Cible de sécurité CSPN

Réf. : VIV20160420-IOS V1.4

Square by Vivaction

Version iOS

25/07/2017

TABLE DES MATIÈRES

1 PRESENTATION DE LA CIBLE DE SECURITE

1.1 VUE D'ENSEMBLE DE LA CIBLE DE SECURITE

Cette cible de sécurité a été élaborée dans le cadre du processus de certification CSPN mis en place par l'ANSSI. Le produit évalué est une application de voix sur IP et de navigation internet sécurisée, ainsi que les infrastructures serveur permettant cette communication et son administration.

Ce document décrit le produit évalué, précise les hypothèses relatives à son environnement d'utilisation, les menaces pouvant l'affecter et ses fonctions de sécurité.

1.2 IDENTIFICATION DU PRODUIT

Organisation éditrice	Vivaction
Lien vers l'organisation	http://www.vivaction.com
Nom commercial du produit	Square by Vivaction
Numéro de la version évaluée	Applications iOS : ▶ Square by Vivaction : 1.5 ▶ Vivaction Phone : 3.0 Serveurs : ▶ Serveur OpenVPN : 2.2.1 ▶ Serveur TSM : b20170323 ▶ Serveur SBC : 7.00A.082.007 ▶ Site client : Secure POP -1
Catégorie de produit	Communication Sécurisée

2 DESCRIPTION DE LA CIBLE D'EVALUATION

2.1 DESCRIPTION GENERALE DU PRODUIT

Square by Vivaction est une solution de voix sur IP et d'échange de data sécurisée sur mobile. Elle permet la communication sécurisée par voix sur IP avec d'autres utilisateurs de la solution, ainsi que des numéros de téléphone classiques. Elle permet également la navigation sur internet au travers de son VPN.

La solution est composée de deux applications mobiles disponibles sur Android et iOS, ainsi que de différents serveurs hébergés par Vivaction.

L'infrastructure de serveurs distants dispose de services variés permettant aussi bien l'accès aux fonctionnalités de communication que l'administration de la solution.

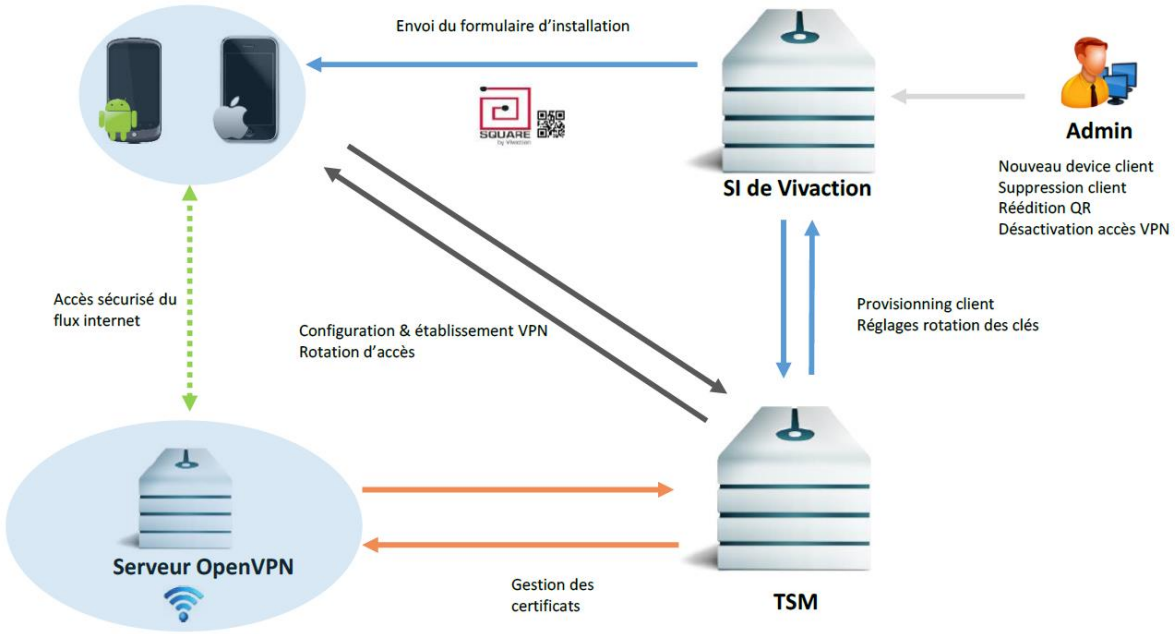

Figure 1 : Architecture de la solution Square by Vivaction

2.2 DESCRIPTION DE L'UTILISATION DU PRODUIT

L'application cliente est installée à l'initiative d'un utilisateur sur son smartphone suite à l'inscription au service ou à la réception d'une invitation envoyée par un utilisateur inscrit. Après la phase d'initialisation par réception d'un QR Code par e-mail, l'application se connecte au VPN de Vivaction et est prête à l'emploi.

Les fonctionnalités principales de l'application sont les suivantes :

- **Initialisation :** après réception d'un e-mail d'inscription contenant un QR Code, l'application est installée par l'utilisateur et se configure à l'aide de webservices sur l'infrastructure de Vivaction. Une fois la configuration effectuée, l'application se connecte au VPN de la solution et est prête à l'emploi ;

- **Utilisation :** toutes les communications (voix sur IP et web) passent par un tunnel VPN initialisé au lancement de l'application. Les échanges par voix sur IP sont ensuite effectués en utilisant les protocoles SIPS et SRTP à l'intérieur de ce VPN. Dans le cas d'un utilisateur invité, il ne sera pas connecté au VPN, mais bénéficiera tout de même de la protection de ses communications par SIPS et SRTP avec son correspondant Square ;
- **Administration :** la gestion des utilisateurs et l'accès aux fonctionnalités d'administration de la solution peuvent être réalisés au travers d'une application web dédiée.

2.3 DESCRIPTION DE L'ENVIRONNEMENT D'UTILISATION PREVU

ENVIRONNEMENT SERVEUR

L'infrastructure serveur est hébergée par Vivaction dans un datacenter sécurisé (Tier III+, firewall applicatif, protection anti-DDoS). Les différents serveurs sont installés d'après des procédures établies sur la base de guides de sécurité fournis par des organismes reconnus tels que le NIST ou l'ANSSI. Ils sont mis à jour régulièrement, en particulier concernant les correctifs liés à la sécurité, et font également l'objet d'audits de sécurité réguliers.

ENVIRONNEMENT CLIENT

La solution est utilisable sur des terminaux iOS (iPhone ou iPad).

Les logiciels clients doivent être installés depuis le « store » de l'environnement mobile.

2.4 DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

La configuration des téléphones est conforme à l'état de l'art : les données sont chiffrées, et le téléphone est protégé par un mot de passe fort. En outre, le système est celui fourni par le constructeur et n'est pas modifié par l'utilisateur (jailbreak). On protège ainsi les données en cas de vol du mobile et le modèle de sécurité du système afin de minimiser l'impact d'une application malveillante.

La sécurité physique des serveurs distants est quant à elle considérée comme sûre.

D'un point de vue logique, il est considéré que les codes source des applications serveurs ne sont pas disponibles.

D'un point de vue organisationnel, les administrateurs de la solution sont considérés comme non hostiles. Les applications mobiles et les mises à jour fournies par Vivaction sont considérées comme sûres : les mécanismes de sécurité du store officiel garantissent l'intégrité et l'authenticité, et on considère qu'elles ne contiennent pas de code malveillant.

2.5 DESCRIPTION DES DEPENDANCES

L'application nécessite l'installation d'OpenVPN, iOS ne gérant pas nativement ce protocole (cf. https://www.apple.com/business/docs/iOS_Security_Guide.pdf)

2.6 DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES

Trois groupes d'utilisateurs interviennent dans l'utilisation et la gestion de la solution :

- **administrateur(s) système**

En charge de la gestion des serveurs de l'infrastructure Square by Vivaction. Un administrateur système dispose de droits d'accès privilégiés sur le système d'exploitation hébergeant les applications serveur. Il s'assure du bon fonctionnement des serveurs et maintient leur niveau de sécurité.

- **administrateur(s) applicatif**

En charge de la gestion du produit. Un administrateur applicatif dispose de droits d'accès à l'interface d'administration de Square by Vivaction. Suivant ses droits, il peut consulter des statistiques sur sa flotte mobile, rédiger des notes d'information, ou modifier des paramètres techniques.

- **utilisateurs finaux**

En charge de l'installation du logiciel client sur leur smartphone. Les utilisateurs de la solution emploient les fonctionnalités de la solution pour naviguer sur le web ou passer des appels sécurisés.

2.7 DEFINITION DU PERIMETRE DE L'EVALUATION

Le périmètre de l'évaluation concerne les composants suivants :

- les applications iOS fournies : l'application Square by Vivaction qui gère la connexion sécurisée au VPN et l'application Vivaction Phone qui gère les appels VoIP ;
- les services et applications web de l'infrastructure Square by Vivaction qui sont accessibles depuis Internet : le portail client (Business center), le serveur OpenVPN, le serveur TSM (Trusted Service Manager) et le serveur SBC (Session Border Control) qui assure la connectivité avec le serveur SIP de Vivaction ;
- les différents échanges pouvant intervenir dans le cadre de l'utilisation des fonctionnalités de la solution Square by Vivaction.

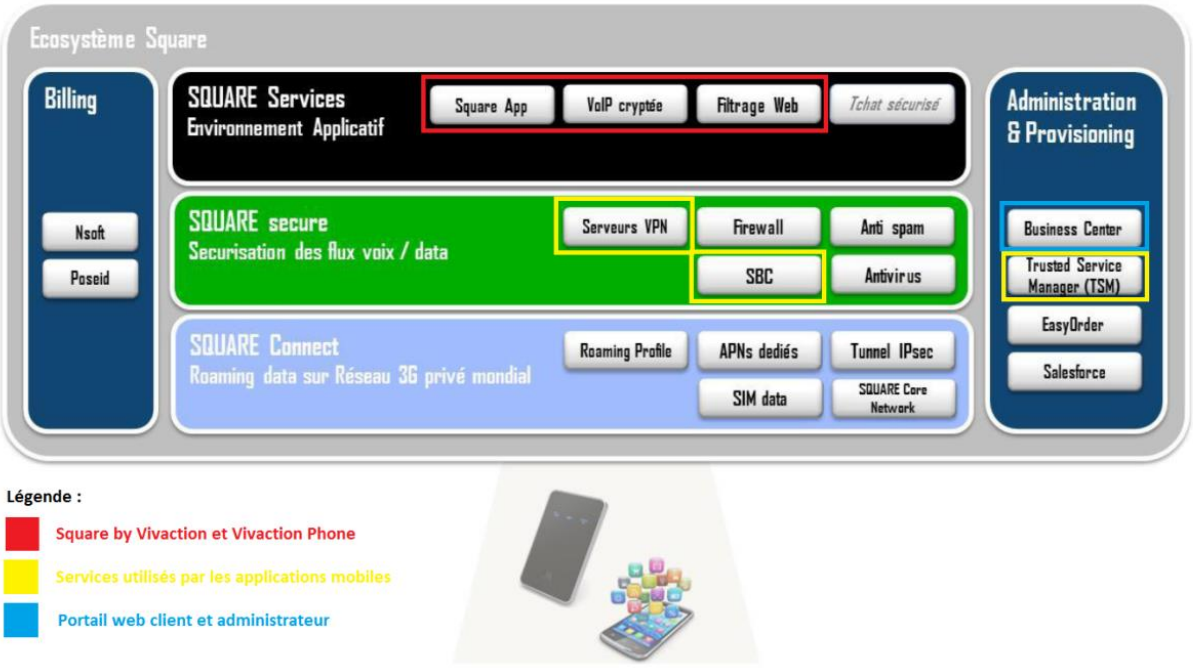

Figure 2 : Périmètre d'évaluation

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 MATERIEL COMPATIBLE OU DEDIE

Le matériel doit disposer du système d'exploitation iOS.

Aucune contrainte matérielle particulière n'est présente. Aussi, un équipement classique de type smartphone est retenu pour l'évaluation. Concernant la partie serveur, l'évaluation reposera sur l'utilisation de l'infrastructure mise en place par Vivaction.

3.2 ENVIRONNEMENT SYSTEME RETENU

L'environnement de test prévu concernant cette évaluation est un smartphone (iPhone 5 ou 6).

4 DESCRIPTION DES BIENS SENSIBLES

Les différents biens que la solution doit protéger sont les suivants :

- **Configuration initiale**

Les informations de configuration nécessaires à l'installation de l'application Square by Vivaction sous la forme d'un QR Code doivent être protégées en confidentialité et en intégrité.

- **Identifiants de connexion utilisateur**

Les identifiants employés par les utilisateurs de la solution doivent être protégés en confidentialité et en intégrité.

- **Identifiants de connexion administrateur**

Les identifiants employés par les administrateurs de la solution doivent être protégés en confidentialité et en intégrité.

- **Interactions client/serveur**

Les données transmises entre l'équipement mobile et les serveurs de Vivaction doivent être protégées confidentialité, intégrité et disponibilité. Ces connexions ont été établies suite à une authentification préalable.

- **Contenu des échanges**

Les appels vocaux échangés entre les utilisateurs doivent être protégés en confidentialité et intégrité.

- **Stockage des données utilisateurs**

Les données stockées sur l'appareil mobile et les serveurs de la solution doivent être protégées (ex. configuration de l'application, certificat VPN, etc.). Ces données doivent rester confidentielles et intègres.

5 DESCRIPTION DES MENACES

Par hypothèse, les administrateurs ne sont pas considérés comme des attaquants potentiels.

Les menaces suivantes ont été identifiées :

- **M1 : Vol smartphone**

Le smartphone de l'utilisateur a été perdu ou volé. Dans cette configuration, on peut avoir affaire à deux cas distincts : le smartphone est verrouillé ou ne l'est pas. Le but est d'accéder aux informations enregistrées par l'application.

- **M2 : Compromission du smartphone**

Une application malveillante est présente sur le smartphone de l'utilisateur. Celle-ci va tenter d'obtenir les informations stockées par l'application, ainsi que le contenu des échanges effectués lors de son utilisation. Elle va également tenter de modifier la configuration ou les communications afin de rediriger l'utilisateur sur des numéros surtaxés par exemple. Elle va également tenter d'abuser de la communication entre les deux applications afin d'obtenir des informations confidentielles ou d'en détourner l'utilisation.

- **M3 : Attaque de l'infrastructure**

Un attaquant ayant connaissance de l'infrastructure Square by Vivaction, cible les services et les applications web accessibles sur Internet pour impacter le bon fonctionnement de la solution (attaques de type DoS), compromettre ou récupérer des données (conversations, données utilisateur, etc…) ou encore obtenir un accès administrateur sur l'interface de gestion du service afin d'en modifier la configuration à son avantage.

- **M4 : Man in the Middle**

Un attaquant situé sur le même réseau qu'un utilisateur effectue une attaque Man-in-the-Middle sur la connexion. Le but est de capturer les informations sensibles (ex. : identifiants, conversations vocales), d'intercepter ou de modifier les données échangées entre l'application mobile et l'infrastructure serveur.

6 DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

Les fonctions de sécurité implémentées au sein de la solution Square by Vivaction sont les suivantes :

- **Authentification**

Différentes authentifications sont utilisées par la solution :

- Sur le site client (Customer Care) accessible sur l'url https://www.selfcare-services.com ;
- Après l'inscription, des informations d'authentification sont fournies sous forme d'un QR Code afin de pouvoir télécharger les informations nécessaires pour le fonctionnement de la solution (configuration VPN) ;
- Le certificat permettant la connexion au VPN est régulièrement renouvelé ;
- Un système d'invitation existe et permet à des personnes n'étant pas clientes de la solution de pouvoir recevoir des appels.

- **Chiffrement des échanges**

L'ensemble des transmissions est chiffré, qu'il s'agisse des connexions au site client, au serveur de gestion de clés, ou au serveur VPN. Les communications vocales sont également chiffrées :

- OpenVPN utilisant l'algorithme DHE-RSA-AES256-SHA afin de créer un tunnel pour les appels vocaux et la navigation web ;
- SIPS / SRTP pour l'émission et la réception d'appels vocaux ;
- HTTPS pour les connexions au site client et au serveur de gestion de certificats VPN ;

- **Mécanismes de protection contre le bruteforce d'authentification**

Le produit inclut des protections empêchant les attaques de type brute force. En cas d'échecs répétés de l'authentification, l'IP fautive sera bannie pendant un certain temps.

- **Intégrité des échanges**

Le contrôle de l'intégrité des échanges réalisés entre les différentes parties de la solution repose sur l'utilisation de la couche de transport SSL/TLS.

- **Protection des données**

Côté serveur, les données utilisateur et techniques sont protégées par les différents mécanismes d'authentification et de transport (confidentialité et intégrité).

- **Communications entre processus**

Les échanges entre l'application principale Square by Vivaction et Vivaction Phone sont effectués de manière sécurisée. Aucune information confidentielle ne transite en clair entre les deux applications, et celles-ci vérifient la provenance des messages échangés afin de ne pas permettre d'utilisation frauduleuse par une application tierce.

7 MATRICES DE COUVERTURE

Biens sensibles / Menaces	Vol	Malware	Attaque de l'infrastructure	MitM
Configuration initiale	X	X	X	X
Identifiants de connexion			X	X
Interactions client/serveur		X	X	X
Contenu des échanges		X	X	X
Données utilisateur	X	X		

Fonctions de sécurité / Menaces	Vol	Malware	Attaque de l'infrastructure	MitM
Authentification	X	X	X	X
Chiffrement des échanges		X	X	X
Protection contre le bruteforce			X	
Intégrité des échanges		X	X	X
Protection des données	X		X	X
Communications entre processus		X		