CRYPTOSMART

CIBLE DE SECURITE

Auteur	Validation	Approbation
Eric Laubacher	**Erwan Brisset**	**Jean Lacroix**
2005-10-14	**2005-10-14**	

Engineering. Réseaux. Communications.
Immeuble NUNGESSER - 13, avenue Morane Saulnier - 78140 VELIZY – France
Tél.: 01 39 46 50 50 **Fax : 01 39 46 25 25**
Tél. international : +33 1 39 46 50 50 **Fax international : +33 1 39 46 25 25**
Web : www.ercom.fr **email :** info@ercom.fr

Ed	Date	Auteur	Désignation / Modification
1.0	**2004-06-17**	**EL**	Création pour évaluation EAL1+
1.1	**2004-10-15**	**EL**	Evolution RSA ; ajout DH
1.2	**2004-12-20**	**EL**	Renommage en CryptoSmart ; passage à EAL2+
1.3	**2005-03-25**	**EL**	Corrections suite à ASE
1.4	**2005-05-12**	**EL**	Corrections suite aux remarques du CESTI
1.5	**2005-06-22**	**EL**	Correction Algo MAC 3DES ; prise en compte des remarques CESTI/DCSSI
1.6	**2005-08-03**	**EL**	Prise en compte des remarques CESTI/DCSSI
1.7	**2005-10-05**	**EL**	Corrections suite au rapport ASE v2.0
1.8	**2005-10-14**	**EL**	Corrections suite au rapport ASE v2.0 (compléments)

TABLE DES MATIERES

0. SUIVI DU DOCUMENT

0.1 HISTORIQUE

Version 1.0 Création pour évaluation EAL1+
Version 1.1 Evolution RSA ; ajout DH
Version 1.2 Renommage en CryptoSmart ; passage à EAL2+
Version 1.3 Corrections suite à ASE
Version 1.4 Corrections suite aux remarques du CESTI
Version 1.5 Correction Algo MAC 3DES ; prise en compte des remarques de la DCSSI et du CESTI
Version 1.6 Prise en compte des remarques de la DCSSI et du CESTI
Version 1.7 Corrections suite au rapport ASE v2.0
Version 1.8 Corrections suite au rapport ASE v2.0 (compléments)

0.2 ABBREVIATIONS

IA	Identification and Authentification.
APDU	Application Protocol Data Unit
DH	Diffie-Hellman
ERCOM	ERCOM S.A.
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation - Appellation CC pour le système en évaluation.
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
CA	Certificate Authority

0.3 TERMINOLOGIE

Ce chapitre présente quelques termes utilisés dans ce document.

Administrateur	Personne autorisée à accéder à la station d'administration pour faire la gestion du parc de cartes à puces : il gère la carte CA.
Attaquant en ligne	Personne mal intentionnée cherchant à corrompre ou à récupérer des informations sensibles en interceptant et/ou modifiant des flux entre équipements utilisant des cartes CryptoSmart. L'attaquant en ligne peut disposer de cartes perdues ou volées de la même famille que la TOE en ayant connaissance de leur code PIN. Il peut aussi s'agir d'un utilisateur légitime d'une autre carte de la même famille que la TOE. L'utilisateur légitime de la TOE, l'utilisateur légitime de la carte avec qui la TOE doit

	établir une session et l'administrateur sont exclus de cette définition.
Attaquant local	Personne mal intentionnée cherchant à corrompre ou à récupérer des informations sensibles en accédant directement à une carte CryptoSmart sans connaissance du code PIN. Il peut s'agir d'un utilisateur légitime d'une carte de la même famille que la TOE. L'utilisateur légitime de la TOE et l'administrateur sont exclus de cette définition.
Authentification	Service permettant de s'assurer de l'identité d'une carte
Carte CA	Carte CryptoSmart en charge de la gestion des certificats pour une famille de cartes
Carte CryptoSmart	Carte à puce incorporant l'applet CryptoSmart
Carte Utilisateur	Carte CryptoSmart en charge de la protection des communications téléphoniques d'un utilisateur
Certificat	Données d'identité et clé publique d'un utilisateur signées par la clé privée de l'autorité de certification
Clé de session	Clé de 1152 bits générée par la carte CryptoSmart à chaque appelet fournie au boîtier (téléphone ou station d'administration) pour effectuer la protection des flux échangés entre boîtiers. On distingue les clés de session U↔U (entre cartes utilisateur) et U↔CA (entre carte utilisateur et carte CA).
Carte clone	Dispositif ayant la capacité à se substituer à une carte légitime, en particulier à s'authentifier de façon identique et à générer une clé de session valide.
CRL	« Certificate Revocation List », liste des certificats qui ne sont plus autorisés
MAC	Message Authentication Code : mécanisme de scellement et de vérification d'intégrité d'un message à clé secrète
Mascarade	Action malveillante visant à tromper un interlocuteur sur son identité réelle
Reset	Réinitialisation de la mémoire volatile de la carte à puce
Station d'administration	Dispositif permettant de gérer un parc de cartes CryptoSmart
Utilisateur	Personne munie d'une carte CryptoSmart de type utilisateur et connaissant son code PIN

0.4 DOCUMENTS APPLICABLES ET DE REFERENCE

Ce chapitre présente les autres documents référencés dans la présente cible de sécurité. En outre, tous les documents utilisés au titre de l'évaluation sont listés dans [PlanDoc], où le dernier numéro de version de chacun est mentionné.

[PlanDoc] Liste de configuration *CryptoSmart*, réf. 2004I/401, v1.8 du 2005-10-14, ERCOM

[Cosmo] *Cosmo64 RSA D V5.2 Technical Brief*, réf. 061103-01-UDD-AA, Oberthur Card Systems.

[Qualif] *Processus de qualification standard v.1 du 28 juillet 2003,* DCSSI

1. INTRODUCTION DE LA CIBLE DE SECURITE

1.1 IDENTIFICATION DE LA CIBLE DE SECURITE ET DE LA TOE

Ce document constitue la cible de sécurité de l'applet CryptoSmart.

- Nom de la ST : **Applet CryptoSmart – Cible de sécurité**
- Version de la ST : **1.8**
- Identifiant de la TOE : **Applet CryptoSmart sur carte à puce Oberthur COSMO64RSA D V5.2**
- Version de la TOE : **2.0-000035-C37DB42C**
- Référence Critères Communs : **Version 2.2 de janvier 2004**

1.2 PRESENTATION GENERALE DE LA CIBLE DE SECURITE

CryptoSmart est une applet (code inclus dans une carte à puce Javacard) dédiée à l'authentification, au contrôle d'accès et à la gestion des clés dans un système de cryptophonie.

1.3 NIVEAU D'EVALUATION

La cible d'évaluation doit être conforme :

- aux Critères Communs version 2.2 de janvier 2004
- à la partie 2 étendue
- à la partie 3
- au niveau EAL2 augmenté de ADV_HLD.2, ADV_IMP.1 (pour la partie cryptographique), ADV_LLD.1 (pour la partie cryptographique), ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 (pour la partie cryptographique), AVA_MSU.1 et AVA_VLA.2 ;

2. DESCRIPTION DE LA TOE

2.1 PRINCIPE GENERAL DE FONCTIONNEMENT DU SYSTEME SECPHONE

2.1.1 INTRODUCTION

Secphone est la première application mettant en œuvre la carte CryptoSmart.

SecPhone est un poste téléphonique destiné à protéger les conversations privées vis-à-vis du risque d'écoute. Le domaine d'utilisation peut être industriel, financier ou gouvernemental, ce qui justifie un niveau de résistance SOF-HIGH.

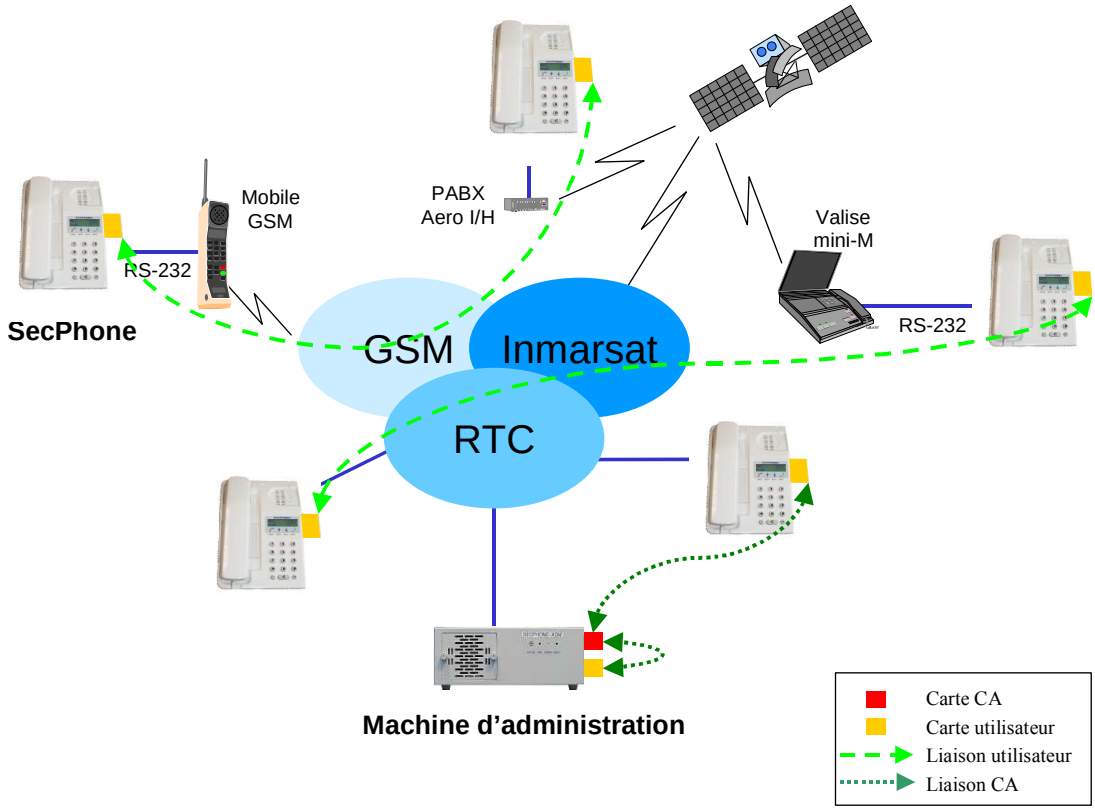
La sécurité repose sur une carte à puce qui permet d'authentifier le correspondant à l'aide d'un algorithme cryptographique asymétrique, et de négocier une clé de session différente à chaque appel.

Le chiffrement de la conversation est réalisé à l'aide d'un algorithme cryptographique symétrique exécuté dans le poste téléphonique.

SecPhone peut se brancher soit au réseau téléphonique traditionnel (RTC), soit à l'aide d'un modem externe au réseau GSM, RNIS, Inmarsat, Thuraya ou Aero I/H.

L'administration des cartes à puce est effectuée à l'aide d'une station d'administration, dispositif indépendant qui permet de créer les cartes localement, puis de les maintenir localement ou à distance.

2.1.2 SYNOPTIQUE



2.1.3 ROLE DE LA CARTE A PUCE CRYPTOSMART

La carte à puce CryptoSmart est indispensable pour l'établissement d'une communication entre deux postes SecPhone.

Elle a pour rôle :

- d'authentifier l'utilisateur par un code PIN,
- d'identifier et d'authentifier les correspondants entre eux,
- de décider si la communication est autorisée,
- de calculer une clé de session différente à chaque appel.

Lors d'un appel entre deux postes, les cartes sont « mises en relation », et s'échangent des données par l'intermédiaire des postes. Les postes n'ont pas connaissance du contenu des échanges (données « noircies »). Lorsque la négociation aboutit, les cartes fournissent aux postes une clé de session de 1152 bits, dont sont extraites deux sous-clés AES de 256 bits, une par sens de communication. Les postes conservent et utilisent ces sous-clefs pour le chiffrement des flux. Les postes effacent les sous-clés à la fin de la communication.

Les données échangées lors de l'établissement d'une session comportent en particulier :

- le sens de l'appel,

- la nature de l'appel (voix, fax ou data),
- les capacités du poste, ces informations étant fournies par le poste préalablement à l'appel.

Les cartes à puce CryptoSmart sont regroupées en familles, dont une des cartes, dite « carte CA », a en charge la gestion des certificats pour l'ensemble de la famille. Les autres cartes sont dites « cartes utilisateur ». Seules des cartes à puce issues d'une même carte CA peuvent dialoguer ensemble. Une famille dispose d'un identifiant textuel « de famille », choisi par l'administrateur lors de la création de la carte CA.

Deux cartes Utilisateur peuvent établir entre elles une session « Utilisateur », permettant l'authentification et la génération d'une clé de session U↔U.

Une carte Utilisateur et la carte CA peuvent établir entre elles une session « CA », permettant l'authentification, la génération d'une clé de session U↔CA et la mise à jour de la carte Utilisateur. Le téléphone n'autorise pas l'utilisation de la carte CA pour établir une conversation téléphonique.

Tout échec d'authentification entre carte provoque l'incrémentation d'un compteur d'échecs d'authentification.

La carte CA possède un bi-clé RSA dédié à la signature des clés publiques d'authentification des cartes de sa famille. Elle possède elle-même un bi-clé RSA d'authentification, comme une carte Utilisateur. Chaque carte Utilisateur connaît sans risque d'usurpation la clé publique de signature de la carte CA.

Chaque carte à puce contient un identifiant numérique personnel unique au sein de sa propre famille, ainsi qu'un identifiant textuel personnel, choisis par l'administrateur à la création de la carte. L'identifiant textuel est modifiable lors des mises à jour.

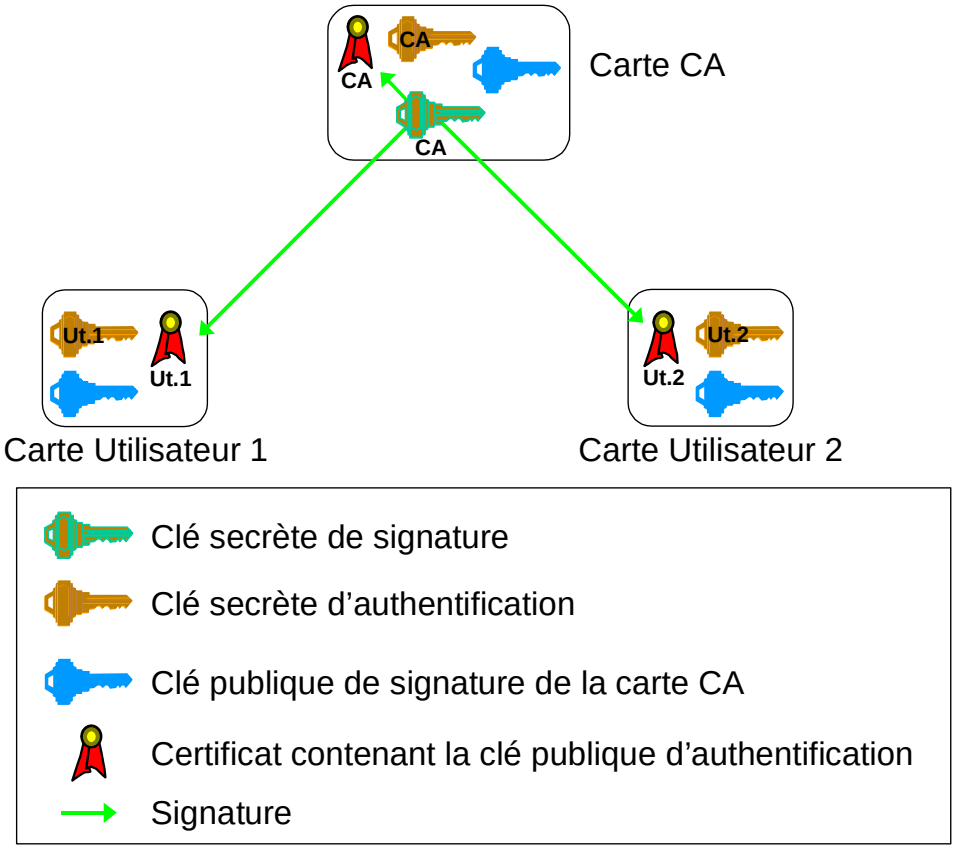
L'identifiant textuel personnel s'affiche :

- au repos, sur l'écran du poste dans lequel la carte est insérée, après saisie du code PIN ;
- sur l'écran du correspondant lors d'un appel.

L'identifiant textuel permet à l'utilisateur de vérifier l'identité de son correspondant.

Chaque carte, hormis la carte CA, contient également un nombre codé sur 8 bits indiquant l'ensemble des groupes d'une même famille auxquels la carte appartient : chaque bit représente l'appartenance à un groupe. Deux cartes utilisateurs ne peuvent établir une session que si elles appartiennent au moins à un groupe commun.

Le schéma suivant illustre l'organisation des bi-clés RSA dans les cartes d'une même famille.



Les cartes Utilisateur comportent un compteur de session, ainsi qu'un drapeau indiquant si ce compteur est activé ou non. La valeur initiale du compteur est fixée pour une famille de carte à la création de la carte CA.

Si le drapeau indique que le compteur est utilisé, le compteur est décrémenté à chaque authentification. Lorsqu'il atteint une valeur nulle, il n'est plus décrémenté, mais ceci interdit l'établissement d'une session entre cartes utilisateurs.

Ce mécanisme vise à obliger une mise à jour périodique de la carte Utilisateur par la carte CA[1].

Les cartes à puce Utilisateur comportent une zone de données accessible en lecture et en écriture par le téléphone après présentation du code PIN. Cette zone n'a aucune influence sur le fonctionnement interne de la carte : elle est utilisée pour stocker un annuaire personnel. Elle est appelée « annuaire » dans la suite du document.

La carte CA inclut pour la réalisation de ses fonctions de gestion une base de données, dite *base de données de famille*, contenant la liste des cartes existantes avec leur identifiant numérique et textuel, leur groupe, leur état de révocation, les commandes en attente (déblocage du code PIN, renouvellement de certificat).

2.1.4 PROTECTION DES ECHANGES ENTRE CARTES

Les principales étapes de l'établissement d'une session entre cartes sont :

[1] Ce mécanisme n'est pas nécessaire à la sécurité de la TOE, et n'est pas mentionné dans les exigences et fonctions de sécurité.

- Echange des certificats.
- Génération d'un aléa.
- Calcul d'une clé publique DH.
- Echange des clés publiques DH chiffrées par la clé publique RSA de la carte distante.
- Calcul du secret partagé DH et dérivation de la clé de session.
- Calcul et échange d'une réponse authentifiant la carte distante.

En plus de l'utilisation de DH et RSA pour l'authentification et la génération de clés de session, tous les échanges entre cartes Utilisateur et/ou CA sont protégés en confidentialité et en intégrité à l'aide de deux clés triple-DES communes à une famille de carte, dites « clés de famille ». Ceci permet notamment de rendre une carte non identifiable. La clé de chiffrement commune est dite « clé d'anonymat ». La clé de vérification d'intégrité commune est dite « clé de scellement ». Ces clefs sont chargées automatiquement dans les cartes Utilisateur lors de leur création par la carte CA.

2.1.5 CODE PIN

2.1.5.1 Carte utilisateur

Chaque carte possède un code PIN comportant de 4 à 8 chiffres que l'administrateur précise à la création de la carte. L'utilisateur peut changer le code PIN.

Après 3 essais infructueux consécutifs, le code PIN est bloqué, ce qui limite le fonctionnement de la carte. Seule une connexion avec la carte administrateur est alors possible.

Une carte Utilisateur peut être débloquée par la carte CA, à la demande explicite de l'administrateur. Dans ce cas, le code PIN est forcé à une valeur par défaut, et doit être changé immédiatement par l'utilisateur.

2.1.5.2 Carte CA

La carte CA possède un code PIN pouvant comporter 6 à 8 chiffres.

Après 6 essais infructueux consécutifs, la carte est définitivement bloquée, et ne peut plus établir de sessions. Il reste néanmoins possible de la recycler à l'aide d'un code secret (voir plus loin dans la description de la station d'administration).

La carte CA non validée peut établir des sessions avec une carte utilisateur, afin de permettre une mise à jour à distance sans présence de l'administrateur.

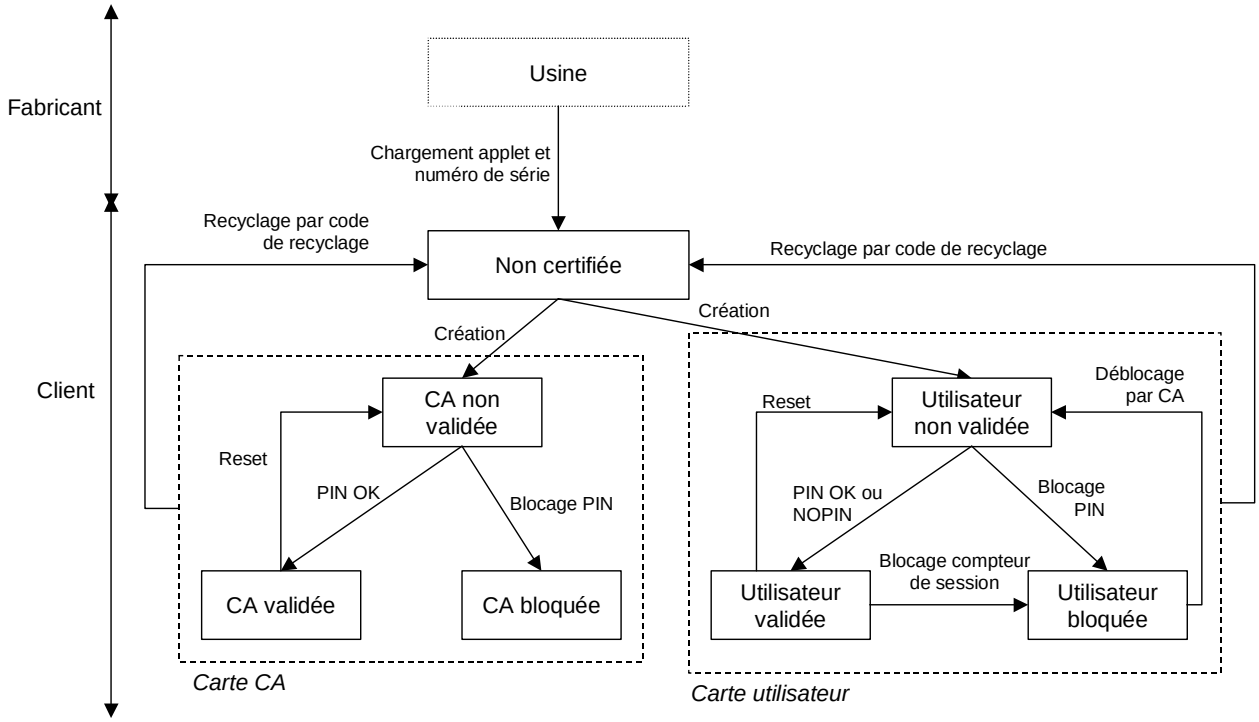
2.1.6 CYCLE DE VIE D'UNE CARTE A PUCE

Les cartes à puce CryptoSmart sont constituées d'une applet Java « CryptoSmart » installée sur une plate-forme Javacard compatible Javacard 2.2 et Global Platform 2.1.1.

Les cartes à puce CryptoSmart peuvent être dans un des états fondamentaux suivants :

Etat	Description
Usine	Carte livrée par le fabricant de cartes à ERCOM. Cet état n'est jamais vu par le client final.
Non certifiée	Carte avec applet CryptoSmart et numéro de série chargés. C'est ainsi que la carte est fournie initialement au client.
CA non validée	Carte CA au repos
CA validée	Carte CA avec code PIN validé
CA bloquée	Carte CA bloquée suite à des erreurs répétées de code PIN
Utilisateur non validée	Carte Utilisateur au repos
Utilisateur validée	Carte Utilisateur avec code PIN validé
Utilisateur bloquée	Carte Utilisateur bloquée suite à des erreurs répétées de code PIN

Le schéma suivant illustre le cycle de vie d'une carte.



Le Reset a lieu lors de la mise hors tension de la carte ou à la demande du boîtier.

Les intervenants dans le cycle de vie sont plus précisément :
- Développeur de l'applet CryptoSmart: ERCOM S.A,
- Développeur de la plate-forme COSMOPOLIC: Oberthur Card Systems,
- Développeur du circuit: Philips Semiconductor,
- Fabricant du circuit: Philips Semiconductor,
- Installation de l'applet: ERCOM S.A.

2.1.7 LISTE DE REVOCATION (CRL)

La carte CA gère une liste de révocation numérotée (version) et signée avec la clé privée de signature de la carte CA. Lors d'une mise en relation d'une carte utilisateur avec la carte CA (établissement d'une session), les versions sont comparées, et une mise à jour est effectuée si nécessaire.

La CRL peut également être lue sur la carte administrateur et exportée par la machine d'administration au moyen d'une clé USB, ce qui permet sa transmission hors session par courrier électronique ou tout autre moyen de transmission. Cette CRL exportée est signée par la clé de signature de la carte CA, puis scellée et chiffrée avec les clés de famille. Elle peut être transmise à une carte Utilisateur au moyen d'un poste téléphonique SecPhone et d'une clé USB.

La mise à jour effective est conditionnée à un numéro de version supérieur, une signature[2], un scellement et un chiffrement valides.

Une carte Utilisateur ou CA mise en relation avec une carte apparaissant dans la CRL refuse l'authentification.

2.1.8 RENOUVELLEMENT DES BI-CLES

Une carte Utilisateur renouvelle son bi-clé d'authentification à la demande de la carte CA. Le certificat est alors mis à jour, les éléments du certificat étant envoyés à la carte CA pour signature. Le mécanisme de protection des échanges entre cartes décrit précédemment rend cette opération possible à distance. Elle peut également être effectuée localement.

La carte CA peut renouveler son bi-clé d'authentification de façon similaire à une carte Utilisateur, à la nuance près que l'opération est purement interne.

Le renouvellement du bi-clé de signature de la carte CA nécessite le recyclage de l'ensemble des cartes et leur recréation.

2.1.9 MISE A JOUR D'UNE CARTE UTILISATEUR

La carte CA peut réaliser certaines actions de mise à jour sur une carte Utilisateur. Le tableau suivant répertorie ces actions, et leur condition de réalisation.

Action	Condition(s) de réalisation
Modification du drapeau d'activation du compteur de session	1) Authentification mutuelle réussie 2) Demande préalable de l'administrateur (stockée dans la carte CA)
Réinitialisation du compteur de session	1) Authentification mutuelle réussie
Déblocage et réinitialisation du code PIN	1) Authentification mutuelle réussie 2) Demande préalable de l'administrateur (stockée dans la carte CA)
Régénération du bi-clé RSA, renouvellement du certificat, modification du nom et du groupe	1) Authentification mutuelle réussie 2) Demande préalable de l'administrateur (stockée dans la carte CA)
Mise à jour de la CRL	Authentification mutuelle réussie
Récupération du compteur d'échecs d'authentification	Authentification mutuelle réussie

[2] Le mécanisme de signature de la CRL par la carte CA n'est pas indispensable à la sécurité de la TOE, et n'est pas mentionné dans les exigences et fonctions de sécurité.

2.1.10 PRESENTATION DU POSTE TELEPHONIQUE SECPHONE

Le poste téléphonique SecPhone se présente comme un téléphone de bureau traditionnel avec fonction écoute amplifiée, et disposant des éléments additionnels suivants :

- Alimentation 12V externe
- Lecteur de carte à puce intégré
- Port RS-232 9 broches mâle
- Port USB
- Afficheur LCD

Son mode d'emploi est similaire à un téléphone traditionnel, avec les différences suivantes :

- L'alimentation électrique est nécessaire au fonctionnement.
- Le démarrage n'est pas immédiat, il faut patienter environ 30 secondes après mise sous tension.
- La carte à puce est nécessaire avant de pouvoir téléphoner. La saisie du code PIN est demandée pour valider la carte (en cas de code PIN bloqué, il est possible d'appeler la station d'administration).
- Après composition du numéro, il faut appuyer sur la touche verte, comme sur un téléphone GSM.
- Une authentification entre cartes est réalisée avant établissement de la voix.
- Lors d'un appel entrant, une pré-sonnerie discrète prévient l'utilisateur. Il n'est pas nécessaire de décrocher dans cette phase. Une fois l'authentification aboutie, une sonnerie normale est produite, sauf si l'utilisateur a déjà décroché.

L'état de validation de la carte locale, ainsi que l'identité et le type de carte distante sont fournis au poste par la carte lors de l'établissement d'une session. Le poste ne permet une communication vocale qu'entre deux cartes utilisateurs validées.

2.1.11 PRESENTATION DE LA STATION D'ADMINISTRATION

La station d'administration est une machine dédiée, disposant d'un système d'exploitation minimaliste, et non connectable en réseau local. Elle permet de créer puis de gérer les cartes à puce utilisateur. Toutes les opérations sur les cartes utilisateurs nécessitent la présence de la carte CA.

La carte CA est elle-même créée à l'aide de la station d'administration.

La gestion des cartes s'effectue soit de manière locale grâce à un second lecteur de carte à puce, soit à distance par appel téléphonique à l'aide d'un modem intégré. La CRL peut également être exportée au moyen d'une clé USB. Toutefois, la station d'administration ne permet les opérations de création d'une carte (CA ou utilisateur) et de recyclage que localement.

Les fonctions d'administration des cartes utilisateurs s'effectuent en mode différé. La demande est d'abord programmée dans la carte CA. Ensuite, dès mise en relation de la carte Utilisateur avec la carte CA, les actions programmées sont réalisées. Ces actions sont :

- Déblocage et réinitialisation de code PIN

- Révocation de cartes
- Régénération du bi-clé RSA et mise à jour du groupe et du nom (les deux actions sont conjointes, et entraînent un nouveau calcul du certificat).
- Activation / Désactivation du compteur de session
- Relevé du compteur d'échecs d'authentification

Les actions de mise à jour de la CRL et de réinitialisation du compteur de session sont systématiquement effectuées lors de la mise en relation avec la carte CA.

Le recyclage d'une carte est réalisé à l'aide d'un code secret propre à une famille de cartes. Ce code de 8 octets, présenté sous forme hexadécimale, est généré lors de la création d'une carte CA, et conservé secret par l'administrateur. Il permet notamment le recyclage d'une famille de carte en cas d'indisponibilité de la carte CA. Tous les secrets contenus dans une carte sont effacés lors d'un recyclage.

2.1.12 STRUCTURE DES CERTIFICATS

Les certificats des cartes CryptoSmart contiennent notamment les informations suivantes :

- Identifiant numérique de famille (nombre de 64 bits déterminé aléatoirement par la carte CA, donc avec un risque de collision infime).
- Identifiant textuel de famille (20 caractères alphanumériques, choisi par l'administrateur).
- Type de carte : (CA ou utilisateur).
- Identifiant numérique personnel (nombre de 16 bits, incrémenté à chaque création de carte, la carte CA ayant le numéro 0).
- Identifiant textuel personnel (20 caractères alphanumériques, choisi par l'administrateur).
- Numéro de groupe de la carte (nombre de 8 bits, sans objet pour la carte CA).
- Clé publique RSA d'authentification de la carte.
- Signature RSA des informations précédentes à l'aide de la clé privée de signature de la carte CA.

2.1.13 SERVICES

Les services de la TOE, en fonction de l'état de la carte, sont décrits ci-après.

Carte quelconque, tous états

- Fourniture d'un statut : la carte indique l'état dans lequel elle se trouve, et la nécessité de présenter un code PIN ou non.

Carte non certifiée

- Génération d'une carte CA : service permettant la création d'une carte CA pour une nouvelle famille.
- Génération d'une carte utilisateur : service permettant la création d'une carte utilisateur liée à une carte CA existante.

Carte utilisateur non validée, validée ou bloquée et carte CA non validée ou validée

- Etablissement d'une session : service permettant l'authentification mutuelle, la génération d'une clé de session, la protection en confidentialité et en intégrité des échanges avec une carte distante, l'incrémentation si nécessaire du compteur d'échecs d'authentification distante.

Carte utilisateur ou carte CA, tous états

- Recyclage par code de recyclage : service permettant le recyclage d'une carte, même bloquée, à l'aide d'un code secret commun à toute une famille.

Carte utilisateur validée ou carte CA validée

- Fourniture du certificat : service permettant de récupérer le certificat de la carte (nécessite état validé).

- Modification du code PIN : service permettant à l'utilisateur ou l'administrateur de choisir un nouveau code PIN.

Carte utilisateur non bloquée ou carte CA non bloquée

- Authentification locale utilisateur/administrateur : service permettant l'authentification de l'utilisateur/administrateur local, à l'aide d'un code PIN.

Carte utilisateur tous états

- Mise à jour par la carte CA : régénération du bi-clé d'authentification, changement de nom et de groupe, renouvellement du certificat, déblocage de PIN, réinitialisation du compteur de session, transfert de la CRL.

Carte utilisateur validée

- Accès annuaire : service permettant l'accès en lecture et écriture de l'utilisateur authentifié à l'annuaire.

- Importation de la CRL : service permettant la mise à jour locale de la CRL par l'utilisateur transmise par un moyen indépendant (clé USB, mail, …).

Carte CA validée ou non validée

- Mise à jour d'une carte Utilisateur : demande de régénération du bi-clé d'authentification, changement de groupe, déblocage de PIN, réinitialisation du compteur de session, transfert de la CRL, récupération des compteurs d'échec d'authentification.

Carte CA validée

- Création d'une carte Utilisateur : service permettant de créer une carte Utilisateur localement, au moyen de la carte CA.

- Gestion des cartes utilisateurs : service permettant localement, depuis la station d'administration, de consulter et de modifier dans la carte CA la base de données de famille. Ceci permet notamment d'effectuer une demande de modification (réinitialisation PIN, activation ou désactivation du compteur de session, révocation et effacement, changement de groupe et/ou de nom, renouvellement de certificat) d'une carte utilisateur au sein de la carte CA.

- Exportation de la CRL : service permettant de récupérer une version chiffrée et scellée de la CRL, transmissible par un moyen indépendant (clé USB, mail, …).
- Régénération du bi-clé d'authentification : service permettant la régénération du bi-clé d'authentification et du certificat correspondant de la carte CA.

2.2 COMPOSITION DE LA TOE

2.2.1 PERIMETRE

La cible d'évaluation est composée de l'applet CryptoSmart.

La plate-forme Javacard, le poste SecPhone et la station d'administration ne font pas partie de la TOE.

2.2.2 IDENTIFICATION DES BIENS PROTEGES PAR LA TOE

Les biens à protéger en confidentialité et en intégrité par la TOE sont :

pour une carte de type utilisateur ou CA :

- Code de la TOE
- PIN
- Clés de famille
- Certificat
- Clé privée d'authentification
- Compteur d'échecs d'authentification distante
- Clé publique CA[3]

pour une carte de type utilisateur :

- CRL
- Clé de session U ↔ U
- Annuaire

pour une carte de type CA :

- Base de données de famille
- Clé privée de signature

[3] Il n'y a pas de nécessité à divulguer cette clé, et sa protection en confidentialité réduit le risque de cryptanalyse.

2.3 CONFIGURATION EVALUEE

L'environnement d'évaluation comporte :

- des cartes Oberthur COSMO64RSA D V5.2 ;
- une station d'administration SecPhone-ADM v1.5 munie d'un lecteur externe Gemplus GemPCTwin USB ;
- deux téléphones Secphone v1.4.

3. ENVIRONNEMENT DE SECURITE

3.1 HYPOTHESES

3.1.1 POSTE

SU1 Le poste téléphonique ne laisse pas fuir la clé de session fournie par la TOE.

SU2 Le poste téléphonique met en œuvre correctement la clé de session fournie par la TOE.

SU3 Le logiciel du poste téléphonique n'est pas corruptible par les données provenant du réseau téléphonique.

SU4 Le poste téléphonique ne laisse fuir aucun élément identifiant (identifiant personnel numérique, identifiant personnel textuel, identifiant de famille numérique, identifiant de famille textuel) de la TOE.

SU5 Le poste téléphonique affiche correctement les identifiants personnels numériques et textuels de la carte distante.

3.1.2 STATION D'ADMINISTRATION

SU6 Les échanges avec la carte CA lors de la création d'une carte Utilisateur ne sont pas divulgués.

SU7 La station d'administration réalise les actions demandées par l'administrateur.

SU8 Le logiciel de la station d'administration n'est pas corruptible par les données provenant du réseau téléphonique.

3.1.3 ADMINISTRATION

SU9 Les administrateurs sont des gens de confiance et ont été formés.

SU10 L'administrateur doit stocker et mettre en œuvre la carte CA et la station d'administration dans un lieu sûr, et non accessible localement (mais potentiellement accessible en ligne). En cas de perte ou vol de la carte CA, il doit récupérer au plus tôt toutes les cartes utilisateurs, les recycler et régénérer un nouveau parc.

SU12 L'administrateur doit tenir à jour la CRL de la carte CA en fonction des déclarations de perte ou vol de cartes, et régulièrement mettre à jour chaque carte Utilisateur pour lui communiquer la CRL modifiée.

SU13 L'administrateur doit périodiquement procéder à la régénération des bi-clés d'authentification, localement ou à distance, afin d'éviter l'usure de ces clés.

SU14 L'administrateur doit périodiquement procéder localement à la régénération de l'ensemble des cartes, afin d'éviter l'usure du bi-clé de signature de la carte CA et des clés de famille.

3.1.4 UTILISATION

SU15 Les utilisateurs doivent changer le code PIN initial de la TOE, en choisissant un code difficile à deviner dont ils assurent la non-divulgation et le renouvellement en cas de soupçon de divulgation.

3.1.5 PLATE-FORME

SU16 La plate-forme Javacard utilisée rend impossible l'accès à la TOE sans passage par les fonctions prévues par la TOE.

SU17 La plate-forme Javacard permet de verrouiller la possibilité d'ajouter une autre applet après installation de la TOE.

SU18 La plate-forme Javacard réalise sans défaut ses fonctions cryptographiques.

3.2 MENACES

3.2.1 MENACES PRISES EN COMPTE PAR LA TOE

T1 Un attaquant local ou en ligne peut obtenir la clé de session U↔U négociée par la TOE et une autre carte afin d'intercepter les données de l'utilisateur protégées par cette clé.

T2 Un attaquant local ou en ligne peut déterminer l'identité de la TOE, soit en accédant à son certificat, soit en établissant un lien avec une communication antérieure.

T3 Un attaquant en ligne[4] peut effectuer une mascarade en se connectant à la TOE ou en s'interposant entre la TOE et une autre carte légitime.

T4 Un attaquant local ou en ligne peut piéger la TOE (i.e. porter atteinte à l'intégrité du code de la TOE, du système d'exploitation ou du circuit).

T5 Un attaquant local ou en ligne peut lire ou corrompre les fichiers sensibles de la TOE.

T6 Un attaquant local ou en ligne peut porter atteinte en confidentialité ou en intégrité aux données transmises lors de la mise à jour en ligne ou hors ligne (notamment exportation de la CRL) de la TOE.

T7 Un attaquant local ou en ligne peut réaliser une carte clone de la TOE.

T8 Un attaquant local ou en ligne peut modifier le code PIN.

T9 Un attaquant local ou en ligne peut falsifier la valeur du compteur d'échecs d'authentification.

[4] Un attaquant en ligne peut par définition disposer de cartes perdues ou volées.

4. OBJECTIFS DE SECURITE

4.1 OBJECTIFS DE SECURITE POUR LA TOE

O1 La TOE doit rendre impossible le recouvrement des clés privées RSA, même par un utilisateur ou administrateur légitime.

O2 La TOE doit rendre impossible le recouvrement par un attaquant en ligne de la clé de session U↔U négociée avec la carte distante dont l'identifiant est fourni par la TOE[5], même s'il acquiert ultérieurement la connaissance des clés privées RSA des deux cartes et s'il a intercepté tous les flux entre cartes de la même famille antérieurement et ultérieurement à la session.

O3 La TOE doit protéger en confidentialité et en intégrité les données échangées lors d'une mise à jour en ligne ou hors ligne (exportation de la CRL).

O4 La TOE doit assurer son anonymat et empêcher l'établissement d'un lien entre sessions vis-à-vis d'un attaquant local ou en ligne.

O5 La TOE doit authentifier correctement la carte distante lors d'une session, et notamment rejeter les cartes perdues ou volées.

O6 La TOE de type utilisateur doit rendre impossible le recouvrement des clés de famille par un attaquant local ou en ligne.

O7 La TOE doit mettre en œuvre une politique de contrôle d'accès à ses fichiers sensibles.

O8 La TOE doit permettre la détection de tentatives d'attaques en ligne.

O9 La TOE doit restreindre la possibilité de modifier le code PIN à l'utilisateur ou l'administrateur légitime.

4.2 OBJECTIFS DE SECURITE POUR L'ENVIRONNEMENT

OE1 Le poste téléphonique doit réaliser sans défaut ses fonctions de sécurité.

OE2 Le responsable de la TOE doit s'assurer que la station d'administration et la carte CA sont situées dans un environnement physiquement protégé (à l'exception d'une ligne téléphonique), où seul l'administrateur peut accéder.

OE3 La station d'administration doit réaliser sans défaut ses fonctions de sécurité.

OE4 Le responsable de la TOE doit s'assurer que l'administrateur est une personne de confiance.

OE5 L'administrateur doit avoir été formé à l'utilisation de la machine d'administration.

OE6 Le responsable de la TOE doit s'assurer que les utilisateurs ont été formés à l'utilisation de la TOE.

[5] L'attaque de l'homme au milieu avec une carte légitime est prise en compte par une combinaison d'objectifs (voir argumentaire relatif à T1).

OE7 La plate-forme Javacard doit rendre impossible la lecture des éléments de la TOE sans passage par les fonctions prévues par la TOE.

OE8 La plate-forme Javacard doit rendre impossible l'installation d'une autre applet après verrouillage.

OE9 La plateforme Javacard doit réaliser sans défaut ses fonctions cryptographiques.

5. EXIGENCES DE SECURITE

5.1 CLASSIFICATION DES DONNEES DE LA TOE

5.1.1 ATTRIBUTS DE SECURITE

La TOE protège en confidentialité et en intégrité les attributs de sécurité (définis par l'administrateur ou l'utilisateur) suivants :

Carte utilisateur et carte CA

- Le code PIN est un secret permettant l'authentification de l'utilisateur.
- Le drapeau de validation du code PIN indique si le code PIN est validé, i.e. si le code PIN présenté correspond bien au code PIN contenu dans la carte.
- Le drapeau de blocage du code PIN indique si le code PIN est actuellement bloqué.

Carte CA

- Base de données de famille : base de données contenant la liste des cartes existantes avec leur identifiant numérique et textuel, leur type, leur groupe, leur état de révocation, les commandes en attente (déblocage du code PIN, renouvellement de certificat).

5.1.2 AUTRES DONNEES DE LA TSF

La TOE protège en confidentialité et en intégrité les données de la TSF (générées par la TOE elle-même) suivantes :

Carte utilisateur

- CRL : liste de révocation signée par la carte CA, déduite de la base de données des cartes utilisateurs.

Carte utilisateur et carte CA

- Clé publique CA : clé publique de signature de la carte CA à laquelle est rattachée la TOE.
- Clés de famille : clés secrètes communes à une famille permettant la protection des échanges entre cartes de la famille. Il s'agit de la clé triple-DES d'anonymat et de la clé triple-DES de scellement.
- Certificat : certificat contenant notamment l'identifiant numérique et textuel, le mode de la carte (CA ou utilisateur), le numéro de carte CA, le groupe, la clé publique d'authentification de la TOE, la signature par la clé privée de signature de la carte CA[6].
- Clé privée d'authentification : clé privée de la TOE correspondant à la clé publique incluse dans le certificat.

[6] Les identifiants numériques et textuels ainsi que le groupe sont issus de la base de données de la carte CA.

- Compteur d'échecs d'authentification distante : compteur permettant de tracer le nombre d'échecs d'authentification entre cartes.

Carte CA

- Clé privée de signature.

5.1.3 DONNEES DE L'UTILISATEUR

La TOE protège en confidentialité et en intégrité les données de l'utilisateur suivantes :

- Clé de session U↔U : clé négociée entre deux cartes utilisateurs (fournie à l'utilisateur lors de l'établissement d'une session réussie). Cette clé fait 1152 bits.

- Annuaire : annuaire stocké dans la carte.

5.2 EXIGENCES DE SECURITE FONCTIONNELLES

Les exigences de sécurité à prendre en compte sont les suivantes :

Classe	Composants
Audit	**FAU_SPE** Audit spécifique limité
Support cryptographique	**FCS_CKM** Gestion des clés cryptographiques
	FCS_COP Opération cryptographique
Protection des données de l'utilisateur	**FDP_ACC** Politique de contrôle d'accès
	FDP_ACF Fonctions de contrôle d'accès
Identification et authentification	**FIA_AFL** Echecs de l'authentification
	FIA_ATD Définition des attributs de l'utilisateur
	FIA_UAU Authentification de l'utilisateur
	FIA_UID Identification de l'utilisateur
Administration de la sécurité	**FMT_MSA** Gestion des attributs de sécurité
	FMT_MTD Gestion des données de la TSF
	FMT_SMF Spécification des fonctions de gestion
	FMT_SMR Rôles pour l'administration de la sécurité
Protection de la vie privée	**FPR_UNL** Impossibilité d'établir un lien
Protection de la TSF	**FPT_ITC** Confidentialité des données de la TSF exportées
	FPT_ITI Intégrité des données de la TSF exportées
	FPT_RVM Passage obligatoire par un moniteur de référence
	FPT_SEP Séparation de domaines

5.2.1 DEFINITION DES SFP

SFP.1 SFP de contrôle d'accès local utilisateur : politique définissant les droits d'accès local des utilisateurs à la TOE.

SFP.2 SFP de contrôle d'accès local administrateur : politique définissant les droits d'accès local de l'administrateur à la TOE.

SFP.3 SFP de contrôle d'accès distant utilisateur : politique définissant les droits d'accès à distance des utilisateurs à la TOE.

SFP.4 SFP de contrôle d'accès distant administrateur : politique définissant les conditions d'accès à distance de l'administrateur à la TOE.

5.2.2 AUDIT DE SECURITE

5.2.2.1 FAU_SPE Audit spécifique limité

Ce composant est non standard.

FAU_SPE.1 Audit spécifique limité

Hiérarchique à : aucun autre composant

FAU_SPE.1.1 La TSF doit pouvoir générer un enregistrement d'audit des événements auditables suivants : [*échec d'authentification distante*].

FAU_SPE.1.2 La TSF doit offrir à [*administrateur*] la capacité de récupérer les enregistrements d'audit.

Dépendances : aucune dépendance

5.2.3 SUPPORT CRYPTOGRAPHIQUE

5.2.3.1 FCS_CKM Gestion de clés cryptographiques

FCS_CKM.1 Génération de clés cryptographiques

FCS_CKM.1.1 [7] La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié [*dérivation du secret commun DH*] et à des tailles de clés cryptographiques spécifiées [1152] qui satisfont à ce qui suit : [*rien*].

FCS_CKM.1.2 [8] La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié [*générateur pseudo-aléatoire*] et à des tailles de clés cryptographiques spécifiées [*168*] qui satisfont à ce qui suit : [*rien*].

FCS_CKM.1.3 [9] La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié [*API Javacard de génération de bi-clés RSA*] et à des tailles de clés cryptographiques spécifiées [*1664*] qui satisfont à ce qui suit : [*rien*].

FCS_CKM.1.4 [10] La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié [*générateur pseudo-aléatoire*] et à des tailles de clés cryptographiques spécifiées [*256*] qui satisfont à ce qui suit : [*rien*].

Dépendances :

FCS_COP.1 Opération cryptographique

---

[7] ce mécanisme sert à générer les clés de session pour le poste

[8] ce mécanisme sert à la génération de clés de famille triple-DES

[9] ce mécanisme sert à la génération de clés RSA

[10] ce mécanisme sert à la génération de secrets pour l'algorithme Diffie-Hellman

FCS_CKM.4 Destruction de clés cryptographiques

FMT_MSA.2 Attributs de sécurité sûrs

FCS_CKM.4 Destruction de clés cryptographiques

FCS_CKM.4.1. La TSF doit détruire les clés cryptographiques conformément à une méthode de distribution de clés cryptographiques spécifiée [*recouvrement de la mémoire*] qui satisfait à ce qui suit : [*rien*].

Dépendances :

FCS_COP.1 Opération cryptographique

FCS_CKM.1 Génération de clés cryptographiques

FMT_MSA.2 Attributs de sécurité sûrs

5.2.3.2 FCS_COP Opération cryptographique

FCS_COP.1.1-1 La TSF doit exécuter [*chiffrement et déchiffrement*] conformément à un algorithme cryptographique [*Triple DES*] et avec des tailles de clés cryptographiques [*168*] spécifiés qui satisfont à ce qui suit : [*FIPS_46-3*].

FCS_COP.1.1-2 La TSF doit exécuter [*MAC*] conformément à un algorithme cryptographique [*Triple DES MAC*] et avec des tailles de clés cryptographiques [*168*] spécifiés qui satisfont à ce qui suit : [*ISO/IEC 9797 Algo 1 Method 2*].

FCS_COP.1.1-3 La TSF doit exécuter [*signature et vérification*] conformément à un algorithme cryptographique [*RSA*] et avec des tailles de clés cryptographiques [*1664*] spécifiés qui satisfont à ce qui suit : [*ISO/IEC 9796-2*].

FCS_COP.1.1-4 La TSF doit exécuter [*chiffrement et déchiffrement*] conformément à un algorithme cryptographique [*RSAEP et RSADP*] et avec des tailles de clés cryptographiques [*1664*] spécifiés qui satisfont à ce qui suit : [*PKCS#1*].

FCS_COP.1.1-5 La TSF doit exécuter [*négociation de clé*] conformément à un algorithme cryptographique [*DH*] et avec des tailles de clés cryptographiques [*1408*] spécifiés qui satisfont à ce qui suit : [*PKCS#3*].

Raffinement :

Les opérations cryptographiques de la TOE reposent sur les fonctions cryptographiques de la plate-forme Javacard.

Dépendances :

FCS_CKM.1 Génération de clés cryptographiques

FCS_CKM.4 Destruction de clés cryptographiques

FMT_MSA.2 Attributs de sécurité sûrs

5.2.4 PROTECTION DES DONNEES UTILISATEUR

5.2.4.1 FDP_ACC Politique de contrôle d'accès

FDP_ACC.2 Contrôle d'accès complet

Hiérarchiquement supérieur à : *FDP_ACC.1*

- **FDP_ACC.2.1-1** La TSF doit appliquer la [*SFP de contrôle d'accès local utilisateur*] aux [
  - *Sujets : utilisateurs*
  - *Objets : annuaire*[11]*]*

et à toutes les opérations sur les sujets et objets couverts par la SFP.

- **FDP_ACC.2.2-1** 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.

Dépendances : *FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité*

- **FDP_ACC.2.1-2** La TSF doit appliquer la [*SFP de contrôle d'accès local administrateur*] aux [
  - *Sujets : administrateurs*
  - *Objets : rien*[12]]

et à toutes les opérations sur les sujets et objets couverts par la SFP.

- **FDP_ACC.2.2-2** 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.

Dépendances : *FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité*

- **FDP_ACC.2.1-3** La TSF doit appliquer la [*SFP de contrôle d'accès distant utilisateur*] aux [
  - *Sujets : utilisateurs*
  - *Objets : clé de session U↔U*[13]]

et à toutes les opérations sur les sujets et objets couverts par la SFP.

- **FDP_ACC.2.2-3** 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.

Dépendances : *FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité*

- **FDP_ACC.2.1-4** La TSF doit appliquer la [*SFP de contrôle d'accès distant administrateur*] aux [
  - *Sujets : administrateurs*

---

[11] pour la TOE en mode Utilisateur

[12] Cette fonction sert de base pour FMT_MSA.1.1-1, ce qui justifie sa présence malgré l'absence de données utilisateur à protéger

[13] Pour la TOE en mode utilisateur

- *Objets : rien*[14]]

et à toutes les opérations sur les sujets et objets couverts par la SFP.

- **FDP_ACC.2.2-4** 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.

Dépendances : *FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité*

5.2.4.2 FDP_ACF Fonctions de contrôle d'accès

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

- **FDP_ACF.1.1-1** La TSF doit appliquer la [*SFP de contrôle d'accès local utilisateur*] aux objets en se basant sur [*type, drapeau de validation du code PIN, drapeau de blocage du code PIN*]

- **FDP_ACF.1.2-1** La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée : [

Les conditions suivantes sont toutes vérifiées :

- *Type=utilisateur*

- *drapeau de blocage du code PIN non activé*

- *drapeau de validation du code PIN activé*]

- **FDP_ACF.1.3-1** La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*aucune*]

- **FDP_ACF.1.4-1** La TSF doit refuser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*aucune*]

- **FDP_ACF.1.1-2** La TSF doit appliquer la [*SFP de contrôle d'accès local administrateur*] aux objets en se basant sur [*type, drapeau de validation du code PIN, drapeau de blocage du code PIN*]

- **FDP_ACF.1.2-2** La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée : [

Les conditions suivantes sont toutes vérifiées :

- *Type=CA*

- *drapeau de blocage du code PIN non activé*

- *drapeau de validation du code PIN activé*]

- **FDP_ACF.1.3-2** La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*aucune*]

[14] Cette fonction sert de base pour FMT_MSA.1.1-3, ce qui justifie sa présence malgré l'absence de données utilisateur à protéger

- **FDP_ACF.1.4-2** La TSF doit refuser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*aucune*]

- **FDP_ACF.1.1-3** La TSF doit appliquer la [*SFP de contrôle d'accès distant utilisateur*] aux objets en se basant sur [Type, *certificat distant,clé publique CA, CRL, groupe local, groupe distant*]

- **FDP_ACF.1.2-3** La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée : [

Les conditions suivantes sont toutes vérifiées :

- *Si Type=utilisateur :*
  - *certificat distant issu de la carte CA de rattachement et valide vis-à-vis de la clé publique CA*
  - *groupe local et groupe distant à intersection non nulle*
  - *drapeau de validation du code PIN activé*
- *si Type=CA :*
  - *certificat distant issu de la TOE et valide vis-à-vis de la clé publique CA*

]

- **FDP_ACF.1.3-3** La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*aucune*]

- **FDP_ACF.1.4-3** La TSF doit refuser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*certificat distant identifié dans la CRL*]

- **FDP_ACF.1.1-4** La TSF doit appliquer la [*SFP de contrôle d'accès distant administrateur*] aux objets en se basant sur [*Type, Certificat distant, clé publique CA, CRL*]

- **FDP_ACF.1.2-4** La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée : [

Les conditions suivantes sont toutes vérifiées :

- Type=utilisateur
- *certificat distant correspondant à la carte CA de rattachement et valide vis-à-vis de la clé publique CA*]

- **FDP_ACF.1.3-4** La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*aucune*]

- **FDP_ACF.1.4-4** La TSF doit refuser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [*certificat distant identifié dans la CRL*]

Dépendances :

FDP_ACC.1 Contrôle d'accès partiel

FMT_MSA.3 Initialisation statique d'attribut

5.2.5 IDENTIFICATION ET AUTHENTIFICATION

5.2.5.1 FIA_AFL Défaillance de l'authentification

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

FIA_AFL.1.1-1 La TSF doit détecter quand [*3*] tentatives d'authentification infructueuses ont eu lieu en relation avec [*authentification de l'utilisateur par code PIN*].

FIA_AFL.1.2-1 Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit [*activer le drapeau de blocage du code PIN*]

FIA_AFL.1.1-2 La TSF doit détecter quand [*6*] tentatives d'authentification infructueuses ont eu lieu en relation avec [*authentification de l'administrateur par code PIN*].

FIA_AFL.1.2-2 Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit [*activer le drapeau de blocage du code PIN*].

Dépendances : *FIA_UAU.1 Programmation de l'authentification*

5.2.5.2 FIA_ATD Définition des attributs de l'utilisateur

FIA_ATD.1 Définition des attributs de l'utilisateur

FIA_ATD.1.1 La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant à des utilisateurs individuels : [

- *code PIN*
- *drapeau de blocage du code PIN*
- *drapeau de validation du code PIN*

]

5.2.5.3 FIA_UAU Authentification de l'utilisateur

FIA_UAU.2 Authentification de l'utilisateur avant toute action

Hiérarchiquement supérieur à : *FIA_UAU.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[15].

[15] Cette exigence s'applique tant à l'utilisateur que l'administrateur, en accès local et distant.

Dépendances : *FIA_UID.1 Programmation de l'identification*

Raffinement :

Cette exigence ne s'applique pas au mécanisme de statut.

5.2.5.4 FIA_UID identification de l'utilisateur

FIA_UID.2 Identification de l'utilisateur avant toute action

Hiérarchiquement supérieur à : *FIA_UID.1*

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[16].

5.2.6 ADMINISTRATION DE LA SECURITE

5.2.6.1 FMT_MSA Gestion des attributs de sécurité

FMT_MSA.1 Administration des attributs de sécurité

FMT_MSA.1.1-1 La TSF doit mettre en œuvre la ou les [*SFP de contrôle d'accès local administrateur*] pour restreindre aux [*administrateur*] l'aptitude de [*consulter, modifier*] les attributs de sécurité [

- *Base de données de famille*
- *Code PIN de la carte CA*[17]

].

FMT_MSA.1.1-2 La TSF doit mettre en œuvre la ou les [*SFP de contrôle d'accès local utilisateur*] pour restreindre aux [*utilisateur*] l'aptitude de [*modifier*] les attributs de sécurité [

- *Code PIN d'une carte utilisateur*

].

FMT_MSA.1.1-3 La TSF doit mettre en œuvre la ou les [*SFP de contrôle d'accès distant administrateur*] pour restreindre aux [*administrateur*] l'aptitude de [*modifier*] les attributs de sécurité [

- *Drapeau de blocage du code PIN*

].

Dépendances :

FDP_ACC.1 Contrôle d'accès partiel

FMT_SMF.1 Spécification des fonctions de gestion

---

[16] Cette exigence s'applique tant à l'utilisateur que l'administrateur, en accès local et distant.

[17] Uniquement modifiable

FMT_SMR.1 Rôles de sécurité

FMT_MSA.2 Attributs de sécurité sûrs

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

Dépendances :

FDP_ACC.1 Contrôle d'accès partiel

FMT_MSA.1 Administration des attributs de sécurité

FMT_SMR.1 Rôles de sécurité

Raffinement :

Cette exigence n'a de sens que pour les clés cryptographiques

FMT_MSA.3 Initialisation statique d'attribut

FMT_MSA.3.1 La TSF doit mettre en œuvre la ou les [

- *SFP de contrôle d'accès local utilisateur*
- *SFP de contrôle d'accès local administrateur*
- *SFP de contrôle d'accès distant utilisateur*
- *SFP de contrôle d'accès distant administrateur*]

afin de fournir des valeurs par défaut [*restrictives*] pour les attributs de sécurité qui sont utilisés pour appliquer les *SFP*.

Raffinement :

Cette exigence n'a de sens que pour les attributs relatifs au mécanisme de PIN.

FMT_MSA.3.2 La TSF doit permettre aux [*administrateur*] de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.

Dépendances :

FMT_MSA.1 Administration des attributs de sécurité

FMT_SMR.1 Rôles de sécurité

5.2.6.2 FMT_MTD Administration des données de la TSF

FMT_MTD.1 Administration des données de la TSF

FMT_MTD.1.1-1 La TSF doit restreindre l'aptitude de [*créer*] les [*carte utilisateur*] aux [*administrateur*].

FMT_MTD.1.1-2 La TSF doit restreindre l'aptitude de [*régénérer*] les [*certificat, clé privée d'authentification*] aux [*administrateur*].

Dépendances :

FMT_SMF.1 Spécification des fonctions de gestion

FMT_SMR.1 Rôles de sécurité

5.2.6.3 FMT_SMF Spécification des fonctions de gestion

FMT_SMF.1 Spécification des fonctions de gestion

FMT_SMF.1.1 La TSF doit être capable de réaliser les fonctions de gestion de la sécurité suivantes : [

- *Contrôle des commandes reçues*
- *Auto-création d'une carte CA ; création d'une carte utilisateur avec choix de la longueur du code PIN.*
- *Gestion de parc*
  - *Pour l'administrateur :*
    - *consultation et modification de la base de données de famille, permettant de réaliser indirectement à distance :*
      - *un changement de groupe et de nom avec renouvellement du certificat*
      - *un déblocage avec réinitialisation du code PIN*
      - *une régénération du bi-clé RSA avec renouvellement du certificat*
      - *une mise à jour de la CRL*
    - *régénération locale du certificat de la carte CA*
    - *exportation de la CRL*
    - *changement du code PIN de la carte CA*
  - *Pour l'utilisateur*
    - *importation de la CRL*
    - *changement de code PIN*

].

5.2.6.4 FMT_SMR Rôles pour la gestion de la sécurité

FMT_SMR.1 Rôles de sécurité

FMT_SMR.1.1 La TSF doit tenir à jour les rôles [*utilisateur, administrateur*].

FMT_SMR.1.2 La TSF doit être capable d'associer des utilisateurs à des rôles.

Dépendances :

FIA_UID.1 Programmation de l'identification

5.2.7 PROTECTION DE LA VIE PRIVEE

5.2.7.1 FPR_UNL Impossibilité d'établir un lien

FPR_UNL.1 Impossibilité d'établir un lien[18]

FPR_UNL.1.1 La TSF doit garantir que [*attaquants en ligne*] sont incapables de déterminer si [*établissement d'une session*] [*ont été déclenchées par le même utilisateur*].

5.2.8 PROTECTION DE LA TSF

5.2.8.1 FPT_ITC Confidentialité des données de la TSF exportées

FPT_ITC.1 Confidentialité inter-TSF pendant une transmission

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.

Raffinement :

Cette exigence s'applique notamment pour la transmission de la liste de révocation (CRL), tant lors d'une mise à jour en ligne que par exportation.

5.2.8.2 FPT_ITI Intégrité des données de la TSF exportées

FPT_ITI.1 Détection inter-TSF d'une modification

FPT_ITI.1.1 La TSF doit offrir la capacité 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 la limite de la métrique suivante : [*scellement par clé triple-DES*].

Raffinement :

Cette exigence s'applique notamment pour la transmission de la liste de révocation (CRL), tant lors d'une mise à jour en ligne que par exportation.

5.2.8.3 FPT_RVM Passage obligatoire par un moniteur de référence

FPT_RVM.1 Capacité de la TSP à ne pas être contournée

FPT_RVM.1.1 La TSF doit garantir que les fonctions qui mettent en œuvre la TSP sont appelées et s'exécutent avec succès avant que chaque fonction dans le TSC ne soit autorisée à démarrer.

[18] Cette exigence implique l'anonymat

5.2.8.4 FPT_SEP Séparation de domaines

FPT_SEP.1 Séparation de domaines pour la TSF

FPT_SEP.1.1 La TSF doit maintenir un domaine de sécurité pour sa propre exécution, qui la protège des interférences et des intrusions par des sujets non sûrs.

FPT_SEP.1.2 La TSF doit appliquer une séparation entre les domaines de sécurité de sujets dans le TSC.

5.2.9 NIVEAU DE RESISTANCE DES FONCTIONS DE SECURITE

Le niveau minimal de résistance des fonctions de sécurité est SOF-high.

5.3 EXIGENCES DE SECURITE D'ASSURANCE

La cible d'évaluation doit être conforme aux parties 2 et 3 des Critères Communs version 2.2 pour le niveau EAL2 augmenté de ADV_HLD.2, ADV_IMP.1 (pour la partie cryptographique), ADV_LLD.1 (pour la partie cryptographique), ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 (pour la partie cryptographique), AVA_MSU.1 et AVA_VLA.2.

6. SPECIFICATIONS GLOBALES DE LA TOE

6.1 FONCTIONS DE SECURITE

6.1.1 INTRODUCTION

L'objet de ce paragraphe est de présenter les fonctions de sécurité (SEF) qui sont intégrées dans la TOE. Les différentes familles de fonctions sont :

- Audit (**AU**) : *cette famille regroupe toutes les fonctions liées à l'audit.*
- Cryptographie (**CR**) : *cette famille regroupe toutes les fonctions liées aux clés de session.*
- Protection et filtrage (**PR**) : *cette famille regroupe toutes les fonctions liées à la protection des données des utilisateurs.*
- Identification et Authentification (**IA**) : *cette famille regroupe toutes les fonctions liées à l'identification et à l'authentification des utilisateurs et des administrateurs.*
- Gestion de la sécurité (**GS**) : *cette famille regroupe toutes les fonctions liées à la gestion des politiques de sécurité.*

6.1.2 AUDIT

La TOE étant intégrée dans une carte à puce, qui ne dispose pas d'horloge et possède une mémoire libre très faible, cette famille de fonctions est très limitée.

6.1.2.1 AU_1

Chaque tentative d'authentification distante en échec provoque l'incrémentation d'un compteur. Ce compteur est relevé par la carte CA à chaque mise à jour et envoyé à la station d'administration pour affichage.

6.1.3 CRYPTOGRAPHIE

6.1.3.1 CR_1

La TOE est capable de mener une phase de négociation de clé de session avec une autre carte. L'enchaînement des opérations cryptographiques lors de l'établissement d'une session est :

- Envoi du certificat de la TOE.
- Génération et envoi d'un aléa Diffie-Hellman chiffré par la clé publique RSA de la carte distante.
- Réception et déchiffrement de l'aléa distant déchiffré par la clé privée RSA de la TOE.
- Calcul et envoi d'une réponse validant la bonne réception de l'aléa distant.
- Réception de la réponse de la carte distante.

- Dérivation de la clé de session à partir du secret commun DH.
- Transmission de la clé de session au poste téléphonique et effacement en mémoire.

6.1.3.2 CR_2

La TOE est capable de chiffrer avec vecteur d'initialisation aléatoire l'ensemble des flux échangés avec une autre carte (y compris la CRL) à l'aide d'une clé commune à la famille de cartes (clé d'anonymat), à l'exception des flux échangés lors de la création d'une carte.

6.1.3.3 CR_3

La TOE est capable de sceller l'ensemble des flux échangés avec une autre carte (y compris la CRL) à l'aide d'une clé commune à la famille de cartes (clé de scellement), à l'exception des flux échangés lors de la création d'une carte.

6.1.4 PROTECTION ET FILTRAGE

6.1.4.1 PR_1

Lors de la mise en relation d'une carte Utilisateur avec une autre carte Utilisateur, après échange des certificats, la carte vérifie qu'elle est dans l'état validée, et qu'elle a au moins un groupe commun avec la carte distante. Dans le cas contraire, l'ouverture de session est avortée.

6.1.4.2 PR_2

Une carte Utilisateur subordonne l'accès en lecture et écriture à l'annuaire à l'état « validée ». Dans le cas contraire, l'accès à l'annuaire est interdit.

6.1.5 IDENTIFICATION ET AUTHENTIFICATION

6.1.5.1 IA_1

Chaque TOE doit posséder les informations suivantes :

- Un certificat composé de :
  - Un identifiant numérique de carte (unique dans une famille)
  - Un rôle (CA ou utilisateur)
  - Un identifiant textuel de carte
  - Un numéro de groupe
  - Une clé publique RSA d'authentification
  - Une signature des éléments précédents par la clé privée de signature de la carte CA
- Une clé privée RSA d'authentification associée.
- La clé publique de signature de la carte CA.

6.1.5.2 IA_2

La TOE est capable de vérifier que le certificat d'une autre carte est valide, i.e. qu'il émane de la même autorité de certification et qu'il n'appartient pas à la CRL.

6.1.5.3 IA_3

La TOE est capable mener une phase d'authentification avec une carte distante dont le certificat est valide afin de prouver la connaissance par la carte distante de la clé privée correspondant au certificat. En cas d'échec, le compteur d'échecs d'authentification distante est incrémenté.

6.1.5.4 IA_4

La TOE de type utilisateur est capable d'authentifier l'utilisateur local par code PIN. Au bout de 3 essais infructueux, la carte est dans le sous-état « bloquée ». Elle peut être débloquée par l'administrateur au moyen de la carte CA.

6.1.5.5 IA_5

La TOE de type CA est capable d'authentifier l'administrateur local par code PIN. Au bout de 6 essais infructueux, la carte est dans le sous-état « bloquée ».

6.1.6 GESTION DE LA SECURITE

6.1.6.1 GS 3

La carte ne comporte qu'une seule APDU spécifique comportant un code de commande. Toutes les commandes sont soumises à une analyse syntaxique et sécuritaire par un moniteur de sécurité.

6.1.6.2 GS 4

La carte CA est auto-générée. Toutes les autres cartes créées à partir de la carte CA sont des cartes utilisateur. La longueur de code PIN peut être fixée par l'administrateur à la création. Toutes les clés sont générées avec des valeurs aléatoires et fortes.

6.1.6.3 GS 6

L'administrateur peut effectuer les tâches de gestion de parc suivantes :

- Consulter et mettre à jour la base de données de famille, et ainsi indirectement par mise en relation ultérieure :
    - changer le groupe et le nom d'une carte avec renouvellement du certificat ;
    - débloquer et réinitialiser le code PIN à distance ;
    - régénérer à distance le bi-clé RSA avec mise à jour du certificat ;
    - mettre à jour la CRL ;
- Provoquer la régénération locale du certificat de la carte CA.
- Exporter la CRL chiffrée et scellée pour transmission par un canal non protégé.
- Changer son code PIN.

L'utilisateur peut effectuer les tâches de gestion suivantes :

- Importer la CRL fournie par la carte CA.
- Changer son code PIN.

6.1.7 NIVEAU DE RESISTANCE DES FONCTIONS DE SECURITE

Le niveau de résistance des fonctions de sécurité est SOF-high.

6.2 MESURES D'ASSURANCE

La cible d'évaluation doit être conforme aux parties 2 et 3 des Critères Communs version 2.2 pour le niveau EAL2 augmenté de ADV_HLD.2, ADV_IMP.1 (pour la partie cryptographique), ADV_LLD.1 (pour la partie cryptographique), ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 (pour la partie cryptographique), AVA_MSU.1 et AVA_VLA.2.

Les documents fournis pour l'évaluation sont décrits dans [PlanDoc].

La matrice suivante fournit détaille la liste des fournitures pour chaque mesure d'assurance.

	[DD]	[DJD]	[SPC]	[SPI]	[SPINT]	[IMP]	[SVN]	[GC]	[TEST]	[LOG]	[VUL]	[ADM]	[USR]	[SUPPORT]	[P9]	[DSEC]	[PINST]	[PLIV]
ACM_CAP.2							X	X										
ADO_DEL.1																		X
ADO_IGS.1																	X	
ADV_FSP.1		X	X	X														
ADV_HLD.2			X	X	X													
ADV_IMP.1						X												
ADV_LLD.1			X		X													
ADV_RCR.1		X																
AGD_ADM.1												X						
AGD_USR.1													X					
ALC_DVS.1															X	X		
ALC_FLR.3														X				
ALC_TAT.1	X																	
ATE_COV.1									X									
ATE_FUN.1									X	X								
ATE_IND.2									X	X								
AVA_MSU.1											X							
AVA_SOF.1											X							
AVA_VLA.2											X							

7. CONFORMITE A UN PROFIL DE PROTECTION

7.1 REFERENCE DU PROFIL DE PROTECTION

La cible de sécurité ne fait référence à aucun profil de protection.

7.2 RAFFINEMENT DU PROFIL DE PROTECTION

Sans objet.

7.3 COMPLEMENT AU PROFIL DE PROTECTION

Sans objet.

8. ARGUMENTAIRE

8.1 ARGUMENTAIRE POUR LES OBJECTIFS DE SECURITE

	O1	O2	O3	O4	O5	O6	O7	O8	O9	OE1	OE2	OE3	OE4	OE5	OE6	OE7	OE8	OE9
T1	X	X			X					X					X	X		X
T2				X		X	X				X	X	X	X	X	X		X
T3	X		X		X		X	X					X	X				X
T4																X	X	
T5							X		X						X	X		
T6			X			X												X
T7	X						X				X	X	X	X		X		
T8									X							X		
T9			X				X											X
SU1										X								
SU2										X								
SU3										X								
SU4										X								
SU5										X								
SU6											X	X						
SU7												X						
SU8												X						
SU9													X	X				
SU10											X			X				
SU12														X				
SU13														X				
SU14														X				
SU15															X			
SU16																X		
SU17																	X	
SU18																		X

T1 est la menace principale sur la TOE. Elle est couverte par les objectifs permettant :

- de garantir l'impossibilité de recouvrir la clé privée RSA (O1), en s'appuyant sur la protection correcte des ressources par la plate-forme Javacard de la carte à puce (OE7) ;

- de rendre impossible le calcul de la clé de session U↔U sans altération de l'identifiant distant fourni par la TOE, même en ayant connaissance a priori ou a posteriori des clés privées RSA et de tous les échanges entre cartes de la même famille (propriété de « perfect forward secrecy ») (O2), O2 s'appuyant sur la justesse des fonctions cryptographiques de la plate-forme (OE9) ;

- de détecter et de parer une attaque par interposition d'une carte légitime (attaque de l'homme au milieu), par l'objectif d'authentification (O5) et l'objectif de contrôle de l'identifiant par l'utilisateur (OE6) ;

- d'éviter une fuite de la clé dans le téléphone (OE1) ;

La liaison entre la TOE et le téléphone est protégée du fait que le lecteur de carte à puce est intégré au téléphone.

T2 est couverte :

- par l'objectif O4 qui assure l'anonymat, et couvrant en particulier les attaques en ligne sur la carte CA ;
- par l'objectif O6 qui garantit la confidentialité des clés de famille ;
- par l'objectif O7 qui protège l'accès au certificat et à la base de données de famille ;
- par l'utilisation correcte du code PIN par l'utilisateur (OE6) ;
- par la résistance de la plate-forme aux tentatives de contournement (OE7) ;
- par la justesse des fonctions cryptographiques de la plate-forme (OE9).

Les cas particuliers d'une attaque par l'administrateur, ou d'une attaque locale sur la carte CA, sont couverts par les objectifs de fonctionnement correct de la station d'administration (OE3), d'absence de malveillance, de négligence ou de maladresse de l'administrateur (OE4 et OE5), et de stockage en lieu sûr de la station d'administration et de la carte CA (OE2).

T3 est couverte par :

- l'impossibilité de recouvrer la clé privée (01) ;
- l'objectif d'authentification (O5), qui s'appuie sur la mise à jour diligente de la CRL et sur un renouvellement des clés d'authentification avant usure, ce que garantie le respect des préconisations du fabricant (OE5) et la confiance dans l'administrateur (OE4) ;
- l'impossibilité de falsifier la CRL en transit (O3) ou sur la TOE (O7). O3 s'appuie sur par la justesse des fonctions cryptographiques de la plate-forme (OE9) ;
- la détection de tentatives d'attaques en lignes (O8), qui renforce la protection face à cette menace.

T4 est couverte par l'impossibilité d'utiliser la plate-forme Javacard de la carte à puce pour contourner l'applet (OE7) et l'absence de risque d'interaction, après verrouillage de la fonction d'installation d'une applet, entre l'applet CryptoSmart et une applet « attaquante » (OE8).

T5 est couverte par :

- l'objectif de mise en œuvre d'une politique de contrôle d'accès aux fichiers sensibles (O7),
- l'impossibilité pour un attaquant de modifier le code PIN (O9),
- l'impossibilité d'utiliser la plate-forme Javacard de la carte à puce pour contourner l'applet (OE7),
- le choix par l'utilisateur d'un code PIN non aisé à deviner (OE6).

T6 est couverte par l'objectif de scellement et de chiffrement des échanges de mise à jour (O3) en s'appuyant sur par la justesse des fonctions cryptographiques de la plate-forme (OE9), et par l'impossibilité de recouvrer les clés de famille (O6).

T7 est couverte :

- pour le cas d'une tentative de copie d'une carte utilisateur, par l'impossibilité d'accès aux clés privées RSA (O1), en s'appuyant sur l'impossibilité d'utiliser la plate-forme Javacard de la carte à puce pour contourner l'applet (OE7),

- pour le cas d'une attaque en ligne sur la carte CA par les objectifs de contrôle d'accès à la base de données de famille (O7) et de bon fonctionnement de la station d'administration (OE3) ;

- pour le cas d'une attaque locale sur la carte CA par les objectifs de contrôle d'accès à la base de données de famille (O7) l'objectif de protection physique de la carte CA (OE2) ;

- pour le cas d'une erreur ou d'une malveillance de l'administrateur par les objectifs d'honnêteté et de compétence de l'administrateur (OE4 et OE5).

T8 est couverte par l'objectif de protection du code PIN (O9), en s'appuyant sur l'impossibilité d'utiliser la plate-forme Javacard de la carte à puce pour contourner l'applet (OE7).

T9 est couverte par l'objectif de contrôle d'accès aux fichiers sensibles (O7), et la protection des données en transit lors de la mise à jour (O3). O3 s'appuie sur par la justesse des fonctions cryptographiques de la plate-forme (OE9).

SU1, SU2, SU3, SU4 et SU5 sont couvertes par le bon fonctionnement du téléphone (OE1).

SU6 est couverte par l'isolation physique de la station d'administration (OE2) et le bon fonctionnement de la station d'administration (OE3).

SU7 et SU8 sont couvertes par le bon fonctionnement de la station d'administration (OE3).

SU9 est couverte par les objectifs d'honnêteté et de compétence de l'administrateur (OE4 et OE5).

SU10 est couverte par la protection physique de la station d'administration (OE2) et l'application des consignes en cas de perte ou vol (OE5).

SU12, SU13 et SU14 sont couvertes par le respect des préconisations du fabricant à l'administrateur (OE5).

SU15 est couverte par le respect des préconisations du fabricant aux utilisateurs (OE6).

SU16 est couverte par l'objectif sur l'environnement correspondant (OE7).

SU17 est couverte par l'objectif sur l'environnement correspondant (OE8).

SU18 est couverte par l'objectif sur l'environnement correspondant (OE9).

8.2 ARGUMENTAIRE POUR LES EXIGENCES DE SECURITE

8.2.1 MATRICE DE COHERENCE EXIGENCES DE SECURITE / OBJECTIFS

	O1	O2	03	O4	O5	O6	O7	O8	O9
FAU_SPE.1								X	
FCS_CKM.1.1		X							
FCS_CKM.1.2						X			
FCS_CKM.1.3	X								
FCS_CKM.1.4		X							
FCS_CKM.4		X							
FCS_COP.1.1-1		X	X	X					
FCS_COP.1.1-2		X	X						
FCS_COP.1.1-3					X				
FCS_COP.1.1-4		X							
FCS_COP.1.1-5		X							
FDP_ACC.2.x-1							X		
FDP_ACC.2.x-2							X		
FDP_ACC.2.x-3		X							
FDP_ACC.2.x-4							X		
FDP_ACF.1.x-1							X		
FDP_ACF.1.x-2							X		
FDP_ACF.1.x-3		X							
FDP_ACF.1.x-4							X		
FIA_AFL.1.x-1							X		X
FIA_AFL.1.x-2							X		X
FIA_ATD.1									X
FIA_UAU.2					X		X		
FIA_UID.2							X		
FMT_MSA.1.1-1							X		X
FMT_MSA.1.1-2							X		X
FMT_MSA.1.1-3							X		X
FMT_MSA.2	X	X				X	X		
FMT_MSA.3							X		
FMT_MTD.1.1-1					X				
FMT_MTD.1.1-2					X				
FMT_SMF.1			X		X		X		X
FMT_SMR.1							X		
FPR_UNL.1				X					
FPT_ITC.1		X	X	X					
FPT_ITI.1		X	X						
FPT_RVM.1	X					X	X		X
FPT_SEP.1	X					X	X		X

O1 est couvert par :

- la résistance de l'algorithme RSA avec la longueur de clé choisie (FCS_CKM.1.3) et le choix de clés fortes (FMT_MSA.2),

- la protection contre les accès par un biais détourné apportée par le passage obligatoire par un moniteur de référence (FPT_RVM.1) et la séparation de domaines (FPT_SEP.1).

O2 est couvert par :

- la solidité du protocole de négociation de clé (dérivation du secret DH par FCS_CKM.1.1, qualité du générateur pseudo-aléatoire par FCS_CKM.1.4 et FMT_MSA.2, surchiffrement RSA par FCS_COP.1.1-4, qualité du DH par FCS_COP.1.1-5) ;

- le scellement des données (FPT_ITI.1 et FCS_COP.1.1-2) ;
- le chiffrement des données (FPT_ITC.1 et FCS_COP.1.1-1) ;
- la destruction des clés de sessions (FCS_CKM.4) ;
- le contrôle d'accès à la clé de session (FDP_ACC.2.x-3 et FDP_ACF.1.x-3)

O3 est couvert par :

- le scellement des données (FPT_ITI.1 et FCS_COP.1.1-2) ;
- le chiffrement des données (FPT_ITC.1 et FCS_COP.1.1-1) ;
- la fonction d'importation et d'exportation de la CRL (FMT_SMF.1).

O4 est couvert par la confidentialité des échanges inter-cartes (FPT_ITC.1 et FCS_COP.1.1-1) et l'impossibilité d'établir un lien (FPR_UNL.1), qui implique l'anonymat.

O5 est couvert par :

- la signature des certificats (FCS_COP.1.1-3),
- l'authentification de la carte distante (FIA_UAU.2),
- la gestion de la CRL (FMT_SMF.1),
- la restriction de l'aptitude à créer des cartes utilisateurs à l'administrateur (FMT_MTD.1.1-1),
- la restriction de l'aptitude à modifier des certificats à l'administrateur (FMT_MTD.1.1-2).

O6 est couvert par la génération aléatoire des clés de famille (FCS_CKM.1.2 et FMT_MSA.2) et la protection contre les accès par un biais détourné apportée par le passage obligatoire par un moniteur de référence (FPT_RVM.1) et la séparation de domaines (FPT_SEP.1).

O7 est couvert par :

- les politiques et les fonctions de contrôle d'accès :
  - pour une carte utilisateur, par l'utilisateur local FDP_ACC.2.x-1 et FDP_ACF.1.x-1
  - pour la carte CA, par l'administrateur local FDP_ACC.2.x-2 et FDP_ACF.1.x-2
  - pour une carte utilisateur, par l'administrateur distant FDP_ACC.2.x-4 et FDP_ACF.1.x-4
- l'identification de l'utilisateur (FIA_UID.2),
- l'authentification de l'utilisateur (FIA_AFL.1.x-1, FIA_AFL.1.x-2 et FIA_UAU.2),
- l'administration correcte de la sécurité (FMT_MSA.1.1-x, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1 et FMT_SMR.1),
- la protection contre les accès par un biais détourné apportée par le passage obligatoire par un moniteur de référence (FPT_RVM.1) et la séparation de domaines (FPT_SEP.1).

O8 est couvert par les fonctions d'audit (FAU_SPE.1).

O9 est couvert par :

- la définition d'un code PIN (FIA_ATD.1)
- les conditions de modification ou de déverrouillage du code PIN (FMT_MSA.1.1-x) ;
- la protection contre les échecs multiples (FIA_AFL.1.x-1, FIA_AFL.1.x-2) ;
- la protection contre la modification par un biais détourné apportée par le passage obligatoire par un moniteur de référence (FPT_RVM.1) et la séparation de domaines (FPT_SEP.1) ;
- la fonction de changement de code PIN (FMT_SMF.1.1).

8.2.2 ETUDE DES DEPENDANCES ET DE LA COMPLEMENTARITE DES EXIGENCES DE SECURITE

- Les exigences de sécurité standard de la classe FAU ne sont pas utilisées en raison de l'absence d'horloge et de la très faible place disponible sur la carte à puce. L'audit spécifique limité est défini ainsi :

FAU_SPE.1 Audit spécifique limité

Hiérarchique à : aucun autre composant

FAU_SPE.1.1 La TSF doit pouvoir générer un enregistrement d'audit des événements auditables suivants : [*liste des événements auditables*].

FAU_SPE.1.2 La TSF doit offrir à [*rôle*] la capacité de récupérer les enregistrements d'audit.

Dépendances : aucune dépendance

- Le tableau suivant résume les dépendances des composants d'exigences de sécurité et justifie leur satisfaction ou non-satisfaction.

Composant	Dépendances	Satisfaction
FAU_SPE.1	Aucune	
FCS_CKM.1	FCS_COP.1	FCS_COP.1
	FCS_CKM.4	FCS_CKM.4
	FMT_MSA.2	FMT_MSA.2
FCS_COP.1	FCS_CKM.1	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
	FMT_MSA.2	FMT_MSA.2
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	Aucune	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	Aucune	
FMT_MSA.1	FDP_ACC.1	FDP_ACC.2
	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.2	ADV_SPM.1	non pertinent au niveau d'assurance visé
	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1

FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	Aucune	
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPR_UNL.1	Aucune	
FPT_ITC.1	Aucune	
FPT_ITI.1	Aucune	
FPT_RVM	Aucune	
FPT_SEP	Aucune	

8.2.3 ETUDE DU NIVEAU D'EVALUATION DEMANDE

Le niveau EAL2 augmenté choisi est défini par [QUALIF].

Le niveau minimal de résistance des fonctions de sécurité SOF-high est cohérent avec [QUALIF].**ARGUMENTAIRE POUR LES SPECIFICATIONS GLOBALES DE LA TOE**

8.3.1 FONCTIONS DE SECURITE

Le tableau ci-dessous montre que chaque fonction de sécurité est prise en compte par au moins une exigence de sécurité et que chaque exigence de sécurité est corrélée avec au moins une fonction de sécurité.

	AU_1	CR_1	CR_2	CR_3	PR_1	PR_2	IA_1	IA_2	IA_3	IA_4	IA_5	GS_3	GS_4	GS_6
FAU_SPE.1	X													
FCS_CKM.1.1		X												
FCS_CKM.1.2													X	
FCS_CKM.1.3													X	X
FCS_CKM.1.4		X												
FCS_CKM.4		X												
FCS_COP.1.1-1			X											
FCS_COP.1.1-2				X										
FCS_COP.1.1-3								X					X	X
FCS_COP.1.1-4		X							X					
FCS_COP.1.1-5		X												
FDP_ACC.2.x-1						X				X				
FDP_ACC.2.x-2											X			
FDP_ACC.2.x-3					X		X	X	X					
FDP_ACC.2.x-4							X	X	X					
FDP_ACF.1.x-1						X				X				
FDP_ACF.1.x-2											X			
FDP_ACF.1.x-3					X		X	X	X					
FDP_ACF.1.x-4							X	X	X					
FIA_AFL.1.x-1										X				
FIA_AFL.1.x-2											X			
FIA_ATD.1							X							
FIA_UAU.2									X	X	X			
FIA_UID.2							X							
FMT_MSA.1.1-1														X
FMT_MSA.1.1-2														X
FMT_MSA.1.1-3														X
FMT_MSA.2													X	
FMT_MSA.3										X	X		X	
FMT_MTD.1.1-1													X	
FMT_MTD.1.1-2														X
FMT_SMF.1												X	X	X
FMT_SMR.1							X						X	
FPR_UNL.1			X											
FPT_ITC.1			X											
FPT_ITI.1				X										
FPT_RVM.1												X		
FPT_SEP.1												X		

FAU_SPE.1 Audit spécifique limité

- Cette exigence est prise en compte par la gestion du compteur d'authentifications distantes échouées (AU_1).

FCS_CKM.1 Génération de clés cryptographiques

- Les exigences FCS_CKM.1.1 et FCS_CKM.1.4 sont prises en compte par la fonction de génération de clés de session CR_1.

- L'exigence FCS_CKM.1.2 est prise en compte par la fonction de création de carte GS_4.
- L'exigence FCS_CKM.1.3 est prise en compte par les fonctions de création de carte GS_4 et de régénération des clés RSA GS_6.

FCS_CKM.4 Effacement de clés cryptographiques

- Cette exigence est prise en compte par la génération de clés de session CR_1.

FCS_COP.1 Opération cryptographique

- L'exigence FCS_COP.1.1-1 est prise en compte par la fonction de chiffrement CR_2, y compris pour le chiffrement de la CRL.
- L'exigence FCS_COP.1.1-2 est prise en compte par la fonction de scellement CR_3, y compris pour le scellement de la CRL.
- L'exigence FCS_COP.1.1-3 est prise en compte par la fonction de création de carte GS_4, de vérification de certificat IA_2, et de renouvellement de certificat GS_6.
- L'exigence FCS_COP.1.1-4 est prise en compte pour la protection des échanges DH par la fonction de négociation de clé de session CR_1, et pour la fonction d'authentification IA_3.
- L'exigence FCS_COP.1.1-5 est prise en compte par la fonction de négociation de clé de session CR_1.

FDP_ACC.2.x-1 Contrôle d'accès complet, pour l'utilisateur local :

- Pour la carte utilisateur, cette exigence est prise en compte par la fonction d'identification IA_4, et la fonction de filtrage PR_2, qui impose l'authentification préalable à l'accès annuaire.
- Il n'y a aucun accès local utilisateur à la carte CA.

FDP_ACC.2.x-2 Contrôle d'accès complet, pour l'administrateur local :

- Il n'y a aucun accès local administrateur à la carte utilisateur.
- Pour la carte CA, cette exigence est prise en compte par la fonction d'identification IA_5.

FDP_ACC.2.x-3 Contrôle d'accès complet, pour l'utilisateur distant :

- Pour la carte utilisateur, cette exigence est prise en compte par les fonctions d'identification IA_1, IA_2 et IA_3 et la fonction de filtrage PR_1.
- Pour la carte CA, cette exigence est prise en compte par les fonctions d'identification IA_1, IA_2 et IA_3.

FDP_ACC.2.x-4 Contrôle d'accès complet, pour l'administrateur distant :

- Pour la carte utilisateur, cette exigence est prise en compte par les fonctions d'identification IA_1, IA_2 et IA_3.
- La carte CA ne peut pas recevoir un accès distant administrateur.

FDP_ACF.1.x-1 Contrôle d'accès basé sur les attributs de sécurité, pour l'administrateur local

- Pour la carte utilisateur, cette exigence est prise en compte par la fonction d'authentification IA_4, ainsi que la fonction de filtrage PR_2 qui impose la saisie préalable du code PIN.

- Il n'y a aucun accès local utilisateur à la carte CA.

FDP_ACF.1.x-2 Contrôle d'accès basé sur les attributs de sécurité, pour l'administrateur local

- Il n'y a aucun accès local administrateur à la carte utilisateur.

- Pour la carte CA, cette exigence est prise en compte par la fonction d'authentification IA_5.

FDP_ACF.1.x-3 Contrôle d'accès basé sur les attributs de sécurité, pour l'utilisateur distant

- Pour la carte utilisateur, cette exigence est prise en compte par les fonctions de filtrage PR_1 qui impose un groupe commun et la validation préalable du code PIN, et par les fonctions d'identification IA_1, IA_2 et IA_3.

- Pour la carte CA, cette exigence est prise en compte par les fonctions d'identification IA_1, IA_2 et IA_3.

FDP_ACF.1.x-4 Contrôle d'accès basé sur les attributs de sécurité, pour l'administrateur distant

- Pour la carte utilisateur, cette exigence est prise en compte par les fonctions d'identification IA_1, IA_2 et IA_3.

- La carte CA ne peut pas recevoir un accès distant administrateur.

FIA_AFL.1.x-1 Gestion d'une défaillance de l'authentification, pour une carte utilisateur

- Cette exigence est prise en compte par la fonction d'authentification locale IA_4.

FIA_AFL.1.x-2 Gestion d'une défaillance de l'authentification, pour une carte CA

- Cette exigence est prise en compte par la fonction d'authentification locale IA_5.

FIA_ATD.1 Définition des attributs d'un utilisateur

- Cette exigence est prise en compte par la fonction d'identification IA_1.

FIA_UAU.2 Authentification de l'utilisateur avant toute action

- Cette exigence est prise en compte par les fonctions d'authentification IA_3, IA_4 et IA_5.

FIA_UID.2 Identification de l'utilisateur avant toute action

- Cette exigence est prise en compte par la fonction d'identification IA_1, chaque utilisateur étant identifié par son certificat.

FMT_MSA.1.1-1 Gestion des attributs de sécurité, accès local à la base de données et au code PIN (carte CA)

- Cette exigence est prise en compte par la fonction de gestion de sécurité GS_6.

FMT_MSA.1.1-2 Gestion des attributs de sécurité, accès local au code PIN (carte utilisateur)

- Cette exigence est prise en compte par la fonction de gestion de sécurité GS_6.

FMT_MSA.1.1-3 Gestion des attributs de sécurité, accès distant au groupe et au code PIN (carte utilisateur)

- Cette exigence est prise en compte par la fonction de gestion de sécurité GS_6, pour la mise à jour à distance d'une carte utilisateur.

FMT_MSA.2 Attributs de sécurité sûrs

- Cette exigence est prise en compte par la fonction de création des cartes GS_4, qui génère des clés aléatoires et fortes.

FMT_MSA.3 Initialisation statique d'attribut

- Pour le drapeau de validation du code PIN, cette exigence est prise en compte par les fonctions de PIN IA_4 et IA_5, qui doivent assurer que l'état par défaut est « non validé ».
- La valeur par défaut de la commande de déblocage du code PIN au sein de la base de données de famille est gérée par GS_4.
- La valeur par défaut de drapeau de blocage de code PIN n'a pas de valeur « restrictive ».
- L'administrateur doit choisir la valeur du code PIN par GS_4.

FMT_MTD.1.1-1 Administration des données de la TSF, création d'une carte

- Cette exigence est prise en compte par la fonction GS_4.

FMT_MTD.1.1-2 Administration des données de la TSF, régénération du certificat

- Cette exigence est prise en compte par la fonction GS_6.

FMT_SMF.1 Spécification des fonctions de gestion

- Cette exigence est prise en compte par les fonctions de gestion de la sécurité GS_3, GS_4 et GS_6.

FMT_SMR.1 Rôles de sécurité

- Cette exigence est prise en compte par les fonctions d'identification IA_1 qui définit le certificat de chaque carte précisant son rôle, et par la fonction de gestion de la sécurité GS_4 qui définit la procédure de création des cartes.

FPR_UNL.1 Impossibilité d'établir un lien

- Cette exigence est prise en compte par le chiffrement avec vecteur d'initialisation aléatoire (CR_2)

FPT_ITC.1 Confidentialité inter-TSF pendant une transmission

- Cette exigence est prise en compte par la fonction de chiffrement CR_2. Le produit de confiance mentionné est une autre TOE.

FPT_ITI.1 Détection inter-TSF d'une modification

- Cette exigence est prise en compte par la fonction de scellement CR_3. Le produit de confiance mentionné est une autre TOE.

FPT_RVM.1 Capacité de la TSP à ne pas être contournée

- Cette exigence est prise en compte par la fonction de sécurité GS_3.

FPT_SEP.1 Séparation de domaines pour la TSF

- Cette exigence est prise en compte par la fonction de sécurité GS_3.

8.3.2 MESURES D'ASSURANCE

8.3.2.1 Classe d'assurance ACM

La classe d'assurance ACM est couverte par les documents [GC] et [SVN] qui présente la gestion de configuration du développement et l'identification de la TOE.

8.3.2.2 Classe d'assurance ADO

La classe d'assurance ADO est couverte par les documents :

- [PINST] qui présente les procédures d'installation, de personnalisation et de verrouillage de la TOE.
- [PLIV] qui présente les procédures de transfert de la TOE à l'utilisateur.

8.3.2.3 Classe d'assurance ADV

La classe d'assurance ADV est couverte par les documents [DJD], [SPINT], [SPI], [SPC] et [IMP], qui présentent les spécifications fonctionnelles, la conception générale et de la conception détaillée jusqu'à l'implémentation pour la partie relative à la cryptographie.

8.3.2.4 Classe d'assurance AGD

La classe d'assurance AGD est couverte par les documents [ADM] et [USR] qui contiennent les procédures d'administration et d'utilisation de la TOE pour une mise en oeuvre sécurisée de la TOE.

8.3.2.5 Classe d'assurance ALC

La classe d'assurance ALC est couverte par les documents :

- [P9] et [DSEC] qui décrivent les mesures de sécurités adoptées lors du développement et de la maintenance de la TOE
- [SUPPORT] qui décrit les techniques mises en œuvre pour gérer le traitement des anomalies de sécurité, la diffusion des informations relatives à ces anomalies, puis des correctifs une fois celles-ci corrigées.
- [DD] qui identifie les outils de développement.

8.3.2.6 Classe d'assurance ATE

La classe d'assurance ATE est couverte par les documents :

- [TEST] qui présente la couverture des tests réalisés comprenant les conditions initiales, les procédures de test et les résultats attendus
- [LOG] qui recueille tous les résultats observés de la couverture de tests

8.3.2.7 Classe d'assurance AVA

La classe d'assurance AVA est couverte par les documents :

- [VUL] qui présente l'analyse de vulnérabilité de la TOE et vérifie que la sécurité de la TOE n'est jamais compromise dans les procédures de mise en œuvre des guides.