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

CSPN SECURITY TARGET

MISTRAL VS9 VIRTUAL IPSEC GATEWAY SOFTWARE

Entity identifier	Business identifier	CTD	Revision
0026-F0057	68922788	306	-D

Changes

Changes record			
Revision	**Date**	**Author**	**Modification**
--	03/05/2022	THALES	Creation
-A	21/06/2022	THALES	Minor fixes on referenced documents, SF7 and wording. Addition of the Linux hardening level.
-B	20/09/2022	THALES	Clarification of the installation chapter.
-C	24/04/2024	THALES	Update
-D	30/05/2024	THALES	Precisions on SF1 and evaluated version.

Table of content

Table index

Figure index

1. INTRODUCTION

1.1 DOCUMENT IDENTIFICATION AND SUMMARY

This document describes the security target of the Mistral VS9 virtual IPsec gateway, developed by Thales within the framework of the CSPN certification scheme.

1.2 APPLICABLE DOCUMENTS

	Title	References	Version
RGS_B	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques	ANSSI-PG-083	**2.04 (2020)**
CSPN	Certification de Sécurité de Premier Niveau des produits de technologie de l'information N° 494/ANSSI/SDE/PSS/CCN	ANSSI-CSPN-CER-P-01	**4.0**
DR PROFILE	Note Crypto Référentiel IPsec DR	2765/ANSSI/DR	16 - Mar - 2021

Table 1: Reference documents

1.3 REFERENCE DOCUMENTS

	Title	References	Version
LINUX_ANSSI	Recommandations de configuration d'un système GNU/Linux.	ANSSI/BP-028	**1.2 -** Mar. 2019
PARTIONNING_ ANSSI	Recommandations pour la mise en place de cloisonnement système.	ANSSI-PG-040	**1 -** 14 Dec. 2017
TLS_ANSSI	Recommandations de sécurité relatives à TLS	SDE-NT-35/ANSSI/SDE/NP	**1.2 –** 26 Mar. 2020
PASSWD_ANSSI	Recommandations de sécurité relatives aux mots de passe	DAT-NT-001	**2.0 –** 8 Oct. 2021

Table 2: Applicable documents

1.4 ABBREVIATION AND ACRONYMS

1.4.1 Administrative acronyms

Acronym	Meaning
ANSSI	National Agency for Information System Security
TOE	Target of Evaluation

Table 3: Administrative acronyms

1.4.2 Technical acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chain
CLI	Command Line Interface
DR	Diffusion Restreinte
ECDSA	Elliptic Curve Digital Signature Algorithm
ECSDSA	Elliptic Curve Schnorr Digital Signature Algorithm
ESN	Extended Serial Number
ESP	Encapsulating Security Payload
HMAC	Hash-based Message Authentication Code
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
MAC	Message Authentication Code
MMC	Mistral Management Center
OS	Operating System
SA	Security Association
SHA	Secure Hash Algorithm
SP	Security Policy
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VM	Virtual Machine
VPN	Virtual Private Network

Table 4: Technical acronyms

1.4.3 Nomenclature rules:

- A.: Assumption prefix,
- D.: Data asset prefix
- SF.: security Function prefix,
- S_: System object of the solution prefix,
- SS_: SubSystem of the system prefix,
- CS_: Cooperative System prefix,
- CSS_: SubSystem of the systems Cooperative prefix,
- T. Threat prefix,

2. TOE IDENTIFICATION

Mistral encryption software for Mistral VS9 system version 9.1.0.13, compatible with NEXIUM SafeCore version 1.5, or above, virtualization infrastructure.

Editor	*THALES SIX GTS France*
Product	*Mistral VS9 Virtual IPsec Gateway*
Evaluated version	*9.1.0.13*

Table 5: Product identification

3. TOE OVERVIEW

3.1 SYSTEM OVERVIEW

Mistral system (S_MISTRAL) protects the dataflow between user endpoints as well as in a complex network with multiple site accesses.

The Mistral system (S_MISTRAL) delivered to clients is typically composed of:

- IPv4 IPsec gateways (**SS_IPSEC_GW**) following French **[DR profile]**,
- Mistral Management Center (**SS_MMC**),

*Nota: The term **SS_IPSEC_GW** encompasses all interoperable Mistral VS9 gateways, them being virtualized (**SS_IPSEC_GW_VM**) or not (**SS_IPSEC_GW_HW**).*

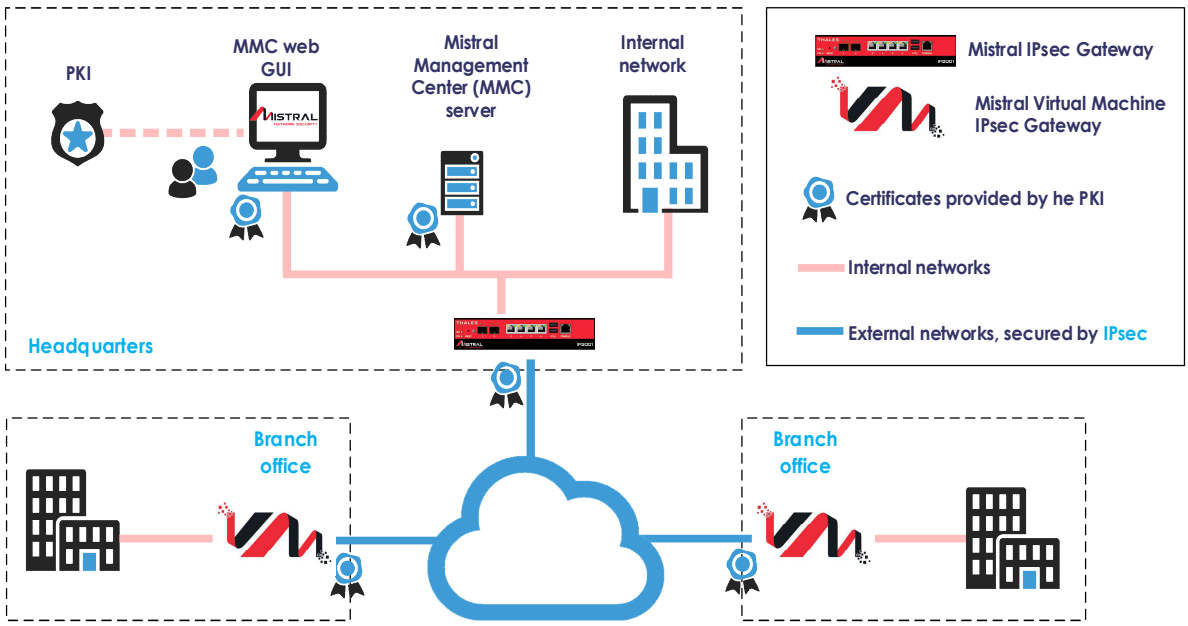

Figure 1: MISTRAL System architecture

3.2 TOE DESCRIPTION

3.2.1 TOE Boundary

The TOE (described in Figure 2) is the **Mistral VS9 software** running in **SS_IPSEC_GW_VM,** in IPv4 environment. It is composed of a hardened Linux OS and the Mistral applications.

The TOE does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the TOE to protect data that originates from or is destined to the device itself, this includes administration/audit data. Traffic that is traversing the network device, destined to another network entity, is not covered by this evaluation. It is assumed that this protection will be covered by other network devices (e.g., firewall).

The Linux OS is hardened and complies with the Intermediate level defined in the guidance document from French administration to secure Linux OS [LINUX_ANSSI] and with the guidance document [PARTIONNING_ANSSI].

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

Hardware equipment and virtualization environment are considered out of scope of the Target of Evaluation described in this Security Target. Following enabling elements, the Mistral Management Center device (SS_MMC), and the Public Key Infrastructure device (CSS_PKI) are outside the TOE.

SS_MMC may be any third party management system compliant with the management interfaces and assumptions. CSS_PKI may be any third party public key infrastructure solution compliant with the certificates and keys interfaces and assumptions.

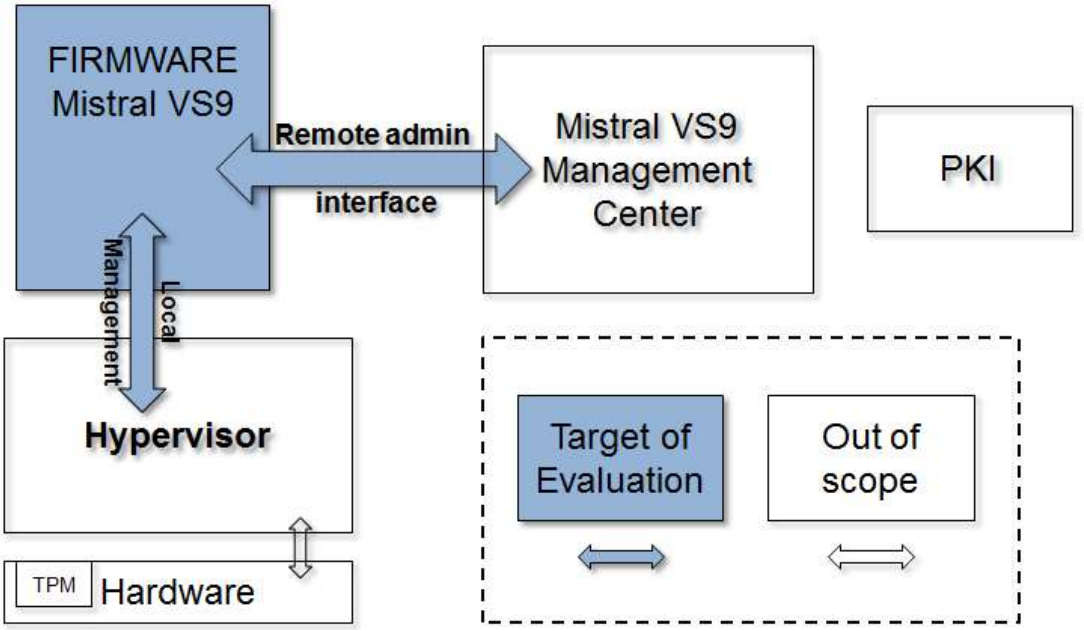

Figure 2: TOE Boundary

3.2.2 TOE Interfaces

Identifier	Description
IF_GW_LOCAL_MGT	**Human-machine Command Line Interface (CLI)** Local interface on SS_IPSEC_GW_VM used by ROLE_GW_OPERATOR and accessed through the hypervisor (requires admin rights on the hypervisor).
IF_IMPORT_EXPORT	**Interface of data import / export via virtual USB and virtual Ethernet port** Local interface used for configuration with INIT_CONF or FULL_CONF files, import of certificates and key containers, and for local data export as archives of EVENT_LOG and certificate requests.
IF_RED_NETWORK	**CSS_RED_NETWORK interface** This interface for interactions with CSS_RED_NETWORK concerning user data flow and network services with other sub-systems of S_MISTRAL on trusted side
IF_BLACK_NETWORK	**CS_BLACK_NETWORK interface** This interface for interactions with CS_BLACK_NETWORK concerning user data flow and network services with other sub-systems of S_MISTRAL on untrusted side.

Table 6: External interfaces

3.2.3 Users and entities

3.2.3.1 ROLE_GW_OPERATOR

TOE local operator interacts with the TOE through IF_GW_LOCAL_MGT and IF_IMPORT_EXPORT. He can:

- Restart the TOE
- Personalize the TOE
- Manage certificates on the TOE
- Load the TOE configuration file
- Update the TOE
- Check events on the TOE

3.2.3.2 ROLE_SYS_ADMIN

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

3.2.4 Installation

The TOE is delivered already installed on appropriate hardware. This means that certificates, keys and configuration files required for its use are already present inside the TOE. Additionally, the following elements are delivered:

- A local administration account.
- User manuals and guides.

Nota: It is important to note that, while user manuals and guides are meant to be read by both the TOE's developer and customer, the integration on NEXIUM SafeCore hypervisor is always done before delivery to the customer.

3.2.5 Available functions

The TOE's main functionalities are:

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

- IPv4 Data flow protection (against disclosure, modification, insertion and replay),
- IPv4 Data flow filtering, at OSI network level 3 and OSI transport level 4,
- Data flow discard if no protection policy has been found for the flow.

Management flow control and protection:

- Management flow protection (against disclosure, modification, insertion and replay).

TOE security management:

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

3.3 ASSUMPTIONS

3.3.1 Securing the TOE

A1 - A.OPERATION_ENVIRONMENT

The host device is assumed to be deployed inside the client's information system according to the sensibility of data handled. Thus, both the TOE's host and devices directly connected to the TOE are considered trusted.

A2 - A. REGULAR_UPDATES

The network device firmware and software is assumed to be updated by ROLE_GW_OPERATOR or ROLE_SYS_ADMIN on a regular basis in response to the release of product updates due to known vulnerabilities or software error.

It is assumed that protection of TOE software updates is performed in a trusted environment, on a trusted device by authorized persons only, in compliance with [RGS_B] requirements.

It is assumed that protection of TOE software updates provides integrity.

3.3.2 Organizational measures

A3 - A.USER_AWERENESS

The TOE's users are considered trusted and trained to its installation, administration and use. They are aware of restricted data handling procedures. The users have access to the documents required for the TOE correct use.

3.3.3 Assumptions regarding administration

A4 - A.ALARM_AUDIT

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

The TOE local operator (ROLE_GW_OPERATOR) may analyze and process alarms after their generation.

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

A5 - A.POLICIES_CONTINUITY

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

A6 - A.ADMIN_CREDENTIALS_SECURE

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

Organizational security procedures are established and known by local and remote administrators, in order to protect all administrator's credentials, for local and remote management of the TOE.

3.3.4 Assumptions regarding management devices

A7 - 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 center device (SS_MMC)
- The TOE local management device (CSS_LMGT)
- The Public Key Infrastructure device (CSS_PKI)
- The TOE host hypervisor (CSS_HYPERVISOR)

A8 - A.ACCESS_CONTROL_MANAGEMENT_DEVICES

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

- The TOE management center device (SS_MMC)
- The TOE local management device (LMGT)
- The Public Key Infrastructure device (CSS_PKI)
- The TOE host hypervisor (CSS_HYPERVISOR)

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).

A9 - A.PHYSICAL_ENV_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 center device (SS_MMC)
- The Public Key Infrastructure device (CSS_PKI)
- The TOE local management device (LMGT)
- The TOE host hypervisor (CSS_HYPERVISOR)
- Any other devices connected to one of the devices listed above

A10 - A.SS_MMC_TO_TOE

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

- through trusted network (red side) or
- through untrusted network (black side) protected with an IPsec VPN provided by Mistral system.

A11 - A.DATA_TRANSPORTATION

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

A12 - A.EXTERNAL_KEYS

When cryptographic keys are imported into the TOE, it is assumed that these keys are:

- Generated by cryptographic mechanisms compliant with ANSSI guidance **[RGS_B],**
- Protected during transfer by a secured container, with a password compliant with ANSSI password rules **[PASSWD_ANSSI]**,
- Deleted after injection into the TOE.

3.3.5 Assumption regarding the TOE's hypervisor host

A13 - A.SECURE_HOST

It is assumed that the TOE's host hypervisor:

- is NEXIUM SafeCore in its version 1.5 or above,
- is hosted on hardware compatible with NEXIUM SafeCore CSPN security target,
- is configured in accordance with NEXIUM SafeCore CSPN security target,
- provides the TOE with a reliable time base.

4. DESCRIPTION OF PROTECTED ASSETS

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

4.1 USER DATA

Alias	Description	Security needs
D. APPLICATIVE_DATA	Sensitive data transmitted from a trusted sub-network to another trusted sub-network through an untrusted network.	Confidentiality, authenticity, anti-replay, integrity
D. TOPOLOGIC_INFO	Topology information of the protected trusted network.	Confidentiality, authenticity, integrity

Table 7: User assets

4.2 TOE DATA

Alias	Description	Security needs
D.CONFIG_PARAM	This asset groups all TOE configuration parameters that do not need any protection against disclosure.	Authenticity, Integrity
D.VPN_KEY_PRIV	This asset groups all asymmetric cryptographic private keys used for IPsec and TLS authentication.	Confidentiality, Integrity
D.IKE_SAs_CRYPTO_KEYS	This asset groups all temporary (i.e. in volatile memory only) cryptographic materials created through IKE protocol.	Confidentiality, Integrity
D.SP_SA	This asset groups all Security Associations (SAs) and Security Policies (SPs) configured within the TOE.	Integrity
D.SUPERVISION_DATA	This asset groups all TOE supervision data and audit record generated by the TOE.	Integrity
D.LOG_KEY	This asset is the key used by the TOE for event log protection	Confidentiality, Integrity
D.TIME_BASE	This asset represents the reliable time base kept within the TOE and used by the TOE.	Integrity
D.PASSWORDS	Users passwords	Confidentiality, Integrity
D.PROVIDER_UPDATE_KEYS	This asset groups all symmetric cryptographic keys used for software update ciphering.	Confidentiality, Integrity
D.PROTECT_PROVIDER_UPDATE_KEYS	This asset is the key used by the TOE for D.PROVIDER_UPDATE_KEY protection while the TOE is running	Confidentiality, Integrity
D.SWUPDATE_CA	This asset is the provider Certificate Authority and its public key used by the TOE to authenticate software updates.	Authentication, Integrity
D.TOE_SOFTWARE	This asset represents the applicative software of the TOE.	Confidentiality, Authenticity, Integrity
D.TOE_OS	This asset represents the operating system of the TOE.	Authentication, Integrity

Table 8: TOE assets

5. THREAT DESCRIPTION

Administrators and operators are not considered attackers. Attackers are entities that can belong to the organization hosting the TOE but do not have authorized access to the TOE.

T1 – T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

- An attacker may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, or performing man-in-the-middle attacks, which would provide access to the administrative session.

T2 – T.UPDATE_COMPROMISE

- An attacker attempts to provide a compromised update to the TOE in order to undermine the security functionality of the device.

T3 – T.USER_DATA_REUSE

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

T4 – T.MISUSE

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

T5 – T.TIME_BASE

- An attacker tampers with the TOE's time base in order to falsify log/audit data or to impact certificates validity period.

T6 – T.RESIDUAL_DATA

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

T7 – T.UNTRUSTED_COMMUNICATION_CHANNELS

- Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to perform successfully man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T8 – T.WEAK_AUTHENTICATION_ENDPOINTS

- Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attackers could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity.

T9 – T.PASSWORD_CRACKING

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

T10 – T.SECURITY_FUNCTIONALITY_COMPROMISE

- Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

T11– T.SECURITY_FUNCTIONALITY_FAILURE

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

T12 – T.HOST_COMPROMISED

- Threat agents may compromise the hypervisor hosting the TOE in order to attack the TOE.

	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	T.UPDATE_COMPROMISE	T.USER_DATA_REUSE	T.MISUSE	T.TIME_BASE	T.RESIDUAL_DATA	T.UNTRUSTED_COMMUNICATION_CHANNELS	T.WEAK_AUTHENTICATION_ENDPOINTS	T.PASSWORD_CRACKING	T.SECURITY_FUNCTIONALITY_COMPROMISE	T.SECURITY_FUNCTIONNALITY_FAILURE	T.HOST_COMPROMISED
D.APPLICATIVE_DATA	X		X				X	X	X	X	X	X
D.TOPOLOGIC_INFO	X						X	X	X	X	X	X
D.CONFIG_PARAM	X						X		X	X	X	X
D.VPN_KEY_PRIV	X					X			X	X	X	X
D.IKE_SAs_CRYPTO_KEYS	X					X			X	X	X	X
D.SP_SA	X			X					X	X	X	X
D.SUPERVISION_DATA	X								X	X	X	X
D.LOG_KEY	X								X	X	X	X
D.TIME_BASE	X				X				X	X	X	X
D.PASSWORDS	X								X	X	X	X
D.PROVIDER_UPDATE_KEYS	X								X	X	X	X
D.PROTECT_PROVIDER_UPDATE_KEYS	X								X	X	X	X
D.SWUPDATE_CA	X								X	X	X	X
D.TOE_SOFTWARE	X	X					X		X	X	X	X
D.TOE_OS	X	X							X	X	X	X

Table 9: Assets coverage by threats

6. SECURITY FUNCTIONS DESCRIPTION

This section describes the security functions implemented by the TOE:

SF1 – SF.AUDIT_AND_EVENTS_LOGGING

The TOE shall store and protect in integrity security events. Events stored contain:

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

Among events, the following are notified as alerts or emergencies:

- Self-test error,
- Authentication failure (after several errors),
- Certificates end of life (imminent and expiration reached),
- Updates installation failure,
- Fast event deletion,
- and some network events considered as errors (Replay, spoofing, IP address conflict and fragmented packet received from untrusted network).

SF2: SF.TRAFFIC_KEYS_AND_CERTIFICATES_MANAGEMENT

There are two key types in the Mistral system:

- **Negotiated keys**: dynamic negotiated keys by IKEv2. They are managed by the IKE service and are directly and only stored in RAM.
- **Generated keys:** keys generated by the TOE or CSS_PKI using cryptographic algorithms. These keys are used for IPsec and TLS authentication.

Generated keys are protected in the TOE and are not sent from any interface**.** After expiration, these keys are cleared by overwriting of zeroes.

The TOE certificates and private keys provided by CSS_PKI are injected in the TOE before it can become operational. They are used for IKE authentication with remote instance of TOE (IPsec) and with SS_MMC (TLS).

The TOE checks certificates validity when they are loaded.

During traffic establishment, certificates are used to authenticate TOE with SS_MMC (TLS) or another TOE instance (IPsec). The TOE checks if the certificate received is linked with a trusted CA (trusted anchor).

SF3: SF.ACCESS_CONTROL

When users are locally authenticated with a password, they are allowed to access to ROLE_GW_OPERATOR commands such as *restart*, *stop*, *status query*, *self-tests* and *configure* using a restricted CLI. The password follows the rules described here:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "+", ",", "-", ".", "/", ":", ";","<", "=", ">", "?", "[", "\", "]", "_", "{", "|", and "}";
- Minimum password length is 15 characters;
- Password is composed with at least 1 upper case letter, 1 lower case letter, 1 number and 1 special character.

TOE allows remote connection of the ROLE_SYS_ADMIN via TLS using X.509 certificates for authentication.

Nota: Remote users do not have their own account on the TOE but use a user profile with limited allowed commands. Remote access profile gives the user access to commands such as restart, stop status query, self-tests, equipment configuration, audit log consulting and updates.

SF4: SF.SOFTWARE_UPDATE

In the Mistral system software, update can be performed at runtime through the remote management protocol or through the local management interfaces. The update consists in the download of a single file protected in authentication (ECDSA secp256r1), integrity (SHA-256) and confidentiality (AES-CBC-256) called firmware. The firmware contains all software components (OS, main software …). No obsolete (anterior to the one currently deployed) version can be downloaded. On firmware activation, after being checked by the current running software of the equipment, the new firmware is written in permanent memory.

SF5: SF.DATA_FLOW_PROTECTION

All incoming and outgoing network flows are systematically analyzed, filtered and have a predefined handling. Possible actions for frames (explicitly allowed by security policies) to be sent through untrusted network are:

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

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

The criteria of filter rules are:

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

SF6: SF.FAILURE_STATE

When one of the following errors occurs, the TOE enters a failure state:

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

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

SF7: SF.SELF_TEST

A self-test is automatically performed at TOE start and can be performed while the TOE is operational. It consists on the following test:

- Event log integrity check

7. RATIONALE

	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	T.UPDATE_COMPROMISE	T.USER_DATA_REUSE	T.MISUSE	T.TIME_BASE	T.RESIDUAL_DATA	T.UNTRUSTED_COMMUNICATION_CHANNELS	T.WEAK_AUTHENTICATION_ENDPOINTS	T.PASSWORD_CRACKING	T.SECURITY_FUNCTIONALITY_COMPROMISE	T.SECURITY_FUNCTIONNALITY_FAILURE	T.HOST_COMPROMISED
SF1 - SF. AUDIT_AND_EVENTS_ LOGGING	X			X						X		X
SF2 - SF.TRAFFIC_KEYS_AND_ CERTIFICATES_ MANAGEMENT			X			X	X					
SF3 - SF.ACCESS_CONTROL	X				X				X	X		
SF4 - SF_SOFTWARE_UPDATE		X								X		
SF5 - SF.DATA_FLOW_PROTECTION			X			X						
SF6 - SF.FAILURE_STATE			X							X	X	X
SF7 - SF.SELF_TEST										X	X	X
A1 - A.OPERATION_ENVIRONMENT	X					X	X	X		X		X
A2 - A.REGULAR_UPDATES		X								X		
A3 - A.USER_AWERENESS			X	X								
A4 - A.ALARM_AUDIT	X			X						X		
A5 - A.POLICIES_CONTINUITY			X	X								
A6 - A.ADMIN_CREDENTIALS_SECURE								X		X		
A7 - A.SECURED_ MANAGEMENT_DEVICES							X	X		X		X
A8 - A.ACCESS_CONTROL_ MANAGEMENT_DEVICE								X		X		X
A9 - A.PHYSICAL_ENVIRONMENT_ MANAGEMENT_DEVICE							X			X		X
A10 - A.SS_MMC_TO_TOE	X	X					X					
A11 - A.DATA_TRANSPORTATION		X				X	X			X		
A12 - A.EXTERNAL_KEYS						X	X			X		
A13 - A.SECURE_HOST	X				X	X	X	X		X		X

Table 10: Threat coverage by Security Functions and Assumptions