Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2018/09

Cloudcard+
Version 3.4.14

Paris, le 30 avril 2018

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2018/09**
Nom du produit **Cloudcard+**
Référence/version du produit **Version 3.4.14**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **IDEMIA** **11 Boulevard Gallieni** **92130 Issy-les-Moulineaux** **France**
Développeur **IDEMIA** **11 Boulevard Gallieni** **92130 Issy-les-Moulineaux** **France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B** **78180 Montigny le Bretonneux** **France**
Fonctions de sécurité évaluées **Communication TLS avec le serveur Cloudcard+ ;** **Canaux d'authentification mutuelle entre l'application et le serveur ;** **Clavier virtuel d'entrée du PIN ;** **Affichage des descriptions des requêtes ;** **Blocage d'entrée du facteur d'authentification si le nombre maximum de tentatives est atteint ;** **Protection des données biométriques faciales ;** **Protection de l'enregistrement et activation d'un keyring ;** **Protection des politiques de sécurité ;** **Protection de l'itinérance ;** **Identification du téléphone portable ;** **Protection de la base de données ;** **Authentification des administrateurs du serveur ;** **Protection des Signature Creation Device ;** **Preuve de transaction**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage **Non**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Cloudcard+, version 3.4.14 » développé par *IDEMIA*. Il se compose de deux éléments : Cloudcard+ *Software Development Kit* (SDK, ou kit de développement logiciel) et Cloudcard+ *Server*.

Ce produit a pour but de dématérialiser un objet de type *Secure Signature Creation Device* (SSCD, typiquement une carte à puce) sur le Cloudcard+ *Server* et d'y avoir accès à distance. Par l'intermédiaire d'une application mobile embarquant le Cloudcard+ SDK, l'utilisateur peut accéder depuis son téléphone portable à son SSCD, aussi appelé *keyring*, afin de lui faire signer des transactions.

La figure ci-dessous explicite l'architecture du produit.

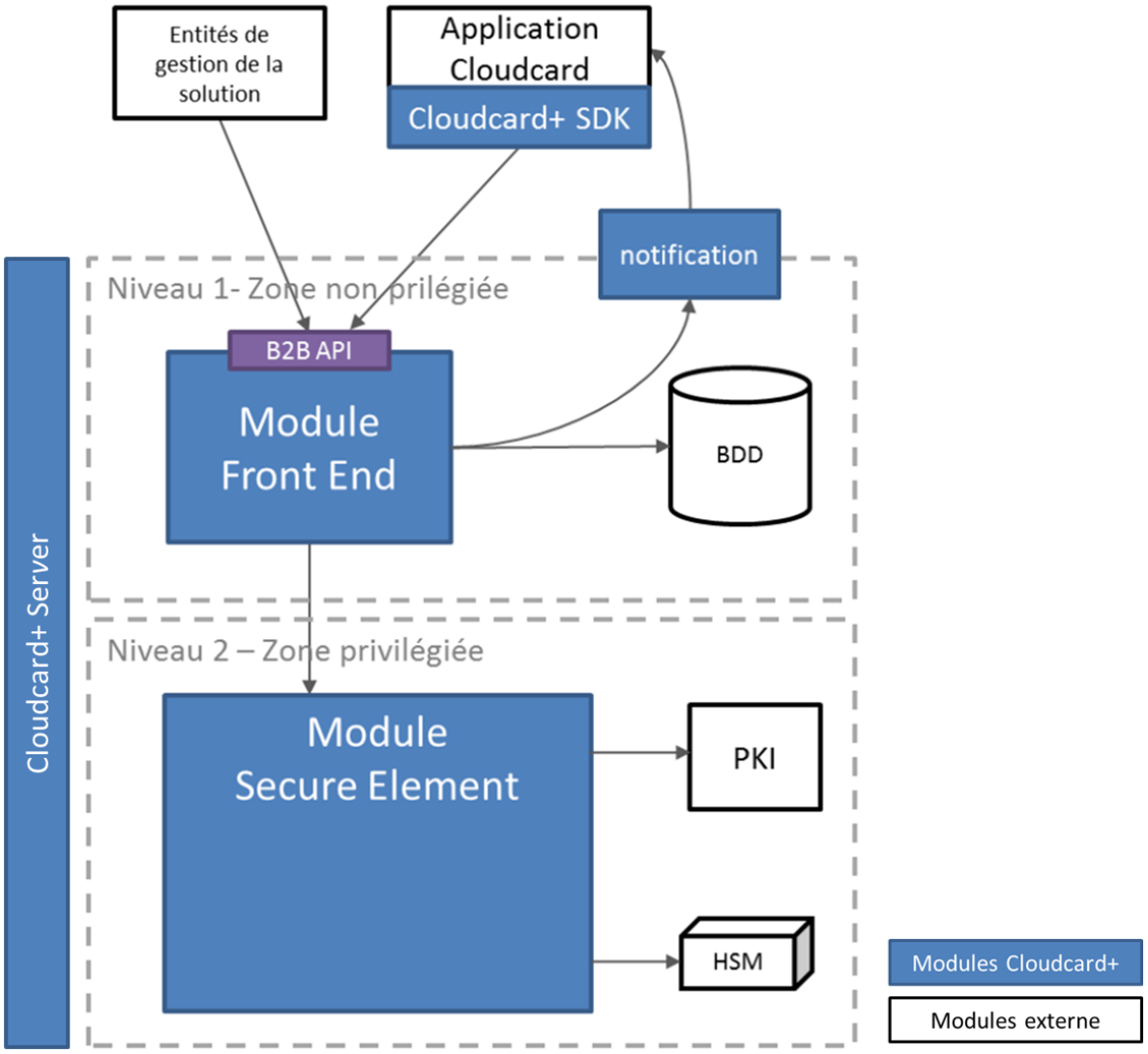

Figure 1 - Architecture produit.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 – détection d'intrusions
☐ 2 – anti-virus, protection contre les codes malicieux
☐ 3 – pare-feu
☐ 4 – effacement de données
☐ 5 – administration et supervision de la sécurité
☒ **6 – identification, authentification et contrôle d'accès**
☐ 7 – communication sécurisée
☐ 8 – messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 – environnement d'exécution sécurisé
☐ 11 – terminal de réception numérique (*Set top box*, STB)
☐ 12 – matériel et logiciel embarqué
☐ 13 – automate programmable industriel
☐ 99 – autre

1.2.2. Identification du produit

Nom du produit	Cloudcard+
Numéro de la version évaluée	3.4.14

La version certifiée du produit peut être identifiée de la manière suivante :

- dans les applications *ANDROID* et *IOS* : l'onglet *Settings* de l'application fait apparaitre la version sous la section *About* ;
- sur le serveur, lors de l'exécution des scripts la version du produit est rappelée.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- communication TLS avec le serveur Cloudcard+ ;
- canaux d'authentification mutuelle entre l'application et le serveur ;
- clavier virtuel d'entrée du PIN ;
- affichage des descriptions des requêtes ;
- blocage d'entrée du facteur d'authentification si le nombre maximum de tentatives est atteint ;
- protection des données biométriques faciales ;
- protection de l'enregistrement et activation d'un keyring ;
- protection des politiques de sécurité ;
- protection de l'itinérance ;
- identification du téléphone portable ;
- protection de la base de données ;
- authentification des administrateurs du serveur ;
- protection des *Signature Creation Device* ;
- preuve de transaction.

1.2.4. Configuration évaluée

Le Cloudcard+ SDK est configuré pour être exécuté par les systèmes d'exploitation mobiles *iOS* et *ANDROID*. Le serveur est configuré pour s'appuyer sur un *Hardware Security Module* (HSM).

La plateforme de test était constituée du Cloudcard+ *Server* sous forme de machines virtuelles prêtes à l'emploi, ainsi que des applications mobiles exécutant Cloudcard+ SDK.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation, aménagée au regard de la spécificité du produit, est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

L'installation a consisté en la création d'un réseau pour faire communiquer les différents sous-ensembles du produit Cloudcard+.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

Aucune non-conformité n'a été relevée.

2.3.1.3. Durée de l'installation

L'installation complète du produit a duré environ deux jours.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit, avec en particulier des guides ([GUIDES]) permettant l'utilisation du produit dans une même configuration que celle évaluée au titre de la CSPN.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source. Il estime que le code est clairement organisé et correctement documenté et que chaque interface est bien commentée.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Aucune recommandation particulière n'est formulée par l'évaluateur. Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté. En particulier, la documentation à destination des développeurs [GUIDES] est complète et d'un bon niveau technique.

2.3.8.4. Notes et remarques diverses

L'évaluateur a mentionné des messages d'erreurs pas assez explicites qui peuvent subvenir lors de l'utilisation de l'application. Ces messages peuvent avoir un impact négatif sur l'utilisation du produit du point de vue de l'utilisateur.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au [RGS] ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. L'évaluateur n'a pas relevé de vulnérabilité exploitable lors de l'analyse.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Cloudcard+, version 3.4.14 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.
L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS] et de l'utilisation des guides mis à sa disposition par le développeur afin d'utiliser de façon sécurisée le SDK lors de la création de son application *Android* ou *iOS*.

Annexe 1. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : *Cloudcard+ Cible de sécurité* Référence : SafranIS_CC+_ST_fr - 2016_2000021689 ; Version : 1.8 ; Date : *9 mars 2018.* Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : *Cloudcard+ Cible de sécurité* Référence : SafranIS_CC+_ST_lite_fr - 2018_2000021689 ; Version : 1.0 ; Date : *27 mars 2018.*
[RTE]	*Rapport Technique d'Evaluation CSPN MERCANTOUR3 – Cloudcard Plus* Référence : OPPIDA/CESTI/MERCANTOUR3/RTE/1.1 ; Version : 1.1 ; Date : *20 mars 2018.*
[GUIDES]	*CloudCard+ Android High Level SDK Documentation* Version: 3.4.14; Date: 20 avril 2017. *CloudCard+ iOS High Level SDK Documentation* Version: 3.4; Date: 20 avril 2017. *Security Guidelines Server* Référence : 2017_2000030298_Security_Guidelines_Server_1.0 ; Version : 1.0 ; Date : n.c. *Security Guidelines for CC+ HL SDK* Référence : Security Guidelines for CC+ HL SDK - v1.1 ; Version : 1.1 ; Date : n.c.

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.