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-2016/13

EZIO mobile SDK for iOS
version 3.2.1 RMW 7

Paris, le 6 janvier 2017

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-2016/13

Nom du produit

EZIO mobile SDK for iOS

Référence/version du produit

Version 3.2.1 RMW 7

Catégorie de produit

Identification, authentification et contrôle d'accès
Stockage sécurisé

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

GEMALTO SA
Avenue du Jujubier
Z.I. Athelia IV
13705 La Ciotat Cedex
France

Centre d'évaluation

SOGETI
24, rue du Gouverneur Général Félix Eboué
92136 Issy-les-Moulineaux Cedex
France

Fonctions de sécurité évaluées

Gestion sécurisée du PIN de l'utilisateur
Protection en confidentialité des clés durant le *provisioning*
Protection en confidentialité des clés stockées pour l'OTP
Protection en confidentialité des clés lors de la génération de l'OTP
Protection en intégrité des données sensibles utilisées pour la génération d'OTP
Protection en confidentialité des clés utilisées pour le stockage sécurisé sur le mobile

Fonction(s) de sécurité non évaluées

Sans objet

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 le « EZIO mobile SDK for iOS, version 3.2.1 RMW 7 » développé par *GEMALTO SA.*

La solution EZIO Mobile se compose des applications pour ordiphones Android ou iOS, et d'un serveur appelé EPS (*Enrollment and Provisioning Server*). *GEMALTO* fournit pour chacun de ces éléments un SDK destiné à être intégré par un opérateur.
Le SDK EZIO Mobile fournit, aux développeurs d'applications mobiles, une couche d'abstraction pour l'implémentation de fonctions d'authentification et de signature à base d'OTP (*One Time Password* ou mot de passe à usage unique).
Une application développée à partir du SDK EZIO Mobile permet, une fois téléchargée depuis un magasin d'application autorisé, de s'authentifier auprès de services distants compatibles.

L'utilisation du service se déroule en trois phases :

- phase d'enrôlement : l'utilisateur s'enregistre auprès du service distant et du serveur EPS, lequel génère un code d'enregistrement et un code PIN (*Personal Identification Number*). Ces éléments sont ensuite envoyés à l'utilisateur par un canal séparé (SMS, courriel ou courrier postal) ;
- phase dite de *provisioning* : l'utilisateur lance l'application EZIO Mobile pour iOS sur son terminal et utilise son code d'enregistrement pour permettre l'établissement d'un canal sécurisé entre l'application et le serveur EPS ; la clé secrète de l'utilisateur est envoyée à l'application, qui la stocke dans un conteneur chiffré ;
- phase d'utilisation : l'utilisateur de l'application EZIO Mobile pour iOS souhaitant accéder au service distant auprès duquel il est déjà enregistré saisit son code PIN et obtient un OTP. Ce dernier est présenté au service distant, le serveur EPS, lui-même connecté au serveur d'authentification EZIO permettant ainsi l'authentification de l'utilisateur.

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

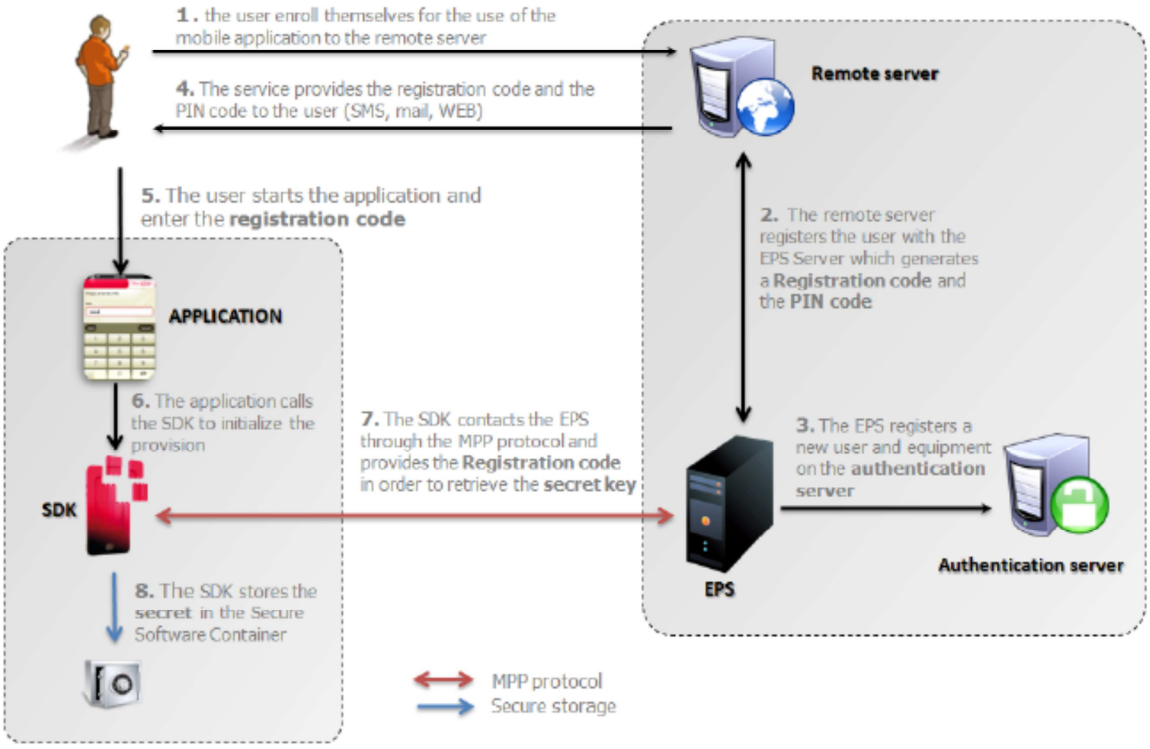

Figure 1 - Architecture générale du système EZIO

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
☐ 14 – autre

1.2.2. Identification du produit

La version du produit analysée est la version 3.2.1.
Le fichier Mach-O correspondant à cette version (dénommé EzioMobile.framework) est identifié par l'empreinte SHA1 suivante : 9b735a681bb36698f1c3aff3d22fdbe126d843b2.

1.2.3. Fonctions de sécurité

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont :

- la gestion sécurisée des données d'authentification de l'utilisateur, selon deux modes :
  - un code PIN défini par l'utilisateur ;
  - l'empreinte digitale de l'utilisateur en utilisant la fonctionnalité *TouchID* du terminal ;
- la protection en confidentialité des clés durant le *provisioning* ;
- la protection en confidentialité des clés stockées pour l'OTP ;
- la protection en confidentialité des clés lors de la génération de l'OTP ;
- la protection en intégrité des données sensibles utilisées pour la génération d'OTP ;
- la protection en confidentialité des clés utilisées pour le stockage sécurisé sur le mobile.

1.2.4. Configuration évaluée

Dans le cadre de l'évaluation, le produit identifié au chapitre 1.2.2 a été livré à l'évaluateur sous deux formes :

- un exécutable au format Mach-O ;
- un ensemble de fichiers source (Objective-C, C).

Bien que l'évaluateur ait utilisé les deux formats pour son analyse, la plupart des tests ont été joués sur le SDK compilé (format Mach-O), accompagné d'un exemple de projet pour Xcode.

Cette configuration, Xcode et SDK compilé, a été jugée comme la plus représentative du produit évalué, lequel ne peut être utilisé comme tel mais doit être intégré dans une application finale développée par l'utilisateur du 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 a été 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, menaces, utilisateurs et 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

Sans objet.

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

La plateforme de test correspond à un ordinateur de type *Macintosh* tournant sous OS 10.10.4 (*Yosemite*) sur lequel est installé *Xcode* en version 6.4. Ce dernier permet d'exécuter le produit au travers du simulateur iOS.

Il a également été utilisé un *iPhone* 4S, sous iOS 8, pour la vérification de la détection du déplombage (*jailbreak*).

L'installation ne pose aucune difficulté particulière ; le fichier Mach-O peut être directement intégré dans l'environnement de développement ou bien le code source peut être importé afin de démarrer le développement d'une application.

2.3.1.3. Durée de l'installation

Non applicable.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

L'analyse de la documentation n'a pas soulevé de manquements particuliers. Le guide du programmeur (*Programmer's guide*) est clair et bien documenté, et fait référence aux recommandations de sécurité contenues dans le guide dédié (*Security guidelines*) ; ce dernier

contient un ensemble de règles et recommandations jugé suffisant pour assurer la qualité de l'application finale intégrant ce SDK.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et estime que le code source est de bonne qualité, clair, bien organisé et correctement commenté. Il fait également références aux règles décrites dans le guide *Security Guidelines* (voir [GUIDES]).
chaque interface est bien commentée.
La maintenabilité du code est assurée par l'utilisation de fonctions clairement définies.

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].

La protection de la communication avec le serveur lors du *provisioning* n'a été testée que partiellement ; le cas d'un certificat signé par une Autorité de Certification Racine non connue du mobile n'a pas fait l'objet de vérifications.

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

Le produit dans sa version évaluée offre des mécanismes globalement robustes et à l'état de l'art.
Le mécanisme de détection de modifications de l'environnement, exclu du périmètre dans la cible de sécurité, a été testé par l'évaluateur ; il a pu être contourné, mais sa mise en œuvre est jugée conforme aux bonnes pratiques.
Même dans le cas où un attaquant obtiendrait les privilèges *root* sur le terminal d'un utilisateur, la conception de la solution EZIO Mobile ne lui permet pas de récupérer le code PIN de l'utilisateur, nécessaire à la génération d'un OTP permettant de l'authentifier[1].

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

2.3.6.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues et exploitables sur ce produit.

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

Il n'a pas été identifié de vulnérabilités exploitables sur ce produit faisant partie de la cible de sécurité.

2.3.1. Accès aux développeurs

Sans objet.

[1] Sous réserve que l'utilisateur ne stocke pas son PIN sur le téléphone, ainsi que recommandé dans les guides.

2.3.2. Analyse de la facilité d'emploi et préconisations

2.3.2.1. Cas où la sécurité est remise en cause

Le produit a pour vocation de fournir une couche d'abstraction pour l'implémentation de fonctions de sécurité. Il est donc important de noter que même si le produit est développé de façon sécurisée, une mauvaise intégration du SDK EZIO Mobile pour Android peut amoindrir la sécurité de l'application finale.

Pour cela, le produit est accompagné de plusieurs documents ([GUIDES]) permettant une bonne compréhension du produit et de la façon de s'y interfacer de façon sécurisée, ainsi que d'un guide (*Security Guidelines*) détaillant les bonnes pratiques pour implémenter du code sécurisé.

Par ailleurs, les fonctions de sécurité du produit sont susceptibles d'être contournées dans le cas où l'attaquant disposerait de droits *root* sur le système Android lors de l'utilisation.

2.3.2.1. Recommandations pour une utilisation sûre du produit

L'évaluateur a listé des recommandations portant sur l'utilisateur du SDK (développeur d'applications) ainsi que l'utilisateur de l'application finale.

Concernant le développeur de l'application finale basée sur ce SDK, il est fortement recommandé que ce dernier :

- ait de bonnes connaissances en cryptographie ;
- s'appuie sur les exemples et la documentation accompagnant le produit.

Concernant l'utilisateur de l'application, il est recommandé qu'il ne stocke pas son code PIN sur l'équipement, ni sur tout autre support pouvant être porté à la connaissance d'un attaquant qui prendrait possession de l'équipement. Il est également fortement recommandé, lors de l'envoi des codes personnels à l'utilisateur (code PIN et code d'enregistrement), de privilégier un canal physique (par exemple le courrier postal). En effet, du fait du fonctionnement du système Android, le contenu d'un courriel ou d'un SMS pourrait être intercepté par une application malveillante.

Il est en outre recommandé que le développeur d'applications intègre les recommandations présentes dans les guides du SDK (voir [GUIDES]) dans sa propre documentation afin que l'utilisateur de l'application finale dispose des informations nécessaires à une utilisation sûre de l'application.

Il est enfin important de noter que la certification du SDK n'affranchit pas le développeur du respect des bonnes pratiques lors du développement de l'application, laquelle devrait également être testée. L'utilisation d'un SDK certifié pour le développement d'une application ne vaut pas certification de cette dernière et ne garantit pas qu'elle soit elle-même exempte de vulnérabilités.

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

Le développeur utilisant le SDK doit posséder des connaissances en développement sécurisé d'applications et en cryptographie, et respecter les règles définies dans les guides ainsi que les bonnes pratiques en vigueur (voir chapitre 2.3.2.1).

2.3.2.3. Notes et remarques diverses

Sans objet.

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 vulnérabilité exploitable.

L'analyse n'a pas relevé de non-conformité au RGS, à l'exception
- de l'utilisation de SHA-1, non recommandé par le RGS ;
- du mécanisme de génération des clés Master Key, AWK et BioFPKey (voir chapitre 2.5).

2.5. Analyse du générateur d'aléas

Le SDK s'appuie sur la fonction *SecRandomCopyBytes* du *framework* Security d'iOS.
L'analyse n'a pas révélé de vulnérabilités exploitables liées à l'utilisation du générateur d'aléas du SDK.

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 « EZIO mobile SDK for iOS, version 3.2.1 RMW 7 » 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, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN ST - EZIO mobile SDK 3.2.1 RMW 7 for iOS* Référence : *GEMALTO-EZIO-IOS-ST v2.1*; Version : *2.1* ; Date : *19 août 2016.*
[RTE]	*EZIO Mobile SDK for iOS 3.2 - CSPN Evaluation Technical Report* Référence : *FR14U12-CSPN-EZIO-SDK-iOS;* Version : 1.0 ; Date : *18 août 2016.*
[GUIDES]	*Ezio Mobile SDK - Software Development Kit 3.2 - Overview* Réference: *NA* Version: *NA* Date : *1 décembre 2015* *Ezio Mobile SDK - Software Development Kit 3.2 - Programmer's Guide* Réference: *NA* Version: *NA* Date : *10 décembre 2015)* *Ezio Mobile SDK - Software Development Kit 3.2 - Programmer's Guide for Multiple Authentication Modes* Réference: *NA* Version: *NA* Date : *14 décembre 2015* *Ezio Mobile SDK - Software Development Kit 3.2 - Security Guidelines* Réference: *NA* Version: *NA* Date : *25 janvier 2016*

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/
[RGS_B_1]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.0 du Version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.