PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2021/21

MobileID Authenticator SDK pour iOS

Version 2.0.12

Paris, le 1er septembre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti 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-2021/21**
Nom du produit **MobileID Authenticator SDK pour iOS**
Référence/version du produit **Version 2.0.12**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **ARIADNEXT** 1219 avenue des Champs Blancs 35510 Cesson Sevigne, France
Développeur **ARIADNEXT** 1219 avenue des Champs Blancs 35510 Cesson Sevigne, France
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées Protection du code confidentiel Protection des données échangées Protection des clés et secrets Protection contre les demandes d'authentification illégitimes Protection contre les signatures illégitimes de demandes d'authentification Vérification locale du certificat présenté par le serveur de gestion d'identité
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

1.1 Présentation du produit

Le produit évalué est « MobileID Authenticator SDK pour iOS, Version 2.0.12 » développé par ARIADNEXT.

Il s'agit d'une brique logicielle fournie aux développeurs d'applications mobiles, pour la génération des clés, l'activation du moyen d'authentification et l'implémentation de fonctions d'authentification et de signature. Le produit permet donc à un usager de s'authentifier au travers d'une application mobile l'intégrant, installée sur son téléphone, et s'interfaçant avec le serveur.

Il offre un cadre sécurisé pour activer, utiliser et révoquer un moyen d'authentification par la mise en œuvre :
- d'un protocole d'échange de clés ;
- d'un mécanisme de signature ;
- de services REST.

La solution offre une authentification à deux facteurs par :
- la possession d'un téléphone hébergeant l'application mobile intégrant le "MobileID Authenticator SDK" ;
- la connaissance d'un code confidentiel.

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	MobileID Authenticator SDK pour iOS
Numéro de la version évaluée	Version 2.0.12

Le produit MobileID Auhtenticator SDK pour iOS se base majoritairement sur le SDK *opensource* PowerAuth en version 1.5.2.

La version certifiée du produit peut être identifiée lors de l'exécution via la commande suivante :

```
/// - Returns: current MobileIDAuthenticatorSDK version
static func sdkVersion() -> String {
    return Bundle(for: MobileIDAuthenticator.self).infoDictionary?["CFBundleShortVersionString"] as? String ?? "N/A"
}
```

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :
- la protection du code confidentiel ;
- la protection des données échangées ;
- la protection des clés et secrets ;
- la protection contre les demandes d'authentification illégitimes ;
- la protection contre les signatures illégitimes de demandes d'authentification ;
- la vérification locale du certificat présenté par le serveur de gestion d'identité.

1.2.4 *Configuration évaluée*

Dans le cadre de l'évaluation, les éléments suivants, correspondant ou intégrant le produit identifié au chapitre 1.2.2, ont été livrés à l'évaluateur :
- le code source du SDK ;
- le package IPA de l'application de démonstration MobileID Authenticator intégrant le SDK ;
- le code source de l'application de démonstration MobileID Authenticator.

Bien que l'évaluateur ait utilisé tous ces éléments pour son analyse, la plupart des tests ont été joués sur le SDK intégré à l'application de démonstration.
En effet, cette configuration, 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 poste Debian 10 ayant le rôle de serveur d'authentification ;
- un Mac OS Catalina (10.15.7) client utilisé par l'évaluateur pour des tests ;
- un iPhone 8 iOS 14.3 avec l'application MobileID Authenticator ;
- un iPhone 6 iOS 12.4.9 « jailbreaké » avec l'application MobileID Authenticator.

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 B.

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'étant pas une application autonome, il ne peut pas être installé indépendamment d'une application. L'utilisateur final téléchargera une application qui utilise le SDK depuis l'*Apple Store*.

Pour l'intégrateur, le SDK est fourni sous forme de librairie binaire qui doit être intégrée dans l'environnement de 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'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 le code source de l'intégralité du produit.

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

Des vulnérabilités publiques existent sur les briques logicielles tierces du produit, mais se sont révélées inexploitables pour le niveau d'attaquant considéré dans le contexte défini par la cible de sécurité [CDS]

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 *Analyse de la facilité d'emploi*

2.3.7.1 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.

2.3.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour l'utilisateur. Enfin, la documentation [GUIDES] permet aux développeurs utilisant le produit de connaître les bonnes pratiques en termes de sécurité.

2.3.7.3 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. Il en ressort que le produit utilise le générateur d'aléa du système d'exploitation, 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 « MobileID Authenticator SDK pour iOS, Version 2.0.12 », 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]	Cible de sécurité – *MobileId Authenticator SDK* pour iOS Référence : MOBILEID_AUTH_SDK_IOS_SEC_TARGET ; Version : 1.5 ; Date : 26 juillet 2021.
[RTE]	Rapport Technique d'Evaluation CSPN – Produit MobileId Authenticator SDK pour IOS – version 2.0.12 ; Référence : CSPN-RTE-MOBILEID_AUTH_SDK_IOS-DR-1.02 ; Version : 1.02 ; Date : 27 juillet 2021. Expertise des mécanismes cryptographiques – MobileID Auth SDK Android verion 2.0.1 et iOS version 2.0.12 ; Référence : CSPN-CRY-MobileID Auth SDK Android v2.0.1 et iOS v2.0.12-DR-1.01 ; Version : 1.01 ; Date : 25 juin 2021.
[GUIDES]	Guide d'intégration – Mobile ID Authenticator SDK pour iOS Référence : MOBILEID_AUTH_SDK_INTEG_IOS ; Version : 1.1 ; Date : 31 mai 2021. Présentation des fonctionnalités et exigences pour intégration – Mobile ID Authenticator SDK Référence : MOBILEID_AUTH_SDK_INTEG_FUNC_DESCR ; Version : 1.1 ; Date : 18 juin 2021.

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.