IDEMIA

11 Boulevard Gallieni
92130 Issy-les-Moulineaux

Cloudcard+ - Cible de sécurité publique

Cloudcard +

Réf. : SafranIS_CC+_ST_lite_fr - 2018_2000021689
Version 1.00 du 27/03/2018

Référence : **Version :** **Date de dernière mise à jour :**	SafranIS_CC+_ST_lite_fr - 2016_2000021689 1.00 27/03/2018
Niveau de confidentialité :	PUBLIQUE

Diffusion

Destinataires	Objet de la diffusion
Publique	Information CSPN CloudCard +

Table des mises à jour du document

N° de version	Etat[1]	Date	Auteur	Objet de la mise à jour
1.0	V	27/10/2018	Idemia	Cible publique produit CloudCard+

[1] **T** : En cours de modification ; **V** : Validé

SOMMAIRE

1. INTRODUCTION

Le présent document décrit la cible de sécurité pour la certification de sécurité de premier niveau (C.S.P.N.) du produit Cloudcard+ de IDEMIA (antérieurement Safran I&S) par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), comprenant la bibliothèque Cloudcard+ SDK intégrée dans une application d'authentification/signature sur son équipement personnel (de type smartphone équipé d'une caméra frontale) et Cloudcard+ Serveur, hébergé sur une infrastructure centralisée et partagée (Cloud).

1.1. Vocabulaire

➢ Application cliente

L'application mobile dans laquelle est intégrée la bibliothèque Cloudcard+ SDK qui forme la partie cliente du produit évalué dans le cadre du présent CSPN.

➢ Cloudcard+ SDK

La bibliothèque qui forme une couche d'abstraction de l'ensemble des fonctions de sécurité pour l'authentification et la signature. Elle gère tous les échanges avec le serveur, ainsi que l'ensemble des interactions avec l'utilisateur liées à la sécurité, y compris donc l'entrée de ses moyens d'authentification (PIN, éléments biométriques) et l'affichage des transactions de demande d'authentification et de signature. L'application cliente hors SDK ne gère que des éléments fonctionnels métiers hors signature et authentification.

➢ Cloudcard+ Server

La partie serveur du système avec laquelle Cloudcard+ SDK communique, qui forme la partie serveur du produit évalué dans le cadre du présent CSPN.

➢ Keyring

Un keyring désigne le contexte associé à un contexte d'identité de l'utilisateur utilisable pour l'authentification et/ou la signature et une entité émettrice de ce contexte. Le keyring permet à l'utilisateur soit de s'authentifier avec cette identité, soit de signer avec l'identité et une paire de clé personnelle qui y est associé.

➢ Porteur

L'utilisateur qui se sert de l'application cliente pour réaliser des authentifications et des signatures.

➢ Itinérance de keyring

L'action qui permet de réaliser la duplication, ou le transfert, de l'accès à un keyring vers une autre instance de l'application sur un autre équipement personnel en possession de l'utilisateur.

1.2. Abréviations

CGA	Certificate Generation Authority

SP	Service Provider
SCD	Signature Creation Data
SVD	Signature Validation Data
SSCD	Secure Signature Creation Device
PAN	Personal Account Number
AAR	Android Application Record
PIN	Personal Identification Number
POI	Point Of Interaction
HI	Human Interface
POP	Proof-of-Possession (of the SCD)
DTBS/R	Data To Be Signed / Representation
RA	Registration Authority
SE	Secure Element
VAD	Verification Authentication Data
RAD	Reference Authentication Data
OTP	One Time Password

1.3. Références externes

[SEC_GUIDE]	Security Recommendations for integration of the High Level SDK - 2017_2000025907 Version 1.1
[SERVER]	Security Recommendations Server configuration 1.0, 1st September 2017

2. IDENTIFICATION DU PRODUIT

Organisation éditrice	IDEMIA (ex. Safran Identity & Security)
Lien vers l'organisation	https://www.idemia.com/
Nom commercial du produit	*Cloudcard+*
Numéro de la version évaluée	3.4 (*)
Catégorie de produit	6. identification, authentification et contrôle d'accès

(*) versions mineures concernées : à partir de la version 3.4.14.8

3. ARGUMENTAIRE

Le contexte d'utilisation consiste en l'utilisation d'une application mobile pour assurer des fonctions d'authentification et de signature. Pour la signature, l'application assure que la clé privée qui est stockée sur un serveur demeure sous le contrôle exclusif de l'utilisateur.

3.1. Description générale

Le système Cloudcard+ est une suite de produits logiciels s'appuyant sur des modules matériels de sécurité (HSM) sécurisant :

- La création, l'utilisation et la gestion de moyens d'authentification, ainsi que de clés de création de signature (SCD, clé privée) ;
- Les interactions homme-machine avec le porteur de cette clé, comprenant l'affichage du contexte d'utilisation, le manifestement de son consentement et la saisie de ses moyens d'authentification PIN ou biométrique.

La partie signature des fonctions proposées s'apparente à un Secure Signature Creation Device (SSCD typiquement une carte à puce) dématérialisé dans le nuage, combiné avec un lecteur comprenant un écran et clavier et/ou capteur biométrique (POI). Cette combinaison est illustrée ci-dessous.

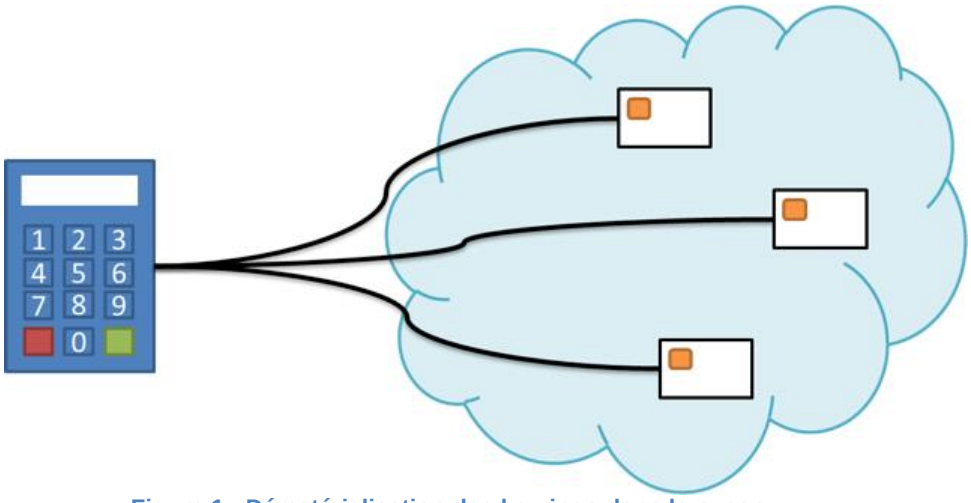

Figure 1 - Dématérialisation des keyrings dans le nuage

Les clés privées de signature sont notamment sécurisées par le système de sorte que le porteur en garde le contrôle exclusif.

Le système permet aussi de réaliser une authentification sans mise en œuvre de clé affectée à l'utilisateur dans le nuage.

Les composants réalisant l'interface homme-machine sont mis en œuvre sous la forme du SDK Cloudcard+ intégré dans une application cliente, installée sur le terminal du porteur (un équipement mobile personnel de type *Smartphone*).

L'enregistrement d'un keyring sur Cloudcard+ passe par un procédé d'activation. Au cours de ce processus, l'utilisateur enregistre le code d'authentification PIN qu'il utilise et/ou ses données biométriques de référence, visage ou empreinte digitale. Si la fonction de signature est activée, après saisie du code PIN, le processus produit au niveau du serveur une preuve de possession (POP) du SCD par le porteur, vérifiable par l'autorité de certification lors de l'émission du certificat d'identité associé à ce SCD

3.1.1. Keyring

Un keyring représente un container sécurisé de secret qui reste sous le contrôle exclusif de l'utilisateur. Il peut contenir divers types de secrets, en pratique, ce sera soit une clé privée (secret) et un certificat associant une identité à cette clé pour signer, soit un secret permettant uniquement l'authentification. Un identifiant unique est de plus associé à un keyring.

Le porteur d'un keyring peut consentir à l'utilisation de son secret dans un contexte spécifique en saisissant son code PIN ou ses données biométriques (visage, empreinte digitale) sur un terminal Cloudcard+ enrôlé (cf. ci-après).

3.1.2. Terminal

Un terminal Cloudcard+ représente une application cliente intégrant le SDK Cloudcard+ de Safran I&S.

Ces terminaux ont la capacité d'activer des keyrings Cloudcard+ ainsi que de proposer leur utilisation à leur porteur.

3.2. Acteurs du système

Les acteurs, personnes ou machines, qui interagissent avec le système Cloudcard+ sont les suivants :

3.2.1. Porteur

Les porteurs sont les propriétaires des clés de création de signature ou d'authentification gérées et protégées par le système.

Ils disposent d'un contrôle exclusif des moyens cryptographiques contenus dans les keyrings qu'ils possèdent. Le porteur interagit avec le système par l'intermédiaire du SDK intégré à l'application installée sur son terminal.

3.2.2. Terminal

Le terminal permet l'accès aux keyrings du porteur pour lui permettre de s'authentifier ou de signer. L'application cliente intégrant le SDK du système est installée sur le terminal et le SDK gère les interactions homme-machine avec le système.

3.2.3. Cloudcard+ Server

Le Cloudcard+ Server est la partie serveur du système Cloudcard+ :

- Il gère la liste des requêtes en attente à destination du porteur, à partir des requêtes de signature ou d'authentification provenant des fournisseurs de service ;
- Il gère les notifications envers le SDK Cloudcard+ ;
- Il gère les demandes d'approbation ou de rejet de requête ;
- Il gère l'enregistrement des keyrings, y compris la génération d'un certificat auprès de l'autorité de certification, ainsi que leur suppression ;
- Il gère les demandes d'itinérance, aussi bien du côté source que destination ;

- Il applique pour le système et chaque keyring la politique de sécurité définie par l'officier de sécurité.

3.2.4. Fournisseurs de services (Service Provider, SP)

Un fournisseur de service est un service externe (hors périmètre de l'évaluation) qui s'appuie sur le système Cloudcard+ pour engager avec le porteur des opérations d'authentification et de transaction électronique à partir de son terminal.

Ces fournisseurs de service regroupent les SCA (Signature Creation Application), les services en ligne ou administration susceptibles de demander une authentification.

La partie serveur du système Cloudcard+ comporte un canal d'accès à disposition des SP pour initier les demandes de création de signature ou d'authentification, réalisée par la suite sous le contrôle exclusif du porteur. Ce canal d'accès est évalué pour vérifier qu'il identifie et réserve l'accès aux SP et protège l'intégrité et la sécurité des données échangées.

3.2.5. Autorité d'enregistrement (AE)

L'autorité d'enregistrement est un service externe (hors périmètre de l'évaluation) qui valide l'identité du porteur avant de transmettre la demande de certificat à l'AC. La partie serveur du système Cloudcard+ comporte un canal d'accès à disposition de l'AE pour demander la création d'un code d'activation à destination du porteur, moyen nécessaire pour activer le keyring à partir de son terminal. Ce canal d'accès entre dans le périmètre de l'évaluation pour vérifier qu'il identifie et réserve l'accès à l'AE et protège l'intégrité et la sécurité des données échangées.

3.2.6. Officier de sécurité (Policy Maker)

L'officier de sécurité est une personne physique qui définit l'ensemble des paramètres régissant :

- Le cycle de vie, le fonctionnement et la personnalisation des keyrings émis par le système. Cet ensemble se matérialise par une politique d'émission.
- Le contrôle des accès aux interfaces du système par les applications tierces. Cet ensemble se matérialise par une politique d'autorisation.

3.2.7. Autorité de certification (AC)

L'autorité de certification est un composant PKI standard (hors périmètre de l'évaluation) qui délivre les certificats X.509 à partir des informations transmises par l'AE et par le système sous le contrôle du porteur. Les paramètres permettant au système de communiquer avec l'autorité se trouvent dans la politique d'émission.

3.3. Architecture du système

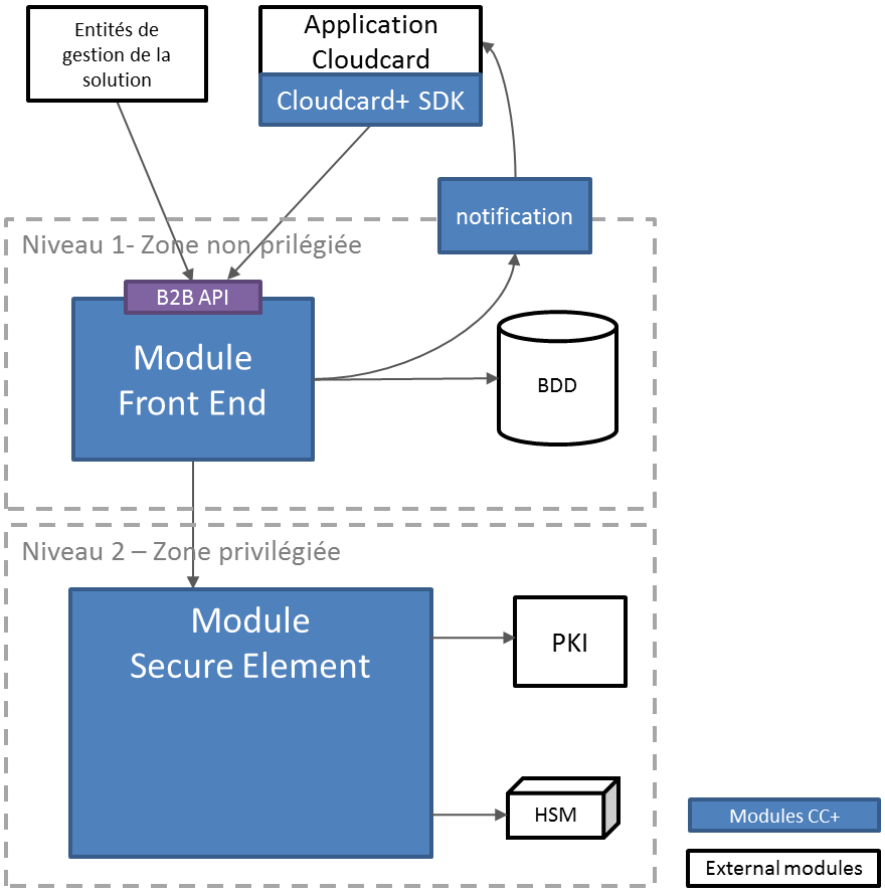

Figure 2 - Architecture du système

3.3.1. Application cliente

Le composant application cliente est installé sur les terminaux personnels des porteurs des keyrings.

La version de l'application utilisée pour l'évaluation CSPN, ainsi que ses mises à jour, sont signées électroniquement par Safran I&S (à travers les mécanismes d'intégrité intégrés aux magasins d'application) avant d'être publiées et accessibles aux porteurs, garantissant ainsi l'authenticité de l'application.

Cette application est distribuée au travers des marchés d'applications tels que l'App Store d'Apple, le Google Play ou le Windows Store.

3.3.2. SDK Cloudcard+

Le SDK Cloudcard+ est la bibliothèque rassemblant l'ensemble des mécanismes de sécurité et des interactions de sécurité avec l'utilisateur, intégrée dans l'application cliente, et qui peut ainsi être réutilisée dans d'autre applications réalisant des traitements métiers spécifiques, apportant ainsi à ces applications l'ensemble des mécanismes évalués.

En sus, il comporte des mécanismes de protection, à base de technique d'obfuscation de code ainsi que de détection de modification du système pour autoriser l'accès aux droits administrateurs, destinés à renforcer sa sécurité et rendre plus difficile les attaques contre ses éléments sensibles.

3.3.3.Niveau 1 – Zone non privilégiée

Le niveau 1 comprend les modules de communication entre le système et les acteurs extérieurs. Une attaque contre les éléments de cette zone non-privilégiée ne doit pas permettre de compromettre la sécurité du système (génération de fausses signatures ou fausses authentifications).

Le SDK Cloudcard+ interagit avec le module Usage de ce composant lors de ses appels serveurs, et avec le module Notification à travers les envois de notification.

➢ Module Usage

Le module Usage gère les interfaces à destination des applications clientes. Il est en charge des fonctions suivantes :

- **Gestion des sessions** : Ce module réceptionne les requêtes des porteurs, récupère les informations correspondantes dans la base d'archive et maintient les sessions ouvertes avec les porteurs pendant la durée de vie du contexte applicatif. Les contextes dans les sessions sont à usage unique, créés et vérifiés par le module SE.
- **Orchestration des opérations** : Ce module relaie les opérations sur les keyrings à l'initiative des porteurs vers le module SE. Il coordonne les appels vers les différents sous-modules pour assurer le bon fonctionnement de la séquence d'opérations. Il réalise l'interface entre le module SE et la base de données pour le stockage des informations

➢ Module Lifecycle

Le module Lifecycle gère les interfaces à destination des applications tierces externes au système (SP, AE, AC, Support). En particulier, il est en charge des fonctions suivantes :

- **Fabrication des keyrings** : Ce module fait l'interface entre l'autorité d'enregistrement et réceptionne les demandes de fabrications de keyring avant de les relayer au module SE du système qui assure le contrôle d'accès ainsi que la création effective des données relatives au nouveau keyring. Il réalise l'interface entre le module SE et la base de données pour le stockage des informations.
- **Demande de génération de certificats** : Ce module fait l'interface avec l'autorité de certification afin de relayer les demandes de certificats émises par le module SE et d'assurer la réception du certificat X.509 dans le cadre de la fonction de signature.
- **Support** : Ce module fait l'interface avec les applications en charge de réaliser les fonctions de support sur les keyrings. Il leur fournit un accès sur l'état des keyrings et l'historique des opérations stockées dans la base de données.

➢ Module Notification

Le composant de notification est en charge d'envoyer des notifications aux porteurs pour signaler l'arrivée d'une demande de signature ou d'authentification. La notification ne contient qu'un identifiant de la requête et pas d'information sensible sur celle-ci.

3.3.4.Niveau 2 – Zone privilégiée

Le niveau 2 est en charge des opérations sensibles de la partie serveur du système, en particulier pour la signature, et est déterminant pour sa sécurité et la garantie du contrôle exclusif de l'usage de la clé. Parmi les hypothèses de l'évaluation, on suppose que tous les administrateurs ayant accès à cette zone sont de confiance.

Le SDK Cloudcard+ envoie les informations sensibles directement vers la partie Secure Element de cette zone. Le module Secure Element gère directement la partie signature protégée suivant le cas, soit par les secrets liés au terminal, soit par ceux liés au PIN. Il sert de relais de sécurité pour la liaison vers le serveur de gestion des éléments biométriques.

Le niveau 2 comprend aussi le module de connexion à l'autorité de certificat pour la génération de certificat.

➢ Module Secure Element

Le module Secure Element est en charge des opérations suivantes :

- **Authentification** : Le module SE est en charge de la gestion effective des authentifications et de la création des contextes d'authentifications qui sont conservés pendant leur durée de vie par le module Usage situé dans la zone non privilégiée. Ces contextes sont revalidés avant d'effectuer le traitement des services offerts aux porteurs des keyrings.
- **Fabrication des keyrings** : Le module SE fabrique les keyrings Cloucard+.
- **Activation des keyrings** : Le module SE est en charge de l'activation des keyrings. Il génère donc la preuve de possession lorsque l'activation est réussie.
- **Création de signature** : Le module SE valide les données et les étapes relatives à l'utilisation d'un keyring permettant de reconstituer le SCD dans le HSM et procède à la signature.
- **Contrôle d'accès** : Le module SE gère le contrôle d'accès aux services qu'il propose en appliquant un contrôle d'accès conformément aux politiques d'émissions et d'autorisation des keyrings concernés.
- **Sécurisation des informations de biométrie**: Le module SE s'occupe du chiffrement et contrôle d'intégrité des données de biométrie capturées, qu'il transmet ensuite au module qui gère leur traitement.

➢ Stockage d'informations

Le module SE fait appel aux modules Usage et Lifecycle pour stocker en base de données les informations persistantes qu'il gère.

3.4. Cycle de vie des keyrings

Le schéma suivant illustre le cycle de vie des keyrings mis en œuvre par le système Cloudcard+.

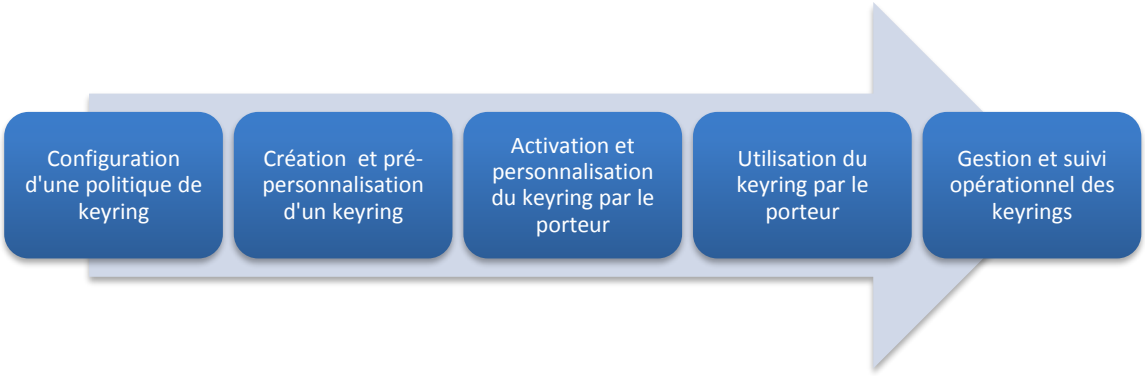

Figure 3 - Cycle de vie des keyrings

1. **Configuration d'une politique de keyring**

   L'officier de sécurité procède à la création de la politique qui régira tous les keyrings émis par son biais.

2. **Création et pré-personnalisation d'un keyring**

   L'autorité d'enregistrement demande la création d'un keyring à destination d'un porteur. Ce keyring est pré-personnalisé avec l'identité du porteur.

   L'autorité d'enregistrement transmet au porteur le ou les facteurs d'activation lui permettant d'utiliser l'application cliente et le SDK Cloudcard+ pour activer son keyring sur son terminal.

   L'autorité d'enregistrement transmet à la partie serveur du système Cloudcard+ une preuve de remise garantissant le lien entre l'identité du porteur et les facteurs d'activations qui lui permettra de valider les informations reçues depuis le SDK Cloudcard+.

3. **Activation et personnalisation du keyring par le porteur**

   Le porteur active son keyring en présentant au SDK Cloudcard+ les facteurs d'activation lui ayant été remis par l'autorité d'enregistrement. Il personnalise le keyring avec son PIN et/ou ses données biométriques tels qu'une image de de son visage ou de ses empreintes digitales.

   Si le keyring est utilisable pour la signature, le couple SCD/SVD est alors généré côté serveur. Avant d'être sécurisé et archivé, le SCD est utilisé pour signer une demande de certificat qui est transmise à l'autorité de certification. Un certificat est alors émis par le CGA.

4. **Utilisation du keyring par le porteur**

   Le keyring est prêt à être utilisé, d'une part en authentification dès lors qu'il est activé et d'autre part en signature dès lors que l'autorité de certification a émis le certificat X.509.

   Le porteur est donc en mesure de se connecter à un fournisseur de service tiers supportant le moyen de signature Cloudcard+ et de réaliser des opérations de signature.

   Il est également en mesure d'être authentifié sur un service en ligne supportant le moyen d'authentification Cloudcard+.

5. **Gestion et suivi opérationnel des keyrings**

   Le porteur, seul ou de manière conjointe avec le personnel de support, est également capable de gérer son keyring. L'étendue des fonctions de gestion (itinérance, désassociation, destruction) est déterminée par la politique associée au keyring.

3.5. Cinématiques et conditions

3.5.1. Création d'un keyring vierge et pré-personnalisation d'un keyring

L'autorité d'enregistrement dispose d'une interface pour demander la fabrication d'un keyring vierge ainsi que sa pré-personnalisation.

La fabrication résulte en un package d'activation signé par le système contenant :

- Un identifiant unique de keyring ;
- Un premier facteur d'activation du keyring sous la forme d'un code d'activation ;
- Un second facteur d'activation optionnel à transmettre au porteur par un deuxième canal, par exemple OTP SMS ;

- Les données techniques représentant le keyring en lui-même.

À ce stade, le keyring n'est pas actif dans le système et reste complètement anonyme.

La pré-personnalisation est la phase où l'autorité d'enregistrement s'engage sur la validation initialement de l'identité du porteur, pour autoriser sa mise en production. Cette identité sera utilisée pour émettre le certificat correspondant au SCD que le keyring protège.

Elle permet d'attester que :

Le porteur en possession des facteurs d'activation F a l'identité I

La pré-personnalisation lie les données suivantes :

- La politique d'émission de keyring ;
- L'identifiant de l'utilisateur propriétaire du keyring ;
- Les facteurs d'activation.

Après la pré-personnalisation, le système met en production le keyring sur le système, celui-ci est prêt à être activé par son porteur.

L'autorité d'enregistrement peut alors transmettre les facteurs d'activation du keyring au porteur par des canaux différenciés de son choix (face à face, voie postale ou électronique).

3.5.2. Activation des keyrings

Le porteur se procure l'application cliente Cloudcard+ App qu'il installe sur son terminal et démarre le processus d'activation de son keyring.

L'activation commence par l'authentification mutuelle entre le porteur qui présente le code d'activation et Cloudcard+ SE à l'aide des secrets d'enregistrement reçus par le porteur.

Une fois l'authentification des deux parties établie, le porteur visualise l'état d'activation du keyring, ainsi que l'identité pré-personnalisée qui sera utilisée par la CGA pour émettre son certificat et confirme que le keyring n'a pas déjà été activé.

Le porteur accepte l'activation de son keyring et l'émission de son certificat en saisissant un code PIN qu'il doit conserver secret. Il peut également enregistrer des facteurs biométriques pour l'usage d'authentification. La longueur du code PIN est paramétrable par le Policy Maker lors de la création de la politique de confiance. Un minimum de 4 chiffres et de 6 chiffres sont néanmoins requis pour les politiques d'authentification et de signature respectivement, tel que défini dans **[RGS-B3]**.

L'activation se termine par la transmission des éléments qui garantiront l'authentification future du porteur, de son terminal ainsi que les éléments qui garantiront le contrôle exclusif du porteur sur le SCD.

Pour les keyring où la fonctionnalité de signature est activée par la politique de confiance, le système procède alors à la génération d'un couple SCD/SVD unique dans le module de sécurité, puis utilise l'identité pré-personnalisée du porteur pour générer une demande de certificat (CSR). Le SCD est utilisé une fois pour signer la demande de certificat avant d'être sécurisé pour garantir le contrôle exclusif du porteur sur les utilisations futures.

Les éléments sensibles qui permettront l'authentification de l'utilisateur, de son terminal, le SCD lui-même lorsqu'il est présent et le certificat sont archivés dans la base de données.

L'autorité de certification procède à l'émission du certificat à partir des informations reçues de la partie serveur.

3.5.3. Utilisation des keyrings

Le système dispose d'une interface permettant à des fournisseurs de services tiers de demander la création d'une signature ou une authentification pour un keyring spécifié.

Cette demande peut intervenir à l'initiative du porteur interagissant avec l'application tierce depuis son terminal (à partir duquel il a activé son keyring) ou depuis un autre terminal. Elle peut également être émise par un tiers sans initiative du porteur.

Le porteur est notifié de la demande sur son terminal à travers le SDK Cloudcard+ et peut donner son consentement à l'utilisation du SCD ou rejeter la demande. Il autorise la signature en saisissant le code PIN de son keyring ce qui débloque de manière transitoire son SCD au sein du SE. Il autorise l'authentification en utilisant suivant le cas soit son code PIN, soit une capture biométrique correspondante à sa donnée biométrique de référence.

3.5.4. Itinérance des keyrings

Le système dispose d'une interface permettant au porteur de transférer les droits d'accès à une Cloudcard+ vers un autre terminal disposant de l'application cliente.

Lors de l'utilisation de cette fonction et après entrée du PIN utilisateur, le terminal source affiche un code 2D à usage unique qui doit être scanné depuis le terminal destination.

Ensuite le code PIN de l'utilisateur doit être entré sur le terminal destination pour activer le keyring.

Si le keyring est utilisé uniquement pour l'authentification avec des facteurs biométriques, ceux-ci peuvent alors aussi être utilisés en remplacement du code PIN pour transférer les droits d'accès.

3.6. Flux de communication

3.6.1.Flux de données avec le Secure Element

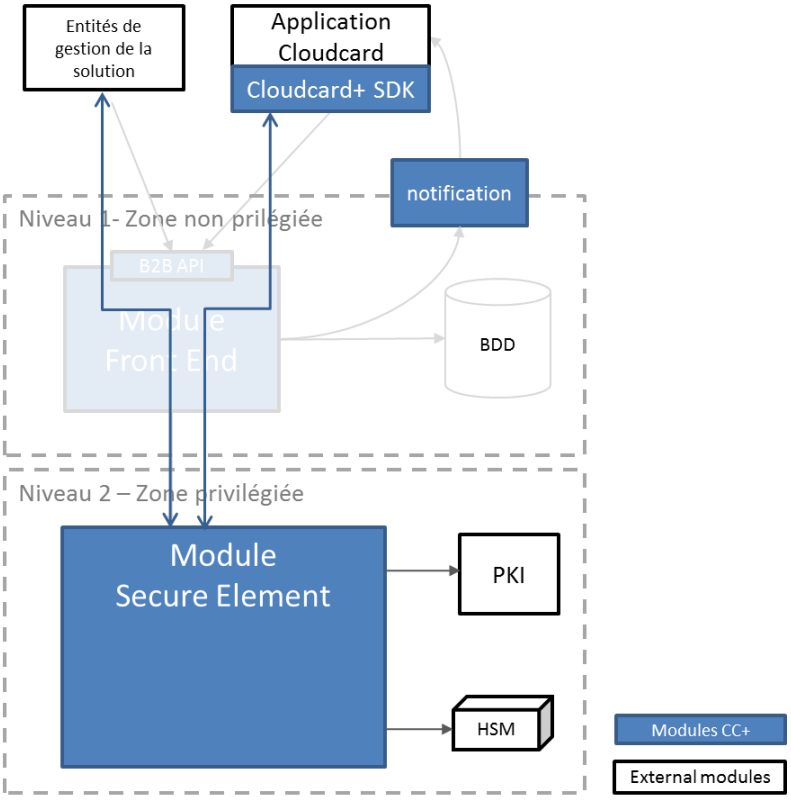

Figure 4 - Flux de communication

Les messages des flux de communication de l'application transitent à travers les modules de la zone non-privilégiée de Cloudcard+ Server.

Les messages échangés avec le module Secure Element sont sécurisés de bout-en-bout depuis les acteurs interagissant avec le système, ainsi que depuis le module Cloudcard+ SDK.

- **Cloudcard+ SDK**

Le SDK Cloudcard+ communique avec le module Secure Element par l'intermédiaire du module Usage du Cloudcard+ Server. Toutes les données sensibles transmises entre Cloudcard+ SDK et Cloudcard+ SE sont protégées en authenticité et confidentialité. Ce flux est représenté sur la Figure 4 en bleu.

Les données qui transitent à travers ces interfaces sont protégées en authenticité et confidentialité au niveau des messages échangés et de manière indépendante de la sécurité au niveau du protocole de transport. De ce fait, la confidentialité de transmission est assurée de bout-en-bout sans rupture.

Le transport des messages entre chaque module est de plus protégé en TLS avec authentification cliente afin d'éviter des attaques par déni de service.

3.6.2.Flux de données biométriques

Cas d'utilisation de la biométrie faciale (visage) :

Lors du processus d'enregistrement, le composant gérant la biométrie dans le module Secure Element authentifie le SDK Cloudcard+ et crée une clé de session qui va être utilisée pour sécuriser les échanges. Les données biométriques capturées par Cloudcard+ SDK sont transmises chiffrées au module Secure Element.. Le gabarit chiffré est envoyé de nouveau à Cloudcard+ SDK pour être stocké localement.

Lors des authentifications suivantes, après l'authentification du terminal, une clé de session est de nouveau créée et utilisée pour échanger les nouvelles données biométriques capturées de manière chiffrée. Le gabarit chiffré est envoyé en même temps que ces nouvelles données biométriques.

Cas d'utilisation des empreintes :

Lorsque le produit est configuré pour une authentification par empreinte digitale, le dispositif de reconnaissance d'empreinte intégré à l'équipement personnel est utilisé et aucune donnée biométrique d'empreinte ne remonte au serveur Cloudcard+.

3.7. Utilisation du produit

3.7.1. Utilisateurs

Une fois installé, le système Cloudcard+ interagit avec différents utilisateurs :

- **Le porteur** : il s'agit de l'utilisateur de l'application cliente qui va traiter l'enregistrement des keyrings, leur suppression, les demandes de signature et d'authentification en attente,
- **Fournisseurs de services (Service Provider, SP)** : Ils initient les demandes de création de signature ou d'authentification, réalisée par le système.
- **L'agent d'enregistrement** : L'agent d'enregistrement interagit avec le système en tant qu'autorité d'enregistrement pour demander la génération d'un keyring au nom du porteur, et obtenir ses codes d'activation.
- **L'officier de sécurité** : L'officier de sécurité interagit avec le système pour la définition des politiques de sécurité associées aux keyring.
- **L'administrateur privilégié :** L'administrateur privilégié interagit avec les parties sensibles du système pour garantir que le système fonctionne correctement, sans avoir de rôle utilisateur. Il est considéré comme de confiance et n'est donc pas considéré comme une menace pour le système.
- **L'administrateur non-privilégié :** L'administrateur non-privilégié interagit avec les parties non-sensibles du système pour garantir que le système fonctionne correctement. Il a notamment accès à la base de données dans laquelle est stockée l'ensemble des données du système. L'administrateur non-privilégié n'est pas supposé de confiance et donc la corruption du celui-ci est considérée comme un vecteur d'attaque.

3.7.2. Scénarios d'utilisation

Dans le cadre de l'évaluation CSPN, les politiques de keyring sont configurées de manière à permettre les deux utilisations suivantes :

- Utilisation du keyring pour permettre un usage d'authentification basé sur l'entrée et vérification du PIN. Ensuite capture et transmission sécurisée d'une donnée biométrique faciale (visage) du porteur ;
- Utilisation du keyring pour permettre un usage d'authentification et de signature activé par l'entrée du PIN par le porteur.

Tout autre usage de l'application et du SDK n'est pas compris dans le périmètre de test et d'évaluation du CSPN.

En particulier, l'authentification basée sur la reconnaissance biométrique, et donc l'évaluation de la fiabilité de sa fonction de capture et de sa fonction de comparaison, est hors périmètre de l'évaluation, le périmètre se limitant à la sécurisation de la gestion des données biométriques afin de garantir leur protection en tant que données personnelles.

3.7.3. Environnement d'évaluation

Le produit Cloudcard+ est compatible avec Android version 4.1 et supérieur, et iOS version 8.1 et supérieur.

Il est évalué sur la configuration suivante à jour avec les correctifs de sécurité :

- Environnement Mobile :
  - Android 5.1.1
  - iOS 9
- Environnement Serveur :
  - CentOS 6.9/Tomcat 7.0.81
  - Oracle 12c (12.1.0.2 avec critical patch update de Juillet 2017)

Comme indiqué dans l'architecture, le composant autorité de certification est présent à l'intérieur de la zone privilégiée, mais n'est pas dans le périmètre de l'évaluation.

Le produit doit être intégré et utilisé conformément aux recommandations sécuritaires de configuration de la politique de sécurité ainsi que celles d'intégration du SDK [SEC_GUIDE] et de déploiement du serveur [SERVER].

3.7.4. Hypothèses d'évaluation

Les hypothèses suivantes sont retenues pour l'évaluation du produit :

- Le porteur est de confiance :
  - Il s'assure que le système d'exploitation de son équipement personnel est à jour avec les derniers correctifs de sécurité ;
  - Il n'installe pas de programme malveillant sur son équipement mobile ou destiné à débloquer l'utilisation administrateur de l'équipement (jailbreak/root) ;
  - Il préserve le secret de son PIN le cas échéant, et ne le rentre pas dans des conditions où celui-ci est directement observable d'un utilisateur extérieur ;
  - Il ne collabore pas avec un attaquant externe en lui fournissant des données biométriques dynamiques.
- L'application cliente suit les recommandations d'utilisation du SDK Cloudcard+ afin de ne pas compromettre sa sécurité.
- Les fournisseurs de service sont de confiance et envoient des requêtes d'authentification ou de signature légitimes.
- L'agent d'enregistrement est de confiance et demande l'enregistrement d'utilisateurs dont l'identité a été dument vérifiée. Il utilise des canaux séparés pour transmettre chacun des facteurs d'activation au porteur.

- L'administrateur privilégié est de confiance, ainsi aucune attaque n'est possible depuis l'intérieur de la zone privilégiée. Il configure correctement les politiques de sécurité des keyring conformément aux usages retenus pour l'évaluation.

3.8. Biens à protéger

3.8.1. Éléments d'authentification de l'utilisateur

B1. Le bien comprend le PIN de l'utilisateur au moment où celui-ci est entré, et les valeurs dérivées du PIN permettant la vérification de sa possession par le serveur. Le terminal protège la valeur du PIN depuis son entrée jusqu'au moment où elle est utilisée, le serveur protège les éléments de vérification du PIN.

Protection en intégrité et en confidentialité sur le terminal et le serveur.

3.8.2. Éléments biométriques de l'utilisateur

B2. Le bien comprend les données biométriques (visage) de l'utilisateur enregistrées ou fraichement capturées.

Protection en intégrité et en confidentialité sur le terminal et sur le serveur.

3.8.3. Facteurs d'activation

B3. Le bien comprend les facteurs d'activation qui permettent au porteur d'activer le keyring.

Protection en intégrité sur le terminal et sur le serveur

3.8.4. Clé d'authentification de terminal

B4. Le bien comprend les clés d'authentification de terminal qui l'identifient auprès du système serveur.

Protection en intégrité et en confidentialité sur le terminal.

3.8.5. Clés de signature personnelle

B5. Pour la fonction de signature, le bien comprend les clés de signature de l'utilisateur, mais aussi la protection de leur accès, de façon à garantir le contrôle exclusif de l'utilisateur sur ses clés.

Protection en intégrité et en confidentialité sur le serveur, et protection et authentification de l'accès pour qu'il soit possible uniquement depuis le terminal.

3.8.6. Clé de déblocage du SCD

B6. Le bien comprend la clé de blocage du SCD qui est dérivée d'éléments secrets. Cette clé est transférée de manière protégée entre le client et le serveur.

Protection en intégrité et en confidentialité sur le terminal et sur le serveur.

3.8.7. Requête de signature/authentification et preuves de transaction

B7. Le bien comprend les demandes de signature et d'authentification, et les preuves de transaction une fois les opérations effectuées. Il inclut aussi le message descriptif de la demande.

Protection en intégrité sur le serveur.

Protection en intégrité et en confidentialité lors des échanges réseaux vers l'extérieur du produit.

3.8.8. Politique de sécurité

B8. Le bien comprend les politiques de sécurité qui ne peuvent être modifiées que par l'officier de sécurité.

Protection en intégrité sur le serveur.

Protection en intégrité et en confidentialité lors des échanges réseaux vers l'extérieur du produit.

3.8.9. Eléments de configuration et d'état des keyring

B9. Le bien comprend les éléments sensibles de configuration et d'état de keyring stockés dans la base de données ainsi que les liens entre les éléments stockés.

Protection en intégrité sur le serveur des éléments sensibles.

3.9. Menaces considérées

3.9.1. Attaques à distance

3.9.1.1. Vol d'un facteur d'activation

L'attaquant vole l'un des facteurs d'activations avant que ceux-ci soient utilisés par le porteur légitime pour activer sa carte. Cette attaque peut intervenir lors de la génération des facteurs par le système, de leur transmission du système vers l'AE, de l'AE vers le porteur et finalement de l'application cliente vers le système.

Bien : B3, attaquant malveillant externe

3.9.1.2. Attaque par force brute sur la clé d'authentification du terminal

L'attaquant connait des éléments externes, comme l'identifiant du terminal, le type de terminal utilisé, la date de l'enregistrement et effectue une attaque par force brute pour tenter de deviner la clé d'authentification associée

Bien : B4, attaquant malveillant externe

3.9.1.3. Attaque par force brute sur le PIN d'une carte

L'attaquant connait l'identifiant de la carte et effectue une attaque par force brute pour tenter de deviner le PIN associé.

Biens : B1, B5 (accès illégitime), attaquant malveillant externe

3.9.1.4. Vol du PIN lors de la frappe

L'attaquant observe à distance l'utilisateur au moment où celui-ci entre le PIN.

Biens : B1, B5 (accès illégitime), attaquant malveillant externe

3.9.1.5. Attaque par déni de service sur le PIN

L'attaquant connait l'identifiant du keyring et effectue une attaque par déni de service sur le PIN pour bloquer l'accès au SCD par le porteur légitime.

Bien : B5 (déni de service), attaquant malveillant externe

3.9.1.6. Demandes de signature trompeuses

Un fournisseur de service tente de présenter au porteur des requêtes dont la description ne sera pas affichée d'une manière lui permettant d'en prendre connaissance utilement, sans que ce soit immédiatement visible lors d'une revue postérieure du contenu de la description.

Bien : B7, erreur du fournisseur de service

3.9.2. Attaques sur le terminal

3.9.2.1. Fausse itinérance

Un attaquant ayant obtenu l'accès au terminal déclenche l'itinérance d'un keyring vers un autre terminal.

Bien : B5, attaquant malveillant avec accès au terminal

3.9.2.2. Détournement de l'itinérance de keyring

Un attaquant capture le code 2D d'itinérance et l'utilise pour activer le keyring à la place de l'utilisateur.

Bien : B5, attaquant malveillant avec accès au terminal

3.9.2.3. Tentative de signature

L'attaquant tente d'effectuer une signature depuis le terminal sans connaître le PIN, avec ou sans connaissance de la clé d'authentification du terminal.

Bien : B5, attaquant malveillant avec accès au terminal

3.9.2.4. Tentative de signature avec vol de la clé du terminal

L'attaquant effectue une attaque par force brute sur le serveur pour tenter de deviner le code PIN du porteur correspondant au terminal en sa possession. Cette attaque suppose que l'attaquant est parvenu à voler la clé de terminal d'un terminal légitime

Biens : B1, B5, attaquant malveillant avec accès au terminal

3.9.2.5. Divulgation des éléments sensibles du terminal

L'attaquant tente de voler les éléments sensibles du terminal dans l'espace mémoire à partir du terminal sans avoir d'accès administrateur.

Biens : B1, B2, B3, B4, B6 attaquant malveillant avec accès au terminal

3.9.3. Attaques Man-In-The-Middle

3.9.3.1. Capture et rejeu de trames réseau

L'attaquant écoute, capture les trames réseaux d'une transaction légitime et tente de rejouer celle-ci afin d'abuser le système.

Biens : B1, B2, B3, B4, B5 (accès illégitime ou bien déni de service), B6, attaquant malveillant externe avec accès actif au réseau

3.9.3.2. Capture et modification des trames réseau

L'attaquant écoute, capture et rejoue des trames réseaux légitimes après les avoir modifiées. L'objectif de cette attaque est de profiter d'une transaction légitime pour abuser du système.

Biens : B1, B2, B3, B4, B5 (accès illégitime ou bien déni de service), B6, attaquant malveillant externe avec accès actif au réseau

3.9.3.3. Usurpation du serveur

L'attaquant redirige les flux du terminal du porteur et tente de se faire passer pour le serveur Cloudcard+ et afin de récupérer les références d'authentification du terminal et du porteur.

Biens : B1, B2, B4, attaquant malveillant externe avec accès actif au réseau

3.9.3.4. Divulgation du PIN, du gabarit biométrique ou de la clé de déblocage de référence par usurpation du serveur

L'attaquant a volé la clé du terminal d'un porteur légitime, utilise celle-ci pour se faire passer pour le serveur Cloudcard+ et tente de récupérer les autres informations confidentielles de l'utilisateur au moment d'une connexion par la suite.

Biens : B1, B2, B6, attaquant malveillant avec accès à la clé de terminal

3.9.4. Attaques depuis la zone non-privilégiée

3.9.4.1. Modification des paramètres de sécurité d'un keyring

L'attaquant modifie les paramètres régissant la sécurité (politique d'émission et d'autorisation) d'un keyring afin d'abaisser son niveau global de sécurité, prévu par l'émetteur de celle-ci.

Bien : B8, attaquant malveillant avec accès à la base de données

3.9.4.2. Création d'un keyring illégitime

L'attaquant tente d'injecter dans le système un keyring illégitime ou modifie les données d'activation d'un keyring légitime dans le but de s'emparer du keyring ciblé

Bien : B9, attaquant malveillant avec accès à la base de données

3.9.4.3. Modification des associations entre données d'authentification et keyring

L'attaquant dispose des accès physiques ou distants pour réaliser des substitutions ou modifications sur les éléments de base de données et tente d'associer les données d'un keyring légitime à un autre keyring.

Bien : B9, attaquant malveillant avec accès à la base de données

3.9.4.4. Modifications des associations entre Terminal et keyring

L'attaquant dispose des accès physiques ou distants pour réaliser des substitutions ou modifications sur les éléments de base de données et tente d'associer un terminal légitime à un keyring légitime pour laquelle le terminal n'a pas été activé.

Bien : B9, attaquant malveillant avec accès à la base de données

3.9.4.5. Hameçonnage du SP

Un attaquant tente de présenter au porteur des requêtes malveillantes de création de signature au nom d'un SP légitime.

Bien : B7, attaquant malveillant avec accès à la base de données

3.9.4.6. Altération du contenu d'une demande de signature

Un attaquant tente d'altérer le contenu d'une demande de signature provenant d'un SP légitime après que le porteur a donné son consentement.

Bien : B7, attaquant malveillant avec accès à la base de données

3.9.4.7. Usurpation d'identité avant activation

L'attaquant tente d'activer le keyring avant le porteur légitime, lui permettant ainsi de prendre le contrôle de celui-ci et de ses droits d'authentification ou de signature associés à l'identité du porteur légitime.

Biens : B3, B9, attaquant malveillant avec accès à la base de données

3.9.5.Attaques sur la clé privée SCD[2]

3.9.5.1. Utilisation de la clé de signature

Un attaquant extrait la clé privée de signature chiffrée de la base de données et tente de l'activer sur le HSM pour réaliser une signature.

Bien : B5, attaquant malveillant avec accès temporaire au HSM

3.9.5.2. Divulgation de la clé de signature

Un attaquant tente d'exporter la clé privée de signature non protégée du système. Cette attaque peut intervenir lors de la génération, du stockage ou de l'utilisation de la clé privée de signature.

Bien : B5, attaquant malveillant avec accès temporaire au HSM ou aux flux vers celui-ci

3.9.5.3. Dérivation de la clé de signature

Un attaquant tente de dériver la clé privée de signature d'informations publiques, de signature légitime ou de toutes informations provenant du système.

Bien : B5, attaquant malveillant avec accès temporaire au HSM ou aux flux depuis celui-ci

[2] L'administrateur de la zone privilégiée est supposé de confiance. Cependant étant donné la sensibilité de la valeur en clair de la clé privée, cette section prend en compte les attaques sur cette valeur qui devraient normalement de ce fait ne pas pouvoir être réalisées ; en particulier pour prendre en compte le risque résiduel qu'un attaquant vole les identifiants d'un administrateur de confiance ou obtienne temporairement un accès physique à la zone privilégiée lui permettant de réaliser des opérations utilisant un accès direct au HSM sans avoir en sa possession les droits d'accès restreint à l'administrateur privilégié.

4. FONCTIONS DE SECURITE

4.1. Communication TLS avec le serveur Cloudcard+

Cloudcard+ SDK et le serveur Cloudcard+ communiquent ensemble à travers un canal sécurisé TLS avec authentification du serveur.

4.2. Canaux d'authentification mutuelle entre le terminal et le serveur

Cloudcard+ SDK et le module SE du serveur Cloudcard+ disposent de canaux d'authentification mutuelle pour échanger les données de manière sécurisée.

4.3. Clavier virtuel d'entrée du PIN

Cloudcard+ SDK utilise un clavier virtuel pour l'entrée du PIN, dont l'emplacement des touches correspondant à chaque chiffre est modifié à chaque utilisation.

4.4. Affichage description requête

Cloudcard+ SDK affiche le texte de description de la requête de manière complète et lisible pour l'utilisateur.

4.5. Blocage client d'entrée du facteur d'authentification

Cloudcard+ SDK bloque l'utilisation du keyring après 3 échecs de vérification du PIN auprès du serveur.

4.6. Protection des données biométriques faciales

Cloudcard+ protège les données biométriques de l'utilisateur (visage) contre toute divulgation.

4.7. Protection de l'enregistrement et activation d'un keyring

Cloudcard+ Server s'assure que les demandes de création et de pré-personnalisation d'un keyring proviennent uniquement de l'autorité d'enregistrement, que la demande d'activation provient du porteur muni de l'ensemble des facteurs d'activation, et que la génération du certificat si une clé de signature est configurée est réalisée avec l'identité indiquée lors de la création du keyring et pour la clé activée par le porteur légitime.

4.8. Protection des politiques de sécurité

Cloudcard+ Server s'assure que les demandes de modification d'une politique de sécurité proviennent uniquement d'un officier de sécurité.

4.9. Protection de l'itinérance

Cloudcard+ SDK demande l'entrée du PIN utilisateur pour autoriser l'itinérance de Cloudcard sur le terminal source. **Cloudcard+ SDK** demande l'entrée du PIN de la Cloudcard en plus du code 2D d'itinérance pour autoriser l'itinérance sur le terminal destination.

4.10. Identification du terminal

Cloudcard+ SDK identifie le terminal de manière unique à travers les données de son environnement d'exécution et l'utilisation de l'application est bloquée si l'image de cet environnement n'est plus conforme à celui dans lequel l'application a été initialisée.

4.11. Protection de la base de données

Cloudcard+ Server protège avec une clé de chiffrement en confidentialité et en intégrité les données sensibles stockées en base de données.

4.12. Authentification des acteurs

Cloudcard+ Server authentifie par certificat l'ensemble des acteurs interagissant avec lui.

4.13. Protection des SCD

Cloudcard+ SE protège les SCD utilisés pour la création de signatures personnelles.

4.14. Preuve de transaction

Cloudcard+ Server génère une preuve de transaction de chaque signature effectuée afin de fournir les éléments de preuve de la transaction.

5. SYNTHESE COUVERTURE DES MENACES

	4.1 Communication TLS avec le serveur Cloudcard+	4.2 Canaux d'authentification mutuelle entre le terminal et le serveur	4.3 Clavier virtuel d'entrée du PIN	4.4 Affichage description requête	4.5 Blocage client d'entrée du facteur d'authentification	4.6 Protection des données biométriques faciales	4.7. Protection de l'enregistrement et activation d'un keyring	4.8. Protection des politiques de sécurité	4.9 Protection de l'itinérance	4.10 Identification du terminal	4.11 Protection de la base de données	4.12 Authentification des acteurs	4.13 Protection des SCD	4.14 Preuve de transaction	Environnement	Résistance cryptographique
3.9.1.1 Vol d'un facteur d'activation	X											X			X	
3.9.1.2 Attaque par force brute sur la clé d'authentification du terminal		X														X
3.9.1.3 Attaque par force brute sur le PIN d'une carte		X			X											
3.9.1.4 Vol du PIN lors de la frappe			X													
3.9.1.5 Attaque par déni de service sur le PIN		X														
3.9.1.6. Demandes de signature trompeuses				X								X		X		
3.9.2.1 Fausse itinérance									X							
3.9.2.2 Détournement de l'itinérance de keyring									X							
3.9.2.3 Tentative de signature		X														
3.9.2.4 Tentative de signature avec vol de la clé du terminal		X			X					X						
3.9.2.5 Divulgation des éléments sensibles du terminal						X				X					X	X
3.9.3.1 Capture et rejeu de trames réseau	X															
3.9.3.2 Capture et modification des trames réseau	X															
3.9.3.3 Usurpation du serveur	X															

	4.1 Communication TLS avec le serveur Cloudcard+	4.2 Canaux d'authentification mutuelle entre le terminal et le serveur	4.3 Clavier virtuel d'entrée du PIN	4.4 Affichage description requête	4.5 Blocage client d'entrée du facteur d'authentification	4.6 Protection des données biométriques faciales	4.7. Protection de l'enregistrement et activation d'un keyring	4.8. Protection des politiques de sécurité	4.9 Protection de l'itinérance	4.10 Identification du terminal	4.11 Protection de la base de données	4.12 Authentification des acteurs	4.13 Protection des SCD	4.14 Preuve de transaction	Environnement	Résistance cryptographique
3.9.3.4. Divulgation du PIN, ou du gabarit biométrique ou de la clé de déblocage de référence par usurpation du serveur	X	X				X										
3.9.4.1 Modification des paramètres de sécurité d'un keyring							X	X			X					
3.9.4.2 Création d'un keyring illégitime							X				X					
3.9.4.3 Modification des associations entre données d'authentification et keyring							X				X					
3.9.4.4 Modifications des associations entre Terminal et keyring							X				X					
3.9.4.5 Hameçonnage du SP												X		X	X	
3.9.4.6 Altération du contenu d'une demande de signature														X	X	
3.9.4.7 Usurpation d'identité avant activation							X							X		
3.9.5.1 Utilisation de la clé de signature													X			
3.9.5.2 Divulgation de la clé de signature													X			
3.9.5.3 Dérivation de la clé de signature																X

Figure 5: correspondance entre menaces et fonctions de sécurité