# Mistral
# TRC 7535

# CIBLE DE SECURITE (CDS) MISTRAL TRC7535 EAL3+


| | Service / Nom | Visa et Date |
|---|---|---|
| Rédigé par | Benoît SALINGUE | |
| Vérifié par | Patrick REDON | |
| Approuvé par | Xavier DE CHATILLON | |

Nombre total de pages : 60
Logiciel : WORD 7.0
Date d'édition : 04/03/2008

Matériel : PC
Date d'application : 04/03/2008

THALES

CODE OTAN: F0057

| REFERENCES DOCUMENT / DOCUMENT REFERENCES | | | |
|---|---|---|---|
| NUMERO / NUMBER | CODE | FORMAT / SIZE | FEUILLE / SHEET |
| 61 485 069 | **805** | **FR** | **1/60** |

| | | | | | | | | -M | IND/LTR ← |
|---|---|---|---|---|---|---|---|---|---|

# EVOLUTIONS

| INDICE DE REVISION | DESCRIPTION |
|---|---|
| A | 09/06/2003 création du document |
| B | 26/11/2003<br>- Finalisation du projet et prise en compte des remarques de lecture |
| C | 26/01/2004<br>- Prise en compte des remarques de la DCSSI (M. Blot)<br>- Refonte des menaces et des objectifs de sécurité |
| D | 09/04/2004<br>- Prise en compte des remarques de la DCSSI (M. Blot) |
| E | 23/04/2004<br>- Prise en compte des remarques de la DCSSI (M. Blot)<br>07/05/2004 : correction des pieds de page pour référencer édition E |
| F | 31/01/2005<br>- Mise à jour pour la version 4.5.2<br>- Prise en compte rapport DCSSI : rapport ASE |
| G | 04/03/2005<br>- Prise en compte rapport DCSSI : rapport ASE |
| H | 26/05/2005<br>- Mise à jour pour la version 4.5.2.2<br>- Prise en compte rapport DCSSI : rapport ASE |
| I | 30/03/07<br>- Mise à jour pour la version 4.6.1 |
| J | 11/12/07<br>- Prise en compte rapport DCSSI : rapport ASE |
| K | 21/02/2008<br>- Prise en compte rapport DCSSI |
| L | 25/02/2008<br>- Prise en compte rapport DCSSI |
| M | 04/03/2008<br>- ST-Lite |

# TABLE DES MATIERES

# TABLE DES FIGURES

# 1. Introduction de la cible de sécurité

## 1.1 Identification de la cible de sécurité

| | |
|---|---|
| Cible d'évaluation (TOE) : | MISTRAL TRC 7535 version 4.6.1 (AES gérant des clés de 128/256 bits et 3DES) |
| Niveau EAL : | **EAL3 augmenté de ALC_FLR.3 et AVA_VLA.2, ainsi que ADV_LLD.1, ALC_TAT.1 et ADV_IMP.1 pour les mécanismes cryptographiques (FCS).** |
| Résistance des fonctions : | **SOF-élevé** |
| Conformité à un PP existant : | Aucune. |
| Référence des CC : | Critères Communs v2.3 d'Août 2005. |

## 1.2 Vue d'ensemble de la cible de sécurité

Le MISTRAL TRC 7535 assure la sécurisation des données échangées à l'intérieur des réseaux locaux privés (LAN) ou lors des interconnexions de réseaux locaux sur un réseau extérieur (WAN).
Basé sur les technologies VPN (Réseaux Privés Virtuels), il offre l'ensemble des services de sécurité indispensables à tout déploiement d'applications sécurisées sur les réseaux IP.
Il est conçu principalement pour sécuriser les réseaux d'entreprises, les réseaux bancaires et les réseaux d'organismes étatiques.
La configuration des boîtiers MISTRAL est assurée par le logiciel Centre de Gestion Mistral (CGM)

## 1.3 Conformité aux Critères Communs

Cette cible de sécurité respecte les exigences des Critères Communs v2.3 d'Août 2005. Tous les composants fonctionnels décris dans cette cible de sécurité sont issus de la Partie 2 des Critères Communs v2.3 d'Août 2005. Le niveau d'assurance EAL3+ retenu est conforme à la Partie 3 des Critères Communs v2.3 d'Août 2005.

## 1.4 Documents en référence

[QUA-STD] Processus de qualification d'un produit de sécurité – niveau standard. Version 1.0, juillet 2003. DCSSI, 001591/SGDN/DCSSI/SDR.

# 2. Présentation de la cible d'évaluation (TOE)

Le but de ce chapitre est d'identifier de la façon la plus précise possible, la cible de l'évaluation (la TOE) et de la replacer dans son environnement.

## 2.1 Le système MISTRAL VPN IP

Le système Mistral comprend :
Deux **produits de chiffrement** :

- le boîtier Mistral (TRC7535) : le chiffreur IP de site,
- le logiciel Mistral Nomade (TRC7955) : le chiffreur IP pour les PC portables,

Deux **produits d'administration** :

- le Centre de Gestion Mistral (CGM) : le logiciel d'administration des chiffreurs,
- le Centre d'Elaboration des Clés Mistral (CEC) : le générateur de clés certifiées,

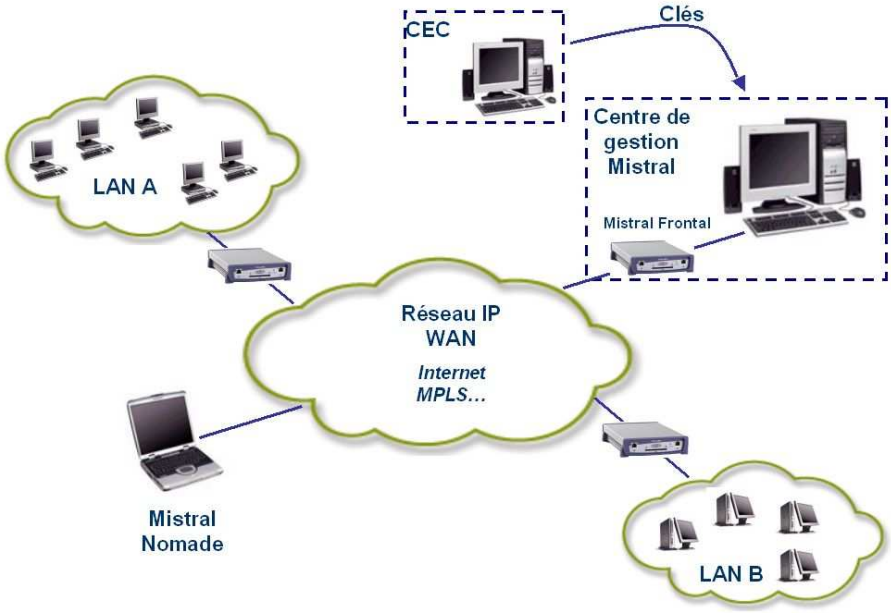



**Figure 1 : Présentation du système Mistral**

### 2.1.1 Produits de chiffrement

Les produits de chiffrement sont le cœur du système Mistral. Ils chiffrent et déchiffrent les flux de communications.
Le **boîtier Mistral (TRC7535)** est un équipement de chiffrement des réseaux IP sensibles. Placé en coupure sur le réseau, il chiffre (et déchiffre) les données échangées avec l'extérieur. Il possède également une fonction de filtrage simple pour protéger les équipements internes (contre des attaques réseaux et les accès non-autorisés).
Le **logiciel Mistral Nomade (TRC7955)** est destiné à sécuriser les accès distants à partir de PC portable. Il comprend le logiciel de sécurité Mistral Nomade et une carte à puce. La carte à puce sert à authentifier l'utilisateur et contient tous les paramètres de sécurité. La carte à puce de l'utilisateur doit être laissée en permanence dans le lecteur, pour maintenir la connexion sécurisée.

### 2.1.2 Produits d'Administration

Les produits d'administration aident à configurer les produits de chiffrement et gérèrent les clés.
Le **Centre de Gestion Mistral (CGM)** est le produit utilisé pour configurer à distance le système Mistral. Il est composé d'un logiciel PC et d'un **boîtier Mistral configuré en Frontal** connecté directement au CGM. Il permet de programmer à distance tous les boîtiers Mistral ***(Figure 1).***
Le **Centre d'Elaboration de Clés Mistral (CEC)** est le produit incontournable pour générer les clés certifiées. Il est composé d'un PC isolé comprenant une carte d'extension et d'un logiciel dédié.

## 2.2 Fonctions offertes par le Mistral

Les fonctions de sécurité du boîtier Mistral (TRC7535) version 4.6.1 sont décrites ci-dessous :

Le boîtier Mistral assure la fonction de chiffrement des trames IP.

- Le boîtier Mistral chiffre les flux IP qui lui arrivent sur son port clair et les retransmet sur son port chiffre après chiffrement et un filtrage éventuel. Inversement, il déchiffre les données qui lui arrivent sur son port chiffre et les retransmet en clair sur son port clair après un éventuel filtrage. Il contrôle la cohérence des politiques de sécurité (inclusion de SP autorisée, imbrication de SP interdite).
- Le boîtier Mistral supporte les algorithmes 3DES (clé de 128 bits)et AES (clés de 128 ou 256 bits).
- Le boîtier Mistral a une capacité de 1000 tunnels pour les versions Fast et Basic et de 6000 tunnels pour sa version 6000 tunnels.
- Le boîtier Mistral supporte plusieurs niveaux de chiffrement :
  - ⇨ les modes transport dit chiffrement simple *fast forward* (IP, TCP entête clair) ou le chiffrement simple étendu *fast forward extended* (IP étendu, TCP entête recopiée étendu ou TCP entête recalculée étendu),
  - ⇨ les modes ESP tunnel et ESP/UDP issus des normes IETF (RFC2406).
- Les modes de chiffrement ESP tunnel et ESP/UDP offrent les services de sécurité suivants : la confidentialité et l'intégrité des trames IP, le masquage des adresses et l'authentification de l'émetteur. Le boîtier gère la fragmentation éventuelle des trames.

Le boîtier Mistral peut retransmettre en clair certaines trames :

- Le boîtier Mistral peut retransmettre en clair (sans modification du datagramme) tous les paquets IP lorsque la politique de sécurité ou le fonctionnement par défaut du boîtier demande leur transmission en clair.
- Le boîtier Mistral peut laisser passer les trames ARP et RARP, BGP, RIP/OSPF et DHCP qui ne lui sont pas destinés en effectuant certains contrôles de validité (débrayables).
- Le boîtier Mistral peut laisser passer certaines trames ICMP Size too big.

Le boîtier Mistral peut réaliser le filtrage des trames.

- Le Mistral réalise des opérations de filtrages de trame (rejet de certaines trames) en fonction de la politique de sécurité. Sont pris en compte les couples d'adresses source et destination (avec masques) et éventuellement les protocoles IP et les ports TCP/UDP.
- Note : La notion de filtrage a pour objectif d'affiner le choix de la SP en ne laissant sortir chiffrées que les trames TCP/UDP portant un numéro de port déterminé (sans distinction source ou destination) et en jetant les autres. Nous attirons l'attention sur le fait qu'il ne s'agit pas d'une fonction de type Firewall.

Le boîtier Mistral est compatible des trames Ethernet et VLAN.

- Il accepte les trames aux formats Ethernet 802.3 et V2, mais aussi au format VLAN 802.1Q. Dans ce cas, il conserve le tag.
- Pour la télégestion et l'administration, le boîtier accepte les trames au format Ethernet V2 et VLAN 802.1Q (avec éventuel apprentissage) mais pas les trames au format 802.3.

Le boîtier Mistral permet de protéger les utilisateurs Nomades.

- Les utilisateurs Nomade disposent d'un Client Nomade qui réalise les fonctions de chiffrement en mode ESP tunnel ou ESP/UDP et de filtrage. Ces utilisateurs peuvent se connecter au réseau via Ethernet ou par un modem RTC ou ADSL.
- Le boîtier Mistral déchiffre les trames ESP tunnel ou ESP/UDP émises par le Mistral Nomade. Il réalise et vérifie l'authentification du client "Nomade".
- Le système est compatible de l'adressage dynamique des fournisseurs d'accès Internet (FAI).

Le boîtier Mistral utilise des clés symétriques.

- Le Système Mistral est basé sur l'utilisation de clés symétriques d'une taille de 128 bits en 3DES et d'une taille de 128 ou 256 bits en AES. Ces clés servent pour chiffrer les flux de télégestion (clés de base) et chiffrer les flux réseau (clés de trafic). Elles sont identifiées par le GIC.

Le boîtier Mistral est administré par la description des politiques de sécurité (SP) et des associations de sécurité (SA). Les SP et les SA sont gérées séparément dans le boîtier.

- Une SP est définie par un couple adresse (masque) IP source et destination, une liste de protocoles IP et de ports TCP/UDP autorisés. Elle permet de configurer le type de traitement à effectuer (clair / traite / bloque), le chiffreur destinataire en mode tunnel. De plus, elle pointe vers une SA par l'intermédiaire de son SPI (identifiant unique).
- Une SA est identifiée par son SPI et spécifie le type de chiffrement à réaliser. La SA contient l'index de la clé, le niveau de chiffrement des paquets, la crypto-période de la clé, le seuil d'usure de la clé et le MTU de la clé en mode tunnel.

Le Centre de Gestion Mistral permet la description centralisée des SP et SA.

- Le Centre de Gestion centralise la description du réseau du client, et en particulier des réseaux, sous-réseaux (masques), ou postes de travail à protéger. Il permet également la description des boîtiers Mistral et la description centralisée des politiques et associations de sécurité.

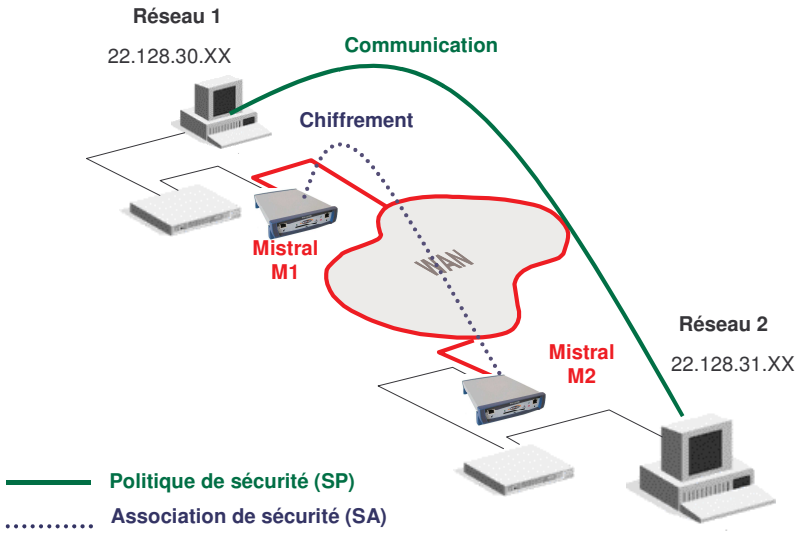



**Figure 2 : Politiques et associations de sécurité**

Le boîtier Mistral peut être télégéré ou recevoir ses éléments par carte à puce.

- Le Centre de Gestion transmet aux boîtiers Mistral ses paramètres d'initialisation (hormis son adresse IP et les paramètres liés à la configuration de la télégestion), les politiques de sécurité et les clés symétriques nécessaires via le réseau par télégestion. Cette télégestion est bien sûr sécurisée.
- Les éléments peuvent également être acheminés hors réseau par carte à puce.

Le boîtier Mistral peut aussi être configuré en mode local (mode console).

- En l'absence de CGM, le fonctionnement local permet à l'opérateur d'exploiter le Mistral.
- L'accès console est protégé par mot de passe. 3 mauvaises saisies consécutives de mot de passe déclenchent l'effacement des clés et éléments sensibles. De plus, le boîtier remonte une alarme vers le Centre de Gestion.

Le boîtier Mistral peut être supervisé via SNMPv1.

- Le Mistral gère la supervision SNMP via trois groupes de la MIB II standard "System", "Interfaces" et "IP". Les groupes "System" et "Interfaces" sont renseignés complètement. Il n'existe pas de MIB privée. Le Mistral visualise 2 interfaces reflétant distinctement l'état du port clair et du port chiffre

Le boîtier Mistral contrôle la durée de vie des clés, l'état du boîtier et les alertes de sécurité.

- L'usure des clés est contrôlée par chaque boîtier en fonction du nombre de paquets chiffrés/déchiffrés. En cas d'usure, une alerte est remontée au Centre de Gestion.
- La crypto-période (durée de vie temporelle) est contrôlée par le Centre de Gestion. En cas de dépassement, une alarme de sécurité est remontée sur le Centre de Gestion.
- Les modifications d'états du boîtier (insertion de carte à puces, …) font l'objet d'alertes de sécurité, qui sont remontées au Centre de Gestion.
- Le boîtier contrôle l'intégrité, l'authentification et le bon déchiffrement des trames. En cas d'erreurs laissant supposer une possible attaque sur le réseau, une alerte de sécurité est remontée au Centre de Gestion.
- Le Centre de Gestion peut effectuer des remontées de configuration de boîtier pour détecter toute désynchronisation de configuration.

Le logiciel du boîtier Mistral peut être upgradé à distance à partir du Centre de Gestion.

- Le logiciel du Mistral est téléchargeable, soit via son port série, soit à distance via le réseau à partir du Centre de Gestion.

Le boîtier Mistral dispose d'un effacement d'urgence sous tension.

- Le Mistral dispose d'un bouton d'effacement d'urgence sous tension qui déclenche l'effacement des clés et éléments sensibles. De plus, le boîtier remonte une alarme vers le Centre de Gestion. L'exploitation par console est alors verrouillée.
- Le boîtier Mistral dispose également d'un mécanisme de détection d'ouverture du boîtier sous tension, qui déclenche l'effacement des clés et éléments sensibles. De plus, le boîtier remonte une alarme vers le Centre de Gestion. L'exploitation par console est alors verrouillée.
- De plus, la remise du boîtier Mistral dans un état opérationnel et précédemment validé est réalisée par l'arrêt puis le redémarrage du boîtier. Il est alors nécessaire de rentrer la configuration par insertion de CAM ou configuration par menu.

## 2.3 Identification de la TOE et de son périmètre

La cible de l'évaluation comprend les éléments suivants :

- ⇒ Le boîtier MISTRAL TRC 7535 version 4, incluant une carte électronique spécifique dont un lecteur de cartes à microprocesseur (CAM) ;
- ⇒ Le logiciel VPN IP version 4.6.1 embarqué dans le boîtier ;
- ⇒ Le logiciel embarqué dans de la ressource cryptographique (FPGA) 3DES v1.0 ou AES v2.0 gérant des clés de 128bits ou 256bits
- ⇒ Le logiciel CGM version 6.1 qui interagit avec un boîtier MISTRAL TRC 7535 frontal, permettant la protection des flux de gestion des autres boîtiers.

Tous les autres composants du système Mistral sont considérés comme hors du périmètre de l'évaluation, en particulier le système d'exploitation du boîtier Mistral TRC 7535 et le système d'exploitation du CGM.

Deux rôles sont définis et gérés par la TOE :

- ⇒ L'administrateur de la TOE. Il est responsable du maintien en condition opérationnelle de la TOE :
  1) Il doit générer depuis le CGM les CAM Utilisateurs
  2) Il doit placer la CAM Utilisateur dans le boîtier MISTRAL TRC 7535 pour lui permettre de démarrer. Selon le mode d'exploitation paramétré (cf. fonction F.GERE_CONF), la CAM Utilisateur doit ou non être laissée en permanence dans le lecteur ;
  3) Via le CGM, il peut accéder aux fonctions d'administration et de téléchargement logiciel (le téléchargement cryptographique n'étant pas possible à distance) ;
- ⇒ Le mainteneur de la TOE qui est un personnel de Thalès qui possède les CAM Superviseur, Téléchargement logiciel et Téléchargement cryptographique et qui peut mettre à jour les logiciels de la TOE, sur site ou après retour usine.

Dans la suite du document, le mot "Utilisateur" correspond aux utilisateurs des réseaux protégés par la TOE, y compris pour les utilisateurs des PC nomades protégés par le logiciel Mistral Nomade (appelés "Utilisateurs Nomades"). Seules exceptions, les exigences FIA et FMT de la CC Part 2 emploient le mot "Utilisateur" pour les utilisateurs ayant un rôle sur la TOE, à savoir l'Administrateur de la TOE et le Mainteneur de la TOE.

Techniquement, le boîtier MISTRAL TRC 7535 dispose de plusieurs interfaces qu'il est important d'identifier et de décrire :

- ○ Interface d'alimentation :

  Le boîtier MISTRAL TRC 7535 possède une alimentation secteur externe.

- ○ Voyants LED :

  Le boîtier boîtier MISTRAL TRC 7535 possède, entre autres, un voyant vert de mise sous tension, un voyant rouge d'alarme qui indique un état d'alarme du boîtier et deux voyants qui marquent l'activité de la ligne.

- ○ Interface série :

  Le boîtier MISTRAL TRC 7535 est entièrement administrable via un terminal externe branché sur le port série (interface RS232-C). Un mot de passe protège l'accès aux fonctions d'administration du boîtier.

- ○ Interface carte à puce :

  Le boîtier MISTRAL TRC 7535 possède un lecteur de cartes à microprocesseur (CAM) lui permettant de récupérer sa configuration initiale sur des cartes créées sur le CGM. Ce lecteur accepte uniquement les cartes GEMPLUS MPCOS 64K.

  Plusieurs types de carte à puce sont utilisés, notamment :
  - CAM Utilisateur : Carte personnalisée par le CGM et associée à un boîtier MISTRAL TRC 7535.
  - CAM Superviseur : Carte personnalisée par le CPC et permettant une administration locale d'un boîtier MISTRAL TRC 7535 par son port série.

- CAM Téléchargement logiciel : Carte personnalisée par le CPC (uniquement pour THALES) et permettant la mise à jour des logiciels du boîtier MISTRAL TRC 7535 (OS et logiciel spécifique)
- CAM Téléchargement cryptographique : Carte personnalisée par le CPC (uniquement pour THALES) et permettant la mise à jour de la ressource cryptographique (FPGA) du boîtier MISTRAL TRC 7535 (algorithmes de chiffrement).
- CAMs OEDP et Série : Cartes personnalisées par le CPC (uniquement pour THALES) et permettant la réalisation de tests usine pour le boîtier MISTRAL TRC 7535.

○ Interfaces Ethernet :

Le boîtier MISTRAL TRC 7535 possède deux interfaces Ethernet 10/100 Mbps, l'une « port clair » et l'autre « port chiffré ».

○ Interface d'effacement d'urgence :

Ce bouton d'effacement d'urgence situé en façade permet de provoquer l'effacement de la configuration du boîtier MISTRAL TRC 7535, quand celui-ci est alimenté. De plus, il existe un dispositif de détection d'ouverture interne au boîtier sous tension.

## 2.4 Biens sensibles protégés par la TOE

### 2.4.1 Biens sensibles de l'utilisateur

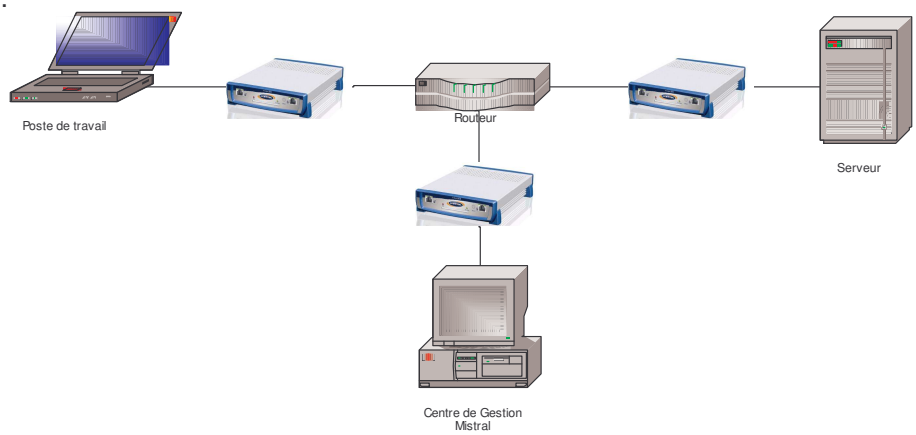
La TOE assure la protection de la confidentialité et/ou l'intégrité (selon le niveau de chiffrement sélectionné) des trames réseau indiquées comme sensibles dans sa configuration et échangées entre les utilisateurs à travers elle.
De plus, elle assure la protection de la confidentialité de la topologie des réseaux (en mode Tunnel ESP tunnel et ESP/UDP) indiqués comme sensibles dans sa configuration et dont les échanges entre les utilisateurs s'effectuent à travers elle.

### 2.4.2 Biens sensibles de la TOE

Le boîtier MISTRAL TRC 7535 assure la protection de l'accès à sa clé de base et aux clés de chiffrement, récupérées dans sa configuration sur CAM, saisies par console ou reçues de son CGM.
De plus, il assure la protection de la confidentialité et l'intégrité de ses paramètres de configuration de sécurité (table des SP, table de SA, table des valeurs des clés cryptographiques et table contenant la liste des protocoles autorisés en clair), des données d'authentification permettant de contrôler l'accès des différents acteurs.
Il assure aussi la protection de l'intégrité des logiciels VPN IP (y compris le système d'exploitation) et cryptographiques.
Enfin, le boîtier MISTRAL TRC 7535 Frontal assure la protection du logiciel CGM.

## 2.5 Plate-forme de tests pour l'évaluation de la TOE

Pour l'évaluation de la TOE, la plate-forme minimale suivante devra être mis en place par l'évaluateur :



# 3. Environnement de sécurité de la TOE

## 3.1 Hypothèses

**H.Adm_No_Evil** Administrateurs de confiance

Les administrateurs et mainteneurs locaux et distants sont des personnes de confiance et sont formés à l'utilisation de la TOE.

**H.Thief** Protection contre le vol d'une TOE

L'environnement de la TOE prévient tout vol de celle-ci.

**H.CGM_Phys_Acs** Protection physique du poste CGM

L'environnement de la TOE protège l'accès physique au poste CGM. Seul le personnel autorisé peut accéder physiquement au poste CGM.

**H.CGM_Acs_Control** Protection logique du poste CGM

L'accès au logiciel CGM nécessite une authentification de l'utilisateur sur le poste.

**H.CGM_Frontal** Connexion entre le poste CGM et le boîtier mistral Frontal

Le poste CGM est connecté directement au boîtier Mistral (la TOE) frontal.

## 3.2 Menaces identifiées

L'attaquant considéré dispose de bonnes compétences (en informatique et en cryptographie), de ressources modérées (plusieurs hommes.mois) et d'une bonne motivation. Ses méthodes d'attaque vont de l'exploitation d'une vulnérabilité connue d'un algorithme cryptographique aux attaques statistiques, « force brute » (essais exhaustifs) et « clair connu » (rejeu ou substitution).

**M.Sniff_User** Récupération d'informations sensibles des utilisateurs par écoute réseau

Un attaquant intercepte les communications réseau entre deux TOE et récupère les données sensibles échangées par des utilisateurs finaux.

**M.Sniff_CGM** Récupération de paramètres de configuration de la TOE par écoute réseau

Un attaquant intercepte les communications réseau entre une TOE et le CGM et récupère les paramètres de configuration de cette TOE, en particulier la table des SP, la table de SA, la table des clés et la table des protocoles clairs.

**M.Bypass** Contournement de la politique de sécurité de la TOE

Un attaquant profite du démarrage de la TOE pour récupérer, via le réseau, des flux réseau non chiffrés et obtenir des clés cryptographiques ou des informations sensibles des utilisateurs.

**M.Repair** Récupération d'informations sur une TOE en panne

Un attaquant analyse une TOE en panne et obtient des clés cryptographiques ou des informations sensibles des utilisateurs.

**M.Software_modif** Téléchargement non autorisé des logiciels de la TOE

Un attaquant tente de provoquer, via le réseau ou le port série, une mise à jour du logiciel spécifique ou de l'algorithme de chiffrement de la TOE et infecte celle-ci avec un logiciel malicieux.

**M.Policy_modif** Modification non autorisée de la configuration de la TOE

Un attaquant tente de modifier, via le réseau, par le port série ou par CAM, les politiques de chiffrement et de filtrage de la TOE, afin d'avoir accès, lors de leur transfert sur le réseau, à des informations sensibles des utilisateurs.

**M.Integrity** Modification non autorisée des paquets réseau entre deux TOE

Un attaquant modifie l'intégrité des paquets IP circulant entre deux TOE sans que les utilisateurs de ces informations s'en aperçoivent.

**M.Topology** Divulgation non autorisée de la topologie réseau des utilisateurs

Un attaquant analyse les paquets IP circulant entre deux TOE et reconstitue la topologie des réseaux des utilisateurs.

**M.Network_Spoof** Usurpation d'identité par modification des entêtes de protocole réseau

Un attaquant modifie les entêtes de protocole réseau des paquets IP circulant entre deux TOE, de telle manière qu'un utilisateur ou la TOE croit que la communication provient d'une source de confiance, différente de celle réellement d'origine.

**M.Alarms** Suppression non autorisée d'une alarme émise par la TOE

Un attaquant tente des attaques sur la TOE, intercepte les alarmes émises par la TOE vers le CGM et empêche leur diffusion, pour éviter une détection des attaques menées.

**M.CAM_Spoof** Usurpation d'identité par utilisation d'une « fausse » CAM

Un attaquant tente de se connecter à la TOE via le port série en présentant une « fausse » CAM, afin de modifier les paramètres de configuration de sécurité ou les logiciels de la TOE.

**M.TOE_Misuse** Mauvaise utilisation de la TOE

Suite à une mauvaise utilisation de la TOE consécutive à une erreur de l'administrateur de la TOE (mauvaise configuration, mauvaise administration), les règles de chiffrement et/ou de filtrage des flux mises en œuvre par la TOE ne sont plus conformes à la politique de sécurité du système d'information.

## 3.3 Politiques de sécurité organisationnelles

La TOE doit se conformer aux politiques de sécurité organisationnelles suivantes :

**P.Chiffrement_Flux** Politique de chiffrement de flux

La TOE doit mettre en œuvre des règles de chiffrement des flux sur la base de la politique de sécurité du système d'information.

**P.Filtrage_Flux** Politique de filtrage de flux

La TOE doit mettre en œuvre des règles de filtrage des flux sur la base de la politique de sécurité du système d'information.

**P.Visu_Regles** Visualisation des règles

La TOE doit offrir des possibilités de visualisation des règles de chiffrement et de filtrage courantes qu'elle met en œuvre, afin de s'assurer de la bonne application de la politique de sécurité du système d'information.

**P.Retour_Etat_Sur** Remise en état opérationnel

La TOE doit pouvoir être remise dans un état opérationnel et précédemment validé, après tout incident d'exploitation.

# 4. Objectifs de sécurité

## 4.1 Objectifs de sécurité pour la TOE

**O.Trusted_Channel** Canal de confiance avec les CAMs

La TOE doit fournir un canal de confiance entre la TOE et les différentes CAMs, pour effectuer des opérations d'authentification des CAMs des opérateurs.

**O.Data_Exch_Conf** Confidentialité des échanges de données

La TOE doit permettre un contrôle et une protection de la confidentialité des flux d'information avec les autres TOEs et avec les clients Mistral Nomade, sur la base de règles de chiffrement des flux.

**O.Data_Exch_Int** Intégrité des échanges de données

La TOE doit permettre un contrôle et une protection de l'intégrité des flux d'information avec les autres TOEs et avec les clients Mistral Nomade, sur la base de règles de chiffrement des flux.

**O.Data_Filter** Filtrage des échanges de données

La TOE doit permettre un contrôle des flux d'information avec les autres TOEs et avec les clients Mistral Nomade, sur la base de règles de filtrage des flux.

**O.Crypto_Key** Gestion des clés cryptographiques

La TOE doit assurer une protection appropriée pour les clés de chiffrement lors du stockage, de l'utilisation et de la destruction de ces clés au sein de la TOE.

**O.Crypto_Self_Test** Auto-test des fonctions cryptographiques

La TOE doit fournir la possibilité de vérifier que les fonctions cryptographiques fonctionnent comme spécifié.

**O.Default_Policy** Comportement par défaut de la TOE

La TOE doit par défaut bloquer tout flux la traversant, tant que sa phase de démarrage n'est pas terminée ou lors de changement de politique de sécurité.

**O.User_I&A** Identification et authentification des administrateurs

La TOE doit contrôler l'accès à la configuration des fonctions de sécurité par le port série, en identifiant et authentifiant les administrateurs possédant une CAM Superviseur, une CAM Téléchargement logiciel ou une CAM Téléchargement cryptographique.

**O.Policy_Admin** Administration de la TOE

La TOE doit pouvoir être administrée soit via le CGM par réseau, soit par CAM générées par le CGM ou soit via le port série à l'aide d'un PC. L'administration permet de décrire les règles de filtrage et de chiffrement des flux sur la TOE.

**O.No_Residual_Info** Effacement des informations résiduelles

La TOE doit offrir la possibilité d'un effacement d'urgence sous tension qui déclenche l'effacement des clés et des paramètres de configuration de sécurité conservés par la TOE.

**O.Soft_Upgrade** Mise à jour sécurisée des logiciels de la TOE

La TOE doit permettre la mise à jour sécurisée des logiciels VPN IP via le réseau en mode ESP tunnel et ESP/UDP par un administrateur depuis le CGM ou par le port série après authentification d'un administrateur possédant une CAM Téléchargement logiciel, et des logiciels cryptographiques uniquement par le port série après authentification d'un administrateur possédant une CAM Téléchargement

cryptographique.

**O.Alarm_Counter** Gestion d'un compteur d'alarmes

La TOE doit alerter le CGM à chaque incident de sécurité, par l'envoi d'une alarme via le réseau. La TOE doit gérer un compteur d'alarmes afin de numéroter de manière incrémentale les messages d'alarme envoyés au CGM.

**O.Visu_Regles** Visualisation des règles de la TOE

La TOE doit offrir des possibilités de visualisation de l'ensemble des règles de chiffrement et de filtrage qu'elle met en œuvre.

**O.Retour_Etat_Sur** Retour à un état opérationnel validé

La TOE doit pouvoir être remise dans un état opérationnel et précédemment validé après tout incident d'exploitation, par l'arrêt puis le redémarrage du boîtier.

## 4.2 Objectifs de sécurité pour l'environnement de la TOE

**OE.Adm_No_Evil** Administrateurs de confiance

L'organisme doit recruter des personnels de confiance comme administrateurs de la TOE et les former à l'utilisation de la TOE.

**OE.Appli_Politique** Mise en application de la politique de sécurité

Les administrateurs de la TOE doivent être formés et sensibilisés à la sécurité. Ils doivent appliquer la politique de sécurité du système d'information et vérifier périodiquement la conformité des règles de chiffrement et de filtrage mises en œuvre par la TOE par rapport à cette politique.

**OE.TOE_Phys_Acs** Contrôle d'accès physique à la TOE

L'organisme doit placer la TOE dans un environnement sécurisé qui prévient tout accès physique non autorisé à celle-ci.

**OE.CAM_Phys_Acs** Contrôle d'accès physique aux CAM

L'organisme doit gérer les CAM de la TOE de manière à prévenir tout accès physique non autorisé à celles-ci.

**OE.Key_Renew** Renouvellement des clés

L'organisme doit renouveler périodiquement les clés cryptographiques utilisées par la TOE, ceci via le CGM.

**OE.CGM_Phys_Acs** Contrôle d'accès physique au CGM

L'organisme doit placer le CGM dans un environnement sécurisé qui prévient tout accès physique non autorisé à celui-ci.

**OE.CEC_Phys_Acs** Contrôle d'accès physique au CEC

L'organisme doit placer le CEC dans un environnement sécurisé qui prévient tout accès physique non autorisé à celui-ci.

**OE.TOE_Install** Installation de la TOE en coupure des réseaux

L'organisme doit placer la TOE en coupure des réseaux à protéger, afin de garantir qu'aucun flux réseau ne peut contourner la TOE.

**OE.CGM_Channel** Canal sécurisé entre le CGM et la TOE

Le CGM communique avec les TOE qu'il supervise, via une TOE configuré en mode « boitier frontal », afin d'utiliser les services de sécurité de cette TOE pour protéger les flux d'administration. Le Frontal est connecté directement au CGM.

**OE.PC_Hyperterminal** Environnement logiciel hébergeant l'hyperterminal

Le terminal servant à l'administration de la TOE via son port console doit être protégé de tout dispositif tant matériel que logiciel (key logger matériel, cheval de Troie,...) permettant de capturer des éléments secrets de la configuration de la TOE lors de son administration locale (clé da base, clé de trafic,...).[1]

**OE.CGM_Acs_Control** Protection logique du poste CGM

L'utilisateur doit s'authentifier sur le poste avant d'accéder au logiciel CGM.

**OE.CGM_Frontal** Connexion entre le poste CGM et le boîtier mistral Frontal

Le poste CGM doit être connecté directement au boîtier Mistral (la TOE) frontal.

[1] On privilégiera la configuration par télégestion/CAM plutôt que l'administration locale par console.

# 5. Exigences de sécurité des Technologies de l'Information

## 5.1 Exigences de sécurité pour la TOE

### 5.1.1 Exigences de sécurité fonctionnelles pour la TOE

Les composants fonctionnels CC sélectionnés pour répondre aux objectifs de sécurité de la TOE sont les suivants :

| Composants CC Part 2 retenus | |
|---|---|
| FAU_ARP.1 | Alarmes de sécurité |
| FAU_SAA.1 | Analyse de violation potentielle |
| FCS_CKM.2 | Distribution de clés cryptographiques |
| FCS_CKM.4 | Destruction de clés cryptographiques |
| FCS_COP.1 | Opération cryptographique |
| FDP_ACC.2 | Contrôle d'accès complet |
| FDP_ACF.1 | Contrôle d'accès basé sur les attributs de sécurité |
| FDP_IFC.1 | Contrôle de flux d'informations partiel |
| FDP_IFF.1 | Attributs de sécurité simples |
| FDP_ITC.1 | Import des données utilisateur sans attribut de sécurité simple |
| FDP_RIP.2 | Protection totale des informations résiduelles |
| FDP_UCT.1 | Confidentialité élémentaire lors d'un échange de données |
| FDP_UIT.1 | Intégrité lors d'un échange de données |
| FIA_AFL.1 | Gestion d'une défaillance de l'authentification |
| FIA_UAU.2 | Authentification d'un utilisateur préalablement à toute action |
| FIA_UID.2 | Identification d'un utilisateur préalablement à toute action |
| FMT_MOF.1 | Gestion du comportement des fonctions de sécurité |
| FMT_MSA.1 | Gestion des attributs de sécurité |
| FMT_MSA.2 | Attributs de sécurité sûrs |
| FMT_MSA.3 | Initialisation statique d'attribut |
| FMT_MTD.1 | Gestion des données de la TSF |
| FMT_SMF.1 | Spécification des fonctions de gestion |
| FMT_SMR.1 | Rôles de sécurité |
| FPR_ANO.1 | Anonymat |
| FPT_AMT.1 | Test de la machine abstraite |
| FPT_ITC.1 | Confidentialité inter-TSF pendant une transmission |
| FPT_ITI.1 | Détection d'une modification inter-TSF |
| FPT_RPL.1 | Détection de rejeu |
| FPT_RCV.1 | Rétablissement manuel |
| FPT_TST.1 | Test de la TSF |
| FTP_TRP.1 | Canal de confiance inter-TSF |

# Classe FAU : Audit de sécurité

## FAU_ARP Réponse automatique de l'audit de sécurité

### FAU_ARP.1 Alarmes de sécurité

*Dépendances : FAU_SAA.1*

FAU_ARP.1.1 La TSF doit entreprendre [spécification : liste des actions les moins perturbatrices] **une remontée d'alarmes vers le CGM** dès détection d'une violation potentielle de la sécurité.

## FAU_SAA Analyse de l'audit de sécurité

### FAU_SAA.1 Analyse de violation potentielle

*Dépendances : FAU_GEN.1*

FAU_SAA.1.1 La TSF doit pouvoir appliquer un ensemble de règles en surveillant les événements audités et indiquer, en fonction de ces règles, une violation potentielle de la TSP.

FAU_SAA.1.2 La TSF doit appliquer les règles suivantes pour la surveillance des événements audités:

a) accumulation ou combinaison de [spécification : sous-ensemble d'événements auditables définis] **défauts logiciels** connus pour indiquer une violation potentielle de la sécurité;

b) [spécification: toutes les autres règles] **apparition d'un des évènements suivants :**

- **Mise sous tension du boîtier**
- **Retrait de la carte à puce**
- **Insertion d'une carte à puce**
- **Saisie à la console d'un mot de passe erroné**
- **Activation et fin d'activation à la console de la configuration du boîtier**
- **Fin d'activation à la console de la configuration du boîtier**
- **Réception d'un message ICMP "size too big"**
- **Echec de vérification de l'intégrité de la trame ESP (avec le champ authentification)**
- **SA inexistante avec ce SPI**
- **SP inexistante pour la trame encapsulée**
- **SP existe, mais paramètres différents de ceux de la trame**
- **Clé bientôt usée**
- **Clé usée**
- **Effacement d'urgence sur authentification**
- **Appui sur le bouton d'effacement d'urgence**
- **Détection d'intrusion**
- **Perte de link**
- **Remontée de link**
- **Alarme température (la température devient supérieure à 55°C mais est inférieure à 65°C, la température devient supérieure à 65°C, la température redevient inférieure à 55°C)**

# Classe FCS : Support cryptographique

## FCS_CKM Gestion de clés cryptographiques

### FCS_CKM.2 Distribution de clés cryptographiques

*Dépendances : [FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4, FMT_MSA.2*

FCS_CKM.2.1 La TSF doit distribuer les clés cryptographiques conformément à une méthode de distribution de clés cryptographiques [spécification : méthode de distribution de clés cryptographiques] **par utilisation d'une clé secrète de chiffrement de clé (clé de base)** qui satisfait à ce qui suit: [spécification: liste des normes] **aucune norme**.

### FCS_CKM.4 Destruction de clés cryptographiques

*Dépendances : [FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FMT_MSA.2*

FCS_CKM.4.1 La TSF doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée de clés cryptographiques [spécification : méthode de destruction de clés cryptographiques] **par réécriture de zéros sur les valeurs de clés en clair** qui satisfait à ce qui suit: [spécification: liste des normes] **aucune norme**.

## FCS_COP Opération cryptographique

### FCS_COP.1 Opération cryptographique

*Dépendances : [FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4, FMT_MSA.2*

FCS_COP.1.1 La TSF doit exécuter [spécification : liste des opérations cryptographiques] **des opérations de chiffrement et de scellement de données** conformément à un algorithme cryptographique spécifié [spécification: algorithme cryptographique] **3DES avec opération d'intégrité** et avec des tailles de clés cryptographiques [spécification : tailles de clés cryptographiques] **128 bits (équivalent à une protection de sécurité de 112 bits)** qui satisfont à ce qui suit: [spécification: liste des normes] **aucune norme**.

FCS_COP.1.1 La TSF doit exécuter [spécification : liste des opérations cryptographiques] **des opérations de chiffrement en CBC et de scellement de données en XCBC–MAC96** conformément à un algorithme cryptographique spécifié [spécification: algorithme cryptographique] **AES** et avec des tailles de clés cryptographiques [spécification : tailles de clés cryptographiques] **128 bits** qui satisfont à ce qui suit: [spécification: liste des normes] **RFC 3566**.

FCS_COP.1.1 La TSF doit exécuter [spécification : liste des opérations cryptographiques] **des opérations de chiffrement en CBC et de scellement de données en XCBC–MAC96** conformément à un algorithme cryptographique spécifié [spécification: algorithme cryptographique] **AES** et avec des tailles de clés cryptographiques [spécification : tailles de clés cryptographiques] **256 bits** qui satisfont à ce qui suit: [spécification: liste des normes] **RFC 3566**.

# Classe FDP : Protection des données de l'utilisateur

## FDP_ACC Politique de contrôle d'accès

### FDP_ACC.2 Contrôle d'accès complet

*Dépendances : FDP_ACF.1*

FDP_ACC.2.1 La TSF doit appliquer la [spécification : SFP de contrôle d'accès] **politique CONSOLE** aux [spécification: liste des sujets et objets] et toutes les opérations sur les sujets et objets couverts par la SFP.

**Sujets : Administrateurs de la TOE ;**
**Informations : Données de configuration de la TOE ;**

FDP_ACC.2.2 La TSF doit garantir que toutes les opérations entre tout sujet du TSC et tout objet du TSC sont couvertes par une SFP de contrôle d'accès.

### FDP_ACC.2 Contrôle d'accès complet

*Dépendances : FDP_ACF.1*

FDP_ACC.2.1 La TSF doit appliquer la [spécification : SFP de contrôle d'accès] **politique CGM** aux [spécification: liste des sujets et objets] et toutes les opérations sur les sujets et objets couverts par la SFP.

**Sujets : Administrateurs de la TOE ;**
**Informations : Données de configuration de la TOE ;**

FDP_ACC.2.2 La TSF doit garantir que toutes les opérations entre tout sujet du TSC et tout objet du TSC sont couvertes par une SFP de contrôle d'accès.

## FDP_ACF Fonctions de contrôle d'accès

### FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité

*Dépendances : FDP_ACC.1, FMT_MSA.3*

FDP_ACF.1.1 La TSF doit appliquer la [spécification: SFP de contrôle d'accès] **politique CONSOLE** aux objets en fonction des [spécification: attributs de sécurité, groupes d'attributs de sécurité cités] **types d'objet (paramètre résident, paramètre d'initialisation, table des SP, table des SA, table des clés, table des protocoles IP clairs)**.

FDP_ACF.1.2 La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée: [spécification: règles qui régissent les accès aux sujets contrôlés et aux objets contrôlés utilisant des opérations contrôlées sur des objets contrôlés] **contrôle de la saisie du mot de passe**.

FDP_ACF.1.3 La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [spécification : règles basées sur les attributs de sécurité, qui autorisent explicitement l'accès de sujets à des objets] **aucune règle**.

FDP_ACF.1.4 La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de [spécification : règles basées sur les attributs de sécurité, qui interdisent explicitement l'accès de sujets à des objets]

- **Les valeurs de clés ne sont pas accessibles,**
- **Toute exécution de code à distance est interdit.**

### FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité

*Dépendances : FDP_ACC.1, FMT_MSA.3*

FDP_ACF.1.1 La TSF doit appliquer la [spécification: SFP de contrôle d'accès] **politique CGM** aux objets en fonction des [spécification: attributs de sécurité, groupes d'attributs de sécurité cités] **types d'objet (paramètre résident, paramètre d'initialisation, table des SP, table des SA, table des clés, table des protocoles IP clairs)**.

FDP_ACF.1.2 La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée: [spécification: règles qui régissent les accès aux sujets contrôlés et aux objets contrôlés utilisant des opérations contrôlées sur des objets contrôlés] **connaissance de la clé de base de la TOE**.

FDP_ACF.1.3 La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [spécification : règles basées sur les attributs de sécurité, qui autorisent explicitement l'accès de sujets à des objets] **aucune règle**.

FDP_ACF.1.4 La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de [spécification : règles basées sur les attributs de sécurité, qui interdisent explicitement l'accès de sujets à des objets]

1) Les valeurs de clés ne sont pas accessibles,
2) Toute exécution de code à distance est interdit,

## FDP_IFC Politique de contrôle de flux d'informations

### FDP_IFC.1 Contrôle de flux d'informations partiel

*Dépendances : FDP_IFF.1*

FDP_IFC.1.1 La TSF doit appliquer la [spécification : SFP de contrôle de flux d'informations] **politique CLAIR** aux [spécification : liste des sujets, des informations et des opérations qui déclenchent le transfert d'informations contrôlées vers et en provenance de sujets contrôlés par la SFP]

**Sujets :** **Utilisateurs externes émettant et recevant des trames au travers de la TOE ;**
**Informations :** **Trames réseau émises par les utilisateurs et traversant la TOE ;**
**Opérations :** **Filtrage.**

### FDP_IFC.1 Contrôle de flux d'informations partiel

*Dépendances : FDP_IFF.1*

FDP_IFC.1.1 La TSF doit appliquer la [spécification : SFP de contrôle de flux d'informations] **politique VPN (hors clair)** aux [spécification : liste des sujets, des informations et des opérations qui déclenchent le transfert d'informations contrôlées vers et en provenance de sujets contrôlés par la SFP]

**Sujets :** **Utilisateurs externes émettant et recevant des trames au travers de la TOE ;**
**Administrateurs de la TOE ;**
**Informations :** **Trames réseau émises par les utilisateurs et traversant la TOE ;**
**Données de configuration de la TOE ;**
**Opérations :** **Filtrage selon le type de protocole IP, chiffrement/déchiffrement selon les adresses IP source et destination.**

## FDP_IFF Fonctions de contrôle de flux d'informations

### FDP_IFF.1 Attributs de sécurité simples

*Dépendances : FDP_IFC.1, FMT_MSA.3*

FDP_IFF.1.1 La TSF doit appliquer la [spécification : SFP de contrôle de flux d'informations] **politique CLAIR** en fonction des types suivants d'attributs de sécurité de sujets et d'informations: [spécification: le nombre minimum et le type des attributs de sécurité] **type de protocole IP, adresses IP source et destination**.

FDP_IFF.1.2 La TSF doit autoriser un flux d'informations entre un sujet contrôlé et des informations contrôlées par l'intermédiaire d'une opération contrôlée si les règles suivantes s'appliquent : [spécification : pour chaque opération, les relations basées sur les attributs de sécurité qui doivent exister entre les attributs de sécurité du sujet et les attributs de sécurité des informations]

- **Trames BGP, RIP/OSPF, DHCP, ARP, RARP, SNMP déclarée, ICMP Size too big déclarée, trame liée au traitement défaut Ethernet et IP, trame liée au SP claire.**
- **Trames ARP valides (égalité entre les adresses ARP source, ARP VRRP, ARP HSRP, ARP Safekit) qui n'est pas à destination du boîtier,**
- **Trames RARP qui n'est pas à destination du boîtier,**
- **Trames SNMP adressées à la TOE par la station d'administration SNMP,**
- **Trames ICMP de type "size too big",**
- **Type de protocole IP contenu dans la table de protocoles IP clairs de la TOE,**
- **Trames Ethernet différent d'ARP, RARP, Ethernet V2, 802.3 et 802.1Q,**
- **Trames IP (Ethernet V2, 802.3 et 802.1Q),**

FDP_IFF.1.3 La TSF doit appliquer les [spécification: règles complémentaires de la SFP de contrôle de flux d'informations] **aucune règle**.

FDP_IFF.1.4 La TSF doit fournir ce qui suit [spécification : liste des capacités complémentaires de la SFP] **aucune capacité**.

FDP_IFF.1.5 La TSF doit autoriser explicitement un flux d'informations en fonction des règles suivantes: [spécification: règles basées sur les attributs de sécurité, qui autorisent explicitement les flux d'informations]

1) **Si la trame ARP est valide (espace adresse, longueur) avec adresses ARP sources identiques, retransmission en clair,**
2) **Si la trame ARP est valide (espace adresse, longueur) avec adresses ARP sources différentes et contrôle ARP source désactivé, retransmission en clair,**
3) **Si la trame ARP de type HSRP est valide (espace adresse, longueur) avec adresses ARP sources différentes et contrôle ARP source activé et le contrôle ARP HSRP est activé, retransmission en clair,**
4) **Si la trame ARP de type VRRP est valide (espace adresse, longueur) avec adresses ARP sources différentes et contrôle ARP source activé et le contrôle ARP VRRP est activé, retransmission en clair,**
5) **Si la trame ARP de type Safekit est valide (espace adresse, longueur) avec adresses ARP sources différentes et contrôle ARP source activé et le contrôle ARP Safekit est activé, retransmission en clair,**
6) **Si le contrôle RARP est passant, retransmission en clair des trames RARP qui ne sont pas destinées à la TOE,**
7) **Si le mode par défaut Ethernet est passant, retransmission en clair de toutes les trames Ethernet différent d'ARP, RARP, Ethernet V2, 802.3 et 802.1Q,**
8) **Retransmission en clair de toutes les trames IP dont le type de protocole IP est contenu dans la table de protocoles IP clairs de la TOE,**
9) **Retransmission en clair de toutes les trames SNMP adressées à la TOE par la station d'administration SNMP,**
10) **Modification du MTU et envoi d'une alarme au CGM lors de la réception d'une trame ICMP de type "size too big" qui n'est pas à destination du boîtier lié aux modes chiffrement simple étendu et le contrôle est passant,**
11) **Modification du MTU et envoi d'une alarme au CGM lors de la réception d'une trame ICMP de type "size too big" à destination du boîtier lié à une SA ESP,**
12) **Trames IP (Ethernet V2, 802.3 et 802.1Q) qui correspondent à une SP claire,**
13) **Trames IP (Ethernet V2, 802.1Q) issues du CGM à destination d'un équipement frontal**

FDP_IFF.1.6 La TSF doit interdire explicitement un flux d'informations en fonction des règles suivantes: [spécification: règles basées sur les attributs de sécurité, qui interdisent explicitement les flux d'informations] **aucune règle**

### FDP_IFF.1 Attributs de sécurité simples

*Dépendances : FDP_IFC.1, FMT_MSA.3*

FDP_IFF.1.1 La TSF doit appliquer la [spécification : SFP de contrôle de flux d'informations] **politique VPN** en fonction des types suivants d'attributs de sécurité de sujets et d'informations: [spécification: le nombre minimum et le type des attributs de sécurité] **type de protocole IP, adresses IP source et destination**.

FDP_IFF.1.2 La TSF doit autoriser un flux d'informations entre un sujet contrôlé et des informations contrôlées par l'intermédiaire d'une opération contrôlée si les règles suivantes s'appliquent : [spécification : pour chaque opération, les relations basées sur les attributs de sécurité qui doivent exister entre les attributs de sécurité du sujet et les attributs de sécurité des informations]

1) **Trames IP (Ethernet V2, 802.3 et 802.1Q),**

FDP_IFF.1.3 La TSF doit appliquer les [spécification: règles complémentaires de la SFP de contrôle de flux d'informations] **aucune règle complémentaire**.

FDP_IFF.1.4 La TSF doit fournir ce qui suit [spécification : liste des capacités complémentaires de la SFP] **aucune capacité complémentaire**.

FDP_IFF.1.5 La TSF doit autoriser explicitement un flux d'informations en fonction des règles suivantes: [spécification: règles basées sur les attributs de sécurité, qui autorisent explicitement les flux d'informations]

1) **Trames IP (Ethernet V2, 802.1Q) issues du CGM qui correspondent à la SA de télégestion à destination d'un équipement nominal,**
2) **Trames IP (Ethernet V2, 802.3 et 802.1Q) qui correspond à une SP traite (c'est à dire chiffre ou déchiffre),**

FDP_IFF.1.6 La TSF doit interdire explicitement un flux d'informations en fonction des règles suivantes: [spécification: règles basées sur les attributs de sécurité, qui interdisent explicitement les flux d'informations].

1) **Trames IP (Ethernet V2, 802.3 et 802.1Q) qui correspond à une SP bloque**

## FDP_ITC Import hors du contrôle de la TSF

### FDP_ITC.1 Import des données utilisateur sans attribut de sécurité simple

*Dépendances : [FDP_ACC.1 ou FDP_IFC.1], FMT_MSA.3*

FDP_ITC.1.1 La TSF doit garantir [le contrôle d'accès SFP et/ou le flux d'information SFP] **la politique VPN, la politique CONSOLE** lors de l'import des données utilisateur, contrôlé par la SFP, hors de la TSC.

FDP_ITC.1.2 La TSF doit ignorer tous les attributs de sécurité simples associé avec les données utilisateur importées hors de la TSC.

FDP_ITC.1.3 La TSF doit garantir que les règles suivantes importées avec les données utilisateur sous le contrôle de la SFP en dehors de la TSC : [règles de contrôle additionnelles] : **aucune règle additionnelle**.

## FDP_RIP Protection des informations résiduelles

### FDP_RIP.2 Protection totale des informations résiduelles

*Dépendances : Aucune*

FDP_RIP.2.1 La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue inaccessible lors des [sélection: allocation de la ressource à, désallocation de la ressource de] **désallocation de la ressource de** tous les objets.

## FDP_UCT Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF

### FDP_UCT.1 Confidentialité élémentaire lors d'un échange de données

*Dépendances : [FTP_ITC.1 ou FTP_TRP.1], [FDP_ACC.1 ou FDP_IFC.1]*

FDP_UCT.1.1 La TSF doit appliquer les [spécification: SFP de contrôle d'accès ou SFP de contrôle de flux d'informations] **politiques VPN** afin de pouvoir [sélection : transmettre, recevoir] **transmettre ou recevoir** des objets d'une façon qui les protège d'une divulgation non autorisée.

## FDP_UIT Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF

### FDP_UIT.1 Intégrité lors d'un échange de données

*Dépendances : [FDP_ACC.1 ou FDP_IFC.1], [FTP_ITC.1 ou FTP_TRP.1]*

FDP_UIT.1.1 La TSF doit appliquer les [spécification: SFP de contrôle d'accès ou SFP de contrôle de flux d'informations] **politique VPN** afin de pouvoir [sélection : transmettre, recevoir] **transmettre ou recevoir** des objets d'une façon qui les protège d'erreurs de [sélection: modification, suppression, insertion, rejeu] **modification, suppression, insertion ou rejeu**.

FDP_UIT.1.2 La TSF doit pouvoir déterminer lors de la réception des données de l'utilisateur si une [sélection: modification, suppression, insertion, rejeu] **modification, suppression, insertion** a eu lieu.

# Classe FIA : Identification and authentification

## FIA_AFL Défaillances de l'authentification

FIA_AFL.1 Gestion d'une défaillance de l'authentification

*Dépendances : FIA_UAU.1*

FIA_AFL.1.1 La TSF doit détecter le fait que [spécification : nombre] **une** tentative d'authentification infructueuse a eu lieu en relation avec [spécification: liste d'événements liés à l'authentification] **l'accès au port console**.

FIA_AFL.1.2 Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit [spécification: liste d'actions] **envoyer une alarme vers le CGM**.

## FIA_UAU Authentification d'un utilisateur

FIA_UAU.2 Authentification d'un utilisateur préalablement à toute action

*Dépendances : FIA_UID.1*

FIA_UAU.2.1 La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

## FIA_UID Identification d'un utilisateur

FIA_UID.2 Identification d'un utilisateur préalablement à toute action

*Dépendances : Aucune*

FIA_UID.2.1 La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

# Classe FMT : Gestion de la sécurité

## FMT_MOF Gestion des fonctions de la TSF

### FMT_MOF.1 Gestion du comportement des fonctions de sécurité

*Dépendances : FMT_SMR.1, FMT_SMF.1*

FMT_MOF.1.1 La TSF doit restreindre la possibilité de [sélection : déterminer le comportement, désactiver, activer, modifier le comportement] **déterminer le comportement, désactiver, activer ou modifier le comportement** des fonctions [spécification: liste des fonctions] **de filtrage et de chiffrement de flux** aux [spécification: rôles autorisés identifiés] **administrateurs de la TOE**.

## FMT_MSA Gestion des attributs de sécurité

### FMT_MSA.1 Gestion des attributs de sécurité

*Dépendances : [FDP_ACC.1 ou FDP_IFC.1], FMT_SMR.1, FMT_SMF.1*

FMT_MSA.1.1 La TSF doit mettre en œuvre la [spécification: SFP de contrôle d'accès, SFP de contrôle des flux d'information] **politique CONSOLE ou CGM** pour restreindre aux [spécification : les rôles autorisés identifiés] **administrateurs de la TOE** la possibilité de [sélection: changer la valeur par défaut, interroger, modifier, supprimer, [spécification: autres opérations] **changer la valeur par défaut, interroger, modifier ou supprimer** les attributs de sécurité [spécification: liste des attributs de sécurité] : **les paramètres d'initialisation, la table des SP, la table des SA, la table des clés et la table des protocoles**.

### FMT_MSA.2 Attributs de sécurité sûrs

*Dépendances : ADV_SPM.1, [FDP_ACC.1 ou FDP_IFC.1], FMT_MSA.1, FMT_SMR.1*

FMT_MSA.2.1 La TSF doit garantir que seules des valeurs sûres sont acceptées pour les attributs de sécurité.

### FMT_MSA.3 Initialisation statique d'attribut

*Dépendances : FMT_MSA.1, FMT_SMR.1*

FMT_MSA.3.1 La TSF doit mettre en œuvre [spécification: SFP de contrôle d'accès, SFP de contrôle des flux d'information] **politique CONSOLE ou CGM** afin de fournir des valeurs par défaut [sélection : restrictives, permissives, autres propriétés] **restrictives** pour les attributs de sécurité qui sont utilisés pour appliquer la SFP.

FMT_MSA.3.2 La TSF doit permettre aux [spécification : les rôles autorisés identifiés] **aucun rôle** de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.

## FMT_MTD Gestion des données de la TSF

### FMT_MTD.1 Gestion des données de la TSF

*Dépendances : FMT_SMR.1, FMT_SMF.1*

FMT_MTD.1.1 La TSF doit restreindre la possibilité de [sélection : changer une valeur par défaut, interroger, modifier, supprimer, effacer [spécification : autres opérations] **changer une valeur par défaut, interroger, modifier, supprimer ou effacer** les [spécification: liste des données de la TSF] **paramètres d'initialisation, tables des SP, des SA, des clés et des protocoles IP clairs** aux [spécification: les rôles autorisés identifiés] **administrateurs de la TOE**.

### FMT_SMF Spécification des fonctions de gestion

FMT_SMF.1 Spécification des fonctions de gestion

*Dépendances : Aucune*

FMT_SMF.1.1 La TSF doit pouvoir réaliser les fonctions de gestion de sécurité suivantes : [l'insertion des éléments initiaux, la définition de la configuration de trafic, la mise à jour du logiciel et la remontée de configuration].

### FMT_SMR Rôles pour la gestion de la sécurité

FMT_SMR.1 Rôles de sécurité

*Dépendances : FIA_UID.1*

FMT_SMR.1.1 La TSF doit tenir à jour les rôles [spécification: les rôles autorisés identifiés] **Administrateur de la TOE et Mainteneur de la TOE**.

FMT_SMR.1.2 La TSF doit être capable d'associer les utilisateurs aux rôles.

# Classe FPR : Protection de la vie privée

### FPR_ANO Anonymat

FPR_ANO.1 Anonymat

*Dépendances : Aucune*

FPR_ANO.1.1 La TSF doit garantir que [spécification: ensemble d'utilisateurs ou de sujets] **des observateurs sur des réseaux publics** sont incapables de déterminer le véritable nom de l'utilisateur associé à [spécification: liste de sujets, d'opérations ou d'objets] **des trames réseau protégées par la TOE en mode ESP tunnel ou ESP/UDP**.

# Classe FPT : Protection des fonctions de sécurité de la TOE

## FPT_AMT Machine de test abstraite sous-jacente

FPT_AMT.1 Test de la machine abstraite

*Dépendances : Aucune*

FPT_AMT.1.1 La TSF doit exécuter une suite de tests [sélection: pendant le démarrage initial, de façon périodique pendant le fonctionnement normal, à la demande d'un utilisateur autorisé, autres conditions] **pendant le démarrage initial** pour démontrer l'application correcte des hypothèses de sécurité fournies par la machine abstraite qui sous-tend la TSF.

## FPT_ITC Confidentialité des données de la TSF exportées

FPT_ITC.1 Confidentialité inter-TSF pendant une transmission

*Dépendances : Aucune*

FPT_ITC.1.1 La TSF doit protéger toutes les données de la TSF transmises depuis la TSF vers un produit TI de confiance distant contre une divulgation non autorisée pendant leur transmission.

## FPT_ITI Intégrité des données de la TSF exportées

FPT_ITI.1 Détection d'une modification inter-TSF

*Dépendances : Aucune*

FPT_ITI.1.1 La TSF doit offrir la possibilité de détecter une modification de toutes les données de la TSF pendant leur transmission entre la TSF et un produit TI de confiance distant dans le cadre de la métrique suivante: [spécification: une métrique de modification définie] **équivalente à MD5 ou SHA-1 en 3DES et XCBC-MAC96 en AES**.

FPT_ITI.1.2 La TSF doit offrir la possibilité de contrôler l'intégrité de toutes les données de la TSF transmises entre la TSF et un produit TI de confiance distant et effectuer [spécification: action à entreprendre] **en mode Tunnel ESP tunnel et ESP/UDP, l'émission d'une alarme vers le CGM** si des modifications sont détectées.

## FPT_RPL Détection de rejeu

FPT_RPL.1 Détection de rejeu

*Dépendances : Aucune*

FPT_RPL.1.1 La TSF doit détecter le rejeu pour les entités suivantes: [spécification: liste des entités identifiées] **en mode Tunnel ESP tunnel et ESP/UDP, que ce soit entre le CGM et la TOE, ou que ce soit entre deux TOE**.

FPT_RPL.1.2 La TSF doit exécuter [spécification : liste des actions spécifiques] **le rejet des trames** quand le rejeu est détecté.

## FPT_RCV Rétablissement manuel

FPT_RCV.1 Rétablissement manuel

*Dépendances : AGD_ADM.1, ADV_SPM.1*

FPT_RCV.1.1 Après [sélection : une liste de défaillances/discontinuité de service] **un autotest incorrect**, la TSF doit entrer dans un mode maintenance où le retour à un état sécurisé est possible.

### FPT_TST Auto test de la TSF

FPT_TST.1 Test de la TSF

*Dépendances : FPT_AMT.1*

FPT_TST.1.1 La TSF doit exécuter une suite d'auto tests [sélection: pendant le démarrage initial, de façon périodique pendant le fonctionnement normal, à la demande de l'utilisateur autorisé, dans les conditions [spécification : conditions dans lesquelles l'auto test devrait intervenir]] **pendant le démarrage initial** pour démontrer le fonctionnement correct de la TSF.

FPT_TST.1.2 La TSF doit fournir aux utilisateurs autorisés la possibilité de contrôler l'intégrité de données de la TSF.

FPT_TST.1.3 La TSF doit fournir aux utilisateurs autorisés la possibilité de contrôler l'intégrité du code exécutable de la TSF mis en mémoire.

## Classe FTP : Chemins et canaux de confiance

### FTP_TRP Canal de confiance TSF - utilisateur

FTP_TRP.1 Canal de confiance TSF-utilisateur

*Dépendances : Aucune*

FTP_TRP.1.1 La TSF doit fournir un canal de communication entre elle-même et un utilisateur [local/distant] **local** qui soit logiquement distinct des autres canaux de communication et qui garantisse l'identification de ses extrémités et la protection des données transitant par le canal contre la modification ou la divulgation.

FTP_TRP.1.2 La TSF doit permettre à [sélection: la TSF, l'utilisateur local, l'utilisateur distant] **la TSF ou l'utilisateur local** d'initier la communication via le canal de confiance.

FTP_TRP.1.3 La TSF doit initier la communication via le canal de confiance pour [spécification : liste des fonctions pour lesquelles un canal de confiance est exigé] **l'identification et l'authentification par CAM**.

### 5.1.2 Exigences de sécurité d'assurance pour la TOE

Le niveau d'assurance visé par la TOE est le niveau :

**EAL3 augmenté de ALC_FLR.3, AVA_VLA.2**
**ainsi que de ADV_LLD.1, ADV_IMP.1 et ALC_TAT.1**
**pour la classe FCS**

Ce qui correspond à la sélection des composants d'assurance CC suivants :

| Composants CC Part 3 retenus | |
|---|---|
| ACM_CAP.3 | Contrôles des autorisations |
| ACM_SCP.1 | Couverture de la TOE par la CM |
| ADO_DEL.1 | Procédures de livraison |
| ADO_IGS.1 | Procédures d'installation, de génération et de démarrage |
| ADV_FSP.1 | Spécifications fonctionnelles informelles |
| ADV_HLD.2 | Conception de haut niveau de sécurité |
| ADV_IMP.1 | Sous-ensemble de l'implémentation de la TSF |
| ADV_LLD.1 | Conception de bas niveau descriptive |
| ADV_RCR.1 | Démonstration de correspondance informelle |
| AGD_ADM.1 | Guide de l'administrateur |
| AGD_USR.1 | Guide de l'utilisateur |
| ALC_DVS.1 | Identification des mesures de sécurité |
| ALC_FLR.3 | Correction d'erreur systématiques |
| ALC_TAT.1 | Outils de développement bien définis |
| ATE_COV.2 | Analyse de la couverture |
| ATE_DPT.1 | Conception de haut niveau |
| ATE_FUN.1 | Tests fonctionnels |
| ATE_IND.2 | Tests indépendants - par échantillonnage |
| AVA_MSU.1 | Examen des guides |
| AVA_SOF.1 | Evaluation de la résistance des fonctions de sécurité |
| AVA_VLA.2 | Analyse de vulnérabilité indépendante |

Ce niveau d'assurance respecte les dépendances entre les composants d'assurance CC mentionnés dans la Partie 3 des Critères Communs. Les composants ADV_LLD.1, ADV_IMP.1, ALC_TAT.1 ne concernent que les mécanismes cryptographiques exigés par la classe fonctionnelle FCS.

## 5.2 Exigences de sécurité pour l'environnement des TI

Aucune exigence particulière pour la TOE.

# 6. Spécifications globales de la TOE

## 6.1 Fonctions de sécurité de la TOE

La cible de l'évaluation réalise les fonctions de sécurité suivantes :

### F.GERE_CONF Gestion des paramètres de configuration

La TOE ne peut pas fonctionner sans être configurée. En sortie d'usine, elle ne contient pas de configuration (pas de clés). Les données de configuration sont réparties en cinq catégories :

- Les paramètres d'initialisation,
- Le fichier des Politiques de Sécurité (SP),
- Le fichier des Associations de Sécurité (SA),
- Le fichier des clés de trafic,
- Le fichier des protocoles IP clairs.

La TOE possède deux modes d'exploitation (modifiables par insertion CAM ou par menu) :

1) avec carte à puce : la TOE ne fonctionne que si une carte à puce est présente. La configuration complète de la TOE (comprenant les clés) est sauvegardée en mémoire volatile et est effacée lors du retrait de la carte à puce ou lors d'une mise hors tension,
2) sans carte à puce : la TOE fonctionne même après le retrait de la carte à puce. La configuration complète de la TOE (comprenant les clés) est sauvegardée en mémoire non volatile.

La TOE possède deux modes de fonctionnement :

1) Le fonctionnement local permet à l'opérateur d'exploiter la TOE sans la présence du CGM sur le réseau. Dans ce mode, si la table des SP est vide, alors la TOE est non opérationnelle.
2) Le fonctionnement télégéré permet à l'opérateur d'exploiter la TOE à distance à partir du CGM. Dans ce mode de fonctionnement, la table des SP peut être vide. Les données de télégestion sont transférées, soit dans la mémoire volatile si le mode d'exploitation est avec carte à puce, soit dans la mémoire non volatile si le mode d'exploitation est sans carte à puce.

Lors d'une mise sous tension, si la TOE a une carte à puce dans son lecteur, elle utilise les données contenues dans celle-ci pour effectuer son initialisation. Les éventuelles données contenues en mémoire non volatile sont alors effacées (si le dernier mode utilisé était le mode sans carte à puce).
Lors d'une mise sous tension, si la TOE n'a pas de carte à puce dans son lecteur, elle utilise les données contenues en mémoire non volatile pour effectuer son initialisation (si le dernier mode utilisé était un mode sans carte à puce). Un contrôle de validité des données est effectué avant leur utilisation.
L'arrêt de la TOE est obtenu, soit dès le retrait de la carte à puce ou après une mise hors tension dans le mode avec carte à puce. Dans cet état arrêt, la TOE ne contient plus aucune information sensible, soit après une mise hors tension dans le mode sans carte à puce. Dans cet état arrêt, la TOE contient des informations sensibles en mémoire non volatile.
La TOE possède trois types de paramètres : les paramètres résidents (enregistrés dans la mémoire non-volatile et uniquement accessibles à l'interface console), les paramètres de configuration (cinq jeux) et le cache ARP.

- La TOE possède un cache ARP qui contient les couples d'adresse Ethernet - IP pour le protocole ARP. Le cache ARP est mémorisé dans la mémoire de tri.
- Les paramètres résidents de la TOE sont l'adresse Ethernet (commune aux deux ports clair et chiffre), le mot de passe (d'accès à la console), le langage de l'interface console.
  Les paramètres résidents sont sauvegardés en mémoire non-volatile. Ils ne sont jamais effacés de la TOE, même après un téléchargement du logiciel.
  L'adresse Ethernet est liée au numéro de série afin de garantir l'unicité des adresses Ethernet. Elle est affectée en usine sur le banc de test final (modifiable qu'avec une CAM superviseur).
- Les paramètres de configuration de la TOE sont les paramètres d'initialisation, la table des SP, la table des SA, la table des clés et la table des protocoles IP clairs (20 maxi).

Les paramètres d'initialisation du boîtier Mistral sont :

| Paramètres du Mistral | Valeur possible | Valeur par défaut |
|---|---|---|
| Fichier de configuration | | |
| Configuration interne | | |
| Type de Mistral | Frontal/nominal | nominal |
| Mode de fonctionnement | local ou télégéré | local |
| Mode d'exploitation | avec ou sans CAM | sans CAM |
| Téléchargement par réseau | autorisé/interdit | autorisé |
| Surveillance tunnel(5) | 0 à 4096 | 0 |
| Configuration réseau | | |
| @ IP Mistral | (1) | 0.0.0.0 |
| @ IP virtuelle Mistral(5) | (1) | 0.0.0.0 |
| Masque de sous réseau | (2) | 0.0.0.0 |
| @ IP routeur côté clair | (1) 0.0.0.0 = pas de routeur | 0.0.0.0 |
| @ IP routeur côté chiffre | (1) 0.0.0.0 = pas de routeur | 0.0.0.0 |
| @ IP administrateur SNMP | (3) 0.0.0.0 = pas d'administrateur | 0.0.0.0 |
| Interface SNMP(5) | chiffre/clair | chiffre |
| Numéro de VLAN SNMP(5) | 0 à 4095 | 0 |
| Apprentissage VLAN SNMP(5) | Autorisé/Interdit | Interdit |
| Perte de link(5) | cloisonnée/propagée | cloisonnée |
| Interface Ethernet | 10 HD, 10 FD, 100 HD, 100 FD, Auto négocié | Auto négocié |
| Configuration sécurité | | |
| @ IP Frontal | (3) | 0.0.0.0 |
| @ IP Centre de Gestion | (3) | 0.0.0.0 |
| @ IP Frontal de secours (5) | (3) | 0.0.0.0 |
| @ IP Centre de Gestion de secours (5) | (3) | 0.0.0.0 |
| Interface de télégestion | chiffre/clair | chiffre |
| Numéro de VLAN de télégestion (5) | 0 à 4095 | 0 |
| Apprentissage VLAN de télégestion (5) | Autorisé/Interdit | Interdit |
| SA de télégestion | Idem SA de trafic | Idem SA de trafic |
| Clé de base | Idem clé de trafic | Idem clé de trafic |
| Port UDP des alarmes | (4) | 8002 |
| Configuration contrôle et traitement par défaut | | |
| Mode par défaut Ethernet | | |
| Type Ethernet inconnu | bloquant, passant | bloquant |
| Contrôle validité @ ARP source | actif, inactif | actif |
| Contrôle validité @ ARP VRRP | actif, inactif | actif |
| Contrôle validité @ ARP HSRP | actif, inactif | actif |
| Contrôle validité @ ARP SafeKit | actif, inactif | inactif |
| RARP | bloquant, passant | passant |
| BGP (7) | bloquant, passant | bloquant |
| RIP/OSPF (7) | bloquant, passant | bloquant |
| DHCP (7) | bloquant, passant | bloquant |
| Mode par défaut IP | | |
| Hors SPD | bloquant, passant | bloquant |
| ICMP Size too big étendu | bloquant, passant | passant |
| Traitement lié à la durée de vie | traite/bloque | traite |

Tableau 1 : Paramètres d'initialisation du boîtier

Contrôles effectués à la saisie des paramètres :

(1) toutes les adresses réseaux sur 32 bits sont autorisées y compris l'adresse nulle

(2) seuls sont autorisés les masques sur 32 bits avec des bits à 1 uniquement dans les bits de poids fort.

(3) les adresses réseaux situées dans le même réseau que la TOE ou que celui du routeur côté port d'administration sont autorisées. Sinon, un warning est généré pour signaler que la TOE essaiera de contacter le destinataire directement même s'il n'est pas dans son sous-réseau et qu'il n'y a pas de routeur.

(4) tous les numéros de ports de 0 à 65535 inclus sont autorisés.

(5) nouvelles fonctionnalités V4.5.2.2.

(6) les paramètres sont réservés pour des versions futures.

(7) nouvelles fonctionnalités V4.6.1

Note 1 : les paramètres de la configuration sécurité (@IP Mistral Frontal, @ IP du Centre de Gestion, interface télégestion, apprentissage VLAN télégestion, numéro VLAN télégestion, port UDP des alarmes, SA de télégestion et clé de base) ne sont utilisés que lorsque le mode de fonctionnement est télégéré.

Note 2 : tous les paramètres sont télégérables sauf :

- @ IP Mistral,
- @ IP Frontal,
- @ IP Centre de Gestion,
- @ IP Frontal de secours,
- @ IP Centre de Gestion de secours ,
- SA de télégestion,
- Clé de base,
- Port UDP des alarmes,
- Type de Mistral,
- Mode de fonctionnement,
- Mode d'exploitation,
- Téléchargement par réseau.

Note 3 : les contrôles décrits ci-dessus sont effectués :

- lors d'une saisie à la console au boîtier,
- lors d'une lecture de carte à puce,
- lors d'une télégestion.

La TOE possède une table des protocoles IP clairs qui peut contenir jusqu'à 20 numéros de protocole. Cette table contient une liste des protocoles parmi ceux proposées par la RFC1700.

## F.GERE_SP_SA Gestion des SP et des SA

Une SP est utilisée par la TOE pour représenter un flux de communication élémentaire. Elle est définie par un sens de communication (chiffrement ou déchiffrement), un couple adresse / masque IP source et un couple adresse / masque IP destination, les listes des protocoles IP, le type de traitement à effectuer (clair / traite / bloque), l'adresse IP et le type du chiffreur destinataire. Lorsque le traitement SP est « traite », le numéro de SPI désigne la SA qui sert à chiffrer ou déchiffrer les données.
A tout paquet IP reçu par la TOE (dont le protocole IP ne correspond pas à la liste de protocoles clairs), est associé une unique SP. La SP détermine ensuite le traitement à effectuer sur le paquet (chiffrement/déchiffrement, transmission en clair, rejet du paquet).

Note : une SP est unidirectionnelle. Il faut donc définir deux SP pour gérer un flux bidirectionnel.

La TOE accepte les inclusions de SP. Par contre, la TOE empêche les imbrications de SP en refusant l'activation de la configuration de sécurité.

Une SA décrit une opération de chiffrement élémentaire. La SA est définie par son numéro de SPI. Elle contient l'index de la clé, le niveau de chiffrement des paquets, la crypto-période de la clé et son seuil d'usure.

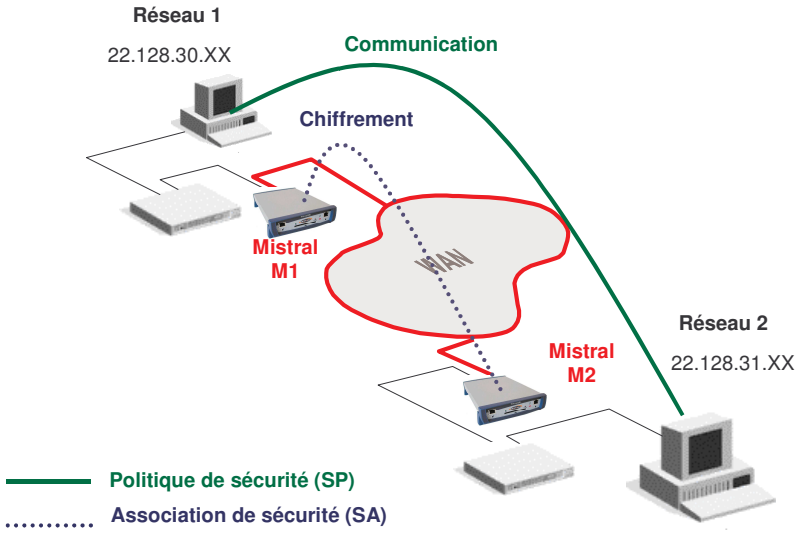



**Figure 3 : Politiques et associations de sécurité**

### F.GERE_CLES Gestion des clés de chiffrement

La TOE utilise des clés secrètes de taille 128 bits en 3DES et 128 ou 256 bits en AES qui sont identifiées par un GIC de 6 octets. Les clés sont de deux types différents :

- des clés de base (pour chiffrer les flux de télégestion),
- des clés de trafic (pour chiffrer les flux réseau provenant d'utilisateurs).

Sauf pour la version AES, la TOE n'accepte que des clés certifiées CONCERTO, l'algorithme de certification de clés de THALES.

L'usure des clés ne s'applique qu'aux SA de trafic et non aux SA de télégestion. Le seuil d'usure est initialisé par l'administrateur de la TOE à la création de la SA. Le compteur d'usure est sauvegardé dans la mémoire volatile de la TOE.

Pour la TOE, le compteur d'usure est initialisé à 0, soit en cas d'arrêt/marche du boîtier, soit lors de la première déclaration de la SA dans la TOE (reçue par télégestion, par carte à puce ou par la console), ou au renouvellement de la clé.

Le compteur d'usure est incrémenté d'une unité à chaque chiffrement et déchiffrement d'une trame qui utilise sa SA.

La TOE possède un paramètre de traitement des trames en cas d'usure d'une clé qui vaut "Continuer" ou bien "Bloquer".

Lorsque le compteur d'usure atteint 80% du seuil d'usure et que le seuil d'usure est différent de 0, la TOE envoie une alarme "SA n°SPI contenant la clé n°GIC usée à 80%" au CGM. Lorsque le compteur d'usure atteint le seuil d'usure et que le seuil d'usure est différent de 0, La TOE envoie au CGM une alarme "SA n°SPI contenant la clé n°GIC usée". Si le paramètre de traitement en cas d'usure est "Bloquer", alors toutes les prochaines trames qui utilisent la SA sont bloquées. Sinon, toutes les prochaines trames qui utilisent la SA sont traitées comme indiqué dans la SP.

La crypto-période est une valeur indiquant la durée d'utilisation de la clé. Elle est gérée par le CGM. Bien qu'elle soit transmise dans le fichier des SA, la TOE ne traite pas cette valeur.

### F.GERE_FLUX_CLAIR Gestion des flux clairs

Le cache ARP est commun aux deux ports. A chaque entrée, sont associées l'adresse IP d'un équipement donné et l'adresse MAC de cet équipement. Le cache ARP est effacé à chaque fois que la configuration du boîtier est activée et fonctionne en mode FIFO.
La TOE émet une requête ARP lorsqu'elle cherche à dialoguer avec un hôte qui n'est pas défini dans le cache ARP. Le cas peut apparaître lors d'un déchiffrement en mode ESP tunnel ou ESP/UDP ou lors de l'émission de données propres à la télégestion (requête, acquittement). Les adresses IP broadcast et muticast ne génèrent pas de demande ARP. Elles sont directement "mappées" à des adresses Ethernet conformément au RFC1042 [page 4] et RFC1112 [page 6]. La TOE est capable de gérer une attente cumulée de 10 requêtes ARP en sauvegardant le datagramme IP ayant déclenché la requête ARP. Au delà, tout datagramme IP nécessitant une requête ARP est jeté. De même, tout datagramme IP nécessitant une adresse en cours de résolution est jetée. Un timeout est déclenché sur tout envoi de requête ARP.
La TOE ne prend en compte une réponse ARP que si celle-ci est corrélée à l'envoi préalable d'une requête ARP. L'attente d'une réponse ARP n'entraîne pas d'indisponibilité du boîtier vis à vis de ses services.
La TOE n'émet pas de ARP gratuit, lors de sa mise sous tension. La TOE prend en compte les ARP gratuits uniquement des équipements ayant une entrée dans le cache ARP.
La TOE émet une réponse ARP uniquement suite à la réception d'une requête ARP lui demandant son adresse MAC.
La TOE contrôle (cohérence des champs du PDU ARP (espace adresse, longueur, …)) puis laisse passer les trames ARP Request et ARP Reply qui ne lui sont pas destinées. Un contrôle de cohérence (débrayable) est effectué sur les adresses ARP source entre l'adresse MAC et le PDU ARP. Lorsque le contrôle est activé, on peut néanmoins contrôler s'il ne s'agit pas d'ARP type VRRP ou HSRP ou Safekit (débrayable pour chaque type). Toute trame incorrecte est jetée.
La TOE ne laisse passer les trames RARP que si le traitement par défaut RARP est passant.
La TOE retransmet en clair tous les paquets IP dont le numéro de protocole IP est contenu dans sa table de protocoles IP clairs. Ceci est valable pour les deux sens (du port chiffre au port clair et inversement) et quelque soit le contenu de sa table des SP.
Si un datagramme à chiffrer en mode ESP tunnel ou ESP/UDP doit être fragmenté alors qu'il possède le bit « Don't Fragment » positionné, la TOE émet un ICMP « size too big » en clair vers l'émetteur du datagramme. La TOE n'émet pas d'ICMP « size too big » si l'adresse émetteur du datagramme ayant déclenché l'envoi du paquet ICMP correspond à une adresse de diffusion (FF.FF.FF.FF).
Lorsque La TOE reçoit un ICMP "size too big" :

- S'il lui est destiné, il envoie une alarme vers le CGM. Il met à jour le MTU de sa ligne en respectant un MTU plancher. Au bout d'un hors temps, le MTU de la ligne reprend sa valeur initiale. Le MTU plancher est fixé à 576 octets.
- S'il ne lui est pas destiné, celui-ci vérifie que le MTU est supérieur à 576 et que le paquet originel correspond à une SP en chiffrement simple étendu. Dans ce cas, si le mode de traitement par défaut IP – ICMP Size too big est passant, il effectue un RAZ des données de la trame répétées et émet la trame sur son autre port. Enfin, à chaque réception d'ICMP size too big, si le paquet originel correspond à une SP en chiffrement simple étendu, le chiffreur émet une alarme au CGM.

La TOE gère une MIB de type MIB II (voir [RFC1213]), consultable par le protocole SNMPv1 (voir [RFC1157]). Elle répond aux requêtes SNMP émises à destination du port UDP 161, mais elle n'émet pas de messages TRAP.
Les requêtes sont issues d'un logiciel d'administration SNMP externe au système Mistral. La TOE répond en clair aux requêtes SNMP en clair émises par l'administrateur SNMP externe déclaré sur la TOE sur son interface SNMP uniquement. L'interface SNMP est soit fixe (clair ou chiffre) soit en mode apprentissage. De plus, les communications peuvent se faire sur un VLAN (apprentissage VLAN possible).
En mode télégéré uniquement, La TOE répond en chiffré aux requêtes SNMP en chiffré émises par le CGM (via le canal de télégestion).

La TOE ne gère que les trois groupes de la MIB II standard "System", "Interfaces" et "IP". Les groupes "System" et "Interfaces" sont renseignés complètement. Il n'existe pas de MIB privée. La TOE visualise 2 interfaces reflétant distinctement l'état du port clair et du port chiffre.

### F.FILTRE_FLUX Filtrage des flux réseau

La TOE est capable de décoder les protocoles IPv4, ARP et RARP dans les trames Ethernet V2 ou Ethernet 802.3 LLC SNAP, avec ou sans TAG 802.1Q. La TOE retransmet les trames de trafic sans changer l'entête Ethernet.
La TOE génère les trames d'administration (télégestion, alarme, SNMP et ping) dans le format Ethernet V2 sans TAG802.1Q.
Si le mode par défaut Ethernet est Bloquant, les trames Ethernet de type différent de IP, ARP et RARP ne sont pas retransmises par la TOE. Si le mode par défaut Ethernet est Passant, les trames Ethernet de type différent de IP, ARP et RARP sont retransmises en clair par la TOE.
Avant d'effectuer le filtrage lié aux SP, la TOE laisse la possibilité de laisser passer en clair les protocoles DHCP, BGP, RIP/OSPF (3 options différentes). Si l'option correspondante au protocole est déclarée à passante, la TOE laisse passer le flux en clair le protocole, sinon la TOE exécute le filtrage lié au SP.
La TOE traite uniquement les paquets au niveau du protocole IP. Le filtrage des trames est effectué sur le couple d'adresses IP. Sauf pour quelques paquets spéciaux, la TOE analyse chaque SP pour déterminer si celle-ci correspond au paquet IP reçu. Pour qu'une SP corresponde à une trame IP, il est nécessaire que :

- la trame IP arrive dans le même sens que celui de la SP,
- l'adresse IP source de la trame IP appartient au sous-réseau défini par la SP,
- l'adresse IP destination de la trame IP appartient au sous-réseau défini par la SP.

Si une ou plusieurs SP correspondent à une trame IP, c'est la SP la plus restrictive qui est choisie pour traiter la trame IP.
Les paramètres indiqués dans la SP dictent les actions à effectuer sur ce paquet. Il y a trois traitements possibles :

- Passant : la trame est transmise en clair,
- Bloquant : la trame est bloquée,
- Traitement : la trame est chiffrée (ou déchiffrée) en utilisant les paramètres de la SA.

Si aucune SP ne correspond à la trame IP, la trame est, soit retransmise en clair si le mode par défaut IP est passant, soit détruite si le mode par défaut IP est bloquant.
Si la liste des protocoles IP est vide, alors la SP donnée autorise tous les protocoles IP. Sinon, si le protocole est dans la liste, alors le paquet est accepté, sinon il est jeté.
Le filtrage des protocoles IP est réalisé en émission et en réception sur tous les fragments IP.

### F.CHIFFRE_FLUX Chiffrement des flux réseau

La TOE utilise les deux interfaces Ethernet port clair et port chiffre. Elle chiffre les données qui lui arrivent sur son port clair et les retransmet sur son port chiffre après chiffrement et un filtrage éventuel. Inversement, elle déchiffre les données qui lui arrivent sur son port chiffre et les retransmet en clair sur son port clair après un éventuel filtrage.
La TOE supporte les algorithmes 3DES, AES (gérant des clés de 128 ou 256 bits).
Pour la TOE, le niveau de chiffrement de la SA peut prendre les valeurs suivantes : chiffrement simple (IP ou TCP entête clair) ou chiffrement simple étendu (IP étendu, TCP entête recalculé étendu ou TCP entête recopié étendu) ou chiffrement ESP tunnel ou ESP/UDP.

1) *chiffrement simple (IP et TCP/UDP entête clair)*
   En mode de chiffrement simple, La TOE assure la confidentialité des communications, mais pas l'intégrité des trames.
   Ce mode de chiffrement ne modifie pas la longueur des trames (donc pas de fragmentation) et ne modifie pas les données non chiffrées. Il chiffre la zone à protéger en confidentialité par bloc indépendants de 64 bits (avec le mode dictionnaire ou reliquat si la taille n'est pas modulo 64 bits).
   Les actions effectuées par la TOE lors du chiffrement simple sont la vérification de la SP, puis le chiffrement.
   Les actions effectuées par la TOE lors du déchiffrement simple sont le déchiffrement en fonction des adresses IP source et destination, puis la vérification de la SP.
   Le mode AES ne dispose pas de chiffrement simple (il y a conversion en mode de chiffrement simple étendu).
2) *chiffrement simple étendu (IP étendu,* TCP entête recalculé étendu ou TCP entête recopié étendu*)*
   En mode de chiffrement simple étendu, la TOE assure la confidentialité des communications, mais pas l'intégrité des trames.
   Ce mode de chiffrement ne modifie pas la longueur des trames. Le mode chiffrement simple étendu chiffre la zone à protéger en confidentialité par blocs chaînés (CBC). Il n'y a pas de reliquat de début et les reliquats de fin sont chaînés. Le bit DF est positionné à 1 et le checksum IP est remis à jour. Le déchiffrement simple étendu ne modifie pas le bit DF. Sinon, le mode de chiffrement simple étendu ne modifie pas les données non chiffrées (hormis le checksum TCP et UDP en TCP entête recalculé étendu).
   Les actions à effectuer lors du chiffrement simple étendu sont les suivantes : la vérification de la SP, le chiffrement, le positionnement s du bit DF à 1 et la mise à jour du checksum IP, et le calcul du checksum TCP/UDP en chiffrement TCP entête recalculé étendu.
   Les actions effectuées par la TOE lors du déchiffrement simple étendu sont la vérification de la SP, la vérification du checksum TCP/UDP en chiffrement TCP entête clair étendu, le déchiffrement en fonction des adresses IP source et destination, et le calcul du checksum TCP/UDP en chiffrement TCP entête recalculé étendu.
3) *ESP tunnel*
   Les services de sécurité offerts par ce mode sont la confidentialité et l'intégrité des trames IP, le masquage des adresses et l'authentification de l'émetteur.
   Le paquet IP d'origine est intégralement chiffré (entête et data) et encapsulé dans une nouvelle trame IP (numéro de protocole est 50 : ESP) où le bit DF est positionné. Outre la trame encapsulée, la nouvelle trame comporte le SPI de la SA de chiffrement, un marquant, un numéro de séquence, un bourrage et un champ authentification. Le chiffrement est indépendant pour chaque paquet IP. Cette trame est à destination de l'équipement de chiffrement distant renseigné dans la SP.
   Les actions effectuées par la TOE lors du chiffrement en mode ESP sont la vérification de la SP, la création du nouveau paquet ESP, puis le chiffrement du datagramme. Si l'adresse IP virtuelle existe, la trame est émise avec comme adresse IP source l'adresse IP virtuelle, sinon, on prend l'adresse IP du boîtier.
   Les actions effectuées par la TOE lors du déchiffrement ESP sont le déchiffrement du datagramme en fonction du SPI pour les trames ayant pour adresse IP destination l'adresse

IP du boîtier ou l'adresse IP virtuelle si elle existe, la vérification de la SP, puis extraction du paquet IP original.
Dans le cas d'un chiffrement ESP tunnel, la zone des données chiffrées et protégées en intégrité s'étend du champ Marquant au champ authentification inclus. La longueur du champ bourrage est telle que la zone des données chiffrées et protégées en intégrité soit un multiple de 8 octets (16 en AES).
En AES, le chiffrement des données se fait en CBC. En AES, le MAC ajouté est XCBC – MAC96 calculé sur les données chiffrées. La clé utilisée pour l'authentification est la clé fournie par la configuration active. La clé utilisée pour le chiffrement est le résultat du chiffrement d'un motif par la clé fournie par la configuration active (cf. RFC 3566).
En mode de chiffrement ESP tunnel, la TOE fragmente avant chiffrement les paquets IP qui ont le bit DF=0 et qui auraient après chiffrement une longueur supérieure au MTU indiqué dans la SA associée. Lors de la fragmentation, les champs modifiés de l'entête IP d'origine sont "total length", "fragment offset" et "header checksum".
Lors de l'activation d'une configuration dans la TOE, le numéro de séquence de chaque SA est initialisé à 0. Le premier paquet IP émis d'une SA ESP donnée possède un numéro de séquence égal à 1. A chaque nouveau paquet IP émis par cette même SA, le numéro de séquence est incrémenté.
La TOE transmet un numéro de séquence qu'elle incrémente pour chaque trame chiffrée. Ainsi, deux trames émises à la suite sont chiffrées différemment. Mais elle ne gère pas l'anti-rejeu à la réception.

4) *ESP/UDP*

Le mode de chiffrement ESP/UDP a les mêmes caractéristiques que le mode de chiffrement ESP tunnel à la différence suivante près : encapsulation de la trame dans une trame UDP avec numéro de port 500 en port source et le port 500 en port destination ou le port homologue naté (appris au déchiffrement).

### F.TELEGERE Télégestion

Tous les échanges entre le CGM et une TOE (configurée en mode "Télégéré") utilisent par boîtier, une clé de base et une SA de télégestion propre à chaque TOE, deux SP (chiffrement/déchiffrement, avec la SA, CGM-TOE équipement distant Frontal ou TOE). Ces paramètres sont transmis par carte à puce ou rentré par menu. Les trames de télégestion ne peuvent pas arriver en 802.3 (PC CGM). La télégestion peut s'effectuer en VLAN (mode apprentissage VLAN possible).
Pour le CGM, la TOE est configurée en mode "Frontal" pour chiffrer toutes les communications à destination des autres TOE à télégérer. Les trames de télégestion de la TOE à télégérer sont en clair entre le CGM et la TOE en mode "Frontal", puis chiffrées entre la TOE en mode "Frontal" et la TOE à télégérer. Les trames de télégestion de la TOE en mode "Frontal" sont en clair.
Le chiffrement/déchiffrement des trames de télégestion s'effectue sur le même port Ethernet de la TOE : déchiffrement en réception et chiffrement en émission. Ce port est soit fixe (clair ou chiffre) soit en mode apprentissage (alarme émise sur le dernier port appris).
La TOE reconnaît son adresse IP dans le champ destinataire de toutes les trames. Elle accepte une trame qui lui est destinée (vérification de l'adresse IP) uniquement si les conditions suivantes sont respectées : mode de fonctionnement télégéré, trame en provenance du CGM (vérification de l'adresse IP), trame en provenance du port de télégestion autorisé (port clair ou chiffre). Dans tous les cas, il n'y a pas de test sur la liste des protocoles clairs.
La télégestion est une fonction basée sur le protocole TCP. Elle est réalisée à l'initiative de l'opérateur CGM permettant de charger via le réseau dans la TOE les données qui le concernant : les paramètres d'initialisation (hormis l'adresse IP Mistral, la SA de télégestion, la SP de télégestion, la clé de base, le port UDP des alarmes, le type de Mistral, le mode de fonctionnement, le mode d'exploitation, le téléchargement par réseau.), la table des SP (2000 maxi en version Fast et Basic, et 12000 en 6000 tunnels), la table des SA (1000 maxi en version Fast et Basic, et 6000 en 6000 tunnels), la table des clés de trafic (1000 maxi en version Fast et Basic, et 6000 en 6000 tunnels) et la table des protocoles clairs (20 maxi). La télégestion efface les données ci-dessus préalablement chargées dans la TOE.
Pour vérifier la configuration sur la TOE, le CGM peut effectuer une remontée de toute la configuration (les paramètres d'initialisation, la table des SP, la table des SA, la table des clés de trafic et la table des protocoles clairs).
La TOE traite les trames ICMP (type 0, code 0) en réponse à une demande d'écho (ping) venant du CGM. La TOE refuse le rejeu de la télégestion si la SA de télégestion est ESP tunnel ou ESP/UDP.
Le CGM permet de renouveler une seule clé dans les paramètres de trafic que la TOE prend immédiatement en compte

### F.TELECHARGE_LOG Téléchargement des logiciels

Le logiciel de la TOE est téléchargeable, via son port série, avec le logiciel Hyperterminal de Windows. Cette opération nécessite une carte à puce de téléchargement.
Le logiciel de la TOE est téléchargeable, via le réseau, à partir du CGM. Le téléchargement via le CGM est autorisé par la TOE si les conditions suivantes sont respectées :

- téléchargement effectué par le CGM (vérification de l'adresse IP du CGM sur la TOE),
- la TOE dans le mode "Télégéré".
- le paramètre "Téléchargement" a la valeur "Autorisé",
- les versions logicielles anciennes et nouvelles sont compatibles,
- les versions logicielles sont compatibles des versions matérielles.

Le fichier à télécharger comprend le code exécutable et un CRC. La mise à jour du logiciel est effectuée si la vérification par la TOE du CRC est correct.
Lorsque le téléchargement est réussi, la TOE est réinitialisée. Toutes les données en mémoire sont effacées, hormis les paramètres résidents ainsi que les paramètres d'initialisation.

Deux mécanismes de contrôle d'accès sont mis en œuvre :

- Contrôle d'accès « Superviseur / Téléchargement ». Ce contrôle d'accès autorise ou non l'accès à aux fonctions Superviseur et aux fonctions de téléchargement.

- Contrôle d'accès « Téléchargement crypto ». Ce contrôle d'accès autorise ou non l'accès à aux fonctions de téléchargement crypto.

Ces contrôles d'accès sont basés sur la saisie d'un mot de passe.

## F.GERE_ALARMES Gestion des alarmes

Le fonctionnement de la TOE est régi par quatre états : initialisation, alarme, non-opérationnel et état opérationnel :

- La TOE passe dans l'état initialisation lors de sa mise sous tension. La TOE est accessible à la console (en lecture seule), initialise ses composants, réalise son autotest et, ne transmet aucune trame Ethernet et n'est pas opérationnel pour les autres services.
- La TOE passe dans l'état opérationnel après le chargement d'une configuration valide.
- La TOE passe dans l'état non-opérationnel, lors d'une absence de paramètres d'initialisation à la mise sous tension, d'un chargement de configuration, d'un chargement du logiciel. Dans l'état non-opérationnel, la TOE est accessible à la console et par carte à puce, mais ne transmet aucune trame Ethernet.
- Dans l'**état alarme**, la TOE se bloque. Aucun service n'est disponible dans cet état mis à part le téléchargement logiciel ou crypto ainsi que la CAM superviseur. De plus, dans ce état, la TOE ne transmet aucune trame Ethernet. Il faut obligatoirement éteindre puis rallumer le boîtier pour l'utiliser à nouveau.

La remontée des alarmes par la TOE est basée sur le protocole UDP. Le numéro du port est paramétrable dans le CGM et est défini dans le fichier de configuration de la TOE.
Tout message d'alarme est numéroté. Ce numéro est issu d'un compteur (sur 2 octets) s'incrémentant pour chaque alarme émise. Lorsque le compteur atteint 0xFFFF, il redémarre à 0. Le compteur est remis à 1 lors d'un arrêt/marche du boîtier.
Les alarmes remontées par la TOE, leurs paramètres et leurs causes sont les suivants :

| Alarme | Paramètres | causes |
|---|---|---|
| Mise sous tension | table des SP : présente / absente | mise sous tension du boîtier |
| Retrait de carte à puce | effacement de la configuration de sécurité : oui / non | retrait de la carte à puce |
| Insertion d'une carte à puce | type de carte :<br>init / complète / non valide | insertion d'une carte à puce |
| Réception ICMP "Size too big" | | Réception d'un message ICMP "size too big" suite à l'envoi d'une trame chiffrée |
| Echec d'authentification | | saisie à la console d'un mot de passe erroné |
| Erreur d'intégrité | SPI de la trame erronée<br>@ IP source de l'entête IP (externe) de la trame erronée | échec de vérification de l'intégrité de la trame ESP lors du déchiffrement<br>erreur sur checksum IP de la trame ESP<br>erreur sur checksum IP de la trame TCP entête clair étendu à déchiffrer * |
| Mauvais numéro de SPI | SPI de la trame erronée<br>@ IP source de l'entête IP (externe) de la trame erronée | lors du déchiffrement d'une trame ESP<br>sur réception d'un ICMP "size too big", il n'existe pas de SA avec ce SPI |
| Erreur de vérification de SP | SPI de l'entête ESP de la trame erronée<br>@ IP source de l'entête IP (externe) de la trame erronée | après déchiffrement ESP tunnel :<br>la SP de la trame encapsulée n'existe pas,<br>la SP existe et ses paramètres sont différents de ceux de la trame (SPI, traitement, adresse IP chiffreur distant, niveau de chiffrement),<br>avant déchiffrement simple, la SP indique un déchiffrement ESP tunnel |
| Activation de la configuration | | Activation à la console de la configuration du boîtier<br>Fin d'activation à la console de la configuration du boîtier |
| Clé bientôt usée | SPI de la SA concernée<br>GIC de la clé | 80 % usure lors du (dé)chiffrement |
| Clé usée | SPI de la SA concernée<br>GIC de la clé | 100 % usure lors du (dé)chiffrement |
| Autotélégestion* | @ IP du chiffreur interne<br>@ IP du chiffreur externe<br>SPI de télégestion, | Alarme mise sous tension<br>Alarme insertion CAM init ou complète<br>Demande via le menu console |
| Effacement d'urgence* | | Appui sur bouton pendant plus de 2 sec<br>Détection d'intrusion<br>3 mauvais mots de passe |
| Perte de link* | | Démarrage ou activation avec au moins une interface activée<br>Remontée ou perte de link |
| Température* | | Franchissement des seuils 55°C et 65°C |

* : Nouvelles alarmes en v4.5.2.2
Lorsque la TOE a émis une alarme « erreur d'intégrité, vérification SP, absence SPI, ICMP Size too big », il ne doit pas émettre d'alarme de même type pendant un délai de 23 s.
Suite aux actions « démarrage boîtier, insertion CAM d'init ou CAM complète OK, demande d'autotélégestion via le menu », la TOE émet des trames d'autotélégestion en ESP/UDP régulièrement au CGM, jusqu'à la télégestion du boîtier ou un message d'arrêt du timer d'autotélégestion. L'alarme autotélégestion est éventuellement concaténée avec l'alarme ayant causée l'autotélégestion. Le CGM permet de récupérer les adresses interne et externe du boîtier à partir de son SPI

### F.CONSOLE Gestion des accès par le port série

La TOE est entièrement exploitable par un terminal externe connecté sur l'interface série, à l'aide du logiciel Hyperterminal de Windows.
Un mot de passe (longueur comprise entre 4 et 8 caractères inclus) protège (mécanisme permutationnel) l'accès aux fonctions d'exploitation du boîtier avec un niveau de résistance visé à SOF_ELEVE. Les fonctions d'exploitation de la TOE sont accessibles par une arborescence en menu.
Le paramètre langage détermine le langage des fonctions d'exploitation (français/anglais).

### F.LECTEUR_CAM Gestion de l'interface CAM

La TOE lit les cartes à puce suivantes :

- Initialisation,
- Complète,
- Téléchargement logiciel (nécessite un mot de passe),
- Test série,
- Test OEDP,
- Test CEM 10Mb/s,
- Test CEM 100Mb/s,
- Superviseur (nécessite un mot de passe),
- Téléchargement crypto (nécessite un mot de passe).

La lecture de la CAM (par calcul de mot de passe associé à la CAM) permet d'authentifier l'Administrateur de la TOE ou le Mainteneur de la TOE afin d'accéder au contenu de celle-ci (paramètres de configuration, règles de filtrage et de chiffrement...).
La TOE accepte un téléchargement par le port série du logiciel de l'algorithme cryptographique après calcul du mot de passe associé à la carte à puce "Téléchargement crypto". Le protocole de transfert du fichier de l'algorithme est XMODEM.
La TOE accepte un téléchargement par le port série du logiciel d'application après calcul du mot de passe associé à la carte à puce "Téléchargement logiciel". Le protocole de transfert du fichier de l'algorithme est XMODEM.

### F.RAZ Effacement d'urgence

La TOE dispose d'un bouton d'effacement d'urgence. En état opérationnel, après 2 secondes d'appui sur le bouton, la TOE passe dans l'**état d'alarme et** les paramètres d'initialisation et de trafic sont effacés.
La TOE dispose également d'un mécanisme de détection d'ouverture du boîtier. En cas d'ouverture du boîtier sous tension, celui-ci passe dans l'état alarme.
La TOE possède une fonction d'autotest qui permet de tester la capacité des différentes mémoires, le composant cryptographique.

**F.GERE_NOMADE** Gestion des flux avec les Mistral Nomades

Lors de la réception d'une trame ESP tunnel ou ESP/UDP émise par un Mistral Nomade, la TOE réalise le déchiffrement de la trame (utilisation du N° SPI), vérifie la SP (avec l'adresse d'identification du Nomade) et que son type d'équipement distant est "Nomade". Si la vérification est OK, elle mémorise l'adresse du fournisseur d'accès du Nomade distant (cette adresse IP est utilisée pour l'émission d'une trame à destination de ce Nomade). En ESP tunnel, la TOE envoie la trame au serveur en remplaçant l'adresse IP source de la trame déchiffrée par l'adresse du fournisseur d'accès. En ESP/UDP, la TOE envoie la trame déchiffrée au serveur.
Lors de l'émission d'une trame ESP tunnel vers le Mistral Nomade, la TOE (cette trame a été émise par le serveur avec l'adresse du fournisseur d'accès du Nomade) recherche la SP concernée avec l'adresse du fournisseur d'accès et dont le type d'équipement distant est "Nomade", remplace dans la trame initiale l'adresse du fournisseur d'accès par l'adresse d'identification du Nomade, chiffre et encapsule la trame, puis émet la nouvelle trame avec l'adresse du fournisseur d'accès.
Lors de l'émission d'une trame ESP/UDP vers le Mistral Nomade, la TOE (cette trame a été émise par le serveur avec l'adresse du fournisseur d'accès du Nomade) recherche la SP concernée avec l'adresse d'identification et dont le type d'équipement distant est "Nomade", chiffre et encapsule la trame, puis émet la nouvelle trame avec l'adresse du fournisseur d'accès.
La TOE accepte le changement d'adresse de fournisseur d'accès par le Mistral Nomade en cours de trafic : le lien adresse fournisseur d'accès courante - adresse interne - SP est maintenu en permanence. Ceci peut arriver essentiellement en cas de changement de fournisseur d'accès, en cas d'une déconnexion / reconnexion sur un fournisseur d'accès avec des adresses dynamiques ou si plusieurs utilisateurs Nomade se partagent le même PC.

## 6.2 Mesures d'assurance

### 6.2.1 Traçabilité

Les mesures d'assurance correspondent aux classes d'assurance définies au 5.1.2, soit un EAL3+. Le tableau suivant permet de faire la traçabilité entre les mesures d'assurances et les classes d'assurance :

| | Matrices | EDP | FCA | PCA | VDD | ARBO ('060) | Procédures Support | Procédures CIO | SUM | ICD | PIDS | SRS | SDD | HRS | IHS | SPE_CRYPTO* | HRS_CRYPTO* | HDD_CRYPTO* | Sources Crypto* | STD | STR | DAR | DAV |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACM_CAP.3 | X | X | X | X | X | X | | | | | | | | | | | | X | | | | | |
| ACM_SCP.1 | X | X | | | | X | | | | | | | | | | | | | | | | | |
| ADO_DEL.1 | X | | | | | | | X | | | | | | | | | | | | | | | |
| ADO_IGS.1 | X | | | | | | | | X | | | | | | | | | | | | | | |
| ADV_FSP.1 | X | | | | | | | | | X | X | X | | | | | | | | | | | |
| ADV_HLD.2 | X | | | | | | | | | | | | X | X | X | | | | | | | | |
| ADV_IMP.1 | X | | | | | | | | | | | | | | | | | | X | | | | |
| ADV_LLD.1 | X | | | | | | | | | | | | | | | X | X | X | | | | | |
| ADV_RCR.1 | X | | | | | | | | | | | | | | | | | | | | | | |
| AGD_ADM.1 | X | | | | | | | | X | | | | | | | | | | | | | | |
| AGD_USR.1 | X | | | | | | | | X | | | | | | | | | | | | | | |
| ALC_DVS.1 | X | X | | | | | | | | | | | | | | | | X | | | | | |
| ALC_FLR.3 | X | X | | | | | X | | | | | | | | | | | | | | | | |
| ALC_TAT.1 | X | | | | | | | | | | | | | | | | | X | | | | | |
| ATE_COV.2 | X | | | | | | | | | | | | | | | | | | | | | | |
| ATE_DPT.1 | X | | | | | | | | | | | | | | | | | | | | | | |
| ATE_FUN.1 | X | | | | | | | | | | | | | | | | | | | X | X | | |
| ATE_IND.2 | X | | | | | | | | | | | | | | | | | | | X | X | | |
| AVA_MSU.1 | X | | | | | | | | X | | | | | | | | | | | | | | |
| AVA_SOF.1 | X | | | | | | | | | | | | | | | | | | | | | X | |
| AVA_VLA.2 | X | | | | | | | | | | | | | | | | | | | | | | X |

* : documents AES et 3DES.

### 6.2.2 Argumentaires

#### 6.2.2.1 Classe d'assurance ACM

La classe d'assurance ACM est couverte par les documents EDP, FCA, PCA, VDD, ARBO, HDD_CRYPTO* qui présentent la gestion et le contrôle du développement, de la production et de la maintenance de la TOE , le système de gestion de configuration des éléments de la TOE et son identification de manière unique.
* : documents AES et 3DES.

#### 6.2.2.2 Classe d'assurance ADO

La classe d'assurance ADO est couverte par les procédures du CIO qui présentent les procédures utilisées pour garantir l'intégrité et l'authenticité de la TOE lors de son transfert vers l'utilisateur
La classe d'assurance ADO est couverte par le SUM pour tout ce qui concerne les procédures d'installation, génération et démarrage de la TOE.

#### 6.2.2.3 Classe d'assurance ADV

La classe d'assurance ADV est couverte par les documents ICD, PIDS, SRS, SDD, HRS, IHS, SPE_CRYPTO*, HRS_CRYPTO*, HDD_CRYPTO* qui présentent les spécifications fonctionnelles, la conception générale, et pour le code crypto uniquement la conception détaillée et le code source de la crypto.
* : documents AES et 3DES.

#### 6.2.2.4 Classe d'assurance AGD

La classe d'assurance AGD est couverte par le document SUM qui donnent les informations détaillées et exactes sur la façon sûre d'utiliser efficacement les privilèges et les fonctions de la TOE.

#### 6.2.2.5 Classe d'assurance ALC

La classe d'assurance ALC est couverte par le document EDP et HDD_CRYPTO* pour identifier les mesures de sécurité adoptées lors du développement et de la maintenance de la TOE.
La classe d'assurance ALC est couverte par le document EDP et les procédures support pour gérer le traitement des anomalies de sécurité lors du développement et de la maintenance, puis la diffusion des correctifs de sécurité dès que les anomalies de sécurité sont corrigées.
La classe d'assurance ALC est couverte par le document HDD_CRYPTO* concernant l'identification des outils techniques de développement (compilateur, …).
* : documents AES et 3DES.

#### 6.2.2.6 Classe d'assurance ATE

La classe d'assurance ATE est couverte par le document STD et STR qui décrivent les test réalisés (procédures et résultats), et démontrent la couverture des tests par rapport aux spécifications fonctionnelles.
De plus, la classe d'assurance est couverte par des tests indépendants réalisés par l'évaluateur sur des TOE mises à disposition par Thalès.

#### 6.2.2.7 Classe d'assurance AVA

La classe d'assurance AVA est couverte par le document DAR et DAV qui analyse des vulnérabilités et de la résistance des mécanismes de sécurité (nature permutationnelle ou probabiliste) face aux attaques.
La classe d'assurance AVA est couverte par le document SUM concernant la prévention d'utilisation impropre de la TOE (possibilité à l'administrateur de déterminer si la TOE est configurée et exploitée de manière non sûre).

# 7. Annonce de conformité à un Profil de Protection

Sans objet.

# 8. Argumentaires

**Certaines parties de ce chapitre sont volontairement supprimées dans la version Lite du document. Le contenu de ce chapitre est disponible dans la cible de sécurité fournie pour l'évaluation et référencée dans le rapport de certification.**

## 8.1 Argumentaire pour les objectifs de sécurité

### 8.1.1 Couverture menaces – objectifs de sécurité

#### 8.1.1.1 Analyse

**Le contenu de ce paragraphe est disponible dans la cible de sécurité fournie pour l'évaluation et référencée dans le rapport de certification.**

#### 8.1.1.2 Traçabilité

**Le contenu de ce paragraphe est disponible dans la cible de sécurité fournie pour l'évaluation et référencée dans le rapport de certification.**

## 8.2 Argumentaire pour les exigences de sécurité

### 8.2.1 Analyse des dépendances des composants fonctionnels

Le tableau ci-dessous démontre la couverture des dépendances entre les composants fonctionnels sélectionnés :

| Composant | Dépendances à respecter | Commentaires |
|---|---|---|
| FAU_ARP.1 | FAU_SAA.1 | Couvert |
| FAU_SAA.1 | FAU_GEN.1 | **Non couvert, la TOE n'enregistre pas de journal d'audit. Il s'agit uniquement d'une surveillance temps réel** |
| FCS_CKM.2 | [FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4, FMT_MSA.2 | Couvert |
| FCS_CKM.4 | [FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FMT_MSA.2 | Couvert |
| FCS_COP.1 | [FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4, FMT_MSA.2 | Couvert |
| FDP_ACC.2 | FDP_ACF.1 | Couvert |
| FDP_ACF.1 | FDP_ACC.1, FMT_MSA.3 | Couvert, car FDP_ACC.2 est hiérarchiquement supérieur à FDP_ACC.1 |
| FDP_IFC.1 | FDP_IFF.1 | Couvert |
| FDP_IFF.1 | FDP_IFC.1, FMT_MSA.3 | Couvert |
| FDP_ITC.1 | [FDP_ACC.1 ou FDP_IFC.1] FMT_MSA.3 | Couvert |
| FDP_RIP.2 | Aucune | Couvert |
| FDP_UCT.1 | [FTP_ITC.1 ou FTP_TRP.1], [FDP_ACC.1 ou FDP_IFC.1] | Couvert |
| FDP_UIT.1 | [FDP_ACC.1 ou FDP_IFC.1], [FTP_ITC.1 ou FTP_TRP.1] | Couvert |
| FIA_AFL.1 | FIA_UAU.1 | Couvert, car FIA_UAU.2 est hiérarchiquement supérieur à FIA_UAU.1 |
| FIA_UAU.2 | FIA_UID.1 | Couvert |
| FIA_UID.2 | Aucune | Couvert |
| FMT_MOF.1 | FMT_SMR.1, FMT_SMF.1 | Couvert |
| FMT_MSA.1 | [FDP_ACC.1 ou FDP_IFC.1], FMT_SMR.1, FMT_SMF.1 | Couvert |
| FMT_MSA.2 | ADV_SPM.1, [FDP_ACC.1 ou FDP_IFC.1], FMT_MSA.1, FMT_SMR.1 | Couvert, **sauf ADV_SPM.1 qui n'est pas justifié pour le niveau d'assurance visé** |
| FMT_MSA.3 | FMT_MSA.1, FMT_SMR.1 | Couvert |
| FMT_MTD.1 | FMT_SMR.1, FMT_SMF.1 | Couvert |
| FMT_SMF.1 | Aucune | Couvert |
| FMT_SMR.1 | FIA_UID.1 | Couvert |
| FPR_ANO.1 | Aucune | Couvert |
| FPT_AMT.1 | Aucune | Couvert |
| FPT_ITC.1 | Aucune | Couvert |
| FPT_ITI.1 | Aucune | Couvert |
| FPT_RPL.1 | Aucune | Couvert |
| FPT_RCV.1 | AGD_ADM.1, ADV_SPM.1 | Couvert, **sauf ADV_SPM.1 qui n'est pas justifié pour le niveau d'assurance visé** |
| FPT_TST.1 | FPT_AMT.1 | Couvert |
| FTP_TRP.1 | Aucune | Couvert |

### 8.2.2 Couverture composants fonctionnels et objectifs sécurité

#### 8.2.2.1 Traçabilité

**Le contenu de ce paragraphe est disponible dans la cible de sécurité fournie pour l'évaluation et référencée dans le rapport de certification.**

#### 8.2.2.2 Analyse

**Le contenu de ce paragraphe est disponible dans la cible de sécurité fournie pour l'évaluation et référencée dans le rapport de certification.**

### 8.2.3 Analyse du niveau d'évaluation demandé

#### 8.2.3.1 Argumentaire pour l'EAL

Le niveau d'assurance de la TOE est EAL3+. Il répond au processus de qualification standard [QUA-STD] qui demande un niveau EAL2+. L'EAL3 correspond à l'EAL2+ augmenté de :

- ⇨ ACM_CAP.3 Authorisations controls
- ⇨ ACM_SCP.1 TOE CM coverage
- ⇨ ATE_COV.2 Analysis of coverage
- ⇨ ATE_DPT.1 Testing : high-level design

Ces composants ont été choisis car elles imposent :

- ⇨ l'utilisation de contrôle d'environnement développement de la TOE.
- ⇨ les tests effectués au niveau des sous-systèmes pour démontrer la conception de haut-niveau a été correctement réalisée.
- ⇨ l'analyse systématique de la couverture des tests par rapport à ses fonctions de sécurité (en vérifiant qu'elles ont été bien implémentées).
- ⇨ le référencement de manière unique de tous les éléments composant la TOE et sa mise en gestion de configuration.

#### 8.2.3.2 Argumentaire pour les augmentations à l'EAL3+

8.2.3.2.1 ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard.

8.2.3.2.2 AVA_VLA.2 Independent vulnerability analysis

Augmentation requise par le processus de qualification standard.

8.2.3.2.3 ADV_IMP.1 Subset of the implementation of the TSF

Cette augmentation est requise par le processus de qualification standard pour la partie cryptographie uniquement.

8.2.3.2.4 ADV_LLD.1 Descriptive low-level design

Cette augmentation est requise par le processus de qualification standard pour la partie cryptographie uniquement.

8.2.3.2.5 ALC_TAT.1 Well-defined development tools

Cette augmentation est requise par le processus de qualification standard pour la partie cryptographie uniquement.

## 8.3 Argumentaire pour les spécifications globales de la TOE

### 8.3.1 Couverture composants fonctionnels – fonctions de sécurité

#### 8.3.1.1 Traçabilité

**Le contenu de ce paragraphe est disponible dans la cible de sécurité fournie pour l'évaluation et référencée dans le rapport de certification.**

#### 8.3.1.2 Analyse

**Le contenu de ce paragraphe est disponible dans la cible de sécurité fournie pour l'évaluation et référencée dans le rapport de certification.**

## 8.4 Argumentaire pour les annonces de conformité à un PP

Sans objet.

# 9. Glossaire

Les acronymes utilisés dans le présent document sont définis ci-dessous :

| *Acronyme* | *Définition anglaise* | *Définition française* |
|---|---|---|
| CAM | Smartcard | Carte à microprocesseur, carte à puce |
| CC | Common Criteria | Critères Communs |
| CEC | Mistral Key Generation Tool | Centre d'Elaboration des Clés Mistral |
| CGM | Mistral Management Tool | Centre de Gestion Mistral |
| CPC | Mistral Smartcard Personalisation Tool | Centre de Pré-personnalisation Mistral |
| DAR | SOF analysis document | Dossier d'Analyse de résistance de fonctions |
| DAV | Vulnerability analysis document | Dossier d'Analyse de vulnérabilité |
| EAL | Evaluation Assurance Level | Niveau d'assurance de l'évaluation |
| EDP | Equipment Development Plan | Plan de développement de l'équipement |
| **FCA** | Funtional Configuration Audit | Audit de configuration fonctionnelle |
| FPGA | Field Programmable Gate Array | Composant électronique programmable |
| GIC | Group Identification Code | Index d'une clé cryptographique |
| **HDD** | Hardware Design Document | Document de conception du matériel |
| **HRS** | Hardware Requirements Specification | Spécification des exigences sur le matériel |
| **HTD** | Hardware Test Description | Description de test du matériel |
| **HTR** | Hardware Test Report | Rapport de test du matériel |
| **ICD** | Interface Control Document | Document de maîtrise d'interface |
| **IHS** | Interface Hard/Soft | Interface Hard/Soft |
| IP | Internet Protocol | Protocole Internet |
| IT | Information Technology | Technologie de l'information |
| IPSEC | IP Security Protocol | Protocole Internet sécurisé |
| LAN | Local Area Network | Réseau local |
| MIB | Management Information Base | Base interrogeable par SNMP |
| PC | Personal Computer | Ordinateur personnel |
| PCA | Physical Configuration Audit | Audit de configuration physique |
| SA | Security Association | Association de sécurité |
| **SDD** | Software Design Document | document de conception du logiciel |
| **SDP** | Software Development Plan | plan de développement du logiciel |
| SF | Security Function | Fonction de sécurité |
| SNMP | Simple Network Management Protocol | Protocole de gestion réseau |
| SOF | Strength Of Function | Résistance des fonctions |
| SP | Security policy | Politique de sécurité |
| **SRS** | Software Requirements Specification | spécification des exigences sur le logiciel |
| **SSS** | System Segment Specification | spécification de système |
| ST | Security Target | Cible de sécurité |
| **STD** | Software Test Description | description de test du logiciel |
| **STP** | Software Test Plan | plan de test du logiciel |
| **STR** | Software Test Report | rapport de test du logiciel |
| **SUM** | Software User's Manual | manuel utilisateur du logiciel |
| TCP | Transmission Control Protocol | Protocole en mode connecté |
| TOE | Target Of Evaluation | Cible d'évaluation |
| TSF | TOE Security Function | Fonctions de sécurité de la TOE |
| UDP | User Datagram Protocol | Protocole en mode non connecté |
| **VDD** | Version Description Document | document de description de version |
| VPN | Virtual Private Network | Réseau privé virtuel |
| WAN | Wide Area Network | Réseau d'opérateur |