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-2020/30

Olvid

Version 0.8.2 pour iOS

Fait le 18 septembre 2020

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-2020/30**
Nom du produit **Olvid**
Référence/version du produit **Version 0.8.2 pour iOS**
Catégorie de produit **Messagerie sécurisée**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Olvid** 9 rue Charlot 75003 Paris, France
Développeur **Olvid** 9 rue Charlot 75003 Paris, France
Centre d'évaluation **SYNACKTIV** 5 boulevard Montmartre 75002 Paris, France
Fonctions de sécurité évaluées Authentification des utilisateurs Authentification des échanges Chiffrement des messages et des pièces jointes Chiffrement des sauvegardes du carnet de contact
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 « Olvid, Version 0.8.2 pour iOS » développé par Olvid.

La solution Olvid est une messagerie instantanée, sur téléphone mobile, permettant un échange de messages entre deux ou plusieurs contacts, avec un chiffrement de bout en bout. Elle s'appuie sur un serveur dont le rôle est uniquement la mise en relation de messages entre les contacts.

Quant à l'application, elle est disponible pour les systèmes d'exploitation mobiles *iOS* et *Android*. Ce présent certificat ne concerne que la version *iOS* de l'application.

La figure ci-dessous illustre le fonctionnement du produit.

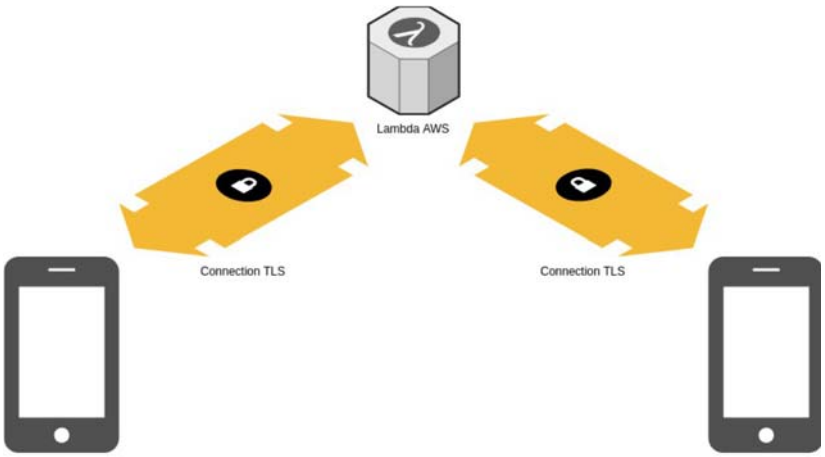

Figure 1 - Fonctionnement du Produit.

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	Olvid
Numéro de la version évaluée	0.8.2, pour la plateforme *iOS*
SHA 256 de l'application	36de819974d9238981456ed708a0e89a34b7ee74c41d62f9f5305fd7cec263d2

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

- au travers de l'application en naviguant dans la section « A propos » (voir Figure 2) ;
- au travers des réglages du téléphone, puis dans l'application *Olvid* (voir Figure 3).

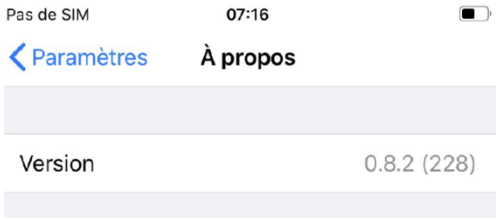

Figure 2 – Version de l'application depuis Olvid

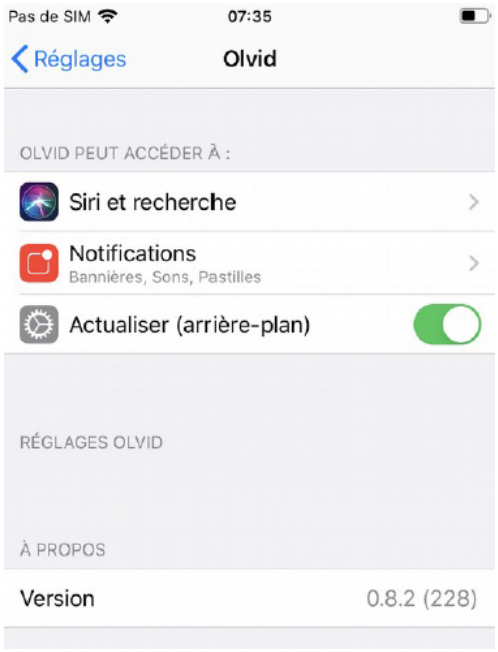

Figure 3 - Version de l'application depuis les réglages du téléphone

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'authentification des utilisateurs ;
- l'authentification des échanges ;
- le chiffrement des messages et des pièces jointes ;
- le chiffrement des sauvegardes du carnet de contact.

1.2.4 *Configuration évaluée*

L'application a été installée depuis l'*App Store* d'APPLE en version 0.8.2.

Les téléphones suivants constituent les plateformes de tests utilisées par le CESTI :

- iPhone 11, avec iOS 13.4.1 ;
- iPhone 8, avec iOS 13.3 ;
- iPhone 7, avec iOS 13.2.3.

Le choix de téléphones a été motivé par le fait de pouvoir désactiver temporairement les sécurités d'*iOS* pour les besoins d'analyse au travers du *jailbreak* CHECKRA1N.

Le serveur ne fait pas partie du périmètre de l'évaluation.

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*

L'application a été installée depuis l'*App Store* d'APPLE.

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

Néant.

2.3.1.3 Durée de l'installation

Néant.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents (code source, Preuve du protocole de *Trust Establishment*) dans le cadre de cette évaluation.

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité du produit. L'analyse a été effectuée manuellement et 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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré.

2.3.7 *Accès aux développeurs*

Le CESTI a eu accès au développeur pendant l'évaluation afin d'aborder les spécifications cryptographiques et pour répondre aux questions sur l'application.

2.3.8 *Analyse de la facilité d'emploi*

2.3.8.1 Cas où la sécurité est remise en cause

L'évaluateur a identifié un cas où la sécurité de la TOE peut être remise en cause. Il est en effet possible d'avoir des homonymes au sein de son propre carnet d'adresse, mais avec la possiblité pour l'utilisateur de donner un surnom au contact.

Une deuxième remarque a été faite concernant la possibilité de mise en relation des contacts par un tiers (voir section 2.2.4 de [CDS]). Dans ce cas, il pourrait être possible d'introduire un tiers malveillant qui serait en pratique un homonyme d'une connaissance de l'utilisateur. Il appartient donc à l'utilisateur d'être particulièrement vigilant lors d'une mise en relation par un tiers et, plus généralement, lorsqu'il ajoute un contact.

2.3.8.2 Avis d'expert sur la facilité d'emploi

L'application est simple d'utilisation et intuitive. Aucune action incomprise ou mal réalisée par un utilisateur légitime ne met en péril la sécurité de l'application.

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 pour le niveau d'attaquant visé.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. Il en ressort que le produit utilise les briques logicielles du système d'exploitation, qui elles n'ont pas fait l'objet d'une analyse au titre de cette évaluation.

Cependant le retraitement cryptographique de l'aléa généré implémenté par le produit a 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 pour le niveau d'attaquant visé.

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 « Olvid, version Version 0.8.2 pour iOS » 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], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, la recommandation suivante.

Afin de garantir l'utilisation sécurisée du produit (voir section 2.3.8.1), il est recommandé à l'utilisateur d'être vigilant quant à l'introduction d'un contact par un tiers. Ceci peut résulter en la création d'homonymes malveillants. En cas de doute il est recommandé à l'utilisateur de vérifier l'origine de la relation de confiance *Trust Origine* du contact.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de Sécurité CSPN Olvid Version : 2.2 ; Date : 05 avril 2020.
[RTE]	Rapport technique d'évaluation OLVID Version : 1.1 ; Date : 24 aout 2020.

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.