drawn from the PP.<br>A refinement has been performed to be more precise about the "administrators". |

| Object Name in [ND_PP] | Object Name in this ST | Rationale |
|---|---|---|
| FPT_TUD_EXT.1.3 | FPT_TUD_EXT.1.3/software | The requirement is drawn from the PP. |
| FPT_TST_EXT.1.1 | FPT_TST.1.1 | The security target uses FPT_TST.1 drawn from [CC] part 2 to specify the self tests that have to be performed and start-up AND on user request.<br>FPT_TST.1.1 refines the [ND_PP] requirement in order to be slightly more precise about tested components. |
| FTA_SSL_EXT.1.1 | FTA_SSL_EXT.1.1/localMngt | The requirement is drawn from the PP.<br>A refinement has been done because the period of inactivity is not configurable. |
| FTA_SSL.3.1 | | The security target does not include this requirement because of the TOE operation. The remote management operations are performed through a trusted path between two TOEs (one in "classic" mode, one in "front-end" mode). the trusted path being a VPN, it is setted up and it never ends. |
| FTA_SSL.4.1 | FTA_SSL.4.1/localMngt | The requirement is drawn from the PP.<br>A refinement has been performed to be more precise about the "administrators". |
| FTA_TAB.1.1 | FTA_TAB.1.1/localMngt | The requirement is drawn from the PP.<br>A refinement has been performed to be more precise about the "administrators". |
| FTP_ITC.1.1 | FTP_ITC.1.1/TOE | The requirement is drawn from the PP. |
| FTP_ITC.1.2 | FTP_ITC.1.2/TOE | The requirement is drawn from the PP. |
| FTP_ITC.1.3 | FTP_ITC.1.3/TOE | The requirement is drawn from the PP. |
| FTP_TRP.1.1 | FTP_ITC.1.1/TOE | The remote management is performed through a trusted channel between two TOEs (one in "classic" mode, the second in "front-end" mode). Therefore the [ND_PP] trusted path FTP_TRP.1.1 requirement becomes a trusted channel FTP_ITC.1.1 requirement in this security target. |
| FTP_TRP.1.2 | FTP_ITC.1.2/TOE | The remote management is performed through a trusted channel between two TOEs (one in "classic" mode, the second in "front-end" mode). Therefore the [ND_PP] trusted path FTP_TRP.1.2 requirement becomes a trusted channel FTP_ITC.1.2 requirement in this security target. |
| FTP_TRP.1.3 | FIA_UID.2.1/sgc<br>FTP_ITC.1.1/TOE | The remote management is performed through a truted channel between two TOEs (one in "classic" mode, the second in "front-end" mode). Therefore the [ND_PP] trusted path FTP_TRP.1.3 requirement does not have an equivalent in FTP_ITC.1. However it is fully covered by the existence of the trusted channel (FTP_ITC.1.1) and by the mandatory identification of the management center device (FIA_UID.2/sgc). |
| FCS_IPSEC_EXT.1.1 | FCS_IPS_EXT.1.1 | The requirement is drawn from the PP.<br>IKEv1 is not selected, therefore following requirements regarding IPSec are refined for IKEv2. |
| FCS_IPSEC_EXT.1.2 | FCS_IPS_EXT.1.2 | The requirement is not applicable as IKEv1 is not selected in FCS_IPS_EXT.1.1 |
| FCS_IPSEC_EXT.1.3 | FCS_IPS_EXT.1.3 | The requirement is drawn from the PP.<br>The requirement is refined for IKEv2. |
| FCS_IPSEC_EXT.1.4 | FCS_IPS_EXT.1.4 | The requirement is drawn from the PP.<br>The requirement is refined for IKEv2. |
| FCS_IPSEC_EXT.1.5 | FCS_IPS_EXT.1.5 | The requirement is drawn from the PP.<br>The requirement is refined because DH Group 14 is not claimed. Only DH Group 20 is required. |

| Object Name in [ND_PP] | Object Name in this ST | Rationale |
|---|---|---|
| FCS_IPSEC_EXT.1.6 | FCS_IPS_EXT.1.6 | The requirement is not applicable as the TOE does not perform IKE peer authentication via certificates and private keys, but only via pre-shared keys. |
| FCS_IPSEC_EXT.1.7 | FCS_IPS_EXT.1.7 | The requirement is drawn from the PP.<br>The requirement is refined : the requirement is applicable to IKE peer authentication. |
| FCS_IPSEC_EXT.1.8 | FCS_IPS_EXT.1.8 | The requirement is not claimed because this peer authentication mechanism is considered too weak. |

## 2.3. PACKAGE CONFORMANCE CLAIM

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

# 3. SECURITY PROBLEM DEFINITION

## 3.1. ASSETS

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

A security need specified as *optional* means that the risk analysis of the system using the TOE shall determine if this security need is required or not for the purposes of the system. If it is, the user will have to configure the TOE such as it provides the appropriate security protection.

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

### 3.1.1. ASSETS PROTECTED BY THE TOE (USER DATA)

#### D.APPLICATIVE_DATA

Applicative data are data which flow through a private network to another through IP encryptors. They are contained in the IP datagrams payload routed up to the cipher units and received and sent by these cipher units. These data can be temporarily stored in IP encryptors to be able to process them (i.e., enforce security services) before sending them on the private or public network.

Applicative data corresponds both to user dataflow and to management dataflow (as the remote management service's architecture uses a remote IP encryptor).

***Security needs:*** *Confidentiality, Integrity, Authentication, No replay*

#### D.TOPOLOGIC_INFO

Information pertaining to private networks topology is contained within IP datagrams headers.

***Security needs:*** *Confidentiality, Integrity, Authentication*

### 3.1.2. ASSETS BELONGING TO THE TOE (TSF DATA)

#### D.SECURITY_POLICIES

This asset groups all Security Associations (SAs) and Security Policies (SPs) configured within the TOE.

Security Associations are caracterised at least by following parameters:

– SPI : unique identifier of the SA

– SA Type : User, Remote management

– Protection mode : IPSec_Tunnel, Enhanced_Simple

– Key management mode : distributed or negociated mode (that is use of IKE protocol)

– Cryptographic secret or private key identifier
– Peer IP address : IP address of a remote instance of the TOE
– Lifetime of IKE SAs keys

Note : Perfect Forward Secrecy (PFS) mode (for IKE protocol) : is always performed.

Security Policies are characterised at least by following parameters:

– Action : Encryption, Bypass, Reject
– Source IP address
– Destination IP address
– SA Identifier (link between SP and SA)
– Authorized protocol and port (for TCP and UDP)

***Security needs:*** *Confidentiality, Integrity*

**D.CONFIG_PARAM**

This asset groups all TOE configuration parameters that are not confidential (TOE IP address, MTU, ...).

It contains at least:

– TOE IP address
– List of authorised routing protocols (in bridge mode)
– List of authorised TOE Management Centre Devices (E.SGC) IP address and related TOE interface

***Security needs:*** *Integrity*

**D.SUPERVISION_DATA**

This asset groups all TOE supervision data that can be queried through SNMP requests.

***Security needs:*** *Integrity*

**D.CRYPTO_KEYS**

This asset groups all (symmetric or asymmetric) cryptographic keys secret values used by VPN Policies (i.e. SAs). It can either be PSK peer authentication keys when using IKE protocol (negotiated mode), or PSK communication channels protection keys when not using IKE protocol (distributed mode).

Secret or private keys are characterised at least by following parameters:

– Key identifier
– Key type : secret keys
– Key length
– Associated cryptographic algorithm
– Key lifetime
– Key value

***Security needs:*** *Confidentiality, Integrity*

**D.IKE_SAs_CRYPTO_KEYS**

This asset groups all temporary (i.e. in volatile memory only) cryptographic keys secret values created through IKE protocol. For IKEv2 protocol it is:

– SKEYSEED: IKEv2 protocol key seed (refer to [RFC 5996])

– IKEv2 SA Keys: Key materials issued from the IKEv2 first exchanges

– IKEv2 Child SAs Keys: Key materials issued from the IKEv2 second exchanges

***Security needs:*** *Confidentiality*

**D.DISTRIB_SAs_CRYPTO_KEYS**

This asset groups all temporary (i.e. in volatile memory only) cryptographic keys secret values created by derivation process of distributed PSK for distributed mode operation.

***Security needs:*** *Confidentiality*

**D.CRYPTO_KEYS_PROTECTION_PWD**

This asset is a temporary data. It is the passphrase entered in order to unprotect the cryptographic private/secret key during their injection in the TOE via the GC interface.

***Security needs:*** *Confidentiality*

**D.AUDIT**

This asset represents audit record generated by the TOE.

***Security needs:*** *Integrity, Authentication*

**D.AUTHENTICATION_DATA**

This asset groups authentication data that is:

– Local administrator's (U.LOCAL_ADMINISTRATOR) password

– Local operator's (U.LOCAL_ADMINISTRATOR) password

It also contains their lifetime. This lifetime is by default infinite.

***Security needs:*** *Confidentiality, Integrity*

**D.SOFTWARE**

This asset represents the TOE (as the TOE is software).

***Security needs:*** *Integrity, Authentication*

**D.SWUPDATE_PUBLICKEYS**

This asset is the cryptographic public key used by the TOE to authenticate its software updates.

***Security needs:*** *Integrity*

**D.TIME_BASE**

This asset represents the reliable time base kept within the TOE and used by the TOE.

***Security needs:*** *Integrity*

## 3.2. USERS AND ENTITIES

**U.LOCAL_ADMINISTRATOR**

TOE local administrator. He interacts with the TOE through the E.SGL. He can uses any commands.

**U.LOCAL_OPERATOR**

TOE local operator. He interacts with the TOE through the E.SGL. He has only access to device initialisation and to a complete view of the device configuration.

**U.CENTRAL_ADMINISTRATOR**

TOE administrator interacting with the TOE through the E.SGC.

**E.SGC**

TOE management centre device. It interacts remotely with the TOE.

It is the network device hosting E.LGC

**E.LGC**

TOE management centre software

This software is a dedicated one, developed for the TOE central administration and delivered with the TOE.

**E.SGL**

TOE local management device. It interacts with the TOE through the GC interface.

It is the network device hosting E.LGL

**E.LGL**

TOE local management software.

This software can either be a dedicated one (developed for the needs of the local administration of the TOE), or hyperterminal, or telnet...

**E.SF**

File server

This device is a TFTP server where TOE can download software updates.

**E.CEC**

Key generation centre device

**E.FPD**

Firmware Packaging Device

## 3.3. THREATS

**T.ADMIN_ERROR**

An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

***Impacted data:***

*- D.SECURITY_POLICIES*

*- D.CONFIG_PARAM*

***Impacted security need:*** *Integrity*

**T.TSF_FAILURE**

Security mechanisms of the TOE may fail, leading to a compromise of TSF Data or User Data.

***Impacted data:***

*- D.SECURITY_POLICIES*

*- D.APPLICATIVE_DATA*

*- D.TOPOLOGIC_INFO*

*- D.CRYPTO_KEYS*

*- D.IKE_SAs_CRYPTO_KEYS*

*- D.DISTRIB_SAs_CRYPTO_KEYS*

***Impacted security need:*** *Confidentiality*

**T.UNDETECTED_ACTIONS**

Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

*Application note:*

*those actions are not logged.*

***Impacted data:***

*- D.SECURITY_POLICIES*

*- D.APPLICATIVE_DATA*

*- D.CRYPTO_KEYS*

*- D.CONFIG_PARAM*

*- D.AUTHENTICATION_DATA*

*- D.IKE_SAs_CRYPTO_KEYS*

*- D.DISTRIB_SAs_CRYPTO_KEYS*

***Impacted security need:*** *Confidentiality, Integrity*

**T.UNAUTHORISED_ACCESS**

A user may gain unauthorized access to the TOE data and TOE executable code.

A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources.

A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

Those actions could lead either to :

– Modification or retrieval of TOE data (that is TSF Data and User Data persistently stored within the TOE)

– Usurpation of the operator or the administrator identity in order to perform administration operations on the TOE

– Modification, insertion or deletion of audit data records while they are transmitted by the TOE to the TOE management centre device (E.SGC).

*Application note:*

*The TOE does not provide persistent storage of audit records. Those are systematically forwarded by the TOE to the management centre device (E.SGC).*

***Impacted data:***

*- D.SECURITY_POLICIES*

*- D.APPLICATIVE_DATA*

*- D.TOPOLOGIC_INFO*

*- D.AUDIT*

*- D.CRYPTO_KEYS*

*- D.CONFIG_PARAM*

*- D.TIME_BASE*

*- D.SOFTWARE*

*- D.AUTHENTICATION_DATA*

*- D.IKE_SAs_CRYPTO_KEYS*

*- D.DISTRIB_SAs_CRYPTO_KEYS*

*- D.SWUPDATE_PUBLICKEYS*

*- D.SUPERVISION_DATA*

*- D.CRYPTO_KEYS_PROTECTION_PWD*

***Impacted security need:*** *Confidentiality, Integrity*

### T.UNAUTHORISED_UPDATE

A malicious party attempts to supply the end user with an update of the product that may compromise the security features of the TOE.

***Impacted data:***

*- D.SOFTWARE*

*- D.SWUPDATE_PUBLICKEYS*

***Impacted security need:*** *Integrity, Authentication*

### T.USER_DATA_REUSE

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

***Impacted data:***

*- D.APPLICATIVE_DATA*

*- D.TOPOLOGIC_INFO*

***Impacted security need:*** *Confidentiality, No replay*

### T.TIME_BASE

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

***Impacted data:***

*- D.TIME_BASE*

***Impacted security need:*** *Integrity*

### T.RESIDUAL_DATA

An 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…).

***Impacted data:***

*- D.SECURITY_POLICIES*

*- D.APPLICATIVE_DATA*

*- D.CRYPTO_KEYS*

*- D.AUTHENTICATION_DATA*

*- D.IKE_SAs_CRYPTO_KEYS*

*- D.DISTRIB_SAs_CRYPTO_KEYS*

*- D.CRYPTO_KEYS_PROTECTION_PWD*

***Impacted security need:*** *Confidentiality*

## 3.4. ORGANISATIONAL SECURITY POLICIES (OSP)

### 3.4.1. REGULATORY POLICIES

**P.CRYPTO_RGS**

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

### 3.4.2. SERVICES

**P.PROVIDED_SERVICES**

The TOE shall enforce VPN security policies defined by the TOE administrator (U.LOCAL_ADMINISTRATOR and U.CENTRAL_ADMINISTRATOR).

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 (in ESP Tunnel mode only),

– confidentiality protection of topologic data (in ESP Tunnel mode only) and

– integrity and authenticity protection of topologic data (in ESP Tunnel mode only) .

Furthermore, the TOE shall provide the capability to separate IP datagrams flows to make communicate subnetworks (of private networks) and enforce a security policy to every communication link between IP subnetworks.

**P.POL_VIEW**

The TOE shall enable the TOE administrators (U.LOCAL_ADMINISTRATOR and U.CENTRAL_ADMINITRATOR) and TOE operators (U.LOCAL_OPERATOR) to view all individual VPN security policies and their security contexts upon each IP encryption device.

**P.SUPERVISION**

The TOE shall enable the system and network administrator to review the operational status of the TOE.

**P.VISUAL_ALARMS**

When a critical event occurs, the TOE shall notify a user through a visual mean (e.g. LED).

### 3.4.3. MISCELLANEOUS

**P.BANNER**

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

**P.SA_SP_PROTECTION**

The TOE shall protect the integrity of the SPD (Security Policies Database) and the SAD (Security Associations Database) while persistently stored and used.

The TOE shall periodically check the integrity of the SPD and the SAD.

**P.KEYS_INJECTION**

Injected keys shall be protected in confidentiality and integrity during their transfert from the Management Center to the TOE whatever is the transportation method (external support, file, through network).

## 3.5. ASSUMPTIONS

### 3.5.1. SECURING THE TOE

**A.NO_GENERAL_PURPOSE**

It is assumed that 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.

In particular, the TOE is configured accordingly to the guidance [LINUX_DGA] and [LINUX_ANSSI].

**A.PHYSICAL_ENVIRONMENT_TOE**

It is assumed that physical security of the TOE, commensurate with the value of the TOE and the data it contains, is provided by the environment.

**A.SW_PROTECTION**

It is assumed that protection of TOE software updates is performed in a trusted environment, on a trusted device. Only authorised persons have access to this device.

It is assumed that protection of TOE software updates provides confidentiality and authentication.

**A.TRUSTED_NETWORKS**

Private Local Area Networks (LAN), i.e. plaintext networks, including the TOE Management centre network, are assumed to be trusted networks.

### 3.5.2. ADMINISTRATION

**A.TRUSTED_ADMIN**

It is assumed that the TOE administrators (U.LOCAL_ADMINISTRATOR and U.CENTRAL_ADMINISTRATOR) are trustworthy and apply the procedure described in the administration guide.

**A.CONFIGURATION_CONTROL**

It is assumed that the TOE administrators (U.LOCAL_ADMINISTRATOR and U.CENTRAL_ADMINISTRATOR) have got means to control the hardware and software configuration of the TOE (including services and assets) with respect to baseline state, or to restore it in a secure state.

*Application note:*

*This assumption especially concerns the software assets.*

**A.ALARM**

It is assumed that the TOE Management Centre (E.SGC) analyses and processes critical security audit data generated and forwarded by the TOE, immediately after reception.

It is assumed that the TOE local administrator (U.LOCAL_ADMINISTRATOR) or the TOE local operator (U.LOCAL_OPERATOR) analyses and processes alarms immediately after their generation.

**A.POLICIES_CONTINUITY**

When a plaintext communication channel is configured, the system shall make sure that the information security policies of the two networks interconnected through the TOE are consistent between each other.

### 3.5.3. ASSUMPTIONS ABOUT MANAGEMENT DEVICES

**A.SECURED_MANAGEMENT_DEVICES**

It is assumed that following devices are properly and securely configured, according the sensitivity of assets they handle:

– The TOE management centre device (E.SGC)

– The TOE local management device (E.SGL)

– The key generation center (E.CEC)

– The firmware packaging device (E.FPD)

It is assumed that their operating system is configured accordingly to the appropriate governmental guidance and that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on those devices, other than services necessary for the operation and support of their functionalities.

In case sensitive data are governmental data at Restricted level of classification (DR, NR, EUR), it is assumed that devices are configured in regards to appropriate rules and regulations.

**A.ACCESS_CONTROL_MANAGEMENT_DEVICES**

It is assumed that the access to following devices is controlled:

– The TOE management centre device (E.SGC)

– The file server (E.SF)

– The TOE local management device (E.SGL)

– The key generation center (E.CEC)

– The firmware packaging device (E.FPD)

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).

**A.PHYSICAL_ENVIRONMENT_MANAGEMENT_DEVICES**

It is assumed that physical security of following devices, commensurate with the value of the data concerning the TOE they contain, is provided by the environment:

– The TOE management centre device (E.SGC)

– The file server (E.SF)

– The TOE local management device (E.SGL)

– The key generation center (E.CEC)

– The firmware packaging device (E.FPD)

– Any other devices connected to one of the devices listed above

In case sensitive data handled by those devices are governmental data at Restricted level of classification (DR, NR, EUR), it is assumed that the physical environment meets appropriate rules and regulations.

**A.AUDIT**

It is assumed that the TOE management centre software (E.LGC) persistently stores any audit data received from the TOE.

It is assumed that the auditor regularly review 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.

**A.SGC_TO_FRONT-END**

It is assumed that the TOE management centre device (E.SGC) is directly connected to the front-end Mistral. The integrity of the link between the two equipments shall be easily checkable by a human.

### 3.5.4. ASSUMPTIONS ABOUT THE CEC

**A.STAND_ALONE_CEC**

It is assumed that the key generation center (E.CEC) is offline and dedicated.

**A.KEY_TRANSPORTATION**

It is assumed that physical devices used to transport cryptographic keys generated by E.CEC are manipulated and traced as sensitive items.

**A.CEC_CRYPTO_REGULATION**

The key generation center (E.CEC) meets ANSSI guidance [RGS_B] when implementing cryptographic mechanisms, generating keys and managing keys.

# 4. SECURITY OBJECTIVES

## 4.1. SECURITY OBJECTIVES FOR THE TOE

### 4.1.1. COMMUNICATION PROTECTION

**O.PROTECTED_COMMUNICATIONS**

The TOE shall provide protected communication channels between itself and a remote instance of the TOE.

This protection shall prevent disclosure, modification, insertion and replay of IP datagrams (payload and/or datagram header).

*Application note:*

*Protected channels between the TOE and a remote instance of the TOE are used to transmit:*

*- User data:*

*- D.APPLICATIVE_DATA*

*- D.TOPOLOGIC_INFO (in ESP Tunnel mode only)*

*- TSF data (for remote management purpose):*

*- D.SECURITY_POLICIES*

*- D.CONFIG_PARAM*

*- D.CRYPTO_KEYS*

*- D.AUDIT*

*- D.SOFTWARE*

*- D.SWUPDATE_PUBLICKEYS*

**O.POL_ENFORCEMENT**

The TOE shall enforce information flow control policies coming in and out its external interfaces, in particular VPN security policies specified through D.SECURITY_POLICIES.

The TOE shall authorise the administrator (R.ADMINISTRATOR) and the TOE management center (R.SGC) only to modify the filtering configuration of the flow control policies.

**O.FLOW_PARTITIONING**

The TOE shall provide the capability to partition IP networks that are interconnected together thanks to TOEs, by permiting creation of a new extended IP network, stacked up to the IP network make up of IP subnetworks.

The TOE shall also provide the capability to enforce a security policy upon every communication link between IP subnetworks.

### 4.1.2. AUDIT

**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 the administrator (R.ADMINISTRATOR), by the operator (R.OPERATOR) or by the TOE management center device (R.SGC)

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.

– If it is an alarm or not.

The TOE shall send stored audit data to the GC interface, at the request of the local administrator (R.ADMINISTRATOR).

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

*Application note:*

*Refer to FAU_GEN.1 for the list of audited security events.*

**O.TIME_BASE**

The TOE provides a time base upon which the audit records are based and ensures its reliability.

**O.AUDIT_PROTECTION**

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

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

**O.SUPERVISION**

The TOE shall authorise the local administrator (R.ADMINISTRATOR) and the TOE management center device (E.SGC) to supervise its operational status.

**O.SUPERVISION_IMPACT**

The TOE shall ensure that the supervision service does not put in danger its sensitive assets.

**O.VISUAL_ALARMS**

When an alarm-type event has occurred, the TOE shall notify local users through a visual or sounding mean (e.g. LED).

### 4.1.3. TOE MANAGEMENT

**O.ROLES**

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

– Administrator (R.ADMINISTRATOR), which is the role corresponding to U.LOCAL_ADMINISTRATOR

– Operator (R.OPERATOR), which is the role corresponding to U.LOCAL_OPERATOR

– TOE management center device (R.SGC), which is the role corresponding to E.SGC

*Application note:*

*The TOE does not know the "central administrator" (U.CENTRAL_ADMINISTRATOR) but it knows the TOE management center device (E.SGC) with which the central administrator interacts.*

**O.I&A**

The TOE shall require the identification of the TOE management center device (R.SGC) before granting it with the TOE management center device access rights.

The TOE shall require the authentication of the user before granting him with the administrator (R.ADMINISTRATOR) access rights.

The TOE shall require the authentication of the user before granting him with the operator (R.OPERATOR) access rights.

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

**O.AUTHENTICATION_FAILURE**

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

**O.DISPLAY_BANNER**

After a successful local management device (R.SGL) identification, the TOE shall send to the network device (E.SGL) from which the user is connected to the TOE an advisory warning regarding use of the TOE.

**O.SESSION_LOCK**

The TOE shall lock any local user (R.ADMINISTRATOR and R.OPERATOR) session after a defined period of inactivity of 3 minutes.

The TOE shall provide the local user (R.ADMINISTRATOR and R.OPERATOR) a mean to terminate his session.

**O.MANAGEMENT**

The TOE shall authorise modification of following data to the administrator (R.ADMINISTRATOR) and to TOE management center device (R.SGC) only:

– D.TIME_BASE

– D.CRYPTO_KEYS

The TOE shall authorise modification of following data to the TOE management center device (R.SGC) only:

– D.SECURITY_POLICIES

– D.CONFIG_PARAM

The TOE shall authorise software (D.SOFTWARES) update to the administrator (R.ADMINISTRATOR) only.

**O.VIEW**

The TOE shall authorise viewing of following data to the administrator (R.ADMINISTRATOR), the operator (R.OPERATOR) and to the TOE management center device (R.SGC) only:

– D.SECURITY_POLICIES

– D.CONFIG_PARAM

– D.TIME_BASE

The TOE shall authorise viewing of following data to no one:

– D.CRYPTO_KEYS

– D.IKE_SAs_CRYPTO_KEYS

– D.DISTRIB_SAs_CRYPTO_KEYS

– D.AUTHENTICATION_DATA

**O.POL_VIEW**

The TOE shall enable to individually view VPN security policies (i.e. security associations) and their security contexts (IKE security associations) upon each IP encryptor.

### 4.1.4. DATA PROTECTION

**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.

**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 in case of emergency.

**O.LOCAL_DATA_PROTECTION**

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

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

*Application note:*

*As a reminder, impacted TSF and User Data by this security objective are:*

*- D.SECURITY_POLICIES*

*- D.CONFIG_PARAM*

*- D.CRYPTO_KEYS*

*- D.AUTHENTICATION_DATA*

*- D.SWUPDATE_PUBLICKEYS*

### 4.1.5. SOFTWARE UPDATE

**O.SOFTWARE_UPDATES**

When a software update is requested, the TOE shall:

– control the integrity and authenticity (done through a digital signature) of the software

– decipher the software

before accepting and installing it.

### 4.1.6. CRYPTOGRAPHY

**O.KEYS_INJECTION**

When a secret key is injected via the Command Line Interface, the TOE shall:

– control the integrity and authenticity of the key

– decipher the key

before accepting and persistently storing it.

**O.CRYPTOPERIOD**

The TOE shall manage a cryptoperiod for any cryptographic key (D.CRYPTO_KEYS) used to protect communication channels (refer to O.PROTECTED_COMMUNICATIONS). For secret keys (i.e. keys for symmetric cryptographic algorithm), this cryptoperiod is part of each key's security attributes.

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

For IKEv2 protocols peer authentication keys, at the end of a key lifetime, the TOE shall either (depending on the key's security attribute):

– close any communication channels and periodically generate a critical severity audit data requiring the peer authentication key to be renewed (in this case no more new communication channels for SAs using this key can be initiated until the key is renewed)

– or periodically generate a critical severity audit data while it continues to proceed the network trafic (in this case new communication channels for SAs using this key can be initiated even if the key is out-of-date)

The period of the generation of audit data is by default 30 minutes.

The TOE shall authorise the administrator (R.ADMINISTRATOR) and the TOE management center device (R.SGC) only to modify this cryptoperiod.

**O.CRYPTO_REGULATION**

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

### 4.1.7. SELF-TEST

**O.SELF_TEST**

The TOE shall run a suite of tests at startup concerning the following security functionalities and data to ensure it is operating properly:

– Cryptographic primitives correct operation

– Cryptographic operations (refer to FCS_COP requirements) correct operation

– TOE software integrity (D.SOFTWARES)

– Persistently stored TSF Data integrity that is:

- D.SECURITY_POLICIES
- D.CONFIG_PARAM
- D.CRYPTO_KEYS
- D.AUTHENTICATION_DATA

The TOE shall also provide the capability to the administrator (R.ADMINISTRATOR) 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 can go in “Running” functional state. Otherwise, at the first self-test failure (that is a result is NOK), the TOE shall go in “Failure” functional state.

## 4.2. SECURITY OBJECTIVES FOR THE TOE ENVIRONMENT

### 4.2.1. THE ADMINISTRATOR

**OE.TRUSTED_ADMIN**

The TOE administrators (U.LOCAL_ADMINISTRATOR, U.CENTRAL_ADMINISTRTOR) shall be trusted to follow and apply all administrator guidance in a trusted manner.

**OE.ALARM**

The TOE central administrator (U.CENTRAL_ADMINISTRATOR) shall analyse and process critical security audit data generated and forwarded by the TOE, immediately after reception.

**OE.POLICIES_CONTINUITY**

When a plaintext communication channel is configured, the system shall make sure that the information security policies of the two networks interconnected through the TOE are consistent between each other.

### 4.2.2. THE AUDITOR

**OE.AUDIT_ANALYSIS**

The TOE central administrator (U.CENTRAL_ADMINISTRATOR) shall regulary analyse audit events generated by the TOE and react accordingly.

**OE.AUDIT_MNGT**

The memory units storing audit events shall be managed so that the TOE central administrator (U.CENTRAL_ADMINISTRATOR) does not lose events.

### 4.2.3. THE TOE

**OE.PHYSICAL_ENVIRONMENT_TOE**

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

**OE.LINUX_GUIDANCE**

The operating system used by the TOE shall be configured accordingly to the appropriate governmental guidance [LINUX_DGA] and [LINUX_ANSSI]. In particular, this guidance requires not to install services other than those necessary for the TOE's operation, administration and maintenance.

**OE.TOE_INTEGRITY**

The TOE environment shall provide the capability to check the integrity of the TOE hardware and software configuration.

**OE.TOE_TRANSPORTATION**

The TOE shall be securely erased (using the mechanism describe within O.DATA_ERASURE) before being brought from a site to another.

**OE.TRUSTED_NETWORKS**

Private Local Area Networks (LAN), i.e. plaintext networks, including the TOE Management centre network, shall be trusted networks.

### 4.2.4. THE CG

**OE.SECURED_SGC**

The TOE management centre device (E.SGC) shall be securely configured and used, in particular, its operating system shall be configured accordingly to the appropriate governmental guidance and no general-purpose computing capabilities (e.g., compilers or user applications) shall be available on this network device, nor any services other than those necessary for the operation and support of the TOE management center software (E.LGC).

In case the device handles governmental data at Restricted level of classification (DR, NR, EUR), it shall be configured in regards to appropriate rules and regulations.

**OE.ACCESS_CONTROL_SGC**

The access to the TOE management center software (E.LGC) is controlled. The overall solution shall allow individual accounting. It can be physical (e.g. physical access restriction to the device E.SGC hosting the software E.LGC) and/or logical (e.g. user authentication by the operating system or by E.LGC itself).

**OE.ACCESS_CONTROL_SF**

The access to the file server (E.SF) is controlled. The overall solution shall allow individual accounting. It can be physical (e.g. physical access restriction to the device hosting the server E.SF) and/or logical (e.g. user authentication by the operating system).

**OE.PHYSICAL_ENVIRONMENT_SGC**

The environment provides physical security to the TOE management centre device (E.SGC), 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 E.SGC and communicating with it, commensurate with the value of the data concerning the TOE they contain.

In case sensitive data handled by those devices are governmental data at Restricted level of classification (DR, NR, EUR), their physical environment shall meet appropriate rules and regulations.

**OE.PHYSICAL_ENVIRONMENT_SF**

The environment provides physical security to the file server (E.SF), commensurate with the value of the data concerning the TOE it contains.

In case sensitive data handled by those devices are governmental data at Restricted level of classification (DR, NR, EUR), their physical environment shall meet appropriate rules and regulations.

**OE.SGC_TO_FRONT-END**

The TOE management centre device (E.SGC) shall be directly connected to the front-end Mistral. The integrity of the link between the two equipments shall be easily checkable by a human.

**OE.AUDIT_RECORD_SGC**

The TOE management center software (E.LGC) shall persistently store any audit data received from the TOE.

**OE.DISPLAY_BANNER_SGC**

Before user identification and authentication, the TOE management center device (E.SGC) shall display an advisory warning describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE and its management center.

### 4.2.5. THE NTP SERVER

**OE.SECURED_NTP_SERVER**

The network device hosting the NTP server shall be securely configured and used, in particular, its operating system shall be configured accordingly to the appropriate governmental guidance and no general-purpose computing capabilities (e.g., compilers or user applications) shall be available on this network device, nor any services other than those necessary for the operation and support of the NTP service.

**OE.ACCESS_CONTROL_NTP_SERVER**

The access to the NTP server is controlled. The overall solution shall allow individual accounting. It can be physical (e.g. physical access restriction to the device hosting the NTP server) and/or logical (e.g. user authentication by the operating system).

**OE.NTP_SERVER_LOCATION**

The device hosting the NTP server shall be located within the Mistral Management Center (CGM) when Mistral IP is operated in connected mode. In autonomous mode, NTP server is located in the trusted network (private LAN).

**OE.PHYSICAL_ENVIRONMENT_NTP_SERVER**

The environment provides physical security to the NTP server.

### 4.2.6. THE FPD

**OE.SECURED_FPD**

The firmware packaging device (E.FPD) shall be securely configured and used, in particular, its operating system shall be configured accordingly to the appropriate governmental guidance and no general-purpose computing capabilities (e.g., compilers or user applications) shall be available on this device, nor any services other than those necessary for the operation and support of the E.FPD.

In case the device handles governmental data at Restricted level of classification (DR, NR, EUR), it shall be configured in regards to appropriate rules and regulations.

**OE.ACCESS_CONTROL_FPD**

The access to the firmware packaging device (E.FPD) is controlled. 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).

**OE.PHYSICAL_ENVIRONMENT_FPD**

The environment provides physical security to the firmware packaging device (E.FPD) commensurate with the value of the data concerning the TOE it contains.

In case sensitive data handled by this device are governmental data at Restricted level of classification (DR, NR, EUR), its physical environment shall meet appropriate rules and regulations.

### 4.2.7. THE SGL

**OE.SECURED_SGL**

The TOE local management device (E.SGL) shall be securely configured and used, in particular, its operating system shall be configured accordingly to the appropriate governmental guidance and no general-purpose computing capabilities (e.g., compilers or user applications) shall be available on this network device, nor any services other than those necessary for the operation and support of the E.LGL.

In case the device handles governmental data at Restricted level of classification (DR, NR, EUR), it shall be configured in regards to appropriate rules and regulations.

**OE.ACCESS_CONTROL_SGL**

The access to the TOE local management device (E.SGL) is controlled. The overall solution shall allow individual accounting. It can be physical (e.g. physical access restriction to the device E.SGL) and/or logical (e.g. user authentication by the operating system or by E.LGL itself).

**OE.SGL_CONNECTION**

The network link between the TOE and the TOE local management device (E.SGL) shall be a trustworthy link.

**OE.PHYSICAL_ENVIRONMENT_SGL**

The environment provides physical security to the TOE local management device (E.SGL), commensurate with the value of the data concerning the TOE it contains.

In case sensitive data handled by this device are governmental data at Restricted level of classification (DR, NR, EUR), its physical environment shall meet appropriate rules and regulations.

### 4.2.8. THE CEC

**OE.SECURED_CEC**

The key generation center (E.CEC) shall be securely configured and used, in particular, its operating system shall be configured accordingly to the appropriate governmental guidance and no general-purpose computing capabilities (e.g., compilers or user applications) shall be available on this device, nor any services other than those necessary for the operation and support of the E.CEC.

In case the device handles governmental data at Restricted level of classification (DR, NR, EUR), it shall be configured in regards to appropriate rules and regulations.

**OE.STAND_ALONE_CEC**

The key generation center (E.CEC) shall be offline and dedicated.

**OE.ACCESS_CONTROL_CEC**

The access to the key generation center (E.CEC) is controlled. 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).

**OE.PHYSICAL_ENVIRONMENT_CEC**

The environment provides physical security to the key generation center (E.CEC), commensurate with the value of the data concerning the TOE it contains.

In case sensitive data handled by this device are governmental data at Restricted level of classification (DR, NR, EUR), its physical environment shall meet appropriate rules and regulations.

**OE.KEY_TRANSPORTATION**

Physical devices used to transport cryptographic keys generated by E.CEC shall be manipulated and traced as sensitive items. The environment provides security of key transportation, commensurate with their confidentiality and integrity level.

**OE.CEC_CRYPTO_REGULATION**

The key generation center (E.CEC) meet ANSSI guidance [RGS_B] when implementing cryptographic mechanisms, generating keys and managing keys.

### 4.2.9. SOFTWARE UPDATES

**OE.SW_PROTECTION**

TOE software updates shall be ciphered, authenticated and digitally signed.

The protection shall be performed within a trusted environment, on a trusted device.

Only authorised persons shall have access to this device.

**OE.SW_UPDATE_KEY**

Cryptographic keys used to protect TOE software updates shall be distinct by 'circle of trust'.

## 4.3. RATIONALE FOR THE SECURITY OBJECTIVES

### 4.3.1. THREATS

**T.ADMIN_ERROR**

This threat is countered by **OE.TRUSTED_ADMIN** which ensures that administrators (U.LOCAL_ADMINISTRATOR and U.CENTRAL_ADMINISTRATOR) apply all guidance in a trusted manner.

**O.AUDIT** contributes to the threat coverage by providing audit data generation for all operations (including viewing operations on TOE sensitive assets) performed by the administrators.

**T.TSF_FAILURE**

This threat is countered by **O.SELF_TEST** and **OE.TOE_INTEGRITY**, because they ensure that the integrity of the software which enforces VPN security policies can be checked.

**T.UNDETECTED_ACTIONS**

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.

**OE_TRUSTED_NETWORKS** contributes to the threat coverage by minimizing the attack surface to the black network.

**T.UNAUTHORISED_ACCESS**

Regarding the threat concerning modification, it is countered:

- for D.SECURITY_POLICIES and D.CONFIG_PARAM:

  - at configuration, by **O.MANAGEMENT** which requires that D.SECURITY_POLICIES and D.CONFIG_PARAM can be modified by authorised entities only, that is E.SGC.

  - when persistently stored, by **O.LOCAL_DATA_PROTECTION** which requires that D.SECURITY_POLICIES and D.CONFIG_PARAM is protected against disclosure when it is persistently stored.

- for D.CRYPTO_KEY:

  - at injection, by **O.MANAGEMENT** which requires that D.CRYPTO_KEY can be modified by authorised entities only, that is E.SGC.

  - when persistently stored, by **O.LOCAL_DATA_PROTECTION** which requires that unauthorised modification of D.CRYPTO_KEY to be detected.

- for D.AUDIT:

  - 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.SGL_CONNECTION** (for communications to E.SGL) and **O.PROTECTED_COMMUNICATIONS** (for communications to E.SGC).

Regarding the threat concerning disclosure, it is countered:

- for D.SECURITY_POLICIES, by **O.VIEW** which requires that VPN security policies and their contexts can be viewed by authorised entities only, that is the administrator and E.SGC. **O.POL_VIEW** contributes to this security objective by requiring the TOE to be able to display individually VPN security policies and their security contexts upon each IP encryptor.

- for D.CONFIG_PARAM and D.AUTHENTICATION_DATA, by:

- **O.LOCAL_DATA_PROTECTION** which requires that unauthorised modification of D.CONFIG_PARAM and D.AUTHENTICATION_DATA to be detected.

- and **O.VIEW** which requires that D.CONFIG_PARAM can be viewed by authorised entities only, that is the administrator, the E.SGL and E.SGC.

- for D.CRYPTO_KEY when persistently stored, by **O.LOCAL_DATA_PROTECTION** which requires that D.CRYPTO_KEY is protected against disclosure when it is persistently stored.

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

- **O.I&A** which requires the administrator to be authenticated before performing any management functions. Protection of TOE local management communication is ensured through **OE.SGL_CONNECTION**. **O.AUTHENTICATION_FAILURE** prevents brute force attacks on the authentication mechanism and **O.SESSION_LOCK** prevents theft of an administrator session.

- **O.I&A** and **O.PROTECTED_COMMUNICATIONS** which require the E.SGC to be identified before performing any management functions and the communication between E.SGC 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 three roles to implement the Identification & Authentication security objective (**O.I&A**) : the administrator, the TOE local management device, the TOE management center device.

Note: there is no authentication of the E.SGC. The E.SGC is part of the management center network which is authenticated to the TOE through a protected communication channel (i.e. a VPN as for user traffic).

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.

- **OE.CEC_CRYPTO_REGULATION** requires the CEC to meet ANSSI cryptographic guidance.

- **O.POL_ENFORCEMENT** requires filtering of data flow coming into the TOE network interfaces. It hardens attacks exploiting protocol vulnerabilities.

**T.UNAUTHORISED_UPDATE**

**O.SOFTWARE_UPDATES** counters this threat by providing a cryptographic authentication mechanism.

**OE.SW_UPDATE_KEY** contributes to the threat's coverage by requiring distinct software keys for distinct systems

**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.

It is also countered by **O.POL_ENFORCEMENT** which requires the TOE to systematically apply the VPN policies when treating user data flow.

**T.TIME_BASE**

This threat is covered by the security objective **O.TIME_BASE** which ensures the time base reliability.

**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.

### 4.3.2. ORGANISATIONAL SECURITY POLICIES (OSP)

**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.CRYPTOPERIOD** contributes to the coverage of the OSP by requiring the TOE to manage key lifetimes.

**OE.CEC_CRYPTO_REGULATION** contributes also by requiring the CEC to meet ANSSI cryptographic guidance.

**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_ENFORCEMENT** and **O.FLOW_PARTITIONING** which require that these security services are enforced and provide the capability to partition IP flows.

**O.AUDIT** and **OE.AUDIT_RECORD_SGC** cover this OSP, because they ensure that operations concerning VPN links are logged and that security critical events are generated to indicate operational failures. They so provide the capability to detect and process errors or attacks after an analysis of audit events and security alarms.

This OSP is covered by **O.SELF_TEST** and **OE.TOE_INTEGRITY**, because they ensure that the integrity of the software which enforces VPN security policies can be checked.

**P.POL_VIEW**

This OSP is covered by **O.POL_VIEW**, because it provides the viewing of VPN security policies on an individual basis, which permits a security administrator to visually check that he defined correctly every VPN security policy.

**P.SUPERVISION**

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

**P.VISUAL_ALARMS**

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

**P.BANNER**

The OSP is covered through the implementation of :

- the sending to the E.SGL of a banner just after its connection establishment (**O.DISPLAY_BANNER**), that the E.LGL will display to the user,
- and the display of a banner by the E.SGC to the user (**OE.DISPLAY_BANNER_SGC**).

**P.SA_SP_PROTECTION**

The OSP is covered by **O.LOCAL_DATA_PROTECTION** which requires the TOE to be able to detect modification of TSF Data, in particular of SAD and SPD.

**P.KEYS_INJECTION**

The OSP is covered by the security objective **O.KEYS_INJECTION** which requires the TOE :

- to check the integrity and authenticity of a key injected via the Command Line Interface before accepting it
- to decipher a key injected via the Command Line Interface before persistently storing it.

### 4.3.3. ASSUMPTIONS

**A.NO_GENERAL_PURPOSE**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.LINUX_GUIDANCE**.

**A.PHYSICAL_ENVIRONMENT_TOE**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.PHYSICAL_ENVIRONMENT_TOE**, which uses the same words as the assumption.

**A.SW_PROTECTION**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.SW_PROTECTION**, which uses the same words as the assumption.

**A.TRUSTED_ADMIN**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.TRUSTED_ADMIN**, which uses the same words as the assumption.

**A.TRUSTED_NETWORKS**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.TRUSTED_NETWORKS**, which uses the same words as the assumption.

**A.CONFIGURATION_CONTROL**

The assumption is upheld by **OE.TOE_INTEGRITY**.

**A.ALARM**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.ALARM**, which uses the same words as the assumption.

**A.POLICIES_CONTINUITY**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.POLICIES_CONTINUITY**, which uses the same words as the assumption.

**A.SECURED_MANAGEMENT_DEVICES**

The assumption is entirely covered through the implementation of the security objectives for the environment **OE.SECURED_SGC, OE.SECURED_SGL, OE.SECURED_FPD, OE.SECURED_CEC and OE.SECURED_NTP_SERVER**.

**A.ACCESS_CONTROL_MANAGEMENT_DEVICES**

The assumption is entirely covered through the implementation of the security objectives for the environment **OE.ACCESS_CONTROL_SGC, OE.ACCESS_CONTROL_SF, OE.ACCESS_CONTROL_SGL, OE.ACCESS_CONTROL_FPD, OE.ACCESS_CONTROL_NTP_SERVER** and **OE.ACCESS_CONTROL_CEC**.

**A.PHYSICAL_ENVIRONMENT_MANAGEMENT_DEVICES**

The assumption is covered through the implementation of the security objectives for the environment **OE.PHYSICAL_ENVIRONMENT_SGC, OE.PHYSICAL_ENVIRONMENT_SF, OE.PHYSICAL_ENVIRONMENT_SGL**, **OE.PHYSICAL_ENVIRONMENT_NTP_SERVER, OE.NTP_SERVER_LOCATION, OE.PHYSICAL_ENVIRONMENT_FPD** and **OE.PHYSICAL_ENVIRONMENT_CEC**.

The security objective **OE.TOE_TRANSPORTATION** comes in order to add security in depth because TOE physical security during TOE carriage from a site to another may not be as high as when the TOE is in used and installed in a site.

**A.AUDIT**

The assumption is entirely covered through the implementation of the three security objectives for the environment **OE.AUDIT_RECORD_SGC**, **OE.AUDIT_ANALYSIS** and **OE.AUDIT_MNGT**, which use the same words as the assumption.

**A.SGC_TO_FRONT-END**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.SGC_TO_FRONT-END**, which uses the same words as the assumption.

**A.STAND_ALONE_CEC**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.STAND_ALONE_CEC**, which uses the same words as the assumption.

**A.KEY_TRANSPORTATION**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.KEYS_TRANSPORTATION**, which uses the same words as the assumption.

**A.CEC_CRYPTO_REGULATION**

The assumption is entirely covered through the implementation of the security objective for the environment **OE.CEC_CRYPTO_REGULATION**, which uses the same words as the assumption.

### 4.3.4. TABLES

| Threats | Security objectives |
|---|---|
| T.ADMIN_ERROR | O.AUDIT<br>OE.TRUSTED_ADMIN |
| T.TSF_FAILURE | O.SELF_TEST<br>OE.TOE_INTEGRITY |
| T.UNDETECTED_ACTIONS | O.AUDIT<br>OE.TRUSTED_NETWORKS |

| Threats | Security objectives |
|---|---|
| T.UNAUTHORISED_ACCESS | O.PROTECTED_COMMUNICATIONS<br>O.ROLES<br>O.AUDIT<br>O.I&A<br>O.SESSION_LOCK<br>O.POL_ENFORCEMENT<br>O.MANAGEMENT<br>O.VIEW<br>O.CRYPTO_REGULATION<br>O.SUPERVISION_IMPACT<br>O.AUDIT_PROTECTION<br>O.AUTHENTICATION_FAILURE<br>O.LOCAL_DATA_PROTECTION<br>OE.TOE_INTEGRITY<br>O.POL_VIEW<br>OE.SGL_CONNECTION<br>OE.CEC_CRYPTO_REGULATION |
| T.UNAUTHORISED_UPDATE | O.SOFTWARE_UPDATES<br>OE.SW_UPDATE_KEY |
| T.USER_DATA_REUSE | O.RESIDUAL_INFORMATION_CLEAR<br>O.POL_ENFORCEMENT |
| T.TIME_BASE | O.TIME_BASE |
| T.RESIDUAL_DATA | O.DATA_ERASURE<br>O.LOCAL_DATA_PROTECTION |

| OSP | Security objectives |
|---|---|
| P.CRYPTO_RGS | O.CRYPTO_REGULATION<br>O.CRYPTOPERIOD<br>OE.CEC_CRYPTO_REGULATION |
| P.PROVIDED_SERVICES | O.PROTECTED_COMMUNICATIONS<br>O.AUDIT<br>O.SELF_TEST<br>O.POL_ENFORCEMENT<br>O.FLOW_PARTITIONING<br>OE.AUDIT_RECORD_SGC<br>OE.TOE_INTEGRITY |
| P.POL_VIEW | O.POL_VIEW |
| P.SUPERVISION | O.SUPERVISION |
| P.VISUAL_ALARMS | O.VISUAL_ALARMS |

| OSP | Security objectives |
|---|---|
| P.BANNER | O.DISPLAY_BANNER<br>OE.DISPLAY_BANNER_SGC |
| P.SA_SP_PROTECTION | O.LOCAL_DATA_PROTECTION |
| P.KEYS_INJECTION | O.KEYS_INJECTION |

| Assumptions | Security objectives |
|---|---|
| A.NO_GENERAL_PURPOSE | OE.LINUX_GUIDANCE |
| A.PHYSICAL_ENVIRONMENT_TOE | OE.PHYSICAL_ENVIRONMENT_TOE |
| A.SW_PROTECTION | OE.SW_PROTECTION |
| A.TRUSTED_ADMIN | OE.TRUSTED_ADMIN |
| A.TRUSTED_NETWORKS | OE.TRUSTED_NETWORKS |
| A.CONFIGURATION_CONTROL | OE.TOE_INTEGRITY |
| A.ALARM | OE.ALARM |
| A.POLICIES_CONTINUITY | OE.POLICIES_CONTINUITY |
| A.SECURED_MANAGEMENT_DEVICES | OE.SECURED_SGC<br>OE.SECURED_SGL<br>OE.SECURED_CEC<br>OE.SECURED_FPD<br>OE.SECURED_NTP_SERVER |
| A.ACCESS_CONTROL_MANAGEMENT_DEVICES | OE.ACCESS_CONTROL_SGC<br>OE.ACCESS_CONTROL_SGL<br>OE.ACCESS_CONTROL_CEC<br>OE.ACCESS_CONTROL_SF<br>OE.ACCESS_CONTROL_FPD<br>OE.ACCESS_CONTROL_NTP_SERVER |
| A.PHYSICAL_ENVIRONMENT_MANAGEMENT_DEVICES | OE.PHYSICAL_ENVIRONMENT_SGC<br>OE.PHYSICAL_ENVIRONMENT_SGL<br>OE.PHYSICAL_ENVIRONMENT_CEC<br>OE.NTP_SERVER_LOCATION<br>OE.TOE_TRANSPORTATION<br>OE.PHYSICAL_ENVIRONMENT_SF<br>OE.PHYSICAL_ENVIRONMENT_FPD<br>OE.PHYSICAL_ENVIRONMENT_NTP_SERVER |
| A.AUDIT | OE.AUDIT_RECORD_SGC<br>OE.AUDIT_ANALYSIS<br>OE.AUDIT_MNGT |
| A.SGC_TO_FRONT-END | OE.SGC_TO_FRONT-END |
| A.STAND_ALONE_CEC | OE.STAND_ALONE_CEC |
| A.KEY_TRANSPORTATION | OE.KEY_TRANSPORTATION |
| A.CEC_CRYPTO_REGULATION | OE.CEC_CRYPTO_REGULATION |

# 5. EXTENDED SECURITY REQUIREMENTS

## 5.1. ETENDED FAMILIES

### 5.1.1. FCS_RBG_EXT - RANDOM BIT GENERATION

#### *5.1.1.1. Definition*

The extended family FCS_RBG_EXT is drawn from [ND_PP].

**Family Behaviour**

This family FCS_RBG_EXT (Random Bit Generation) extends the functional class FCS with the capability to generate random bits.

**Component levelling**

FCS_RBG_EXT.1 Random Bit Generation, requires that the TSF has the capability to generate random bits in conformance to a specified standard.

**Management: FCS_RBG_EXT.1**

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 dependencies.**

**FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [*selection, choose one of: NIST Special Publication 800-90 using* [*selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)*]*; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES*] seeded by an entropy source that accumulated entropy from *[selection, one or both of: a software-based noise source; a TSF-hardware-based noise source]*.**

**FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [*selection, choose one of: 128 bits, 256 bits*] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.**

#### *5.1.1.2. Rationale*

The extended family FCS_RBG_EXT is drawn from [ND_PP].

This family was defined because part 2 of [CC] does not contain any SFR which allow to generate random bits.

### 5.1.2. FPT_SIE_EXT - SECURITY INFORMATION ERASURE

#### *5.1.2.1. Definition*

**Family Behaviour**

This family FPT_SIE_EXT (Security Information Erasure) extends the functional class FPT with the capability to erase and make unavailable TSF data stored within the TOE.

**Component levelling**

FPT_SIE_EXT.1 Subset information erasure, requires that the TSF ensure that a defined subset of TSF data is made unavailable after a list of actions occurs.

FPT_SIE_EXT.2 Complete information erasure, requires that the TSF ensure that all TSF data is made unavailable after a list of actions occurs.

**Management: FPT_SIE_EXT.1, FPT_SIE_EXT.2**

There are no management activities foreseen.

**Audit: FPT_SIE_EXT.1, FPT_SIE_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 the activity.

**FPT_SIE_EXT.1 SUBSET INFORMATION ERASURE**

**Hierarchical to:** **No other components.**

**Dependencies:** **No dependencies.**

**FPT_SIE_EXT.1.1 The TSF shall ensure that [assignment: *parts of TSF data*] are made unavailable after [assignment: *list of actions*].**

**FPT_SIE_EXT.2 COMPLETE INFORMATION ERASURE**

**Hierarchical to:** **FPT_SIE_EXT.1 Subset information erasure.**

**Dependencies:** **No dependencies.**

**FPT_SIE_EXT.2.1 The TSF shall ensure that TSF data is made unavailable after [assignment: *list of actions*].**

#### *5.1.2.2. Rationale*

This family was defined because part 2 of [CC] does not contain any SFR which makes unavailable after an erasure TSF data stored within the TOE.

### 5.1.3. FCS_IPS_EXT - IPSEC

The extended family FCS_IPS_EXT is drawn from [ND_PP].

#### *5.1.3.1. Definition*

**Family Behaviour**

This family FCS_IPS_EXT (IPSec) extends the functional class FCS with the capability to specify the cryptographic algorithms used within IPSec and IKE protocols.

**Component levelling**

FCS_IPS_EXT.1 IPSec, requires the TSF to meet specifed cryptographic algorithms when implementing IPSec and IKE protocols.

**Management: FCS_IPS_EXT.1**

There are no management activities foreseen.

**Audit: FCS_IPS_EXT.1**

There are no auditable events foreseen.

**FCS_IPS_EXT.1 IPSEC**

**Hierarchical to:** **No other components.**

**Dependencies:** **FDP_ITC.1 Import of user data without security attributes, FCS_COP.1 Cryptographic operation**

**FCS_IPS_EXT.1.1 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [*selection: no other algorithms, AES-GCM-128, AES-GCM-256 as specified in RFC 4106*], and using [*selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]*].**

**FCS_IPS_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.**

**FCS_IPS_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.**

**FCS_IPS_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [*assignment: number between 100 - 200*] MB of traffic for Phase 2 SAs.**

**FCS_IPS_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [*selection: 24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP),* [*assignment: other DH groups that are implemented by the TOE*], *no other DH groups*].**

**FCS_IPS_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the [*selection: DSA, rDSA, ECDSA*] algorithm.**

**FCS_IPS_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.**

**FCS_IPS_EXT.1.8 The TSF shall support the following:**

- **Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters [*selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")" [assignment: other characters]*];**
- **Pre-shared keys of 22 characters and [*selection:* [*assignment: other supported lengths*], *no other lengths*].**

#### *5.1.3.2. Rationale*

This family was defined because part 2 of [CC] does not contain any SFR which allows to specify cryptographic algorithms used by IPSec and IKE protocols.

### 5.1.4. FIA_UIA_EXT - IDENTIFICATION AND AUTHENTICATION

The extended component FIA_UIA_EXT.1 is drawn from [ND_PP].

#### *5.1.4.1. Definition*

**Family Behaviour**

The family FIA_UIA_EXT (Identification and Authentication) extends the functional class FIA with the capability to identify and authenticate a user.

**Component levelling**

FIA_UIA_EXT.1 User Identification and Authentication, requires to allow some actions before requiring user identification and authentication.

**Management: FIA_UIA_EXT.1**

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

a) All use of the authentication mechanism.

**Audit: FIA_UIA_EXT.1**

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_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 identification and authentication process:**

- **Display the warning banner in accordance with FTA_TAB.1;**
- ***[selection: no other actions, [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.**

#### *5.1.4.2. Rationale*

This family was defined because part 2 of [CC] does not contain any SFR which allows to specify identification and authentication of a user in the same SFR.

### 5.1.5. FIA_PMG_EXT - PASSWORD MANAGEMENT

The extended family FIA_PMG_EXT is drawn from [ND_PP].

#### *5.1.5.1. Definition*

**Family Behaviour**

The family FIA_PMG_EXT (Password Management) extends the functional class FIA with the capability to management password-based authentication mechanism.

**Component levelling**

FIA_PMG_EXT.1 Pass management, provides the TSF with password management capabilities.

**Management: FIA_PMG_EXT.1**

There are no management activities foreseen.

**Audit: FIA_PMG_EXT.1**

There are no auditable events foreseen.

**FIA_PMG_EXT.1 PASSWORD MANAGEMENT**

**Hierarchical to:** **No other components.**

**Dependencies:** **No dependencies.**

**FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:**

– **Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: other characters]]**

– **Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;**

#### *5.1.5.2. Rationale*

This component was defined because part 2 of [CC] does not contain any SFR which allows managing password-based authentication mechanisms.

### 5.1.6. FPT_SKP_EXT - PROTECTION OF TSF DATA (FOR READING OF ALL SENSITIVE KEYS)

The extended family FPT_SKP_EXT is drawn from [ND_PP].

#### *5.1.6.1. Definition*

**Family Behaviour**

The family FPT_SKP_EXT (Protection of TSF Data) extends the functional class FPT with the capability to prevent reading secret and private keys.

**Component levelling**

FPT_SKP_EXT.1 Protection of TSF Data, requires the TSF to prevent reading secret and private keys.

**Management: FPT_SKP_EXT.1**

There are no management activities foreseen.

**Audit: FPT_SKP_EXT.1**

There are no auditable events foreseen.

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

**Hierarchical to:** **No other components.**

**Dependencies:** **No dependencies.**

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

#### *5.1.6.2. Rationale*

This family was defined because part 2 of [CC] does not contain any SFR which specifically allows preventing reading secret and private keys.

### 5.1.7. FPT_APW_EXT - PROTECTION OF PASSWORDS

The extended family FPT_APW_EXT is drawn from [ND_PP].

#### *5.1.7.1. Definition*

**Family Behaviour**

This family FPT_APW_EXT (Protection of passwords) extends the functional class FPT with the capability to protect authentication data during their storage.

**Component levelling**

FPT_APW_EXT.1 Protection of password, requires the TSF to protect authentication data during their storage.

**Management: FPT_APW_EXT.1**

There are no management activities foreseen.

**Audit: FPT_APW_EXT.1**

There are no auditable events foreseen.

**FPT_APW_EXT.1 PROTECTION OF PASSWORDS**

**Hierarchical to:** **No other components.**

**Dependencies:** **No dependencies.**

**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.**

#### *5.1.7.2. Rationale*

This family was defined because part 2 of [CC] does not contain any SFR which specifically allows protecting authentication data during their storage.

### 5.1.8. FPT_TUD_EXT - TRUSTED UPDATE

The extended family FPT_TUD_EXT is drawn from [ND_PP].

#### *5.1.8.1. Definition*

**Family Behaviour**

This family FPT_TUD_EXT (Trusted Update) extends the functional class FPT with the capability to update TSF firmware/software parts.

**Component levelling**

FPT_TUD_EXT.1 Trusted Update, requires the TSF to provide a trusted firmware/software update mechanism.

**Management: FPT_TUD_EXT.1**

There are no management activities foreseen.

**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) Minimal: Initiation of update.

**FPT_TUD_EXT.1 TRUSTED UPDATE**

**Hierarchical to:** **No other components.**

**Dependencies:** **FCS_COP.1 Cryptographic operation**

**FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.**

**FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.**

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

#### *5.1.8.2. Rationale*

This family was defined because part 2 of [CC] does not contain any SFR which allows specifying requirements about trusted firmware/software update.

### 5.1.9. FPT_SDP_EXT - STORED TSF DATA PROTECTION

#### *5.1.9.1. Definition*

**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 it is stored within containers controlled by the TSF.

**Component levelling**

FPT_SDP_EXT.1 Stored TSF Data protection capability, requires that the TSF protect TSF data from disclosure and/or alteration while it is stored within containers controlled by the TSF.

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

**Management: FPT_SDP_EXT.1, FPT_SDP_EXT.2**

There are no management activities foreseen.

**Audit: FPT_SDP_EXT.1, 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.1 STORED TSF DATA PROTECTION CAPABILITY**

**Hierarchical to:** **No other components.**

**Dependencies:** **No dependencies.**

**FPT_SDP_EXT.1.1 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 STORED TSF DATA PROTECTION CAPABILITY AND ACTION**

**Hierarchical to:** **FPT_SDP_EXT.1 Stored TSF data protection capability.**

**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 Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].**

### *5.1.9.2. 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.

## 5.2. EXTENDED COMPONENTS

### 5.2.1. FAU_GEN_EXT.3 - EXTERNAL MEANS

#### *5.2.1.1. Definition*

**Family Behaviour**

Cf. part 2 [CC].

The family FAU_GEN is extended with the new component FAU_GEN_EXT.3 which provides the capability to the TSF to indicate to a user through a visual or sounding mean that an (or a list of) event(s) has occurred.

**Component levelling**

FAU_GEN_EXT.3 External means, requires to indicate to users through a visual mean that a specified list of events have occurred.

**Management: FAU_GEN_EXT.3**

There are no management activities foreseen.

**Audit: FAU_GEN_EXT.3**

There are no auditable events foreseen.

| **FAU_GEN_EXT.3 EXTERNAL MEANS** |
|---|

**Hierarchical to:** **No other components.**

**Dependencies:** **FAU_GEN.1 Audit Data Generation**

**FAU_GEN_EXT.3.1 The TSF shall indicate to the user through a visual or a sounding mean when [assignment : *list of events*] occur(s).**

#### *5.2.1.2. Rationale*

This component was defined because part 2 of [CC] does not contain any SFR which allows indicating through a visual mean that specific events occurred. For the TOE described in this ST it was necessary to provide such capability.

### 5.2.2. FTA_SSL_EXT.1 - TSF-INITIATED SESSION LOCKING

The extended component FTA_SSL_EXT.1 is drawn from [ND_PP].

#### *5.2.2.1. Definition*

**Family Behaviour**

Cf. part 2 [CC].

The component FTA_SSL.1 is extended with the capability to the TSF to configure the time period of inactivity.

**Component levelling**

FTA_SSL_EXT.1 TSF-initiated Session Locking, requires TSF-initiated of a user session locking after a configured time period of user inactivity.

**Management: FTA_SSL_EXT.1**

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

a) Time period of user inactivity.

**Audit: FTA_SSL_EXT.1**

The following actions should be auditable if FTA_SSL_EXT.1 TSF-initiated Session Locking is included in the PP/ST:

a) Minimal: Locking of an interactive session by the session locking mechanism.

| **FTA_SSL_EXT.1 TSF-INITIATED SESSION LOCKING** |
|---|

**Hierarchical to:** **No other components.**

**Dependencies:** **No dependencies.**

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

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

**after a Security Administrator-specified time period of inactivity.**

#### *5.2.2.2. Rationale*

This component was defined to detail usage of the FTA_SSL.1 component of part 2 of [CC] within the [ND_PP].

### 5.2.3. FAU_STG_EXT.1 - EXTERNAL AUDIT TRAIL STORAGE

The extended component FAU_STG_EXT.1 is drawn from [ND_PP].

#### *5.2.3.1. Definition*

**Family Behaviour**

Cf. part 2 [CC].

The component FAU_STG.1 is extended with the capability to the TSF to send audit trail to an external storage.

**Management: FAU_STG_EXT.1**

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

a) Managing key lifetime value.

**Audit: FAU_STG_EXT.1**

There are no auditable events foreseen.

| **FAU_STG_EXT.1 EXTERNAL AUDIT TRAIL 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 [*selection: transmit the generated audit data to an external IT entity, receive and store audit data from an external IT entity]* using a trusted channel implementing the [*selection: IPsec, SSH, TLS, TLS/HTTPS*] protocol.**

#### *5.2.3.2. Rationale*

This component was defined because part 2 of [CC] does not contain any SFR which allows transmitting audit trail to an external storage capability. For the TOE described in this ST it was necessary to provide such capability.

### 5.2.4. FAU_STG_EXT.3 - ACTION IN CASE OF LOSS OF AUDIT SERVER CONNECTIVITY

#### *5.2.4.1. Definition*

**Family Behaviour**

Cf. part 2 [CC].

The component FAU_STG.3 is extended with the capability to the TSF to take actions when audit trail are lost that is in case of loss of external link connectivity.

**Management: FAU_STG_EXT.3**

There are no management activities foreseen.

**Audit: FAU_STG_EXT.3**

The following actions should be auditable if FAU_STG_EXT.3 Action in Case of Loss of Audit Server Connectivity is included in the PP/ST:

a) Minimal: Loss of connectivity.

| **FAU_STG_EXT.3 ACTION IN CASE OF LOSS OF AUDIT SERVER CONNECTIVITY** |
|---|

**Hierarchical to:** **No other components.**

**Dependencies:** **FAU_STG_EXT.1 External audit trail storage**

**FAU_STG_EXT.3.1 The TSF shall [*assignment: action*] if the link to the external IT entity collecting the audit data generated by the TOE is not available.**

#### *5.2.4.2. Rationale*

FAU_STG_EXT.3 was extended in order to be consistent with FAU_STG_EXT.1.

### 5.2.5. FIA_UAU_EXT.2 - PASSWORD-BASED AUTHENTICATION MECHANISM

The extended component FIA_UAU_EXT.2 is drawn from [ND_PP].

### *5.2.5.1. Definition*

**Family Behaviour**

The family FIA_UAU is extended with the new component FIA_UAU_EXT.2 to explicitly specify a password-based authentication mechanism and its constraint on password change.

**Component levelling**

FIA_UAU_EXT.2 Password-based Authentication Mechanism, requires to use a password-based authentication mechanism and explicitly specify its constraint on password change.

**Management: FIA_UAU_EXT.2**

There are no management activities foreseen.

**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 dependencies.**

**FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [*selection:* [*assignment: other authentication mechanism(s)*], *none*] to perform administrative user authentication.**

### *5.2.5.2. Rationale*

This component was defined because part 2 of [CC] does not contain any SFR explicitly concerning password-based authentication mechanism.

## 5.2.6. FCS_CKM_EXT.4 - CRYPTOGRAPHIC KEY ZEROIZATION

The extended component FCS_CKM_EXT.4 is drawn from [ND_PP].

### *5.2.6.1. Definition*

**Family Behaviour**

Cf. part 2 [CC].

The family FCS_CKM is extended with the new component FCS_CKM_EXT.4 which provides the capability to zeroise cryptographic keys.

**Component levelling**

FCS_CKM_EXT.4 Cryptographic Key Zeroization, requires to zeroise cryptographic keys when no longer required

**Management: FCS_CKM_EXT.4**

There are no management activities foreseen.

**Audit: FCS_CKM_EXT.4**

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

a) Minimal: Success and failure of the activity, the object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

| **FCS_CKM_EXT.4 CRYPTOGRAPHIC KEY ZEROIZATION** |
|---|

**Hierarchical to:** **No other components.**

**Dependencies:** **FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]**

**FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.**

### *5.2.6.2. Rationale*

This component was defined to require any cryptographic keys to be zeroised.

### 5.2.7. FCS_CKM_EXT.5 - CRYTOGRAPHIC KEY LIFETIME

#### *5.2.7.1. Definition*

**Family Behaviour**

Cf. part 2 [CC].

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

**Component levelling**

FCS_CKM_EXT.5 Cryptographic key lifetime, requires to specify and monitor 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.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*** **].**

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

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

### *5.2.7.2. 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. SECURITY REQUIREMENTS

## 6.1. SECURITY FUNCTIONAL REQUIREMENTS

### 6.1.1. TERMS USED WITHIN SFRS

#### *6.1.1.1. External Entities*

Quite all subjects used within SFRs are defined previously in section "Security Problem Definition".
Subjects that are not defined in that section are:

– Remote (instance of the) TOE: it is a remote TOE with which the TOE described through the SFRs communicates.

– Network Device on the WAN: it is any network device connected to the network which is not the TOE nor a Remote TOE.

#### *6.1.1.2. Objects et Informations*

Objects and Information used within the SFRs are defined previously in section "Security Problem Definition" (section 3.1 Assets).

#### *6.1.1.3. Security Attributes*

Security attributes used within the SFRs are:

For IP datagrams :
- datagram protocol type
- datagram protocol version
- datagram topologic data (i.e. source and destination IP addresses)
- datagram IPSec protection mode

For NTP datagrams :
- datagram protocol type
- datagram protocol version
- datagram topologic data (i.e. source and destination IP addresses)

For the TOE plaintext and cipher interfaces :
- TOE main IP address

For cryptographic keys :
- key identifier,
- key type,
- key lifetime (for symmetric keys only),
- key value

#### *6.1.1.4. Operations*

Operations used or described within the SFRs are:

– equipment (TOE) Start-up

– Full erasure

– CH interface parameters erasure
– equipment (TOE) Shutdown
– Emission of security events (FAU_SEG.1)
– Parameter query (i.e. read access)
– Password modification
– TSF Data configuration
– TSF Software upgrade
– Ciphering / Deciphering of
  - IP datagram
  - Sensitive TSF Data
  - Sensitive User Data
– Computing and verification of authentication pattern of
  - IP Datagram
  - Sensitive TSF Data
  - Sensitive User Data
– Deciphering of
  - TOE software
  - Injected IKE Peer Authentication PSK
– Verification of authentication pattern of
  - TOE software
  - Injected IKE Peer Authentication PSK
– Processing (i.e. filtering and cryptographic operations) of information coming in CH and CL interfaces

### 6.1.2. AUDIT

| **FAU_GEN.1 - 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 **basic** level of audit;

c) **All administrative actions;**

d) **and all auditable events listed in the table below (by default event is NORMAL-severity, otherwise its severity is mentionned)**

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FAU_GEN.1 | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FAU_GEN.2 | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FAU_GEN_EXT.3 | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FAU_STG_EXT.1 | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FAU_STG_EXT.3 | Loss of connectivity. | Loss of connectivity to the remote instance of the TOE in front of the E.SGC. (ALARM) |
| FPT_STM.1 | Changes to the time | Change to the time due to NTP synchronisation<br>Change to the time due to configuration command |
| FCS_RBG_EXT.1 | Failure of the randomization process | Failure of the randomization process (ALARM) |
| FCS_CKM.3/keyRenewal | Success and failure of the activity<br>The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). | Success and failure of a key renewal<br>The event log shall include the key type (IKEv1 Phase 1 key, …), the SPI of the associated SA |
| FCS_CKM_EXT.4/anyPlainTextData | Success and failure of the activity<br>The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). | Success and failure of key erasure.<br>The event log shall include the key identifier, the key type (IKEv1 Phase 1 key, …), the SPI of the associated SA |
| FCS_CKM_EXT.5/pskDistribMode | Expiration of a cryptographic key<br>The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). | Almost expiration of PSK (of distributed mode)<br>Expiration of PSK (of distributed mode) (ALARM)<br>The event log shall include the key identifier, the SPI of all impacted SAs |
| FCS_CKM_EXT.5/deriv-pskDistribMode | Expiration of a cryptographic key<br>The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). | Almost expiration of PSK derivated key (of distributed mode)<br>Expiration of PSK derivated key (of distributed mode) (ALARM)<br>The event log shall include the key identifier, the SPI of all impacted SAs |
| FCS_CKM_EXT.5/pskIKE | Expiration of a cryptographic key<br>The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). | Almost expiration of PSK (of negociated mode)<br>Expiration of PSK (of negociated mode) (ALARM)<br>The event log shall include the key identifier, the SPI of all impacted SAs |
| FCS_CKM_EXT.5/ikeV2SA | Expiration of a cryptographic key<br>The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). | NO GENERATED AUDIT DATA<br>Rationale : expiration of a negociated IKE key is not required to be logged as it could saturate the audit data and the network link between the TOE and the TOE management centre. |
| FCS_CKM_EXT.5/ikeV2childSA | Expiration of a cryptographic key<br>The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). | NO GENERATED AUDIT DATA<br>Rationale : expiration of a negociated IKE key is not required to be logged as it could saturate the audit data and the network link between the TOE and the TOE management centre. |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FPT_SIE_EXT.1/allPlainTextData | Success or failure of the activity | Success of keys erasure operation<br>Failure of keys erasure operation (ALARM)<br>An event log per key shall be generated. |
| FCS_COP.1/aes-cbc | Success and failure, and the type of cryptographic operation<br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Failure of the cryptographic operation (ALARM)<br>Rationale: this cryptographic operation is used to protect and unprotect IP datagram. Successful of the operation is not required to be logged as it would saturate the audit data and the network link between the TOE and the TOE management centre. |
| FCS_COP.1/aes-gcm | Success and failure, and the type of cryptographic operation<br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Failure of the cryptographic operation (ALARM)<br>Rationale: this cryptographic operation is used to protect and unprotect IP datagram. Successful of the operation is not required to be logged as it would saturate the audit data and the network link between the TOE and the TOE management centre. |
| FCS_COP.1/aes-xcbc | Success and failure, and the type of cryptographic operation<br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Failure of the cryptographic operation (ALARM)<br>Rationale: this cryptographic operation is used to protect and unprotect IP datagram. Successful of the operation is not required to be logged as it would saturate the audit data and the network link between the TOE and the TOE management centre. |
| FCS_COP.1/aes-cbcSw | Success and failure, and the type of cryptographic operation<br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Failure of the cryptographic operation (ALARM) |
| FCS_COP.1/aes-xcbcSw | Success and failure, and the type of cryptographic operation<br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Failure of the cryptographic operation (ALARM) |
| FCS_COP.1/ecdsaSw | Success and failure, and the type of cryptographic operation<br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Success of the cryptographic operation<br>Failure of the cryptographic operation (ALARM) |
| FCS_COP.1/aes-gcmLocalData | Success and failure, and the type of cryptographic operation<br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Failure of the cryptographic operation (ALARM)<br>Rationale : Successful of the operation is not required to be logged because it is implicit : in case of successful operation, parameters can be retrieved and the TOE is operational. |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FCS_COP.1/sha | Success and failure, and the type of cryptographic operation<br><br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | NO GENERATED AUDIT DATA<br><br>Rationale: There is no need to generate audit data for this type of cryptographic operation. |
| FCS_COP.1/hmac | Success and failure, and the type of cryptographic operation<br><br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | NO GENERATED AUDIT DATA<br><br>Rationale: There is no need to generate audit data for this type of cryptographic operation. |
| FCS_COP.1/hmacTrunc | Success and failure, and the type of cryptographic operation<br><br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | NO GENERATED AUDIT DATA<br><br>Rationale: There is no need to generate audit data for this type of cryptographic operation. |
| FCS_COP.1/prf-sha | Success and failure, and the type of cryptographic operation<br><br>Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | Failure of the cryptographic operation (ALARM)<br><br>Rationale: this cryptographic operation is used by the key negociation protocol (IKE). Successful of the operation is not required to be logged as it could saturate the audit data and the network link between the TOE and the TOE management centre. |
| FTP_ITC.1/TOE | All attempted uses of the trusted channel functions.<br><br>Identification of the initiator and target of all trusted channel functions. | Success and failure of initiation of a protected communication channel.<br><br>The event log shall include the identifier of the security policy. |
| FDP_UCT.1/TOE | The identity of any unauthorised user or subject attempting to use the data exchange mechanisms. | NO GENERATED AUDIT DATA<br><br>Rationale: There is no need to generate audit data for this type of cryptographic operation is done through FDP_IFF.1/VPN. |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FDP_UIT.1/TOE | The identity of any user or subject using the data exchange mechanisms.<br><br>The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so.<br><br>A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data.<br><br>Any identified attempts to block transmission of user data. | NO GENERATED AUDIT DATA<br><br>Rationale:<br>this mechanism is used to exchange IP datagram. The identifty of any subject using the mechanism is not required to be logged as it would saturate the audit data and the network link between the TOE and the TOE management centre.<br>Logging unauthorised use of the mechanism is done through FDP_IFF.1/VPN. |
| FCS_IPS_EXT.1 | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FDP_ITC.2/VPN | All attempts (successful or not) to import user data, including any security attributes. | NO GENERATED AUDIT DATA<br><br>Rationale: this function is used to import IP datagram. No logging of the operation is not required as it would saturate the audit data and the network link between the TOE and the TOE management centre. |
| FDP_ETC.2/VPN | All attempts (successful or not) to export user data, including any security attributes. | NO GENERATED AUDIT DATA<br><br>Rationale: this function is used to export IP datagram. No logging of the operation is not required as it would saturate the audit data and the network link between the TOE and the TOE management centre. |
| FDP_IFC.1/VPN | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FDP_IFF.1/VPN | All decisions on requests for information flow. | Unfound SP/SA<br>Detection of IPSec datagram modification.<br>Detection of IPSec datagram replay. (ALARM)<br><br>Rationale: this function is used to control vpn IP datagram flow. All successful decisions is not required to be logged as it would saturate the audit data and the network link between the TOE and the TOE management centre. |
| FDP_ITC.2/pskDistribmode | All attempts (successful or not) to import user data, including any security attributes. | Key (PSK for distributed mode) injection operation.<br><br>The event log shall include the key identifier, the user identitiy (user role or management device's IP adress). |
| FDP_ITC.2/pskIKE | All attempts (successful or not) to import user data, including any security attributes. | Key (PSK for negociated mode) injection operation.<br>The event log shall include the key identifier, the user identitiy. |
| FDP_UCT.1/keysInjection | The identity of any unauthorised user or subject attempting to use the data exchange mechanisms. | NO GENERATED AUDIT DATA<br>Rationale: logging of use of this mechanism is done through FDP_ITC.2/pskDistribmode and FDP_ITC.2/pskIKE. |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FDP_UIT.1/keysInjection | The identity of any user or subject using the data exchange mechanisms.<br><br>The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so.<br><br>A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data.<br><br>Any identified attempts to block transmission of user data. | Detection of key modification.<br><br>Rationale:<br>this mechanism is used to inject cryptographic key. The use of the mechanism is not required to be logged as it is done through FDP_ITC.2/***.<br>Logging unauthorised use of the mechanism is done through FDP_IFF.1/keyInjection. |
| FDP_IFC.1/keysInjection | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FDP_IFF.1/keysInjection | All decisions on requests for information flow. | Detection of key modification. |
| FPT_TDC.1/keysInjection | Use of the TSF data consistency mechanisms<br><br>Identification of which TSF data have been interpreted<br><br>Detection of modified TSF data | NO GENERATED AUDIT DATA<br><br>Rationale : no audit data is generated by this SFR as they are already generated by FDP_UIT.1/keysInjection (for data modification) and FMT_MTD.1/configuration (for data import).<br>Use of the consistency mechanism is implicit when the data is accepted by the TOE. |
| FDP_IFC.1/ntp | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FDP_IFF.1/ntp | All decisions on requests for information flow. | Detection of key modification.<br>(the event log shall include the entire content of the protected key (not the deciphered content))<br>Success of key integrity checking. |
| FMT_MSA.3 | Modifications of the default setting of permissive or restrictive rules.<br><br>All modifications of the initial values of security attributes. | Any modification a parameter value.<br><br>Rationale: modification of default value is not logged as it is not possible to modifiy default settings. |
| FMT_SMR.1/user | Modifications to the group of users that are part of a role | NO GENERATED AUDIT DATA<br><br>Rationale: the TOE implements roles only. |
| FMT_SMR.1/devices | Modifications to the group of users that are part of a role | NO GENERATED AUDIT DATA<br><br>Rationale: the TOE implements roles only. |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FIA_UID.2/sgc | All use of the user identification mechanism, including the<br>user identity provided | NO GENERATED AUDIT DATA<br><br>Rationale: the audit data are generated through FDP_IFF.1/VPN since the identity of the SGC is checked through the SP/SA filtering and verification process. If an error occurs, the corresponding audit data is logged by the SP/SA filtering and verification mechanism. |
| FIA_UIA_EXT.1/localMngt | All use of the authentication mechanism. | Successful and failure (for all attempts) of the authentication of a user.<br><br>The event log shall include the user's role. |
| FIA_UAU_EXT.2/localMngt | All use of the authentication mechanism | Successful and failure (for all attempts) of the authentication of a user.<br><br>The event log shall include the user's role. |
| FIA_UAU.6/localMngt | All reauthentication attempts. | Successful and failure (for all attempts) of the re-authentication of a user.<br><br>The event log shall include the user's role. |
| FIA_UAU.7/localMngt | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FIA_AFL.1/localMngt | The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal) | Failure of an authentication attempt |
| FIA_PMG_EXT.1/localMngt | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FTA_SSL_EXT.1/localMngt | Locking of an interactive session by the session locking mechanism | Termination of an interactive session by the session locking mechanism |
| FTA_SSL.4/localMngt | Termination of an interactive session by the user | Termination of an interactive session by the user |
| FTA_TAB.1/localMngt | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FMT_SMF.1 | Use of the management functions | Use of the management functions<br><br>The event log shall include the origin of the management order : TOE local management or TOE management centre. |
| FMT_MOF.1/localMngt | All modifications in the behaviour of the functions in the TSF. | Enabling of the TOE local management functionality<br><br>Disabling of the TOE local management functionality |
| FMT_MTD.1/query | All modifications to the values of TSF data. | NO GENERATED AUDIT DATA |
| FMT_MTD.1/supervision | All modifications to the values of TSF data. | NO GENERATED AUDIT DATA |
| FPT_SKP_EXT.1 | All modifications to the values of TSF data. | NO GENERATED AUDIT DATA |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FMT_MTD.1/configuration | All modifications to the values of TSF data. | All modifications to the values of parameters of D.SECURITY_POLICIES and D.CONFIG_PARAM.<br><br>The event log shall include the name of the paramter and the involved interface. |
| FMT_MTD.1/dateTime | All modifications to the values of TSF data. | All modifications to the values of parameters of D.TIME_BASE.<br><br>The event log shall include the name of the paramter and the involved interface. |
| FMT_MTD.1/keys | All modifications to the values of TSF data. | Modification (injection) of a PSK |
| FMT_MTD.1/keyLifetime | All modifications to the values of TSF data. | Modification of a key lifetime.<br>The event log shall include the name of the key and the previous and the new lifetime values. |
| FMT_MTD.1/adminPwd | All modifications to the values of TSF data. | Modification of the administrator password. |
| FMT_MTD.1/opePwd | All modifications to the values of TSF data. | Modification of the operator password. |
| FMT_MTD.1/software | All modifications to the values of TSF data. | NO GENERATED AUDIT DATA<br><br>Rationale : generated events are given by FPT_TUD_EXT.1/software. |
| FPT_TUD_EXT.1/software | Initiation of update. | Taking into account an uploading command request<br>(the event log shall include the IP address of the TFTP server)<br><br>Success and failure (integrity error, ...) of the software signature. |
| FPT_APW_EXT.1 | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |
| FPT_FLS.1 | Failure of the TSF | Failure of the software (ALARM)<br><br>Failure of a parameter loading (ALARM)<br>(the event log shall include the failed parameter name and the type of failure)<br><br>Failure of a self-test (ALARM) |

| SFR | Auditable events (drawn from CC Part 2) | Interpretation regarding the TOE |
|---|---|---|
| FPT_TST.1 | Execution of the TSF self tests and the results of the tests | Start of the execution of the self-test process<br><br>Success each self-test.<br>Failure of a self-test (ALARM)<br>At least :<br>· cryptographic auto-tests<br>· software auto-tests<br>· data integrity, this includes:<br>· D.SECURITY_POLICIES<br>· D.CONFIG_PARAM<br>· D.CRYPTO_KEYS<br><br>End of the execution of the self-test process.<br><br>The event log shall include any additional information generated by the tests (beyond “success” or “failure”). |
| FPT_SDP_EXT.2 | Success or failure of integrity check of TSF data | Failure of integrity check of<br>· D.SECURITY_POLICIES<br>· D.CONFIG_PARAM<br>· D.CRYPTO_KEYS |
| FDP_RIP.2 | There are no auditable events foreseen. | NO GENERATED AUDIT DATA |

FAU_GEN.1.2

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

– a) Date and time of the event,

– b) Type of event,

– c) **(refinement) User** identity **or the origin network interface (in case a network device caused the event)** (if applicable),

– d) Outcome (success or failure) of the event.

– e) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,

- **Severity of the event, at least:**
  - **NORMAL**
  - **ALARM**
- **Information specified in column three of the table above**.

**FAU_GEN.2 - USER IDENTITY ASSOCIATION**

FAU_GEN.2.1

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

**FAU_GEN_EXT.3 - EXTERNAL MEANS**

FAU_GEN_EXT.3.1

The TSF shall indicate to the user through a visual or a sounding mean when **an ALARM-type event** occurs.

**FAU_STG_EXT.1 - EXTENDED : EXTERNAL AUDIT TRAIL STORAGE**

FAU_STG_EXT.1.1

The TSF shall be able to **transmit the generated audit data to an external IT entity when required, and transmit all generated ALARM-type event data to an external IT entity** using a trusted channel implementing the **IPSec** protocol **(refinement) (trusted channel defined in FTP_ITC.1/TOE)**.

**FAU_STG_EXT.3 - EXTENDED : ACTION IN CASE OF LOSS OF AUDIT SERVER CONNECTIVITY**

FAU_STG_EXT.3.1

The TSF shall **generate an ALARM-type event and continue its operation** if the link to the external IT entity collecting the audit data generated by the TOE is not available.

**FPT_STM.1 - RELIABLE TIME STAMPS**

FPT_STM.1.1

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

*Application note:*

*TOE reference of time is its start-up.*

## 6.1.3. CRYPTOGRAPHY

### *6.1.3.1. Key Management*

**FCS_RBG_EXT.1 - EXTENDED : RANDOM BIT GENERATION**

FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with **NIST Special Publication 800-90 using CTR_DRBG (AES)** seeded by an entropy source that accumulated entropy from **TSF-hardware-based noise source**.

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded with a minimum of **256 bits** of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

### FCS_CKM.3/KEYRENEWAL - CRYPTOGRAPHIC KEY (REFINEMENT) RENEWAL

FCS_CKM.3.1/keyRenewal

The TSF shall perform **(refinement) key renewal** in accordance with a specified cryptographic **(refinement) key renewal** method **(refinement) peer authentication key injection (negociated mode) and session distributed key injection (distributed mode) (for D.CRYPTO_KEYS) and IKE SAs keys renewal (for D.IKE_SAs_CRYPTO_KEYS) and derived distributed PSK renewal (for D.DISTRIB_SAs_CRYPTO_KEYS)** that meets the following: **ANSSI cryptographic referential [RGS_B]**.

### FCS_CKM_EXT.4/ANYPLAINTEXTDATA - CRYPTOGRAPHIC KEY DESTRUCTION

FCS_CKM_EXT.4.1/anyPlainTextData

The TSF shall zeroize **(refinement) all plaintext secret cryptographic keys and CSPs (Cryptographic Critical Security Parameters) when no longer required, that is :**

- **Any plaintext cryptographic key symbolised through D.CRYPTO_KEYS:**
  - **any plaintext Distributed mode PSK (during injection, or during TOE operation, ...)**
  - **any plaintext IKE peer authentication PSK (during injection, or during TOE operation, ...)**
- **Any plaintext cryptographic key symbolised through D.IKE_SAs_CRYPTO_KEYS:**
  - **any plaintext IKEv2 SAs keys**
  - **any plaintext IKEv2 Child SAs keys**
- **any plaintext CSPs (i.e. SKEYSEED for IKEv2 protocol, the seed for the PRNG (refer to FCS_RBG_EXT.1), ...)**
- **Any plaintext cryptographic key symbolised through D.DISTRIB_SAs_CRYPTO_KEYS:**
  - **any plaintext derivated keys of Distributed mode PSK**
- **the Local Protection Key**

**(refinement) in accordance with a specified cryptographic key destruction method called zeroisation that overwrites keys and data value through one pass of bits '0' and one pass of bits '1'**.

### FCS_CKM_EXT.5/PSKDISTRIBMODE - DISTRIBUTED MODE PSK KEY CRYPTOPERIOD

FCS_CKM_EXT.5.1/pskDistribMode

The TSF shall manage **a cryptoperiod** for **the Distributed mode PSK**.

FCS_CKM_EXT.5.2/pskDistribMode

The TSF shall calculate the key lifetime from **key first use**.

FCS_CKM_EXT.5.3/pskDistribMode

The TSF shall **either (depending on the key security attribute values)**

– **close any communication channels using this key and periodically generate a critical severity audit data requiring the peer authentication key to be renewed (in this case no more new communication channels for SAs using this key can be initiated until the key is renewed)**

– **or periodically generate a critical severity audit data while it continues to proceed the network trafic (in this case new communication channels for SAs using this key can be initiated even if the key is out-of-date)**

after the key has expired.

### FCS_CKM_EXT.5/DERIV-PSKDISTRIBMODE - DISTRIBUTED MODE PSK DERIVATED KEY CRYPTOPERIOD

FCS_CKM_EXT.5.1/deriv-pskDistribMode

The TSF shall manage **a cryptoperiod** for **the Distributed mode PSK derivated key**.

FCS_CKM_EXT.5.2/deriv-pskDistribMode

The TSF shall calculate the key lifetime from **key first use**.

FCS_CKM_EXT.5.3/deriv-pskDistribMode

The TSF shall **either (depending on the key security attribute values)**

– **close any communication channels using this key and periodically generate a critical severity audit data requiring the peer authentication key to be renewed (in this case no more new communication channels for SAs using this key can be initiated until the key is renewed)**

– **or periodically generate a critical severity audit data while it continues to proceed the network trafic (in this case new communication channels for SAs using this key can be initiated even if the key is out-of-date)**

after the key has expired.

### FCS_CKM_EXT.5/PSKIKE - IKE PEER AUTHENTICATION PSK KEY CRYPTOPERIOD

FCS_CKM_EXT.5.1/pskIKE

The TSF shall manage **a cryptoperiod** for **the IKE peer authentication PSK**.

FCS_CKM_EXT.5.2/pskIKE

The TSF shall calculate the key lifetime from **key first use**.

FCS_CKM_EXT.5.3/pskIKE

The TSF shall **either (depending on the key security attribute values)**

– **close any communication channels using this key and periodically generate a critical severity audit data requiring the peer authentication key to be renewed (in this case no more new communication channels for SAs using this key can be initiated until the key is renewed)**

– **or periodically generate a warning severity audit data while it continues to proceed the network trafic (in this case new communication channels for SAs using this key can be initiated even if the key is out-of-date)**

after the key has expired.

**FCS_CKM_EXT.5/IKEV2SA - IKEV2 IKE SA KEY CRYPTOPERIOD**

FCS_CKM_EXT.5.1/ikeV2SA

The TSF shall manage **a cryptoperiod** 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 a key has expired.

*Application note:*

*IKE v2 ([RFC 5996) introduces the notion of Initial Exchange. It is quite similar to the IKE v1 phase 1.*

*In IKE v2 protocol, during the initial exchange, the two end-points exchange their Diffie-Hellman key public-parts in order to generate and derive key material. This key material will then be used by the IKE SA corresponding to the channel between those two end-points in order to protect next IKE v2 exchange (known as Child SA Exchange) and to generate new key material during this latter exchange.*

**FCS_CKM_EXT.5/IKEV2CHILDSA - IKEV2 CHILD SAS KEY CRYPTOPERIOD**

FCS_CKM_EXT.5.1/ikeV2childSA

The TSF shall manage **a cryptoperiod** 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 a key has expired.

*Application note:*

*IKE v2 ([RFC 5996]) introduces the notion of Child SA Exchange. It is quite similar to the IKE v1 phase 2.*

*In IKE v2 protocol, during the child SA exchange, the two end-points negociate the algorithm to be used to protect User Dataflows. During this exchange, they also derive their key material that will then be used by the Child SA in order to protect the User Data flows.*

**FPT_SIE_EXT.1/ALLPLAINTEXTDATA - EXTENDED : SUBSET INFORMATION ERASURE**

FPT_SIE_EXT.1.1/allPlainTextData

The TSF shall ensure that **plaintext secret cryptographic keys and CSPs (Cryptographic Critical Security Parameters) as required by FCS_CKM_EXT.4** are made unavailable after:

– **A full erasure (which can be activated by a command on the CLI, the erasure push-button on the front panel, or the remote erasure interface on the rear panel).**

### *6.1.3.2. Cryptographic Operations*

**FCS_COP.1/AES-CBC - AES-CBC CRYPTOGRAPHIC OPERATION**

FCS_COP.1.1/aes-cbc

The TSF shall perform **ip datagram encryption and decryption** in accordance with **(refinement) AES operating in CBC mode** and cryptographic key sizes **(refinement) 256 bits** that meet the following:

– **FIPS 197 (Advanced Encryption Standard (AES))**

– **NIST SP 800-38A**

**FCS_COP.1/AES-GCM - AES-GCM CRYPTOGRAPHIC OPERATION**

FCS_COP.1.1/aes-gcm

The TSF shall perform **ip datagram encryption with authentication and decryption with authentication verification** in accordance with **(refinement) AES operating in GCM mode** and cryptographic key sizes **(refinement) 256 bits** that meet the following:

– **FIPS 197 (Advanced Encryption Standard (AES))**

– **NIST SP 800-38D**

**FCS_COP.1/AES-XCBC - AES-XCBC CRYPTOGRAPHIC OPERATION**

FCS_COP.1.1/aes-xcbc

The TSF shall perform **ip datagram authentication and authentication verification** in accordance with **(refinement) AES operating in XCBC-MAC-96 mode** and cryptographic key size **128 bits** that meet the following:

– **RFC 3566**

**FCS_COP.1/AES-CBCSW - AES-CBC FOR SOFTWARE UPDATE CRYPTOGRAPHIC OPERATION**

FCS_COP.1.1/aes-cbcSw

The TSF shall perform **software update decryption** in accordance with **(refinement) AES operating in CBC mode** and cryptographic key sizes **256 bits** that meet the following:

– **FIPS 197 (Advanced Encryption Standard (AES))**

– **NIST SP 800-38A**

**FCS_COP.1/AES-XCBCSW - AES-XCBC FOR SOFTWARE UPDATE CRYPTOGRAPHIC OPERATION**

FCS_COP.1.1/aes-xcbcSw

The TSF shall perform **software update authentication verification** in accordance with **(refinement) AES operating in XCBC-MAC-96 mode** and cryptographic key size **128 bits** that meet the following:

– **RFC 3566**

**FCS_COP.1/ECDSASW - ECDSA FOR SOFTWARE UPDATE CRYPTOGRAPHIC OPERATION**

FCS_COP.1.1/ecdsaSw

The TSF shall perform **software update cryptographic signature verification** in accordance with **(refinement) SHA512 and Elliptic Curve Digital Signature Algorithm (ECDSA)** and cryptographic key size **521 bits** that meet the following:

– **FIPS 186-4 (Digital Signature Standard)**

– **(refinement) and RFC 5639 (Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation)**

### FCS_COP.1/AES-GCMLOCALDATA - AES-GCM LOCAL DATA CRYPTOGRAPHIC OPERATION

FCS_COP.1.1/aes-gcmLocalData

The TSF shall perform **local data containers encryption with authentication and decryption with authentication verification** in accordance with **(refinement) AES operating in GCM mode** and cryptographic key sizes **256 bits** that meet the following:

– **FIPS 197 (Advanced Encryption Standard (AES))**

– **NIST SP 800-38D**

### FCS_COP.1/SHA - SHA CRYPTOGRAPHIC OPERATION

FCS_COP.1.1/sha

The TSF shall perform **cryptographic hashing** in accordance with **(refinement) SHA-256, SHA-384 and SHA-512 and message digest sizes 160, 384 and 512 bits** that meet the following:

– **FIPS 180-3 (Secure Hash Standard)**

### FCS_COP.1/HMAC - HMAC CRYPTOGRAPHIC OPERATION

FCS_COP.1.1/hmac

The TSF shall perform **keyed-hash message authentication and authentication verification** in accordance with **(refinement) HMAC-SHA-256 and HMAC-SHA-384** and cryptographic key sizes **respectively 256 and 384, (refinement) and message digest sizes 256 and 384 bits** that meet the following:

– **FIPS 198-1 (The Keyed-Hash Message Authentication Code)**

– **FIPS 180-3 (Secure Hash Standard)**

### FCS_COP.1/HMACTRUNC - TRUNCATED HMAC CRYPTOGRAPHIC OPERATION

FCS_COP.1.1/hmacTrunc

The TSF shall perform **truncated keyed-hash message authentication and authentication verification** in accordance with **(refinement) HMAC-SHA-256-128** and cryptographic key sizes **respectively 256 bits, (refinement) and truncated message digest size 128 bits** that meet the following:

– **FIPS 198-1 (The Keyed-Hash Message Authentication Code)**

– **FIPS 180-3 (Secure Hash Standard)**

– **SP 800-107 (Recommendations for Applications Using Approved Hash Algorithms)**

– **RFC 4868 (Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec)**

### FCS_COP.1/PRF-SHA - PRF-SHA CRYPTOGRAPHIC OPERATION

FCS_COP.1.1/prf-sha

The TSF shall perform **pseudo random function** in accordance with **(refinement) SHA-384** that meet the following:

– **FIPS 180-3 (Secure Hash Standard)**

## 6.1.4. COMMUNICATIONS PROTECTION AND FLOW CONTROLS

### *6.1.4.1. Communications Protection*

#### 6.1.4.1.1. Inter-TOE Communications Protection

**FTP_ITC.1/TOE - INTER-TSF TRUSTED CHANNEL**

FTP_ITC.1.1/TOE

The TSF shall **(refinement) use IPSec to** provide a **(refinement) trusted** communication channel between itself and **(refinement) authorized IT entities supporting the following capabilities: audit server, NTP server, TOE Management center device, a remote instance of the TOE** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **(refinement) disclosure and modification of the channel data**.

FTP_ITC.1.2/TOE

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

FTP_ITC.1.3/TOE

The TSF shall initiate communication via the trusted channel for **communication with a remote instance of the TOE**.

**FDP_UCT.1/TOE - INTER-TSF BASIC DATA EXCHANGE CONFIDENTIALITY**

FDP_UCT.1.1/TOE

The TSF shall enforce the **VPN SFP** to be able to **transmit and receive** user data in a manner protected from unauthorised disclosure **(refinement) between itself and a remote instance of the TOE**.

**FDP_UIT.1/TOE - INTER-TSF DATA EXCHANGE INTEGRITY**

FDP_UIT.1.1/TOE

The TSF shall enforce the **VPN SFP** to be able to **transmit and receive** user data in a manner protected from **modification, insertion and replay errors (refinement) between itself and a remote instance of the TOE**.

FDP_UIT.1.2/TOE

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

**FCS_IPS_EXT.1 - EXTENDED : IPSEC**

FCS_IPS_EXT.1.1

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using: **(refinement)**

- **for IPSEC Mistral mode,** the cryptographic algorithms AES-CBC-256 (specified by RFC 3602) **for confidentiality and XCBC-MAC96 (specified by RFC 3566) for Integrity**

and using:

- **IKEv2 as defined in RFCs 5996, 4307**
- **PSK derivation algorithm for distributed mode**

FCS_IPS_EXT.1.2

**(refinement) not applicable.**

FCS_IPS_EXT.1.3

The TSF shall ensure that **(refinement) IKEv2 SA lifetimes are able to be limited to 24 hours for IKE SAs and 8 hours for IKE Child SAs**.

FCS_IPS_EXT.1.4

The TSF shall ensure that **(refinement) IKEv2 SA lifetimes are able to be limited to 200 MB of traffic for IKE Child SAs**.

FCS_IPS_EXT.1.5

The TSF shall ensure that **(refinement) IKEv2** protocols implement:

- **DH Group 20 (384-bit Random ECP) (RFC 5903)**

FCS_IPS_EXT.1.6

**(refinement) not applicable.**

FCS_IPS_EXT.1.7

The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its **(refinement) IKEv2** connections.

FCS_IPS_EXT.1.8

**(refinement) requirement removed.**

*Application note :*

*FCS_IPS_EXT.1.8 has been removed in regards to [ND_PP] because it is considered too weak. The TOE authorises only PSK peer authentication for the IKE protocols using either symmetric cryptographic keys.*

### 6.1.4.1.2. Central Management Communications Protection

The central management of the TOE is performed through a secured communication link provided by the TOE and a remote instance of the TOE. Therefore, no added security TOE requirements about securing the central management link are necessary in regards to those specified for the "Inter-TOE Communications Protection".

### *6.1.4.2. Flow Controls*

#### 6.1.4.2.1. VPN Policy flow control

**FDP_ITC.2/VPN - VPN IMPORT OF USER DATA WITH SECURITY ATTRIBUTES**

FDP_ITC.2.1/VPN

The TSF shall enforce the **VPN SFP** when importing **(refinement) IP datagrams to send to a remote private network or IPSec datagrams**, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/VPN

The TSF shall use the **(refinement) IP datagrams protocol and topologic data** associated with the imported **(refinement) IP datagrams payload**.

FDP_ITC.2.3/VPN

The TSF shall ensure that the protocol used provides for the unambiguous association between the **(refinement) IP datagrams protocol and topologic data** and the **(refinement) IP datagrams payload** received.

FDP_ITC.2.4/VPN

The TSF shall ensure that interpretation of the **(refinement) IP datagrams protocol and topologic data** of the imported **(refinement) datagrams payload** is as intended by the source of the **(refinement) IP datagrams**.

FDP_ITC.2.5/VPN

The TSF shall enforce the following rules when importing **(refinement) IP datagrams** controlled under the SFP from outside the TOE: **no additional importation control rules**.

**FDP_ETC.2/VPN - VPN EXPORT OF USER DATA WITH SECURITY ATTRIBUTES**

FDP_ETC.2.1/VPN

The TSF shall enforce the **VPN SFP** when exporting **(refinement) IP datagrams**, controlled under the SFP, outside of the TOE.

FDP_ETC.2.2/VPN

The TSF shall export the **(refinement) IP datagrams payload** with the **(refinement) IP datagrams protocol and topologic data** associated security attributes.

FDP_ETC.2.3/VPN

The TSF shall ensure that the **(refinement) IP datagrams protocol and topologic data**, when exported outside the TOE, are unambiguously associated with the exported **(refinement) IP datagrams payload**.

FDP_ETC.2.4/VPN

The TSF shall enforce the following rules when **(refinement) IP datagrams are** 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** on :

– **Subjects :**
  - **Encrypted Data Interface**
  - **Plain Text Data Interface**
– **Information :**
  - **IP datagrams**
– **Operations :**
  - **OP.Receiving : Processing of information coming from the Subject**
  - **OP.Sending : Emission of information to the Subject**

**FDP_IFF.1/VPN - VPN SIMPLE SECURITY ATTRIBUTES**

FDP_IFF.1.1/VPN

The TSF shall enforce the **VPN SFP** based on the following types of subject and information security attributes:

– **Subjects and their security attributes :**
  - **Encrypted Data Interface : the TOE main IP address**
  - **Plain Text Data Interface : the TOE main IP address**
– **Information and their security attributes :**
  - **Protocol datagrams : protocol type, protocol version, source IP address, destination IP address, (if available:) IPSec protection mode**

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**
    – **If SA's protection mode is IPSec ESP Tunnel:**
      - **The IPSec protection mode contain within the IP datagram is the same as the one specified within the SA**
      - **The IP datagram has not been inserted (refer to FDP_UIT.1/TOE)**
      - **The IP datagram has not been modified (refer to FDP_UIT.1/TOE)**
      - **The IP datagram has not been replayed (refer to FDP_UIT.1/TOE)**
      - **The TSF can find an associated SP using the source and destination IP addresses of the deciphered IP datagram**
      - **The deciphered IP datagram contains an authorised specified port**
      - **The deciphered IP datagram contains an authorised protocol**
  - **If the IP datagram does not contain a SPI**
    – **If bridge mode is activated:**
      - **If the IP datagram specifies a routing protocol, the routing protocol shall be explicitly authorised through the configuration of the TSF (D.CONFIG_PARAM)**

- **Otherwise the TSF applies the rules below**
- **The TSF can find an associated SP using the source and destination IP addresses of the IP datagram**
- **The SP specifies "bypass" action (that is authorises a plaintext IP datagram)**
- **The IP datagram contains an authorised specified port**
- **The IP datagram contains an authorised protocol**

– **OP.Receiving (from Plaintext Data Interface):**

- **The IP datagram contains an authorised specified port**
- **The IP datagram contains an authorised protocol**
- **The TSF can find an associated SP using the source and destination IP addresses of the IP datagram**

– **OP.Sending (to Encrypted Data Interface):**

- **The datagram has been properly protected according to the SA referred by the associated SA and SP**

– **OP.Sending (to Plaintext Data Interface):**

- **The datagram has been properly checked and deprotected according to the associated SA and SP**

FDP_IFF.1.3/VPN

The TSF shall **(refinement) not** enforce **additional rules**.

FDP_IFF.1.4/VPN

The TSF shall explicitly authorise an information flow based on the following rules: **none**.

FDP_IFF.1.5/VPN

The TSF shall explicitly deny an information flow based on the following rules:

– **In bridge mode, when the IP datagram does not specifies an authorised routing protocol and when no VPN SP has been explicitly defined for the given IP datagram (no match with the given source IP address and destination IP address) the default screening rule applies. This latter rule shall reject the IP datagram, without sending it to any interface (either external intefaces such as Plaintext Data Interface, Enciphered Data Interface, …, nor internal interfaces (such a TOE management)).**

– **When the given VPN SP specifies that sending IP packets to the destination address (specific to a subnetwork) is forbidden, no sending is performed.**

– **When an error occurs during the application or verification of security protections, no sending of IP packets is authorized.**

#### 6.1.4.2.2. Import of Cryptographic Keys

**FDP_ITC.2/PSKDISTRIBMODE - DISTRIBUTED PSK IMPORT OF USER DATA WITH SECURITY ATTRIBUTES**

FDP_ITC.2.1/pskDistribmode

The TSF shall enforce the **Keys Injection SFP** when importing **(refinement) the distributed mode's PSK**, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/pskDistribmode

The TSF shall use the security attributes associated with the imported **(refinement) the distributed mode's PSK**.

FDP_ITC.2.3/pskDistribmode

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/pskDistribmode

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/pskDistribmode

The TSF shall enforce the following rules when importing **(refinement) the distributed mode's PSK** controlled under the SFP from outside the TOE: **no additional control rules**.

**FDP_ITC.2/PSKIKE - IKE PSK IMPORT OF USER DATA WITH SECURITY ATTRIBUTES**

FDP_ITC.2.1/pskIKE

The TSF shall enforce the **Keys Injection SFP** when importing **(refinement) the IKE peer authentication PSK**, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/pskIKE

The TSF shall use the security attributes associated with the imported **(refinement) the IKE peer authentication PSK**.

FDP_ITC.2.3/pskIKE

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/pskIKE

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/pskIKE

The TSF shall enforce the following rules when importing **(refinement) the IKE peer authentication PSK** controlled under the SFP from outside the TOE: **no additional control rules**.

**FDP_UCT.1/KEYSINJECTION - KEYS BASIC DATA EXCHANGE CONFIDENTIALITY**

FDP_UCT.1.1/keysInjection

The TSF shall enforce the **Keys Injection SFP** to be able to **receive (refinement) cryptographic secret keys** in a manner protected from unauthorised disclosure.

**FDP_UIT.1/KEYSINJECTION - KEYS DATA EXCHANGE INTEGRITY**

FDP_UIT.1.1/keysInjection

The TSF shall enforce the **Keys Injection SFP** to be able to **receive (refinement) cryptographic keys** in a manner protected from **modification, insertion and replay errors**.

FDP_UIT.1.2/keysInjection

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

**FDP_IFC.1/KEYSINJECTION - KEYS INJECTION SUBSET INFORMATION FLOW CONTROL**

FDP_IFC.1.1/keysInjection

The TSF shall enforce the **Keys Injection SFP** on :

- **Subjects :**
  - **Encrypted Data Interface**
  - **Plaintext Data Interface**
  - **Command Line Interface**
  - **Smartcard Interface**
- **Information :**
  - **Keys**
- **Operations :**
  - **OP.Injection : Processing of information coming from the Subject**

**FDP_IFF.1/KEYSINJECTION - KEYS INJECTION SIMPLE SECURITY ATTRIBUTES**

FDP_IFF.1.1/keysInjection

The TSF shall enforce the **Keys Injection SFP** based on the following types of subject and information security attributes:

- **Subjects and their security attributes :**
  - **Encrypted Data Interface**
  - **Plaintext Data Interface**
  - **Command Line Interface**
  - **Smartcard Interface**
- **Information and their security attributes :**
  - **Key : key identifier, key type, key lifetime (for symetric keys only), key value**

FDP_IFF.1.2/keysInjection

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 key and its security attributes are consistent**
- **For the operation OP.Injection (from Plaintext Data Interface):**
  - **The key and its security attributes are consistent**
- **For the operation OP.Injection (from Command Line Interface):**
  - **The key and its security attributes have not been modified**
  - **The Local Administrator is successfully authentified**
  - **The key and its security attributes are consistent**
- **For the operation OP.Injection (from Smartcard Interface):**

- **The key and its security attributes are consistent**

FDP_IFF.1.3/keysInjection

The TSF shall **(refinement) not** enforce **additional rules**.

FDP_IFF.1.4/keysInjection

The TSF shall explicitly authorise an information flow based on the following rules: **none**.

FDP_IFF.1.5/keysInjection

The TSF shall explicitly deny an information flow based on the following rules: **none**.

**FPT_TDC.1/KEYSINJECTION - INTER-TSF BASIC TSF DATA CONSISTENCY**

FPT_TDC.1.1/keysInjection

The TSF shall provide the capability to consistently interpret

– **the IKE peer authentication PSK**

– **the communication channels protection keys PSK (for distributed mode)**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/keysInjection

The TSF shall use **key format** when interpreting the TSF data from another trusted IT product.

### 6.1.4.2.3. NTP Synchronisation

**FDP_IFC.1/NTP - NTP SYNCHRONISATION SUBSET INFORMATION FLOW CONTROL**

FDP_IFC.1.1/ntp

The TSF shall enforce the **NTP SFP** on :

– **Subjects :**
  - **Encrypted Data Interface**
  - **Plaintext Data Interface**

– **Information :**
  - **NTP datagram**

– **Operations :**
  - **OP.Receving : Processing of information coming from the Subject**

**FDP_IFF.1/NTP - NTP SYNCHRONISATION SIMPLE SECURITY ATTRIBUTES**

FDP_IFF.1.1/ntp

The TSF shall enforce the **NTP SFP** based on the following types of subject and information security attributes:

– **Subjects and their security attributes :**
  - **Encrypted Data Interface**

- **Plaintext Data Interface**

– **Information and their security attributes :**

- **NTP datagram: protocol type, protocol version, source IP address, destination IP address**

FDP_IFF.1.2/ntp

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.Receiving (from Encrypted Data Interface):**

- **The Interface is authorised to receive NTP synchronisation datagram**
- **The source IP address is an authorised NTP server IP address**
- **The NTP datagram is received into an IP datagram corresponding to a SP (Security Policy). That is : the NTP datagram shall come from a remote LAN protected by a remote TOE. The SP can either define a VPN protection or a "bypass" protection.**

– **For the operation OP.Receiving (from Plaintext Data Interface):**

- **The Interface is authorised to receive NTP synchronisation datagram**
- **The source IP address is an authorised NTP server IP address**

FDP_IFF.1.3/ntp

The TSF shall **(refinement) not** enforce **additional rules**.

FDP_IFF.1.4/ntp

The TSF shall explicitly authorise an information flow based on the following rules: **none**.

FDP_IFF.1.5/ntp

The TSF shall explicitly deny an information flow based on the following rules: **none**.

#### 6.1.4.2.4. TSF Data Default Values

**FMT_MSA.3 - STATIC ATTRIBUTE INITIALISATION**

FMT_MSA.3.1

The TSF shall enforce the **VPN SFP and Keys Injection SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP **(refinement) that is**:

– **Protection mode : IPSec_Tunnel**

– **Key management mode : IPSec_Tunnel**

– **Lifetime of IKE SAs keys : 28800 seconds**

– **Lifetime of IKE Child SAs keys : 3600 seconds**

– **Perfect Secrecy (PFS) mode (for IKE protocol) : activated**

– **List of authorised TOE Management Centre Devices (E.SGC) IP address : 0.0.0.0 / none**

FMT_MSA.3.2

The TSF shall allow **Local Administrator and TOE Management Centre Device** to specify alternative initial values to override the default values when an object or information is created.

## 6.1.5. USERS AND DEVICES

### *6.1.5.1. Roles*

**FMT_SMR.1/USER - SECURITY ROLES**

FMT_SMR.1.1/user

The TSF shall maintain the roles

– **Local Administrator (corresponding to a human user U.LOCAL_ADMINISTRATOR)**.

– **Local Operator (corresponding to a human user U.LOCAL_OPERATOR)**.

FMT_SMR.1.2/user

The TSF shall be able to associate users with roles.

**FMT_SMR.1/DEVICES - SECURITY ROLES**

FMT_SMR.1.1/devices

The TSF shall maintain the roles

– **TOE Management Centre Device (corresponding to a network device E.SGC)**

FMT_SMR.1.2/devices

The TSF shall be able to associate **(refinement) devices** with roles.

### *6.1.5.2. Identification and Authentication*

#### 6.1.5.2.1. TOE Management Centre Device

**FIA_UID.2/SGC - E.SGC IDENTIFICATION BEFORE ANY ACTION**

FIA_UID.2.1/sgc

The TSF shall require each **(refinement) TOE Management Centre Device** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **(refinement) TOE Management Centre Device**.

*Application note :*

*In CC Part 2, FIA_UID targets users. Taking into account TOE operation, the security target refines this component : in this case the user is indeed a network device. The identification of the device is performed through its network address (IP address).*

*Note that no authentication of E.SGC is required nor necessary. Indeed, the E.SGC can access the TOE only through a protected communication channel between the TOE and a remote instance of the TOE (the channel is IPSec, as for user data flow).*

#### 6.1.5.2.2. Users

**FIA_UIA_EXT.1/LOCALMNGT - LOCAL HUMAN USERS TIMING OF AUTHENTICATION**

FIA_UIA_EXT.1.1/localMngt

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the **(refinement) authentication** process:

- Display the warning banner in accordance with FTA_TAB.1
- **equipment (TOE) Start-up**
- **equipment (TOE) Shutdown**
- **Full erasure**
- **Equipment and network interfaces status query**
- **Events viewing**
- **TOE self-test request**

FIA_UIA_EXT.1.2/localMngt

The TSF shall require **(refinement) the Local Administrator and Local Operator** to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that **(refinement) Local Administrator and Local Operator**.

*Application note :*

*This requirement only targets the administrator and the operator performing TOE local management actions. Remote administration actions are performed through the management center which shall require user authentication at its level.*

**FIA_UAU_EXT.2/LOCALMNGT - EXTENDED : PASSWORD-BASED AUTHENTICATION MECHANISM**

FIA_UAU_EXT.2.1/localMngt

The TSF shall provide a local password-based authentication mechanism, **(refinement)** to perform **(refinement) Local Administrator and Local Operator** authentication.

**FIA_UAU.6/LOCALMNGT - RE-AUTHENTICATING**

FIA_UAU.6.1/localMngt

The TSF shall re-authenticate the **(refinement) Local Administrator or Local Operator when he changes his password**.

**FIA_UAU.7/LOCALMNGT - PROTECTED AUTHENTICATION FEEDBACK**

FIA_UAU.7.1/localMngt

The TSF shall provide only obscured feedback to the **(refinement) Local Administrator and Local Operator** while the authentication is in progress at the local console.

**FIA_AFL.1/LOCALMNGT - AUTHENTICATION FAILURE HANDLING**

FIA_AFL.1.1/localMngt

The TSF shall detect when **three (3)** unsuccessful successive authentication attempts occur related to **the user authentication functionality**.

FIA_AFL.1.2/localMngt

When the defined number of unsuccessful successive authentication attempts has been **met**, the TSF shall :

- **Send an alert message (FAU_SEG.1)**
- **Lock the authentication functionality for 3 minutes**
- **After the locking time, authentication functionality the TSF shall unlock the authentication functionality : the user can try again to log on (FIA_AFL.1.1)**.

**FIA_PMG_EXT.1/LOCALMNGT - PASSWORD MANAGEMENT**

FIA_PMG_EXT.1.1/localMngt

The TSF shall provide the following password management capabilities for **(refinement) Local Administrator and Local Operator** passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")**", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "[", "\", "]", "_", "{", "|", and "}"**;
- **(refinement) Password length shall be** of **(refinement) 8** characters or greater;
- **(refinement) Password is composed with at least 1 upper case letter, 1 lower case letter, 1 number and 1 special character;**

### *6.1.5.3. Local Management Sessions*

**FTA_SSL_EXT.1/LOCALMNGT - TSF-INITIATED SESSION LOCKING**

FTA_SSL_EXT.1.1/localMngt

The TSF shall, for local interactive session **terminate the session** after **(refinement) three (3) minutes of user inactivity**.

**FTA_SSL.4/LOCALMNGT - USER-INITIATED TERMINATION**

FTA_SSL.4.1/localMngt

The TSF shall allow **(refinement) Local Administrator and Local Operator**-initiated termination of the **(refinement) (respectively) Local Administrator's and Local Operator**'s own interactive session.

**FTA_TAB.1/LOCALMNGT - DEFAULT TOE ACCESS BANNERS**

FTA_TAB.1.1/localMngt

Before establishing a **(refinement) Local Administrator and Local Operator** user session, the TSF shall display **(refinement) a security specified** advisory **(refinement) notice and consent** warning message regarding unauthorised use of the TOE.

### 6.1.6. 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 (TSF Software upgrade)**
- **Ability to configure the cryptographic functionality**
- **TOE Supervision**

**FMT_MOF.1/LOCALMNGT - MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR**

FMT_MOF.1.1/localMngt

The TSF shall restrict the ability to **disable and enable** the functions **Local Operator role** to **TOE Management Centre Device**.

*Application note :*

*Disabling Local Operator role means that no user can log on the TOE as an operator.*

**FMT_MTD.1/QUERY - MANAGEMENT OF TSF DATA (CONFIGURATION AND STATUS VIEWING)**

FMT_MTD.1.1/query

The TSF shall restrict the ability to **query** the **TSF configuration and the TOE status, that is the following data:**

- **D.SECURITY_POLICIES**
- **D.CONFIG_PARAM**
- **D.TIME_BASE**

to **Local Administrator, to Local Operator and to TOE Management Centre Device**.

**FMT_MTD.1/SUPERVISION - MANAGEMENT OF TSF DATA (SUPERVISION)**

FMT_MTD.1.1/supervision

The TSF shall restrict the ability to **query** the **TSF supervision data, that is the following data:**

- **D.SUPERVISION_DATA**

to **Local Administrator and TOE Management Centre Device**.

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

FPT_SKP_EXT.1.1

The TSF shall prevent reading all pre-shared keys, symmetric keys, private keys **(refinement) that is:**

- **D.CRYPTO_KEYS**
- **D.IKE_SAs_CRYPTO_KEYS**
- **D.DISTRIB_SAs_CRYPTO_KEYS**

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

FMT_MTD.1.1/configuration

The TSF shall restrict the ability to **modify** the **TSF configuration, that is the following data:**

- **D.SECURITY_POLICIES**
- **D.CONFIG_PARAM**

to **TOE Management Centre Device**.

**FMT_MTD.1/DATETIME - MANAGEMENT OF TSF DATA (DATE AND TIME MODIFICATION)**

FMT_MTD.1.1/dateTime

The TSF shall restrict the ability to **modify** the **TSF date and time, that is the following data:**

- **D.TIME_BASE**

to **Local Administrator and TOE Management Centre Device**.

**FMT_MTD.1/KEYS - MANAGEMENT OF TSF DATA (KEYS INJECTION)**

FMT_MTD.1.1/keys

The TSF shall restrict the ability to **modify the value of (i.e. to inject)** the **keys**

- **D.CRYPTO_KEYS**

to **Local Administrator and to TOE Management centre device**

.

**FMT_MTD.1/KEYLIFETIME - MANAGEMENT OF TSF DATA (KEY LIFETIME)**

FMT_MTD.1.1/keyLifetime

The TSF shall restrict the ability to **modify** the **following key lifetimes:**

- **IKE SA keys' lifetime**
- **IKE Child SAs keys' lifetime**
- **Distributed PSK and derivated keys' lifetime for distributed mode**

to **Local Administrator**.

**FMT_MTD.1/ADMINPWD - MANAGEMENT OF TSF DATA (LOCAL ADMINISTRATOR PASSWORD)**

FMT_MTD.1.1/adminPwd

The TSF shall restrict the ability to **modify** the **password of the Local Administrator** to **Local Administrator**.

**FMT_MTD.1/OPEPWD - MANAGEMENT OF TSF DATA (LOCAL OPERATOR PASSWORD)**

FMT_MTD.1.1/opePwd

The TSF shall restrict the ability to **modify** the p**assword of the Local Operator** to **Local Administrator and Local Operator**.

**FMT_MTD.1/SOFTWARE - MANAGEMENT OF TSF DATA (SOFTWARE UPDATE)**

FMT_MTD.1.1/software

The TSF shall restrict the ability to **update** the **TOE software (D.SOFTWARES)** to **Local Administrator and Management centre device**.

**FPT_TUD_EXT.1/SOFTWARE - EXTENDED : TRUSTED UPDATE**

FPT_TUD_EXT.1.1/software

The TSF shall provide **(refinement) Local Administrator, Local Operator and TOE Management Centre Device** the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2/software

The TSF shall provide **(refinement) Local Administrator and TOE Management Centre Device** the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3/software

The TSF shall provide a means to verify firmware/software updates to the TOE using a **digital signature mechanism** prior to installing those updates.

**FPT_APW_EXT.1 - EXTENDED: PROTECTION OF 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.

### 6.1.7. MISCELLANEOUS

**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.1 - TSF TESTING**

FPT_TST.1.1

The TSF shall run a suite of self tests **during initial start-up and at the request of the authorised user** to demonstrate the correct operation of **following parts of the TSF:**

– **All cryptographic operations (all FCS_COP.1 requirements)**

– **Hardware parts used by the TSF : RAM, network interfaces, …**

FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of

– **D.SECURITY_POLICIES**

– **D.CONFIG_PARAM**

– **D.CRYPTO_KEYS**

– **D.AUTHENTICATION_DATA**

FPT_TST.1.3

The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code**.

*Application note :*

*FPT_TST.1.2 shall be implemented using keyed-cryptographic mechanisms.*

*FPT_TST.1.3 shall be implemented using cryptographic mechanisms, not necessarely keyed-mechanisms (such as digest calculation).*

**FPT_SDP_EXT.2 - STORED TSF DATA PROTECTION CAPABILITY AND ACTION**

FPT_SDP_EXT.2.1

The TSF shall protect

– **D.SECURITY_POLICIES**

– **D.CONFIG_PARAM**

– **D.CRYPTO_KEYS**

– **D.AUTHENTICATION_DATA**

stored in containers controlled by the TSF from **disclosure** and shall detect **integrity errors** on those data **(refinement) using FCS_COP.1/aes-gcmLocalData**.

FPT_SDP_EXT.2.2

Upon detection of a data integrity error, the TSF shall

– **generate an event (FAU_GEN.1),**

– **and preserve a secure state (FPT_FLS.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 **deallocation of the resource from** all objects.

*Application note :*

*"Resources" in the context of this requirement are network packets being sent through (as opposed to "to", as is the case when an administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet.*

## 6.2. 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:

– ADV_ARC.1

– ADV_FSP.3

– ADV_TDS.2

– AGD_OPE.1

– AGD_PRE.1

– ALC_CMC.3

– ALC_CMS.3

– ALC_DEL.1

– ALC_DVS.1

– ALC_FLR.3

– ALC_LCD.1

– ASE_CCL.1

– ASE_ECD.1

– ASE_INT.1

– ASE_OBJ.2

– ASE_REQ.2

– ASE_SPD.1

– ASE_TSS.1

– ATE_COV.2

– ATE_DPT.1

– ATE_FUN.1

– ATE_IND.2

– AVA_VAN.3

## 6.3. RATIONALE FOR THE SECURITY REQUIREMENTS

### 6.3.1. RATIONALE FOR THE SECURITY FUNCTIONAL REQUIREMENTS

#### *6.3.1.1. Security Objectives for the TOE*

**O.PROTECTED_COMMUNICATIONS**

This security objective is covered in one hand by the security requirements **FTP_ITC.1/TOE**, **FDP_UCT.1/TOE** and **FDP_UIT.1/TOE** 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.

In another hand, the security objective is covered by **FCS_IPS_EXT.1** which requires the trusted channel to implement IPSec and IKE.

Finally the security objective is covered by all cryptographic operations used by IPSec and IKE, that is : **FCS_COP.1/aes-cbc**, **FCS_COP.1/aes-gcm**, **FCS_COP.1/aes-xcbc**, **FCS_COP.1/hmac, FCS_COP.1/hmacTrunc and FCS_COP.1/prf-sha**.

**O.POL_ENFORCEMENT**

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/VPN**, 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.FLOW_PARTITIONING**

This objective is covered by the VPN enforcement policy (**FDP_IFC.1/VPN**, **FDP_IFF.1/VPN** and **FDP_ETC.2/VPN**), because it controls the sending of IP datagrams on the appropriate subnetworks of private network.

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

**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 an external device), since the TSF does not locally store generated audit records. If the link with this external device is not available, **FAU_STG_EXT.3** requires the TSF to generate a critical security event in order to inform a local user (refer to O.LED).

**O.TIME_BASE**

This objective is covered by the requirement **FPT_STM.1** on one hand, and by **FDP_IFC.1/ntp** and **FDP_IFF.1/ntp** on the other hand..

**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.

If the link with this external device is not available, **FAU_STG_EXT.3** requires the TSF to generate a critical security event in order to inform a local user (refer to O.VISUAL).

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

**O.SUPERVISION**

This objective is covered by **FMT_SMF.1** and **FMT_MTD.1/Supervision**.

**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/keysInjection** and **FDP_IFF.1/keysInjection**.

**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/query**, **FMT_MTD.1/configuration**, **FMT_MTD.1/keys** and **FMT_MTD.1/keyLifetime**.

**O.VISUAL_ALARMS**

This security objective is covered by **FAU_GEN_EXT.3**.

**O.ROLES**

This security objectives is covered by **FMT_SMR.1/user** and **FMT_SMR.1/devices** which respectively define roles for users and roles for devices the TSF shall maintain.

**O.I&A**

This security objective is covered by **FIA_UID.2/sgc** and **FIA_UIA_EXT.1/localMngt** 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/localMngt**).

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

**O.AUTHENTICATION_FAILURE**

This security objective is covered by **FIA_AFL.1/localMngt**.

**O.DISPLAY_BANNER**

This security objective is covered by **FTA_TAB.1/localMngt**.

**O.SESSION_LOCK**

This security objective is covered by **FTA_SSL_EXT.1/localMngt** and **FTA_SSL.4/localMngt**.

**O.MANAGEMENT**

This security objective is covered by **FMT_SMF.1**. All instances of **FMT_MTD.1** (except those about viewing (query) and supervision), **FPT_TUD_EXT.1/software**, **FIA_UAU.6/localMngt** and **FMT_MOF.1/localMngt** provide details on management functionalities.

**O.VIEW**

This security objective is covered by the protection policy of TSF configuration and cryptographic keys (**FMT_SMF.1**, **FMT_MDT.1/query**, **FMT_SKP_EXT.1**, **FPT_TUD_EXT.1/software**) by controlling their access to the action allowing review.

**O.POL_VIEW**

This security objective is covered by the protection policy of VPN security policies (**FMT_MTD.1/query**) by controlling access to the action allowing review of VPN security policies and of their contexts.

**O.RESIDUAL_INFORMATION_CLEAR**

This security objective is covered by **FDP_RIP.2**.

**O.DATA_ERASURE**

This security objective is covered by **FPT_SIE_EXT.1/allPlainTextData**. **FCS_CKM_EXT.4/anyPlainTextData** gives the method of erasure.

**O.LOCAL_DATA_PROTECTION**

This security objective is covered by **FPT_SDP_EXT.2** and cryptography operation **FCS_COP.1/aes-gcmLocalData**.

**O.SOFTWARE_UPDATES**

This security objective is covered by **FPT_TUD_EXT.1/software** and cryptography operation **FCS_COP.1/aes-cbcSw**, **FCS_COP.1/aes-xcbcSw** and **FCS_COP.1/ecdsaSw**.

**O.KEYS_INJECTION**

This objective is covered by the keys injection policy (**FDP_IFC.1/keysInjection**, **FDP_IFF.1/keysInjection**, **FDP_ITC.2/pskIKE, and FDP_ITC.2/pskDistribMode**) which controls keys flows of keys injection. In addition, **FDP_UCT.1/keysInjection** and **FDP_UIT.1/keysInjection** ensure the integrity of all keys and the confidentiality of secret keys during their transmission.

**FMT_MSA.3** supports FDP_IFF.1/keysInjection, providing default values.

**FPT_TDC.1/keysInjection** supports FDP_ITC.2/pskIKE and FDP_ITC.2/pskDistribMode, providing data consistency check.

**O.CRYPTOPERIOD**

This security objective is covered by all instances of **FCS_CKM_EXT.5** security requirements.

**O.CRYPTO_REGULATION**

This objective is covered by requirements concerning cryptographic keys and cryptographic operations: **FCS_RBG_EXT.1**, **FCS_CKM.3/keyRenewal**, **FCS_CKM.4/anyPlainTextData**, and all instances of **FCS_COP.1**.

**O.SELF_TEST**

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

### 6.3.2. TABLES

| Security objectives | SFR |
|---|---|
| O.PROTECTED_COMMUNICATIONS | FCS_COP.1/aes-cbc<br>FDP_UCT.1/TOE<br>FDP_UIT.1/TOE<br>FTP_ITC.1/TOE<br>FCS_COP.1/aes-xcbc<br>FCS_COP.1/aes-gcm<br>FCS_COP.1/hmac<br>FCS_COP.1/hmacTrunc<br>FCS_IPS_EXT.1<br>FCS_COP.1/prf-sha |
| O.POL_ENFORCEMENT | FDP_IFC.1/VPN<br>FDP_IFF.1/VPN<br>FMT_MSA.3<br>FDP_ITC.2/VPN<br>FDP_ETC.2/VPN |

| Security objectives | SFR |
|---|---|
| O.FLOW_PARTITIONING | FDP_IFC.1/VPN<br>FDP_IFF.1/VPN<br>FMT_MSA.3<br>FDP_ETC.2/VPN |
| O.AUDIT | FAU_GEN.1<br>FAU_GEN.2<br>FAU_STG_EXT.1<br>FAU_STG_EXT.3 |
| O.TIME_BASE | FPT_STM.1<br>FDP_IFC.1/ntp<br>FDP_IFF.1/ntp |
| O.AUDIT_PROTECTION | FDP_UCT.1/TOE<br>FDP_UIT.1/TOE<br>FAU_STG_EXT.1<br>FAU_STG_EXT.3<br>FTP_ITC.1/TOE<br>FCS_IPS_EXT.1 |
| O.SUPERVISION | FMT_SMF.1<br>FMT_MTD.1/supervision |
| O.SUPERVISION_IMPACT | FDP_IFC.1/VPN<br>FDP_IFF.1/VPN<br>FMT_MSA.3<br>FMT_MTD.1/query<br>FMT_MTD.1/configuration<br>FMT_MTD.1/keys<br>FMT_MTD.1/keyLifetime<br>FDP_IFC.1/keysInjection<br>FDP_IFF.1/keysInjection |
| O.VISUAL_ALARMS | FAU_GEN_EXT.3 |
| O.ROLES | FMT_SMR.1/user<br>FMT_SMR.1/devices |
| O.I&A | FIA_PMG_EXT.1/localMngt<br>FIA_UIA_EXT.1/localMngt<br>FIA_UID.2/sgc<br>FIA_UAU.7/localMngt<br>FIA_UAU_EXT.2/localMngt<br>FPT_APW_EXT.1 |
| O.AUTHENTICATION_FAILURE | FIA_AFL.1/localMngt |
| O.DISPLAY_BANNER | FTA_TAB.1/localMngt |

| Security objectives | SFR |
|---|---|
| O.SESSION_LOCK | FTA_SSL_EXT.1/localMngt<br>FTA_SSL.4/localMngt |
| O.MANAGEMENT | FIA_UAU.6/localMngt<br>FMT_SMF.1<br>FMT_MOF.1/localMngt<br>FMT_MTD.1/configuration<br>FMT_MTD.1/keys<br>FMT_MTD.1/adminPwd<br>FMT_MTD.1/software<br>FPT_TUD_EXT.1/software<br>FMT_MTD.1/keyLifetime<br>FMT_MTD.1/opePwd<br>FMT_MTD.1/dateTime |
| O.VIEW | FMT_SMF.1<br>FMT_MTD.1/query<br>FPT_SKP_EXT.1<br>FPT_TUD_EXT.1/software |
| O.POL_VIEW | FMT_MTD.1/query |
| O.RESIDUAL_INFORMATION_CLEAR | FDP_RIP.2 |
| O.DATA_ERASURE | FCS_CKM_EXT.4/anyPlainTextData<br>FPT_SIE_EXT.1/allPlainTextData |
| O.LOCAL_DATA_PROTECTION | FPT_SDP_EXT.2<br>FCS_COP.1/aes-gcmLocalData |
| O.SOFTWARE_UPDATES | FCS_COP.1/ecdsaSw<br>FPT_TUD_EXT.1/software<br>FCS_COP.1/aes-cbcSw<br>FCS_COP.1/aes-xcbcSw |
| O.KEYS_INJECTION | FDP_ITC.2/pskDistribmode<br>FMT_MSA.3<br>FDP_ITC.2/pskIKE<br>FDP_UCT.1/keysInjection<br>FDP_UIT.1/keysInjection<br>FDP_IFC.1/keysInjection<br>FDP_IFF.1/keysInjection<br>FPT_TDC.1/keysInjection |
| O.CRYPTOPERIOD | FCS_CKM_EXT.5/pskDistribMode<br>FCS_CKM_EXT.5/deriv-pskDistribMode<br>FCS_CKM_EXT.5/ikeV2childSA<br>FCS_CKM_EXT.5/ikeV2SA<br>FCS_CKM_EXT.5/pskIKE |

| Security objectives | SFR |
|---|---|
| O.CRYPTO_REGULATION | FCS_CKM_EXT.4/anyPlainTextData<br>FCS_COP.1/aes-cbc<br>FCS_RBG_EXT.1<br>FCS_COP.1/ecdsaSw<br>FCS_CKM.3/keyRenewal<br>FCS_COP.1/aes-xcbc<br>FCS_COP.1/aes-gcm<br>FCS_COP.1/sha<br>FCS_COP.1/hmac<br>FCS_COP.1/hmacTrunc<br>FCS_COP.1/prf-sha<br>FCS_COP.1/aes-cbcSw<br>FCS_COP.1/aes-xcbcSw<br>FCS_COP.1/aes-gcmLocalData |
| O.SELF_TEST | FPT_FLS.1<br>FPT_TST.1 |

### 6.3.3. 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.

### 6.3.4. AVA_VAN.3 FOCUSED VULNERABILITY ANALYSIS

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

### 6.3.5. ALC_FLR.3 SYSTEMATIC FLAW REMEDIATION

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

### 6.3.6. DEPENDENCIES

#### *6.3.6.1. Dependencies for the Security Functional Requirements*

| SFR | CC dependencies | Satisfied dependencies |
|---|---|---|
| FAU_GEN.1 | (FPT_STM.1) | FPT_STM.1 |

| SFR | CC dependencies | Satisfied dependencies |
|---|---|---|
| FAU_GEN.2 | (FAU_GEN.1)<br>et (FIA_UID.1) | FAU_GEN.1<br>FIA_UIA_EXT.1/localMngt<br>FIA_UID.2/sgc |
| FAU_GEN_EXT.3 | (FAU_GEN.1) | FAU_GEN.1 |
| FAU_STG_EXT.1 | (FAU_GEN.1)<br>et (FTP_ITC.1) | FAU_GEN.1<br>FTP_ITC.1/TOE |
| FAU_STG_EXT.3 | FAU_STG_EXT.1 | FAU_STG_EXT.1 |
| FPT_STM.1 | No dependencies. | |
| FCS_RBG_EXT.1 | No dependencies. | |
| FCS_CKM.3/keyRenewal | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FCS_RBG_EXT.1<br>FDP_ITC.2/pskDistribmode<br>FDP_ITC.2/pskIKE |
| FCS_CKM_EXT.4/anyPlainTextData | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) | FDP_ITC.2/pskDistribmode<br>FCS_RBG_EXT.1<br>FDP_ITC.2/pskIKE |
| FCS_CKM_EXT.5/pskDistribMode | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM_EXT.4)<br>et (FPT_STM.1) | FPT_STM.1<br>FCS_CKM_EXT.4/anyPlainTextData<br>FDP_ITC.2/pskDistribmode |
| FCS_CKM_EXT.5/deriv-pskDistribMode | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM_EXT.4)<br>et (FPT_STM.1) | FPT_STM.1<br>FCS_CKM_EXT.4/anyPlainTextData |
| FCS_CKM_EXT.5/pskIKE | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4)<br>et (FPT_STM.1) | FPT_STM.1<br>FCS_CKM_EXT.4/anyPlainTextData<br>FDP_ITC.2/pskIKE |
| FCS_CKM_EXT.5/ikeV2SA | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4)<br>et (FPT_STM.1) | FPT_STM.1<br>FCS_CKM_EXT.4/anyPlainTextData<br>FCS_IPS_EXT.1 |
| FCS_CKM_EXT.5/ikeV2childSA | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4)<br>et (FPT_STM.1) | FPT_STM.1<br>FCS_CKM_EXT.4/anyPlainTextData<br>FCS_IPS_EXT.1 |
| FPT_SIE_EXT.1/allPlainTextData | No dependencies. | |
| FCS_COP.1/aes-cbc | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FCS_IPS_EXT.1 |
| FCS_COP.1/aes-gcm | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FCS_IPS_EXT.1 |
| FCS_COP.1/aes-xcbc | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FCS_IPS_EXT.1 |
| FCS_COP.1/aes-cbcSw | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)<br>et (FCS_CKM.4) | FPT_TUD_EXT.1/software |

| SFR | CC dependencies | Satisfied dependencies |
|---|---|---|
| FCS_COP.1/aes-xcbcSw | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4) | FPT_TUD_EXT.1/software |
| FCS_COP.1/ecdsaSw | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4) | FPT_TUD_EXT.1/software |
| FCS_COP.1/aes-gcmLocalData | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FCS_RBG_EXT.1 |
| FCS_COP.1/sha | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4) | |
| FCS_COP.1/hmac | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FDP_ITC.2/pskDistribmode<br>FCS_RBG_EXT.1<br>FDP_ITC.2/pskIKE |
| FCS_COP.1/hmacTrunc | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FDP_ITC.2/pskDistribmode<br>FCS_RBG_EXT.1<br>FDP_ITC.2/pskIKE |
| FCS_COP.1/prf-sha | (FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4) | FCS_CKM_EXT.4/anyPlainTextData<br>FDP_ITC.2/pskDistribmode<br>FDP_ITC.2/pskIKE |
| FTP_ITC.1/TOE | No dependencies. | |
| FDP_UCT.1/TOE | (FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1) | FDP_IFC.1/VPN<br>FTP_ITC.1/TOE |
| FDP_UIT.1/TOE | (FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1) | FDP_IFC.1/VPN<br>FTP_ITC.1/TOE |
| FCS_IPS_EXT.1 | (FDP_ITC.1)<br>et (FCS_COP.1) | FCS_COP.1/aes-cbc<br>FDP_ITC.2/pskDistribmode<br>FCS_COP.1/aes-xcbc<br>FCS_COP.1/aes-gcm<br>FCS_COP.1/sha<br>FCS_COP.1/hmac<br>FCS_COP.1/hmacTrunc<br>FCS_COP.1/prf-sha<br>FDP_ITC.2/pskIKE |
| 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 |
| FDP_ETC.2/VPN | (FDP_ACC.1 or FDP_IFC.1) | FDP_IFC.1/VPN |

| SFR | CC dependencies | Satisfied dependencies |
|---|---|---|
| FDP_IFC.1/VPN | (FDP_IFF.1) | FDP_IFF.1/VPN |
| FDP_IFF.1/VPN | (FDP_IFC.1) et (FMT_MSA.3) | FDP_IFC.1/VPN<br>FMT_MSA.3 |
| FDP_ITC.2/pskDistribmode | (FDP_ACC.1 or<br>FDP_IFC.1)<br>and (FTP_ITC.1 or<br>FTP_TRP.1)<br>and (FPT_TDC.1) | FTP_ITC.1/TOE<br>FDP_IFC.1/keysInjection<br>FPT_TDC.1/keysInjection |
| FDP_ITC.2/pskIKE | (FDP_ACC.1 or<br>FDP_IFC.1)<br>and (FTP_ITC.1 or<br>FTP_TRP.1)<br>and (FPT_TDC.1) | FTP_ITC.1/TOE<br>FDP_IFC.1/keysInjection<br>FPT_TDC.1/keysInjection |
| FDP_UCT.1/keysInjection | (FDP_ACC.1 ou FDP_IFC.1)<br>et (FTP_ITC.1 ou FTP_TRP.1) | FDP_ITC.2/pskDistribmode<br>FDP_ITC.2/pskIKE<br>FDP_IFC.1/keysInjection |
| FDP_UIT.1/keysInjection | (FDP_ACC.1 ou FDP_IFC.1)<br>et (FTP_ITC.1 ou FTP_TRP.1) | FDP_ITC.2/pskDistribmode<br>FDP_ITC.2/pskIKE<br>FDP_IFC.1/keysInjection |
| FDP_IFC.1/keysInjection | (FDP_IFF.1) | FDP_IFF.1/keysInjection |
| FDP_IFF.1/keysInjection | (FDP_IFC.1) et (FMT_MSA.3) | FMT_MSA.3<br>FDP_IFC.1/keysInjection |
| FPT_TDC.1/keysInjection | No dependencies. | |
| FDP_IFC.1/ntp | (FDP_IFF.1) | FDP_IFF.1/ntp |
| FDP_IFF.1/ntp | (FDP_IFC.1) et (FMT_MSA.3) | FMT_MSA.3<br>FDP_IFC.1/ntp |
| FMT_MSA.3 | (FMT_MSA.1)<br>et (FMT_SMR.1) | |
| FMT_SMR.1/user | (FIA_UID.1) | FIA_UIA_EXT.1/localMngt |
| FMT_SMR.1/devices | (FIA_UID.1) | FIA_UID.2/sgc |
| FIA_UID.2/sgc | No dependencies. | |
| FIA_UIA_EXT.1/localMngt | (FTA_TAB.1) | FTA_TAB.1/localMngt |
| FIA_UAU_EXT.2/localMngt | No dependencies. | |
| FIA_UAU.6/localMngt | No dependencies. | |
| FIA_UAU.7/localMngt | (FIA_UAU.1) | FIA_UIA_EXT.1/localMngt |
| FIA_AFL.1/localMngt | (FIA_UAU.1) | FIA_UIA_EXT.1/localMngt |
| FIA_PMG_EXT.1/localMngt | No dependencies. | |
| FTA_SSL_EXT.1/localMngt | No dependencies. | |
| FTA_SSL.4/localMngt | No dependencies. | |
| FTA_TAB.1/localMngt | No dependencies. | |

| SFR | CC dependencies | Satisfied dependencies |
|---|---|---|
| FMT_SMF.1 | No dependencies. | |
| FMT_MOF.1/localMngt | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMF.1<br>FMT_SMR.1/devices |
| FMT_MTD.1/query | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1<br>FMT_SMR.1/devices |
| FMT_MTD.1/supervision | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1<br>FMT_SMR.1/devices |
| FPT_SKP_EXT.1 | No dependencies. | |
| FMT_MTD.1/configuration | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1<br>FMT_SMR.1/devices |
| FMT_MTD.1/dateTime | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1<br>FMT_SMR.1/devices |
| FMT_MTD.1/keys | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1<br>FMT_SMR.1/devices |
| FMT_MTD.1/keyLifetime | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1<br>FMT_SMR.1/devices |
| FMT_MTD.1/adminPwd | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1 |
| FMT_MTD.1/opePwd | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1 |
| FMT_MTD.1/software | (FMT_SMF.1)<br>et (FMT_SMR.1) | FMT_SMR.1/user<br>FMT_SMF.1 |
| FPT_TUD_EXT.1/software | (FCS_COP.1) | FCS_COP.1/ecdsaSw |
| FPT_APW_EXT.1 | No dependencies. | |
| FPT_FLS.1 | No dependencies. | |
| FPT_TST.1 | No dependencies. | |
| FPT_SDP_EXT.2 | No dependencies. | |
| FDP_RIP.2 | No dependencies. | |

#### 6.3.6.1.1. Rationale for the Unsatisfied Dependencies

| SFR | SFR unsatisfied dependencies |
|---|---|
| FCS_CKM_EXT.5/ikeV2SA | **FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2 dependency of FCS_CKM_EXT.5/ikeV2SA is unsatisfied,** because it is replaced by FCS_IPS_EXT.1 because cryptographic key generation is done during the IKE negociation key phase. |

| SFR | SFR unsatisfied dependencies |
|---|---|
| FCS_CKM_EXT.5/ikeV2childSA | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_CKM_EXT.5/ikeV2childSA is unsatisfied,** because it is replaced by FCS_IPS_EXT.1 because cryptographic key generation is done during the IKE negociation key phase. |
| FCS_CKM_EXT.5/deriv-pskDistribMode | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_CKM_EXT.5/deriv-pskDistribMode unsatisfied,** because cryptographic key generation is done by derivation of the distributed mode PSK . |
| FCS_COP.1/aes-cbc | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_COP.1/aes-cbc is unsatisfied,** because it is replaced by FCS_IPS_EXT.1 because cryptographic keys are negotiated via IKE protocol. |
| FCS_COP.1/aes-xcbc | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_COP.1/aes-xcbc is unsatisfied,** because it is replaced by FCS_IPS_EXT.1 because cryptographic keys are negotiated via IKE protocol. |
| FCS_COP.1/aes-cbcSw | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_COP.1/aes-cbcSw is unsatisfied,** because it is replaced by the software update itself (FPT_TUD_EXT.1/software) : cryptographic keys are renewed during this operation.<br>**FCS_CKM_EXT.4 dependency of FCS_COP.1/aes-cbcSw is unsatisfied,** because no emergency erasing of software update keys is performed out of the software update itself. |
| FCS_COP.1/aes-xcbcSw | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_COP.1/aes-xcbcSw is unsatisfied,** because it is replaced by the software update itself (FPT_TUD_EXT.1/software) : cryptographic keys are renewed during this operation.<br>**FCS_CKM_EXT.4 dependency of FCS_COP.1/aes-xcbcSw is unsatisfied,** because no emergency erasing of software update keys is performed out of the software update itself. |
| FCS_COP.1/ecdsaSw | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_COP.1/ecdsaSw is unsatisfied,** because it is replaced by the software update itself (FPT_TUD_EXT.1/software) : cryptographic keys are renwed during this operation.<br>**FCS_CKM_EXT.4 dependency of FCS_COP.1/ecdsaSw is unsatisfied**, because no emergency erasing of software update keys is performed out of the software update itself. |
| FCS_COP.1/aes-gcmLocalData | **FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 dependency of FCS_COP.1/aes-gcmLocalData is unsatisfied,** because it is replaced by FCS_RBG_EXT.1 which randomly generates the local data protection key. |
| FCS_COP.1/sha | **FCS_COP.1/sha dependencies are unsatsified,** because SHA cryptographic function does not require use of cryptographic keys. |
| FCS_IPS_EXT.1 | **FDP_ITC.1 dependency of FCS_IPS_EXT.1 is unsatisfied,** because it is replaced by FDP_ITC.2/pskIKE and FDP_ITC.2/pskDistribmode which offers better protection during import of user data. |
| FMT_MSA.3 | **FMT_MSA.1 and FMT_SMR.1 dependencies of FMT_MSA.3 are unsatisfied,** because default settings values cannot be modified. |
| FMT_SMR.1/user | **FIA_UID.1 dependency of FMT_SMR.1/user is unsatisfied,** because it is replaced by FIA_UIA_EXT.1/localMngt dependency. |
| FIA_UAU.7/localMngt | **FIA_UAU.1 dependency of FIA_UAU.7/localMngt is unsatisfied,** because it is replaced by the extended component FIA_UIA_EXT.1/localMngt. |
| FIA_AFL.1/localMngt | **FIA_UAU.1 dependency of FIA_AFL.1/localMngt is unsatisfied**, because it is replaced by the extended component FIA_UIA_EXT.1/localMngt. |

### *6.3.6.2. Dependencies for the Security Assurance Requirements*

| SAR | CC dependencies | Satisfied dependencies |
|---|---|---|
| ADV_ARC.1 | (ADV_FSP.1)<br>et (ADV_TDS.1) | ADV_FSP.3<br>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 |

| SAR | CC dependencies | Satisfied dependencies |
|---|---|---|
| AGD_PRE.1 | No dependencies. | |
| ALC_CMC.3 | (ALC_CMS.1)<br>et (ALC_DVS.1)<br>et (ALC_LCD.1) | ALC_CMS.3<br>ALC_DVS.1<br>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)<br>et (ASE_INT.1)<br>et (ASE_REQ.1) | ASE_ECD.1<br>ASE_INT.1<br>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)<br>et (ASE_OBJ.2) | ASE_ECD.1<br>ASE_OBJ.2 |
| ASE_SPD.1 | No dependencies. | |
| ASE_TSS.1 | (ADV_FSP.1)<br>et (ASE_INT.1)<br>et (ASE_REQ.1) | ADV_FSP.3<br>ASE_INT.1<br>ASE_REQ.2 |
| ATE_COV.2 | (ADV_FSP.2)<br>et (ATE_FUN.1) | ADV_FSP.3<br>ATE_FUN.1 |
| ATE_DPT.1 | (ADV_ARC.1)<br>et (ADV_TDS.2)<br>et (ATE_FUN.1) | ADV_ARC.1<br>ADV_TDS.2<br>ATE_FUN.1 |
| ATE_FUN.1 | (ATE_COV.1) | ATE_COV.2 |
| ATE_IND.2 | (ADV_FSP.2)<br>et (AGD_OPE.1)<br>et (AGD_PRE.1)<br>et (ATE_COV.1)<br>et (ATE_FUN.1) | ADV_FSP.3<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_COV.2<br>ATE_FUN.1 |
| AVA_VAN.3 | (ADV_ARC.1)<br>et (ADV_FSP.4)<br>et (ADV_IMP.1)<br>et (ADV_TDS.3)<br>et (AGD_OPE.1)<br>et (AGD_PRE.1)<br>et (ATE_DPT.1) | ADV_ARC.1<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_DPT.1 |

#### 6.3.6.2.1. Rationale for the Unsatisfied Dependencies

**The dependency ADV_IMP.1 of AVA_VAN.3 is not satisfied.** The dependency ADV_IMP.1 is not satisfied as required by the "Standard" assurance level of the ANSSI "Qualification" process.

**The dependency ADV_TDS.3 of AVA_VAN.3 is not satisfied.** The dependency ADV_TDS.3 is not satisfied as required by the "Standard" assurance level of the ANSSI "Qualification" process.

**The dependency ADV_FSP.4 of AVA_VAN.3 is not satisfied.** The dependency ADV_FSP.4 is not satisfied as required by the "Standard" assurance level of the ANSSI "Qualification" process.

# 7. TOE SUMMARY SPECIFICATIONS

## 7.1. SECURITY FUNCTIONS

**F.AUDIT AND EVENTS LOGGING**

Definitions :

An **event** is the result of known/specified action in the Mistral system. An event has a unique type and a Syslog kind severity level. The type is not a sequence number.

There is a special event kind named **alarm**. An alarm is an event with a severity level strictly superior to the 4th syslog level: Warning.

Actions performed after each event analysis depend on the equipment state machine.

Same alarms can produce a **LED blinking**. This functionality is a user configurable global parameter.

Using :

Events are written in a local file based on **Syslog** format to allow the viewing of past actions history and detected problems. This file can be distant in case of remote manageable equipment.

Alarms are logged in the event file and can be sent to the Command Line Interface and sent to Management Centre Devices. Events log file is different from the Syslog files managed by the OS but the Syslog presentation format is used to store events and alarms.

An **alarm filter** is provided to prevent flooding of a single alarm such as anti-replay or bad decryption alarms.

**F. STORAGE AND PROTECTION OF LOCAL DATA**

Definitions :

Data can be gathered in 2 groups:

**Permanent data** : saved in the non volatile memory of the encryptors between two starts.

**Non permanent data** : not saved after the shutdown or the retsart of the equipment.

Permanent data are divided in the following groups :

**Factory data** : default command line interface user profiles. Not erasable, those data are written in concerned data containers during full erasure.

**Hardware data** : serial numbers and Ethernet addresses. Set once during the equipment manifacturing and not erasable after.

**Network data** : parameters of all network interfaces.

**Security data for remote managemen**t : security rules (Security Association / Security Policies), keys, 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) and password (stored SHA-256 hashed).

**Events log file** : storage of events/alarms detected by the equipment.

Using :

Permanent data groups are stored in logical separated containers in order to modify and supress them independently. During an emergency erasing, containers are erased depending on the erasing type (security user's rules or complete).

Containers are **protected in confidentiality and integrity** with **AES256-GCM** and a **key of 256 bits** length.

At the equipment start permanent parameters are loaded in the running configuration. Those parameters are used and stored in RAM while equipment is running.

When the configuration is changed by a user command, the new parameters can be saved in permanent containers with a special command. It means the saving operation is not mandatory and automatic if the configuration is changed manually by a user on the command line interface.

If a new configuration is pushed by remote management, a secured configuration file or a smart card, the saving in permanent containers is automatic.

**Erasing** of permanent data consists in a **writing of 0 followed by a writing of 1** in the memory spaces concerned.

## F. KEYS MANAGEMENT

Definitions :

**Keys** are used for network flows protection and authentication of counterpart equipments.

Keys using :

There are 3 key types in the Mistral system:

- **Pre-Shared keys** (PSK) : keys given by Mistral management centers and saved between 2 starts;
    - o peer authentication keys when using IKE protocol (negotiated mode),

    - communication channels protection keys when not using IKE protocol (distributed mode)
- **Negociated keys** : dynamic negociated keys by IKEv2. There are not saved between 2 starts.
- **Derivated keys :** temporary keys specified by cryptographic algorithms used to perform ciphering and/or integrity cryptographic primitives for distributed mode.

PSK are stored in the following containers: security data for remote management and security data for user data flows, depending of their final using (remote management or “user flow”).

Used keys are **loaded in the FPGA** when cryptographic operations are hardware ones, **or in RAM** when they are software ones.

Each key have a **lifetime** in number of packets and a lifetime in number of days of using. Those parameters are defined by the management center or manually on the software management interface if the equipment is not manageable remotely.

## F. USERS, CONFIGURATION AND MONITORING

Definitions :

Mistral encryptors are manageable with the **command line interface** or with management centers and allowed stations through the network.

Command interface access is limited with the active user profile.

Equipment monitoring corresponds to configuration check and statistic viewing (network interfaces, operating system, …).

User management :

Command line interface is accessible localy with a **RS232 link**. Users do not have their own account but use a user profile to define the allowed commands.

**"No_User" profile** is a narrowed profile which does not require any authentication. It has only access to a few commands essentially linked to information and statistics viewing : equipment reboot, equipment and network interfaces status, locally-stored events viewing, software version query, self-test query.

**Operator profile** needs a password authentication and is allowed to load secured configuration files but without being able to define parameters manually. He can use more monitoring commands in addition of the user profile ones.

**Administrator profile** needs a password authentication too and gives the user access to all commands. Administrator profile is allowed to configure manually the equipment.

User session termination : it is done by the user, or automatically after 3 minutes of inactivity.

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

Configuration and monitoring :

**Command line interface** lets configuration and monitoring of the Mistral equipments. All parameters are configurable with commands. Parameters can be set individually or imported from a secured file containing all or part of the configuration.

Configuration and monitoring can also be performed by management centers.

**SNMPv2c** protocol is available to view network and system parameters for allowed stations.

Software upgrade :

In the Mistral system software, update can be performed by a user command on the command line interface or through the remote management protocol. The upgrade consists in the download of a single file protected in authentication (SHA512 + ECDSA-521), integrity (AES-XCBC-MAC96) and confidentiality (AES-CBC) called firmware. The firmware contains all software components (bios, OS, FPGA software, main software, …).

After being checked by the current running software of the equipment, the new firmware is written in permanent memory.

Key injection :

PSK are injected in the equipment manually with a secured configuration file (via Command Line Interface, administrator rights needed) or directly by a Mistral Management Center.

Note : the secured configuration file is protected by cryptographic key derivated (through HMAC-SHA-256-128) from a passphrase.

Negociated keys are injected by the IKE service and are directly and only stored in RAM/FPGA.

Time management :

Mistral encryptors have to manage time (event log, …) but don’t have a clock available between two starts. The equipment can manage a default uptime from its starting but need in addition to be synchronized with a trustable time.

There are 2 ways to configure time :

- Manually with a **user command**
- Automatically with a **NTP synchronization**

## F. FILTERING AND PROTECTION OF NETWORK DATA FLOWS

Definitions :

Network frame processing is performed in a component named Commutation. This component is in charge of frame filtering and protection.

Mistral encryptors have one processing mode : bridge mode. In **bridge mode**, encryptors are transparent for IP (IPv4/IPv6) sending and receiving stations. All network interfaces of the equipment share the same IP address.

All incoming and outgoing network flows are analyzed and have a predefined handling. Possible actions for frames are:

**Discard** : the frame is destroyed.

**Bypass** : the frame is allowed to be forwarded without modification on the destination interface.

**Protect** : the frame must be encrypted/decrypted depending on the mode defined in the SA.

**Transmit control** : the frame is allowed to be forwarded to a local management service.

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

Network flow filtering :

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

A blocking/bypass filtering of non IP protocols is also available. For the bridge mode, some frames must be allowed to be forwarded (for example: ARP) to ensure the transparency of encryptors on network segments.

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. This contains at least :

Algorithm and key for **confidentiality protection**

Algorithm and key for **integrity protection**

Encapsulation mode : tunnel

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

If the encryptor receives an **ESP** frame on a plain or 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 modes :

Two modes are available :

- Enhanced Simple (Simple renforcé), **which is outside the scope of the evaluation**
- IPSec Mistral

Those modes define IKE et IPSec algorithms:

- Enhanced Simple
  - IKE protocol (IKE SA) parameters
    - Key exchange : ECDH 384-bit random ECP-group
    - Authentication mode : Preshared key
    - Key derivation : PRF-SHA-384
    - IKE protocol confidentiality algorithm : AES-GCM16 with 256-bits long key
    - IKE protocol integrity algorithm : AES-GCM16 with 256-bits long key
  - IPSec (Child SA) parameters
    - IPSEC protocol confidentiality algorithm : AES-GCM8 with 256-bits long key
    - IPSEC protocol integrity algorithm : AES-GCM8 with 256-bits long key
- IPSec Mistral
  - IKE protocol (IKE SA) parameters
    - Key exchange : ECDH 384-bit random ECP-group
    - Authentication mode : Preshared key
    - Key derivation : PRF-SHA-384
    - IKE protocol confidentiality algorithm : AES-GCM16 with 256-bits long key
    - IKE protocol integrity algorithm : AES-GCM16 with 256-bits long key
  - IPSec (Child SA) parameters
    - IPSEC protocol confidentiality algorithm : AES-CBC with 256-bits long key
    - IPSEC protocol integrity algorithm : AES-XCBC-MAC-96 with 128-bits long key

## F. FAILURE STATE

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

- FPGA access error
- Autotest failure
- Failure of a service start
- Writing memory error

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

**F. AUTOTEST**

At start an autotest is performed with the following tests:

Encryption/decryption of data by the FPGA

Encryption/decryption of data by the cryptographic library

Writing/reading in permanent memory

While the equipment is running and operational a cryptographic autotest is also available.

## 7.2. SFR AND SECURITY FUNCTIONS MAPPING

| SFR | Security functions |
|---|---|
| FAU_GEN.1 | F.Audit and events logging |
| FAU_GEN.2 | F.Audit and events logging |
| FAU_GEN_EXT.3 | F.Audit and events logging |
| FAU_STG_EXT.1 | F.Audit and events logging |
| FAU_STG_EXT.3 | F.Audit and events logging |
| FPT_STM.1 | F. Users, configuration and monitoring |
| FCS_RBG_EXT.1 | F. Storage and protection of local data<br>F. Filtering and protection of network data flows |
| FCS_CKM.3/keyRenewal | F. Keys management<br>F. Filtering and protection of network data flows |
| FCS_CKM_EXT.4/anyPlainTextData | F. Keys management |
| FCS_CKM_EXT.5/pskDistribMode | F. Keys management |
| FCS_CKM_EXT.5/deriv-pskDistribMode | F. Keys management |
| FCS_CKM_EXT.5/psk | F. Keys management |
| FCS_CKM_EXT.5/ikeV2SA | F. Keys management |
| FCS_CKM_EXT.5/ikeV2childSA | F. Keys management |
| FPT_SIE_EXT.1/allPlainTextData | F. Users, configuration and monitoring |
| FCS_COP.1/aes-cbc | F. Filtering and protection of network data flows |
| FCS_COP.1/aes-gcm | F. Filtering and protection of network data flows |
| FCS_COP.1/aes-xcbc | F. Filtering and protection of network data flows |
| FCS_COP.1/aes-cbcSw | F. Users, configuration and monitoring |
| FCS_COP.1/aes-xcbcSw | F. Users, configuration and monitoring |
| FCS_COP.1/ecdsaSw | F. Users, configuration and monitoring |
| FCS_COP.1/aes-gcmLocalData | F. Filtering and protection of network data flows |

| | |
|---|---|
| FCS_COP.1/sha | F. Storage and protection of local data<br>F. Users, configuration and monitoring<br>F. Filtering and protection of network data flows |
| FCS_COP.1/hmac | F. Keys management<br>F. Filtering and protection of network data flows |
| FCS_COP.1/hmacTrunc | F. Users, configuration and monitoring |
| FCS_COP.1/prf-sha | F. Keys management |
| FTP_ITC.1/TOE | F. Filtering and protection of network data flows |
| FDP_UCT.1/TOE | F. Filtering and protection of network data flows |
| FDP_UIT.1/TOE | F. Filtering and protection of network data flows |
| FCS_IPS_EXT.1 | F. Keys management<br>F. Filtering and protection of network data flows |
| FDP_ITC.2/VPN | F. Filtering and protection of network data flows |
| FDP_ETC.2/VPN | F. Filtering and protection of network data flows |
| FDP_IFC.1/VPN | F. Filtering and protection of network data flows |
| FDP_IFF.1/VPN | F. Filtering and protection of network data flows |
| FDP_ITC.2/pskDistribmode | F. Users, configuration and monitoring |
| FDP_ITC.2/pskIKE | F. Users, configuration and monitoring |
| FDP_UCT.1/keysInjection | F. Users, configuration and monitoring |
| FDP_UIT.1/keysInjection | F. Users, configuration and monitoring |
| FDP_IFC.1/keysInjection | F. Users, configuration and monitoring |
| FDP_IFF.1/keysInjection | F. Users, configuration and monitoring |
| FPT_TDC.1/keysInjection | F. Users, configuration and monitoring |
| FDP_IFC.1/ntp | F. Users, configuration and monitoring |
| FDP_IFF.1/ntp | F. Users, configuration and monitoring |
| FMT_MSA.3 | F. Users, configuration and monitoring |
| FMT_SMR.1/user | F. Users, configuration and monitoring |
| FMT_SMR.1/devices | F. Users, configuration and monitoring |
| FIA_UID.2/sgc | F. Users, configuration and monitoring |
| FIA_UIA_EXT.1/localMngt | F. Users, configuration and monitoring |
| FIA_UAU_EXT.2/localMngt | F. Users, configuration and monitoring |
| FIA_UAU.6/localMngt | F. Users, configuration and monitoring |
| FIA_UAU.7/localMngt | F. Users, configuration and monitoring |
| FIA_AFL.1/localMngt | F. Users, configuration and monitoring |
| FIA_PMG_EXT.1/localMngt | F. Users, configuration and monitoring |
| FTA_SSL_EXT.1/localMngt | F. Users, configuration and monitoring |
| FTA_SSL.4/localMngt | F. Users, configuration and monitoring |

| | |
|---|---|
| FTA_TAB.1/localMngt | F. Users, configuration and monitoring |
| FMT_SMF.1 | F. Users, configuration and monitoring |
| FMT_MOF.1/localMngt | F. Users, configuration and monitoring |
| FMT_MTD.1/query | F. Users, configuration and monitoring |
| FMT_MTD.1/supervision | F. Users, configuration and monitoring |
| FPT_SKP_EXT.1 | F. Users, configuration and monitoring |
| FMT_MTD.1/configuration | F. Users, configuration and monitoring |
| FMT_MTD.1/dateTime | F. Users, configuration and monitoring |
| FMT_MTD.1/keys | F. Users, configuration and monitoring |
| FMT_MTD.1/keyLifetime | F. Users, configuration and monitoring |
| FMT_MTD.1/adminPwd | F. Users, configuration and monitoring |
| FMT_MTD.1/opePwd | F. Users, configuration and monitoring |
| FMT_MTD.1/software | F. Users, configuration and monitoring |
| FPT_TUD_EXT.1/software | F. Users, configuration and monitoring |
| FPT_APW_EXT.1 | F. Storage and protection of local data<br>F. Users, configuration and monitoring |
| FPT_FLS.1 | F. Failure state |
| FPT_TST.1 | F. Autotest |
| FPT_SDP_EXT.2 | F. Storage and protection of local data |
| FDP_RIP.2 | F. Storage and protection of local data |