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-2017/21

Square by Vivaction pour iOS
Version 1.5

Paris, le 6 septembre 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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-2017/21

Nom du produit

Square by Vivaction pour iOS

Référence/version du produit

Version 1.5

Catégorie de produit

Communication sécurisée

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

Vivaction
2 rue des bourets
92150 Suresnes
France

Développeur

Vivaction
2 rue des bourets
92150 Suresnes
France

Centre d'évaluation

Lexfo
5 rue Drouot
75009 Paris
France

Fonctions de sécurité évaluées

Authentification de l'utilisateur
Chiffrement et intégrité des données échangées
Protection contre une attaque en force brute
Protection en confidentialité et intégrité des données stockées sur le téléphone
Communications entre processus

Fonction(s) de sécurité non évaluées

Aucune

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 « Square by Vivaction pour iOS, version 1.5 » développé par *VIVACTION*. Il s'agit d'une application pour terminaux mobiles équipés de la plateforme iOS d'*APPLE* dont le but est de réaliser des communications sécurisée au travers de la voix sur IP (*VoIP*).

L'application Square by Vivaction pour iOS est le « centre de contrôle » de la solution. Elle initie des communications avec les serveurs de *VIVACTION*, démarre le logiciel OpenVPN, puis permet à l'utilisateur de lancer « Vivaction Phone », l'application gérant la *VoIP*, au travers d'un raccourci depuis ce « centre de contrôle ».

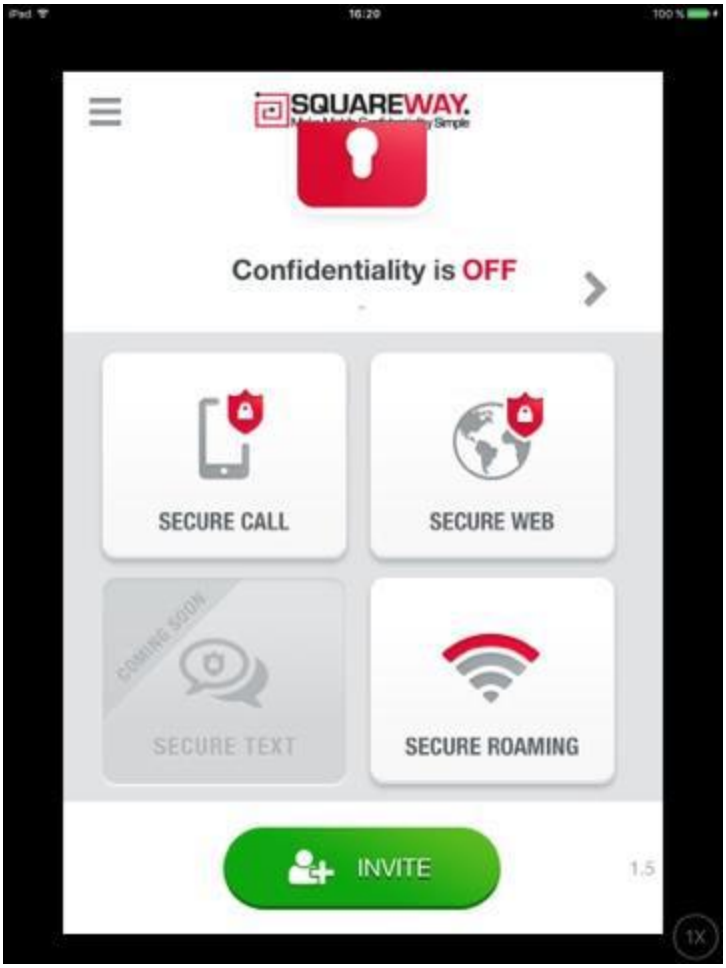

Figure 1: Page principale de l'application Square by Vivaction.

La gestion du réseau privé virtuel (*Virtual Private Network*, VPN) sur la plateforme iOS est telle qu'une fois activée, tout le trafic réseau du périphérique passe par ce VPN, de façon transparente pour toutes les applications. De fait, l'application « Vivaction Phone » tire ainsi profit de ce réseau privé virtuel en termes de confidentialité et d'intégrité.

Comme le détaille la figure ci-dessous, l'application évaluée est intégrée dans une infrastructure plus large composée notamment d'un site client (*Business center*), d'un serveur

OpenVPN, d'un serveur *Trusted Service Manager* (TSM) et d'un serveur *Session Border Control* (SBC) qui assure la connectivité avec le serveur *Session Initiation Protocol* (SIP) de *VIVACTION* en charge de la *VoIP*.

La figure ci-dessous explicite l'architecture de la solution.

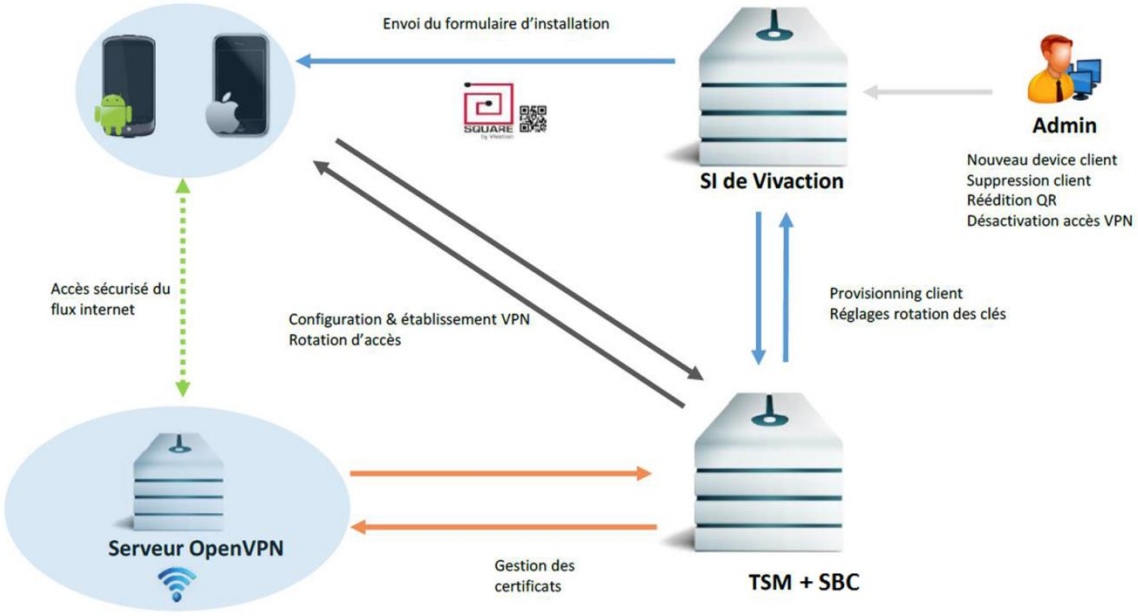

Figure 2 - Architecture de la solution.

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	Square by Vivaction pour iOS
Numéro de la version évaluée	1.5

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

- avant téléchargement : le magasin d'applications d'*APPLE* affiche le numéro de version ;
- après téléchargement : la page d'accueil de « Square by Vivaction pour iOS » expose le numéro de version en bas à droite de l'écran.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- l'authentification de l'utilisateur ;
- le chiffrement et intégrité des données échangées ;
- la protection contre une attaque en force brute ;
- la protection en confidentialité et intégrité des données stockées sur le téléphone ;
- les communications entre processus.

1.2.4. Configuration évaluée

La configuration évaluée s'appuie sur deux logiciels indispensables au fonctionnement de la solution qu'il faut télécharger indépendamment depuis le magasin d'applications d'*APPLE* :

- Vivaction Phone, en version 3.0 ;
- OpenVPN Connect en version 1.1.1.

La plateforme de test est constituée des serveurs suivants :

- OpenVPN en version 2.2.1, serveur gérant le réseau privé virtuel (VPN) ;
- TSM en version b20170323, serveur en charge du provisioning des clients et de la communication de la configuration du VPN à l'application « OpenVPN Connect » du client ;
- SBC en version 7.00A.082.007, serveur utilisé comme passerelle SIP. Ce serveur n'est accédé qu'au travers du VPN et est situé « derrière » le TSM.

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].

2.3.1. Installation du produit

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

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

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

L'installation nécessite un accès au magasin d'applications d'*APPLE*.

2.3.1.3. Durée de l'installation

L'installation consiste à télécharger les applications « Square by Vivaction pour iOS », « Vivaction Phone » et « OpenVPN Connect » depuis le magasin d'applications d'*APPLE*.

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.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et 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.

En revanche, l'évaluateur a mis en évidence des vulnérabilités jugées mineures sur le serveur menant à une fuite d'information non critiques, sans conséquences sur la sécurité de la solution.

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

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.3.8.4. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le RTE.

2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit se base sur une libraire cryptographique pour l'ensemble des services cryptographiques. Aucune non-conformité au RGS, ni vulnérabilité exploitable n'ont été identifiées pendant l'évaluation.

2.5. Analyse du générateur d'aléas

Le produit se base sur une libraire cryptographique pour l'ensemble des services cryptographiques. Aucune non-conformité au RGS, ni vulnérabilité exploitable n'ont été identifiées pendant l'évaluation.

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 « Square by Vivaction pour iOS, version 1.5 » 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Square by Vivaction Version iOS* Référence : VIV20160420-IOS v1.4 ; Version : 1.4 ; Date : *25 juillet 2017*
[RTE]	*Square by Vivaction Version iOS* Référence : VIV20170622-iOS V1.2 ; Version : 1.2 ; Date : *25 juillet 2017*
[GUIDES]	Guide d'installation des applications mobiles ; Référence : Guide install IOS MAJ 2 08012016_1. Référence : Guide Install Vivaction softphone v1_0 ; Version : 1.0. Guide d'utilisation des applications mobiles ; Référence : CustomerCare_User Guide v1_2 ; Version 1.2. Référence : Guide utilisation Square v2 jan2016 ; Version : 2.0. Documentation d'architecture ; Référence : Architecture_SquareByVivaction_160113. Référence : Architecture_TSM_PKI_oVPN_0.3 ; Version : 0.3. Référence : Architecture_TSM_vs_oVPN_0.3 ; Version : 0.3. Référence : Specification Architecture de la solution SQUARE 9jan2016 v2 ; Version 2.0. Référence : Specification Securite et cryptographie de la solution v2 ; Version : 2.0. Référence : INTEG_cahier_charge_SWC_Square. Spécifications des API du serveur ; Référence : Spec_SquareByVivaction_API_iOS_160112. Référence : Spec_SquareByVivaction_API_SIVivaction_151119.

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/