PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2020/37

Protector OATH SDK for IOS

Version 5.4.0

Paris le 9 décembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2020/37**
Nom du produit **Protector OATH SDK for IOS**
Référence/version du produit **Version 5.4.0**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **THALES DIS France S.A.** Av. du Jujubier, Z. I. Athelia IV 13705 La Ciotat Cedex, France
Développeur **THALES DIS France S.A.** Av. du Jujubier, Z. I. Athelia IV 13705 La Ciotat Cedex, France
Centre d'évaluation **THALES / CNES** 290, allée du Lac 31670 Labège, France
Fonctions de sécurité évaluées Gestion sécurisée du PIN de l'utilisateur Gestion sécurisée des données biométriques Génération d OTP Confidentialité de la clé secrète de l'utilisateur pendant le provisionnement Confidentialité de la clé secrète de l'utilisateur utilisée pour l OTP Confidentialité des clés pendant le calcul de l'OTP
Fonctions de sécurité non évaluées Néant
Restriction(s) d'usage Non

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit 6
1.1 Présentation du produit 6
1.2 Description du produit évalué 8
1.2.1 Catégorie du produit 8
1.2.2 Identification du produit 8
1.2.3 Fonctions de sécurité 8
1.2.4 Configuration évaluée 8
2 L'évaluation 10
2.1 Référentiels d'évaluation 10
2.2 Charge de travail prévue et durée de l'évaluation 10
2.3 Travaux d'évaluation 10
2.3.1 Installation du produit 10
2.3.2 Analyse de la documentation 10
2.3.3 Revue du code source (facultative) 11
2.3.4 Analyse de la conformité des fonctions de sécurité 11
2.3.5 Analyse de la résistance des mécanismes des fonctions de sécurité 11
2.3.6 Analyse des vulnérabilités (conception, construction, etc.) 11
2.3.7 Accès aux développeurs 11
2.3.8 Analyse de la facilité d'emploi 11
2.4 Analyse de la résistance des mécanismes cryptographiques 12
2.5 Analyse du générateur d'aléas 12
3 La certification 13
3.1 Conclusion 13
3.2 Recommandations et restrictions d'usage 13
ANNEXE A. Références documentaires du produit évalué 14
ANNEXE B. Références à la certification 15

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Protector OATH SDK for IOS, Version 5.4.0 » développé par THALES DIS France S.A..

Ce produit fait partie d'une solution de génération de mots de passe, de stockage sécurisé et d'échange des messages *out-of-band*. Cette solution est composée de la librairie Protector OATH SDK for IOS, également appelée ici *Mobile Protector* (objet de la présente évaluation), d'un serveur appelé EPS (*Enrolment and Provisioning Server*), d'un serveur appelé MSM (*Mobile Secure Messenger*) et d'un appelé AS (*Authentication Server*).

La librairie *Mobile Protector* 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).

Mobile Protector fournit deux modes d'authentification :

- authentification par PIN : ce mode est activé par défaut et ne peut pas être désactivé ;
- authentification par biométrie (empreinte digitale ou identification faciale en fonction de l'équipement utilisé) : ce mode peut être activé ou désactivé par l'utilisateur.

L'utilisation du service se déroule en trois phases :

- l'enrôlement : un *Customer Server* demande au serveur EPS de créer un nouvel utilisateur. Cela implique la génération du secret qui sera injecté dans l'équipement mobile de l'utilisateur final à l'étape suivante, du PIN initial et d'un code d'enregistrement (*Registration Code – RC*) qui identifie le secret de manière unique. Le serveur EPS enverra également le secret au serveur AS. Cette première phase est obligatoire pour l'enregistrement d'un nouvel utilisateur, *Mobile Protector* n'est pas impliqué dans ce processus ;
- le *provisioning* : *Mobile Protector* récupérera le secret par le serveur EPS ;
- l'utilisation : l'utilisateur souhaitant accéder au service distant, auprès duquel il est déjà enregistré, s'authentifie en utilisant son code PIN ou ses identifiants biométriques afin d'obtenir un OTP. Ce dernier peut être envoyé au *Customer Server* ou fourni à l'utilisateur pour utilisation dans un autre contexte.

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

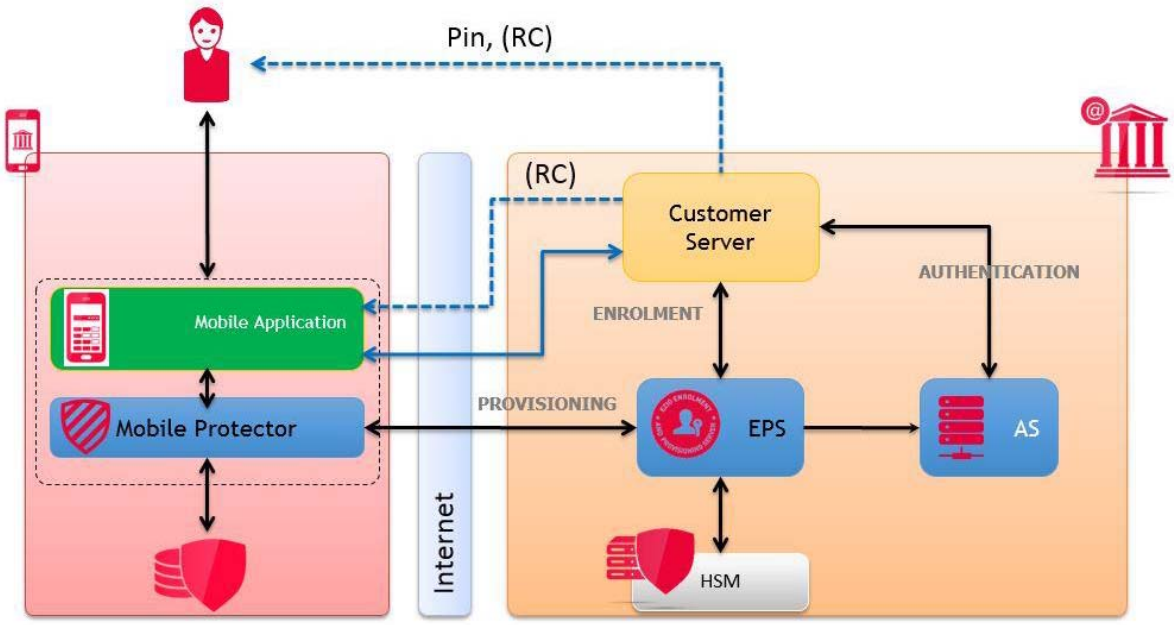

Figure 1 - Architecture Produit.

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*

Produit	
Nom du produit	Protector OATH SDK for IOS
Numéro de la version évaluée	Version 5.4.0

L'identification de *Mobile Protector* est possible grâce à l'utilisation d'une API dédiée.

L'extraction du code ci-dessous est une illustration de l'identification du SDK :

```
NSString* version = [EMCore version] ;
```

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la gestion sécurisée du PIN de l'utilisateur final ;
- la gestion sécurisée des données biométriques ;
- la génération d'OTP ;
- la confidentialité de la clé secrète de l'utilisateur pendant le provisionnement ;
- la confidentialité de la clé secrète de l'utilisateur utilisée pour l'OTP ;
- la confidentialité des clés pendant le calcul de l'OTP.

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 l'utilisation 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.

La plateforme de test est constituée des éléments suivants :

- un ordinateur desktop de type Mac Mini sur lequel est installé Xcode ;
- un iPhone 6 jailbreaké sous iOS 11.3 ;
- un iPhone 7 jailbreaké sous iOS 12.1 ;
- un iPhone 8 sous iOS 12.3 ;
- un iPhone X sous iOS 12.3.

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

Le SDK n'est pas à installer indépendamment d'une application et n'est pas une application autonome

L'utilisateur considéré dans le cadre de cette évaluation est l'intégrateur du SDK. Pour cet intégrateur, le SDK est fourni comme une librairie sous la forme d'un binaire qui doit être directement intégré dans l'environnement de développement afin de démarrer le développement d'une application.

L'utilisateur final téléchargera une application qui utilise le SDK depuis l'*Appstore*.

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'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu et analysé le code source de l'intégralité du produit. L'évaluateur estime que le code est clairement organisé et correctement documenté.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

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*

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 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.

2.3.8.3 Notes et remarques diverses

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

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 (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. Le produit implémente un générateur de nombres pseudo-aléatoires qui utilise comme source d'entropie le générateur des nombres aléatoires de la plateforme sous-jacente, hors du périmètre de l'évaluation (voir [RTE]).

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 « Protector OATH SDK for IOS, Version 5.4.0 » 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 Recommandations et 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].

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.

ANNEXE A. Références documentaires du produit évalué

[CDS]	*Protector OATH SDK v5.4.0– Security Target – iOS – Light Version* Version : 1.3 ; Date : juin 2020.
[RTE]	Rapport Technique d'Évaluation CSPN – *PROTECTOR_OATH_SDK5.4_for_IOS* Référence : ProtectorOATHiOS_CSPN_RTE ; Version : 1.0 ; Date : 10 septembre 2020. *Analysis of cryptographic mechanisms – Protector OATH SDK* Référence : ProtectorOATH_Crypt_RTE ; Version : 2.0 ; Date : 19 octobre 2020.
[GUIDES]	*Protector OATH SDK Programmers' Guide* Référence : EzioMobileSDK_programmers_guide ; Date : 5 septembre 2019. *Protector OATH SDK Security Guideline* Référence : EzioMobileSDK_security_guideline ; Date : 5 septembre 2019. *Protector OATH SDK Documentation* Référence : Protector OATH SDK V5.4 ; Date : 5 septembre 2019.

ANNEXE B. 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, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. 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..