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-2020/36

SEALD-SDK

Goatee, version 2.1

Paris, le 4 décembre 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-2020/36**
Nom du produit **SEALD-SDK**
Référence/version du produit **Goatee, version 2.1**
Catégorie de produit **Communication sécurisée**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **SEALD SAS** 13 rue Georges-Bizet 78380 Bougival, France
Développeur **SEALD SAS** 13 rue Georges-Bizet 78380 Bougival, France
Centre d'évaluation **SYNACKTIV** 5 boulevard Montmartre 75002 Paris, France
Fonctions de sécurité évaluées Chiffrement des documents Chiffrement des clés symétriques de chiffrement et d'intégrité Gestion d'une base de données de chaîne de signatures
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 « SEALD-SDK, Goatee, version 2.1 » développé par SEALD SAS.

Ce produit est une solution permettant de chiffrer n'importe quel fichier ou *email* à destination de personnes possédant la solution ou non. Une fois sécurisé par SEALD, le fichier ou l'*email* peut être transféré par n'importe quel moyen (*email*, *FTP*, *SSH*, plateforme de téléchargement, *P2P*, clé *USB*,…). Il transitera dans un format propriétaire, journalisant toutes les actions effectuées sur celui-ci (tentatives d'ouverture, ouvertures avec succès, échecs d'ouverture, …), même si le destinataire ne possède pas la solution SEALD.

Dans le cadre de cette évaluation, SEALD prend la forme d'une bibliothèque *NodeJS* pouvant être intégrée dans un projet afin de disposer de fonctions d'échange sécurisé de fichiers et de messages. Cette bibliothèque est nommée SEALD-SDK et est chargée :

- de la génération de bi-clés de signature et de chiffrement ;
- du renouvellement de ces bi-clés ;
- du chiffrement et du déchiffrement de fichiers et d'*email* ;
- de maintenir une base de données locale contenant de chaînes de signatures et les clés publiques de signature et de chiffrement des destinataires connus.

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	SEALD-SDK
Numéro de la version évaluée	Goatee, version 2.1

La version du produit est spécifiée dans son fichier package.json.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le chiffrement des documents ;
- le chiffrement des clés symétriques de chiffrement et d'intégrité ;
- la gestion d'une base de données de chaînes de signatures.

La génération de bi-clés n'a pas été évaluée.

1.2.4 *Configuration évaluée*

SEALD-SDK est une bibliothèque *NodeJS* pouvant être intégrée dans un projet afin de fournir des fonctionnalités d'échange sécurisé de fichiers et de messages. L'utilisation du produit requiert la création d'un client *NodeJS* appelant les API de SEALD-SDK.

Le produit est architecturé dans un mode client-serveur. L'environnement prévu se compose donc de deux parties :

- le client utilisant la bibliothèque SEALD-SDK;
- le serveur *Beard* hébergé par la société SEALD qui ne rentre pas dans le cadre de cette évaluation.

Le serveur Beard fournit l'accès aux informations suivantes :

- l'annuaire des utilisateurs ;
- les différentes chaînes de signatures (*sigchain*) ;
- les clés symétriques des messages, chiffrées par les clés publiques des destinataires.

L'évaluation porte sur la bibliothèque SEALD-SDK configurée avec les options suivantes :

- *strict-mode* activé ;
- api-url : URL donnée par les équipes de Seald, correspondant au serveur *Beard* ;
- *keySize* : 4096 ;
- sscrypto : le module 'sscrypto/node' de la bibliothèque sscrypto en version 0.4.2.

La plateforme de test est constituée d'un ordinateur *desktop* sous le système d'exploitation *Debian 10 buster*.

La plupart des tests a été jouée sur une application de démonstration : le client Seald-Cli. Cette application a été jugée être une utilisation 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 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.

L'utilisation de la bibliothèque SEALD-SDK nécessite l'installation d'un exécuteur JavaScript. À ce titre les composants logiciels suivant doivent être présents sur le système :

- Node.js 12.16.3 LTS ;
- Npm 6.14.1.

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

Dans le cadre de l'évaluation, l'installation retenue pour la TOE est celle fournie par le projet *goatee-cli* dans un fichier *Dockerfile*. Le SDK ainsi que ses dépendances sont installés à l'aide de la ligne de commande suivante :

```
$ npm i logger-0.2.1.tgz follicle-1.1.2.tgz hairless-template-1.0.0.tgz hairless-0.7.0.tgz goatee-2.1.0.tgz
```

Pour l'installation du client fourni pour tester le SDK, la commande suivante a été utilisée :

```
$ npm run build-bin-prod
```

2.3.1.3 Durée de l'installation

L'installation ne prend que quelques minutes.

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.

La documentation fournie permet d'instancier le composant principal du SDK dans de bonnes conditions de sécurité. La documentation d'utilisation décrit clairement les limitations imposées par l'utilisation du *strictMode.* Néanmoins les paramètres choisis par l'utilisateur, chargé d'intégrer cette bibliothèque SEALD-SDK, peuvent altérer le niveau de protection fourni par le SDK. Une lecture attentive de la documentation et des paramètres à utiliser pour le cadre d'utilisations similaires à celle de l'évaluation est nécessaire afin de fournir un niveau de sécurité équivalent.

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

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

Néanmoins, il existe des vulnérabilités connues pour les dépendances du produit mais elles ne sont pas exploitables dans le contexte d'utilisation du SDK.

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

Les risques identifiés lors de l'évaluation entraînent des recommandations d'usage pour l'utilisateur (voir chapitre 3.2).

2.3.8.2 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 un utilisateur ayant des connaissances de base en cryptographie et sécurité des systèmes d'exploitation.

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 a identifié des non-conformités au RGS (voir [RGS]) mais qui ne remettent pas en cause la sécurité du produit.

Aucune vulnérabilité exploitable n'a été découverte.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé, il en ressort qu'il repose sur la fonction *RAND_bytes* de la bibliothèque *OpenSSL*.

Aucune vulnérabilité exploitable n'a été découverte sur le générateur d'aléa.

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 « SEALD-SDK, version Goatee, version 2.1 » 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, les recommandations du « Guide d'utilisation sécurisée de Sead-SDK» ([GUIDES]), notamment :

- appliquer la méthode proposée pour le chiffrement des clés privées ;
- vérifier le condensat du dernier bloc des chaînes de signatures des destinataires ;
- ne pas redéfinir certaines méthodes/variables comme la fonction *overrideMassReencrypt.*

ANNEXE A. Références documentaires du produit évalué

[CDS]	Seald - Cible de Sécurité CSPN ; Version : 1.1 ; Date : 17 juillet 2020.
[RTE]	Seald – Rapport d'audit sécurité – Rapport Technique d'Évaluation Version : 1.1 ; Date : 7 octobre 2020.
[GUIDES]	Guide d'utilisation sécurisée de Sead-SDK Version : 1.0 ; Date : 6 octobre 2020. Fichier d'installation de Seald-SDK Référence : 01-Seald-SDK-Installation.md. Fichier d'installation de Seald-CLI Référence : 02-Seald-CLI-Installation.md. Guide de Seald-CLI Référence : Goatee-CLI.md. Documentation HTML de l'API Goatee.

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.