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-2017/20

Cardlet Mobile Connect
Version 1.8

Paris, le 14 août 2017

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

Emmanuel GERMAIN
[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-2017/20

Nom du produit

Cardlet Mobile Connect

Référence/version du produit

Version 1.8

Catégorie de produit

Identification, authentification et contrôle d'accès

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

Orange Applications for Business
4 rue de la Châtaigneraie, CS 51766,
35517 Cesson-Sevigné cedex
France

Développeur

FIME
8 rue Commodore J.H. Hallet
14000 Caen
France

Centre d'évaluation

THALES (TCS – CNES)
290 Allée du Lac,
31670 Labège,
France

Fonctions de sécurité évaluées

Création du code personnel
Saisie et validation du code personnel
Blocage du code personnel
Stockage sécurisé du code personnel
Stockage de la configuration de la *cardlet*
Réponse à une demande de validation

Fonctions de sécurité non évaluées

Aucune

Restriction(s) d'usage

Oui (cf. §3.2)

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 la « Cardlet Mobile Connect, version 1.8 » développée par *FIME*. C'est une *applet* JavaCard, aussi appelée *cardlet*, destinée à être installée sur des cartes SIM conformes au standard 3GPP Release 6 (R6).

La fonction principale de la *cardlet* est la validation de demandes émises par un système tiers au moyen de SMS binaires, chiffrés et signés, échangés au travers du réseau de téléphonie mobile. Ces demandes sont de deux types :

- validation d'une opération (mode « Click OK ») : l'utilisateur accepte ou non l'opération qui est présentée sur l'écran de son téléphone ;
- authentification d'une opération (mode « Code personnel ») : comme pour la validation d'une opération, l'utilisateur accepte ou non l'opération, mais il doit au préalable saisir son code personnel.

La *cardlet* fait ainsi office de second facteur d'authentification pour les deux modes de validation précédemment cités, comme détaillé dans les images suivantes :

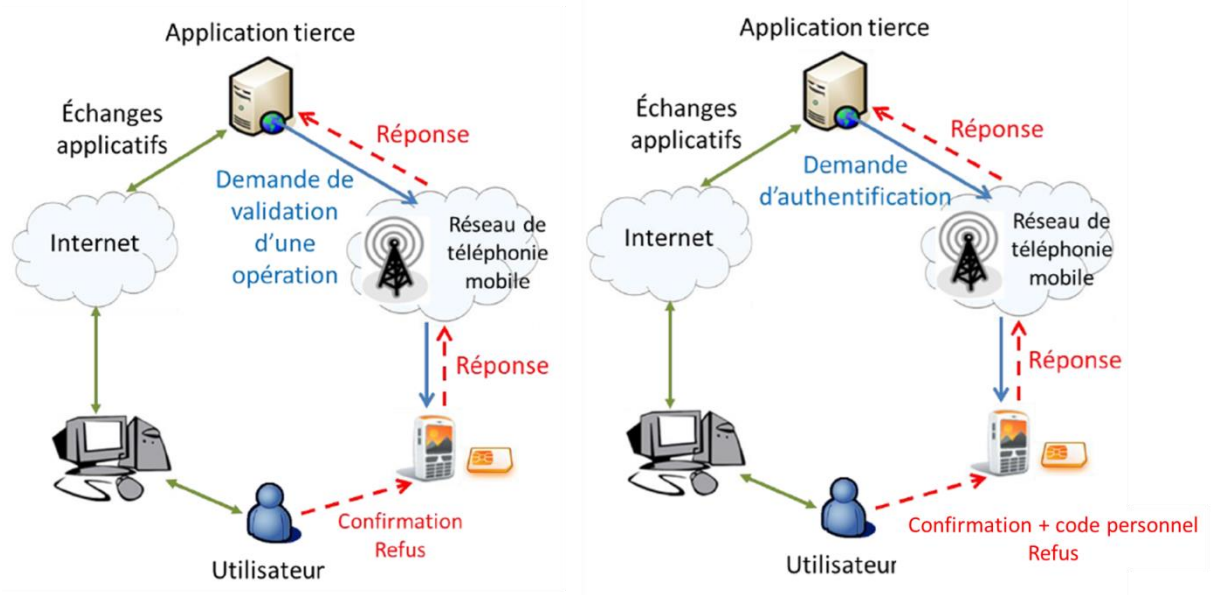

Figure 1 : Demandes de validation d'une opération et d'authentification

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	Cardlet Mobile Connect
Numéro de la version évaluée	1.8
Organisation éditrice	Orange Applications for Business (OAB)
Identification du produit	MC23 FR

La version certifiée du produit peut être identifiée par la commande *GET APPLET DATA* implémentée dans la *cardlet*. La réponse est à interpréter de la façon suivante :

Etiquette (Tag)	Longueur	Valeur	Interprétation
c1	09	*4f4142* ffff *4d433233*	OAB MC23
c2	02	*0108*	1.8
c3	06	66726c61*4652*	FR

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- création du code personnel utilisateur ;
- saisie et validation du code personnel utilisateur ;
- blocage du code personnel utilisateur ;
- stockage sécurisé du code personnel utilisateur ;
- stockage sécurisé de la configuration de la *cardlet* ;

- réponse à une demande de validation : émission de réponses aux demandes protégées en intégrité et authenticité (via la génération d'un code d'authentification du message[1]).

1.2.4. Configuration évaluée

La *cardlet* a été installée et personnalisée en suivant les étapes décrites dans le guide d'installation (voir [GUIDES]).
La *cardlet* est installée dans l'*Issuer Security Domain* de la carte SIM.

Les deux modes de validation offerts par la *cardlet* ont été couverts par l'évaluation.

L'évaluateur a utilisé les terminaux suivants pour réaliser son analyse :

- un smartphone *APPLE* iPhone 6S Gold 16Gb équipé d'une carte SIM compatible (voir [CDS]) ;
- un smartphone *SAMSUNG* Galaxy S4 équipé du système d'exploitation Android en version 4.4.2.

Les deux terminaux embarquaient, pour les besoins de l'évaluation, une carte SIM Orange/Gemalto NFC N9 certifiée conformément au profil de protection [PP USIM] (voir [CER-PTF]).

[1] La *cardlet* se base sur la plateforme sous-jacente, à savoir la carte SIM, pour l'ensemble des services cryptographiques.

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 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].

À noter que le mode « Click OK » ne couvre pas l'ensemble des menaces identifiées de 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 du produit nécessite l'utilisation du portail web Mobile Connect d'*ORANGE*.

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

Après avoir renseigné son numéro de téléphone sur le portail web Mobile Connect d'*ORANGE*, l'utilisateur est prévenu par SMS que le produit est installé. Il ne lui reste plus qu'à initialiser la TOE en créant son code personnel.

2.3.1.3. Durée de l'installation

L'installation ne dure que quelques minutes.

2.3.1.4. Notes et remarques diverses

La procédure d'installation est claire et ne présente pas de problème particulier. Il suffit de se rendre sur le portail web et de suivre les instructions.

2.3.2. Analyse de la documentation

La documentation et les instructions associées au produit sont suffisantes, claires et cohérentes.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source qui lui a permis de conclure que le développement de la TOE a été réalisé en tenant compte des bonnes pratiques de codage et en intégrant des mesures de sécurité contre des attaques visant à perturber son exécution.
En outre l'évaluateur a pu vérifier l'implémentation correcte des fonctions de sécurité s'appuyant sur des mécanismes de la plateforme sous-jacente.

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], sauf une. En effet, alors que la cible de sécurité mentionne un *timer* de 30 secondes pour la saisie du code personnel (F_CREAT-PC), dans la pratique cette durée est d'une minute. Toutefois cela n'a pas d'impact sur la sécurité du produit.

Les fonctions suivantes s'appuient sur des mécanismes évalués au titre de la certification de la plateforme sous-jacente (voir [CER-PTF]) ; elles n'ont pas fait l'objet de tests mais l'évaluateur a vérifié la bonne implémentation des appels aux fonctions exposées par la plateforme, tels que décrit dans les guides de la plateforme :

- stockage sécurisé du code personnel utilisateur ;
- stockage sécurisé de la configuration de la *cardlet* ;
- réponse à une demande de validation.

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

Toutes les fonctions de sécurité ont subi des tests de pénétration ou ont fait l'objet d'une analyse de code afin de confirmer qu'elles atteignaient bien le niveau de résistance attendu.

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 ou à son implémentation pouvant remettre en cause la sécurité du produit sur le périmètre évalué et ses fonctions de sécurité.

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.
Toutefois, il est à noter que le mode « Click OK » ne permet pas l'authentification de l'utilisateur et, de ce fait, ne garantit pas, au-delà du respect des restrictions d'usage énoncées au 3.2, qu'une demande a bien été validée par l'utilisateur légitime.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Aucune recommandation particulière concernant l'utilisation du produit 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.
Il est cependant recommandé que l'utilisateur utilise un code PIN non trivial pour verrouiller/déverrouiller la carte SIM.

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

L'utilisation du produit est relativement simple et ne présente pas de difficulté.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

Non applicable.

2.5. Analyse du générateur d'aléas

Non applicable.

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 « Cardlet Mobile Connect, version 1.8 » 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 s'assurer de la mise en œuvre des recommandations suivantes :

- la *cardlet* ne doit être installée que sur une SIM certifiée conformément au profil de protection *(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations (Basic configuration)* (voir [PP USIM]) ;
- l'utilisateur doit utiliser un code PIN non trivial pour verrouiller/déverrouiller la carte SIM ;
- l'utilisateur doit configurer sur son terminal le verrouillage automatique de l'écran, avec déverrouillage à base de code ou motif.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cardlet Mobile Connect Cible de sécurité* Référence : MOB001-CDS01-1.5.0 ; Version : 1.5.0 ; Date : *13 novembre 2016.*
[RTE]	*Rapport Technique d'Evaluation CSPN Projet: CSPN CARDlet Mobile Connect* Référence : Mobile_Connect_CSPN_RTE ; Version : 1.0 ; Date : *02 mars 2017.*
[GUIDES]	*Guide installation* Référence : Mobile Connect_Installation_V2.0 ; Version : 2.0 ; Date : *07 octobre 2016.* *Guide utilisateur* Référence : MC_Manuel_Utilisateur_V1.2 ;Version : 1.2 ; Date : *07 octobre 2016.* *Guide administration* Référence : MC_Guide_d'administration_V1.2 ; Version : 1.2 ; Date : *07 octobre 2016.*
[PP USIM]	*(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations (Basic configuration) ;* Référence : PU-2009-RT-79 Version : 2.0.2 ; Certifié sous la référence ANSSI-CC-PP-2010/04 le 12 juillet 2010.
[CER-PTF]	Plateforme Orange NFC v2 G1 release B sur composant ST33F1ME. Certifié sous la référence ANSSI-CC-2012/48 le 30 juillet 2012.

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 (CSPN) 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/