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-2021/18

YubiKey 5 Series

Version firmware 5.4.2

Paris, le 13 juillet 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-2021/18**
Nom de la gamme de produits **YubiKey 5 Series**
Référence/version de la gamme de produits **Version firmware 5.4.2**
Catégorie de la gamme de produits **Matériel et logiciel embarqué**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **YUBICO AB** Kunhsgatan 44, 2nd floor SE-111 35 Stockholm, Suède
Développeur **YUBICO AB** Kunhsgatan 44, 2nd floor SE-111 35 Stockholm, Suède
Centre d'évaluation **SERMA SAFETY & SECURITY** 14, rue Galilée, CS 10071 33608 Pessac Cedex, France **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Génération d'aléa Authentification utilisateur Stockage sécurisé Opérations cryptographiques Vérification de la présence utilisateur au travers du capteur tactile
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 Les produits

1.1 Présentation des produits

Les produits évalués correspondent à la gamme « YubiKey 5 Series » développée par YUBICO AB, et exécutant la version 5.4.2 du *firmware*.

La YubiKey est un périphérique d'authentification matérielle protégeant l'accès aux services en ligne, aux ordinateurs ou aux réseaux. Une fois insérée dans l'équipement informatique de l'utilisateur, la clé permet une authentification à double facteurs (*two-factor authentication* – 2FA), ou à multiple facteurs (*multi-factor authentication* – MFA) ou le stockage de mots de passe.

Le périphérique supporte les mots de passe à usage unique (*One Time Password*, OTP), le chiffrement et l'authentification par clé publique, OpenPGP et les protocoles FIDO *Universal 2nd Factor* (U2F) et FIDO2. Pour cela, elle s'appuie sur le microcontrôleur sécurisé d'INFINEON, le M7893 B11, certifié EAL 6+, faisant parti de la famille des contrôleurs SLE78.

La figure ci-dessous explicite l'architecture des produits.

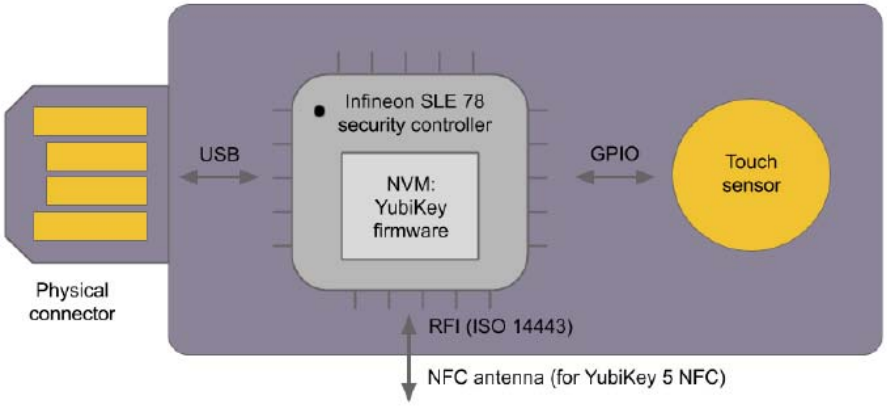

Figure 1 - Architecture des produits.

1.2 Description des produits évalués

La cible de sécurité [CDS] définit les produits évalués, leurs fonctionnalités de sécurité évaluées et leur environnement d'exploitation.

1.2.1 *Catégorie des produits*

☐	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 de la gamme de produits*

Gamme de produits	
Nom de la gamme de produits	YubiKey 5 Series
Numéro de la version évaluée	5
Version du *firmware*	5.4.2
Microcontroller Unit (MCU)	INFINEON M7893 B11
Version du *firmware* du MCU	78.019.03.4
Version de la cryptolib du MCU	1.03.006

Le logiciel « YubiKey Manager » permet d'identifier la version du *firmware,* ainsi que le numéro de série, du produit YubiKey. L'utilisateur peut ainsi comparer ces résultats avec le numéro de série gravé sur la clé YubiKey.

La gamme de produits comprend les six périphériques suivants :

- YubiKey 5 NFC ;
- YubiKey 5 Nano ;
- YubiKey 5C ;
- YubiKey 5C NFC ;
- YubiKey 5C Nano ;
- YubiKey 5Ci.

Tous contiennent le même microcontrôleur M7893 B11 et ils diffèrent dans les interfaces physiques exposées : USB-A, USB-C et/ou *Lightning*. En accord avec la [NOTE-21] les tests ont été faits sur des produits de référence.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la génération d'aléa ;
- l'authentification utilisateur ;
- le stockage sécurisé[1] ;
- les opérations cryptographiques[1] ;
- la vérification de la présence utilisateur au travers du capteur tactile.

1.2.4 *Configuration évaluée*

La configuration du produit est celle décrite dans la section 3.1 de la cible de sécurité [CDS], à savoir :

- le capteur tactile doit être actionné pour la génération d'OTP, l'authentification FIDO U2F et FIDO2 ;
- le capteur tactile doit être actionné et l'utilisation d'un PIN est exigée pour les authentifications FIDO2 ;
- le nombre d'essai du PIN doit être fixé à la valeur par défaut pour le *Personal Identity Verification-compatible* (PIV) et OpenPGP ;
- la longueur du mot de passe doit être de 20 octets pour OATH ;
- la longueur du *user access code* pour chaque *credential* doit être de 16 octets pour YubiHSM Auth.

[1] Fonction de sécurité apportée par le M7893 B11.

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

L'installation a été faite en suivant les guides du développeur, [GUIDES].

2.3.1.3 Durée de l'installation

La durée d'installation est relativement courte.

2.3.1.4 Notes et remarques diverses

Néant.

2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents du développeur dans le cadre de cette évaluation. Ces documents sont accessibles sur le site du développeur, voir [GUIDES].

Le produit se basant sur le MCU M7893 B11 d'INFINEON, le CESTI a vérifié que le développement logiciel prenait bien en compte les recommandations du guide accompagnant le MCU.

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques 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.

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 *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.

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 mis en œuvre 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.

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 la gamme de produits « YubiKey 5 Series, Version firmware 5.4.2 » 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.

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]	*CSPN Security Target YubiKey 5 Series* Version : 1.3.1 ; Date : 23 avril 2021.
[RTE]	*Evaluation Technical Report - project ARIANE2* Référence : ARIANE2_ETR_CSPN_v1.0 ; Version : 1.0 ; Date : 15 mai 2021.
[GUIDES]	Guide d'utilisateur *YubiKey Manager* https://developers.yubico.com/yubikey-manager-qt/ *YubiKey Manager (ykman) CLI & GUI Guide* https://docs.yubico.com/software/yubikey/tools/ykman/ Guide d'installation en mode CSPN *CSPN Mode Configuration Yubikey 5 Series* Version : 1.1.

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.
[NOTE-21]	Note d'application - Méthodologie pour l'évaluation d'une gamme de produits, référence ANSSI-CC-NOTE-21, version 1.0, 1er février 2017.