Cible de sécurité CSPN

Winkeo FIDO2

Statut du document

Auteur	MOUILLE Stéfane, CLR Labs
Version actuelle	1.5
Date	11/03/2022

	Développeurs	**Commanditaire**	**Evaluateur**
Organisme(s)	NEOWAVE	NEOWAVE	CEA-LETI

Diffusion

Nom	**Organisation**
BERNARD Bruno	NEOWAVE
BOUCHY Frédéric	NEOWAVE
COMMERCIAL Sean	NEOWAVE
CHUZEL Julie	ANSSI
Centre de Certification National (CCN)	ANSSI
LEMAITRE Benoit	CEA-LETI
HERVE Guillaume	CEA-LETI
PUJOL Hubert	CLR Labs
MOUILLE Stéfane	CLR Labs

Sommaire

1. Synthèse

1.1. Identification de la cible de sécurité

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN [1] et d'une qualification élémentaire [2].

1.2. Identification du produit à évaluer

Catégorie	Identification
Nom commercial du produit	Winkeo FIDO2 et Winkeo-C FIDO2
Numéro de la version évaluée	1.4.9
Catégorie de produit	Identification, authentification et contrôle d'accès

1.3. Références

Code	Référence	Nom et source
[1]	CSPN_CERT	ANSSI PROCEDURE - CERTIFICATION DE SECURITE DE PREMIER NIVEAU DES PRODUITS DES TECHNOLOGIES DE L'INFORMATION 13 janvier 2020 https://www.ssi.gouv.fr/uploads/2015/01/anssi-cspn-cer-p-01-certification_de_securite_de_premier_niveau_v2.1.pdf
[2]	Qualif	ANSSI PROCESSUS DE QUALIFICATION D'UN PRODUIT(QUAL-PROD-PROCESS/1.0) 12 Janvier 2017 https://www.ssi.gouv.fr/uploads/2014/11/qual_prod_process-processus-de-qualification-d-un-produit.pdf
[3]	RGS	ANSSI Référentiel Général de Sécurité Version 1.0 du 6 mai 2010 https://www.ssi.gouv.fr/uploads/2015/09/RGSv1-0.pdf
[4]	CRYPTO	ANSSI PROCEDURE - MODALITES POUR LA REALISATION DES ANALYSES CRYPTOGRAPHIQUES ET DES EVALUATIONS DES GENERATEURS DE NOMBRES ALEATOIRES 11 février 2020 https://www.ssi.gouv.fr/uploads/2014/11/anssi-cc-cry-p-01-modalites-pour-la-realisation-des-analyses-cryptographiques-v4.0.pdf
[5]	RGS_B1	ANSSI Référentiel Général de Sécurité, version 2.0, Annexe B1 Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques Version 2.03 du 21 février 2014 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf
[6]	RGS_B2	ANSSI Référentiel Général de Sécurité, version 2.0, Annexe B2 Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques

		Version 2.00 du 8 juin 2012 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf
[7]	RGS_B3	ANSSI Référentiel Général de Sécurité, version 1.0, Annexe B3 Authentification – Règles et recommandations concernant les mécanismes d'authentification Version 1.0 du 13 janvier 2010 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B3.pdf
[8]	SOG_IS_CRYPTO	SOG-IS Crypto Working Group SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms Version 1.1, June 2018 https://www.sogis.eu/
[9]	ST_MS6003	Wisekey MS6003 Security Target-Lite - TPG0235A 10 March 2020 https://www.ssi.gouv.fr/uploads/2020/04/anssi-cible-cc-2020_20en.pdf
[10]	RC_MS6003	ANSSI Rapport de certification ANSSI-CC-2020/20 - MS6003 (Rev C) 16 avril 2020 https://www.ssi.gouv.fr/uploads/2020/04/anssi-cc-2020_20fr.pdf
[11]	FIDO_SECREF	FIDO Security Reference FIDO Alliance, Proposed Standard, 11 April 2017 https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-security-ref-v1.2-ps-20170411.html
[12]	FIDO_CRYPTO	FIDO Authenticator - Allowed Cryptography List FIDO Alliance, 29 June 2018 https://fidoalliance.org/specs/fido-security-requirements-v1.2-2018/fido-authenticator-allowed-cryptography-list-v1.0-wd-20180629.html
[13]	FIDO_U2F_IMPL	FIDO U2F Implementation Considerations - FIDO Alliance, Proposed Standard, 11 April 2017 https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-implementation-considerations-v1.2-ps-20170411.html
[14]	FIDO_METADATA	FIDO Authenticator Metadata Requirements - FIDO Alliance, 16 November 2019 https://fidoalliance.org/specs/fido-security-requirements-v1.0-fd-20170524/fido-authenticator-metadata-requirements_20170524.html
[15]	FIDO2	Client to Authenticator Protocol (CTAP) - Proposed Standard, January 30, 2019 https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html
[16]	PP084	Eurosmart Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, version 1.0, 19 February 2014.
[17]	FIDO_U2F	FIDO U2F Raw Message Formats - FIDO Alliance Proposed Standard 11 April 2017 https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-raw-message-formats-v1.2-ps-20170411.html
[18]	eIDAS	RÈGLEMENT (UE) No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
[19]	France connect	https://franceconnect.gouv.fr/
[20]	Guide d'administration du Token	NEOWAVE Winkeo FIDO2 Guide d'administration V1.1

[21]	Guide d'utilisation du Token	Winkeo FIDO2 Guide d'utilisation V1.2

1.4. Abréviations et terminologie

Les spécifications FIDO U2F et FIDO2 n'utilisent pas les mêmes termes pour faire référence aux mêmes éléments de données. L'équivalence entre les termes est donnée dans le tableau suivant :

Termes FIDO U2F	Termes FIDO2
Key Pair, User Public Key	Credential Key Pair
Key Handle	Credential Id

Les termes FIDO2 seront de préférence utilisés dans ce document.

1.5. Glossaire

Authentificateur, second facteur	Un authentificateur FIDO qui agit uniquement comme un second facteur. Les authentificateurs de second facteur nécessitent toujours de fournir une clé unique avant de répondre à une commande Sign. Ils peuvent ou non avoir une méthode de vérification des utilisateurs. On suppose que ces authentificateurs peuvent ou non avoir un matcher interne.
Attestation de l'authentificateur	Processus de communication d'une assertion cryptographique à une partie de confiance selon laquelle une clé présentée lors de l'enregistrement de l'authentificateur a été créée et protégée par un authentificateur authentique avec des caractéristiques vérifiées.
Client	Ce terme est utilisé « en contexte » et peut faire référence à un client FIDO ou à un autre type de client, par ex. un client TLS. Voir Client FIDO.
Client FIDO	Il s'agit de l'entité logicielle qui traite les messages du protocole U2F et FIDO2 sur le dispositif utilisateur FIDO. Les clients FIDO

	peuvent prendre l'une des deux formes suivantes : - Un composant logiciel implémenté dans un agent utilisateur (navigateur Web ou application native). - Un logiciel autonome partagé par plusieurs agents utilisateurs (navigateurs Web ou applications natives).
Compteur de signature	Un compteur à croissance monotone maintenu par l'authentificateur. Il est augmenté à chaque utilisation de la clé UAuth.priv. Cette valeur peut être utilisée par le serveur FIDO pour détecter les authentificateurs clonés.
Confirmation de la transaction	Une opération dans le protocole FIDO qui permet à une partie de confiance de demander qu'un client FIDO, et un authentificateur avec les capacités appropriées, d'afficher certaines informations à l'utilisateur, de demander à l'utilisateur de s'authentifier localement auprès de son authentificateur FIDO pour confirmer les informations et de fournir une preuve de possession du matériel de clé préalablement enregistré et une attestation de confirmation à la partie utilisatrice.
Découverte	Phase d'un protocole FIDO dans laquelle une partie utilisatrice est en mesure de déterminer la disponibilité des capacités FIDO sur l'appareil du client, y compris les métadonnées sur les authentificateurs disponibles.
Désinscription	Une phase d'un protocole FIDO dans laquelle une partie utilisatrice demande à un authentificateur FIDO d'oublier un élément spécifié (ou la totalité) du matériel de clé géré localement associé à un compte de partie utilisatrice spécifique, au cas où ces clés ne seraient plus considérées comme valides par la partie utilisatrice.
Facteur de vérification	Le moyen spécifique par lequel la vérification de l'utilisateur local est effectuée. Par

	exemple : empreinte digitale, empreinte vocale ou code PIN.
Inscription	Une opération de protocole FIDO dans laquelle un utilisateur génère et associe un nouveau matériel clé à un compte chez la partie utilisatrice, sous réserve de la politique définie par le serveur, et d'une attestation acceptable pour que l'authentificateur et l'enregistrement correspondent à cette politique.
Nom d'utilisateur	Chaîne lisible par l'homme identifiant le compte d'un utilisateur chez une partie de confiance.
Partie utilisatrice (Relying Party)	Un site Web ou une autre entité qui utilise un protocole FIDO pour authentifier directement les utilisateurs (c'est-à-dire qui effectue une authentification d'entité homologue). Notez que si FIDO est composé de protocoles de gestion d'identité fédérés (par exemple, SAML, OpenID Connect, etc.), le fournisseur d'identité jouera également le rôle d'une partie de confiance FIDO.
Serveur FIDO	Logiciel serveur généralement déployé dans l'infrastructure de la partie de confiance qui répond aux exigences des serveurs des protocoles U2F et FIDO2.
Token	Dans FIDO U2F et FIDO2, le terme Token est souvent utilisé pour désigner ce qu'on appelle un authentificateur.
Universal Second Factor (U2F)	Le protocole FIDO et la famille d'authentificateurs qui permettent à un service cloud d'offrir à ses utilisateurs la possibilité d'utiliser un dispositif de second facteur basé sur des normes ouvertes, facile à utiliser et hautement sécurisé pour l'authentification. Le protocole s'appuie sur le serveur pour connaître l'utilisateur avant de déclencher l'authentification.
Utilisateur	Utilisateur de la partie utilisatrice et propriétaire de l'authentificateur FIDO.
Vérification de la présence de l'utilisateur	La vérification de la présence de l'utilisateur dans l'authentificateur vérifie qu'un utilisateur

	est présent dans l'authentificateur et accepte une opération d'authentification générique.
Vérification de l'utilisateur	Processus par lequel un authentificateur FIDO autorise localement l'utilisation du matériel clé, par exemple via une touche, un code PIN, une correspondance d'empreinte digitale ou autre biométrique.

2. Argumentaire

2.1. Description générale du produit à évaluer

Le produit à évaluer (Token) selon la méthodologie de certification de premier niveau, et à qualifier au niveau élémentaire par l'ANSSI, est un Token d'authentification électronique qui se présente sous la forme d'une clé USB (avec bouton de type capacitif, une led et un Secure Element certifié [10]) qui est conforme aux spécifications FIDO U2F [17] et FIDO2 [15]. Le Token est nommé un « authenticator » dans le langage FIDO.

Les spécifications FIDO décrivent un protocole d'authentification électronique basé sur un schéma à base de cryptographie asymétrique entre le serveur FIDO et le Token.

Dans le but de couvrir le maximum de cas d'usages et de fournir une compatibilité ascendante avec les infrastructures existantes de type FIDO U2F [13] tout en répondant aux nouveaux besoins couverts par la version FIDO2 [15], le Token dispose donc de deux applications répondant aux deux différentes versions de FIDO : FIDO U2F [17] et FIDO2 [15]

Le Token est composé de trois parties :

NEOWAVE a développé 2 produits quasi identiques appelés Winkeo-C FIDO2 et Winkeo FIDO2. Seul le design et la connectique sont différents. Le produit Winkeo-C FIDO2 utilise un connecteur USB type C, le produit Winkeo FIDO2 utilise un connecteur USB type A. Dans les 2 produits, on retrouve exactement les mêmes caractéristiques ci-dessous :

Une première partie - physique :

- Le boîtier ;
- Le bouton de type capacitif ;
- Une led (RGB) ;
- Le connecteur USB.

Une deuxième partie - électronique :

- Une carte électronique ;
- Une puce de type « Secure Element » de la société Wisekey et certifiée EAL5+ AVA_VAN.5 sur le profil de protection PP BSI 084 édité par Eurosmart et disposant d'une certification de la part de l'ANSSI [10]. Cette puce génère les éléments aléatoires, qui sont retraités par le logiciel embarqué (voir ci-dessous), afin de créer les clés privées aux applications FIDO (FIDO U2F et FIDO2) du Token.

Une troisième partie- logiciels embarqués :

- Un logiciel embarqué qui comprend les fonctions génériques aux spécifications FIDO U2F et FIDO2, ce logiciel est non visible par l'environnement extérieur ;
- Un logiciel embarqué dédié aux fonctions spécifiques à la spécification FIDO U2F ;
- Un logiciel embarqué dédié aux fonctions spécifiques à la spécification FIDO2.

Dans le document les termes « Token » ou « Token Winkeo FIDO2 » font référence aux 2 produits Winkeo-C FIDO2 et Winkeo FIDO2.

2.2. Description de l'utilisation du produit à évaluer

Les spécifications FIDO répondent à l'enjeu de créer un standard international et interopérable pour renforcer le niveau de sécurité de l'authentification électronique.

Ce renforcement du niveau de sécurité passe par l'utilisation d'un Token conforme aux spécifications FIDO :

- Soit en complétant le couple Login/Password par l'utilisation d'un second facteur d'authentification conforme aux spécifications FIDO U2F [17] ;
- Soit en réalisant une authentification forte à deux facteurs : ce que je possède (le Token) et ce que je connais (PIN utilisateur du Token), ce qui correspond aux spécifications FIDO2 [15].

Les deux spécifications FIDO ont été conçues à des périodes différentes.

Le produit à évaluer répond à deux utilisations principales

Utilisation numéro 1 : Authentification électronique forte pour :

- Les services en ligne équipés de serveurs FIDO ;
- Les autorités d'émission de certificats qualifiés désirant mettre en place une solution de serveur de signature (règlement eIDAS [18]) et qui désirent avoir une authentification forte au server de signature ;
- Les fournisseurs d'identité numérique désirant être qualifiés au niveau substantiel dans le système FranceConnect [19]).

Utilisation numéro 2 : Mode off-line : mode de fonctionnement « off-line » cette fonctionnalité n'est disponible que sur l'application Winkeo FIDO2. Cette utilisation n'est pas incluse dans la cible d'évaluation.

Cycle de vie défini par le protocole FIDO

Le cycle de vie est défini en cinq étapes :

<u>Pre-Personnalisation :</u>

1. Création et chargement des Certificats d'attestation (format X509) et des clés privées associées (certificat et clé privée par batch et non uniques au Token) ; les modalités de choix de l'autorité de certification, les processus et éléments techniques du chargement sont décrits dans le Guide d'administration du Token [20]. De même, la taille du batch de clés privées est définie par l'administrateur du Token conformément au Guide d'administration du Token [20].

<u>Utilisation par l'utilisateur final :</u>

2. Enregistrement à des fournisseurs de services en ligne (incluant la définition de la valeur du code PIN lors du premier l'enregistrement qui le demande, il est à noter qu'il n'y a qu'une valeur de PIN pour l'application FIDO2 [15]);
3. Utilisation du Token pour réaliser une authentification électronique forte ;
4. Changement de PIN comme défini dans le protocole FIDO2 [15]), (uniquement disponible sur FIDO2), cette opération est réalisée par l'utilisateur final à sa convenance et conformément au Guide d'utilisation [21].
5. Remise à l'état initial du Token ; c'est-à-dire à l'état de sortie de pré-personnalisation (présence uniquement des clés d'attestation et certificats d'attestation, il y une vérification de l'effacement des clés pour garantir la remise à l'état initial du Token), cette remise à l'état initial du Token est réalisée grâce à la commande « authenticatorReset » de la spécification FIDO2 [15] grâce à deux appuis successifs sur le bouton conformément au Guide d'utilisation [21] ;

2.3. Description de l'environnement d'utilisation prévue

Le Token est utilisé dans un environnement composé de trois parties :

- Un ordinateur permettant la connectivité à internet ;
- Un serveur d'authentification compatible aux spécifications FIDO ;
- Un service internet (relying party) qui a besoin de gérer l'identification et l'authentification électronique pour garantir l'accès aux services qu'il propose.

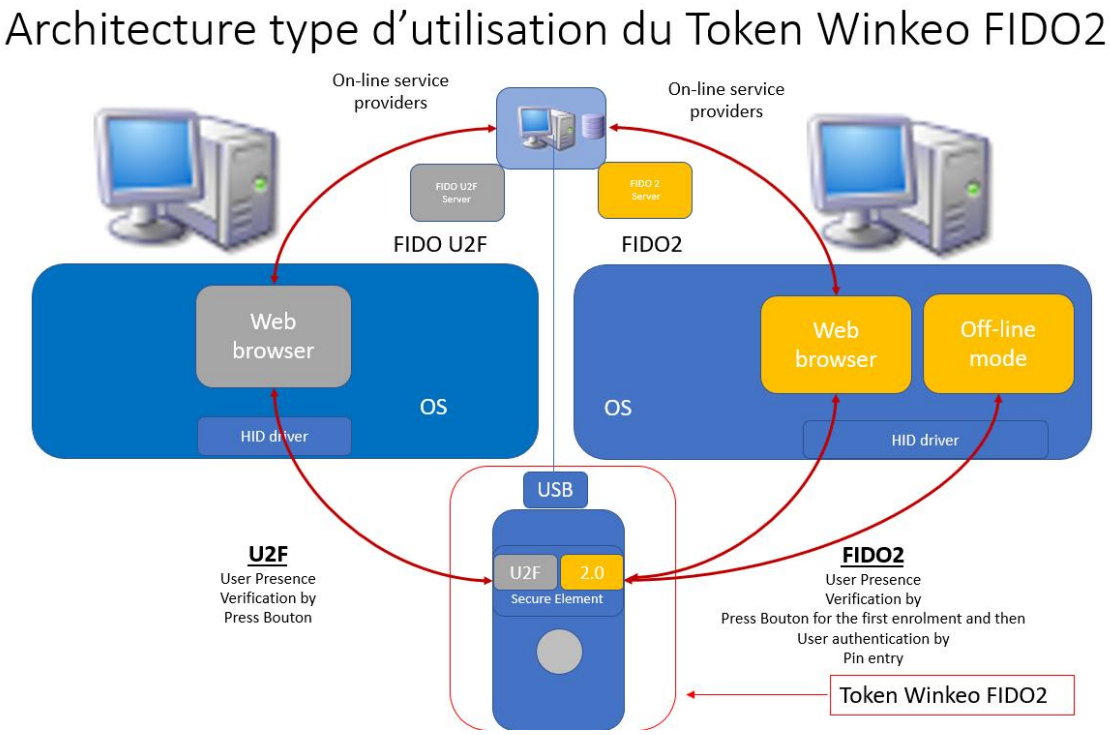

Figure 1 : architecture type d'utilisation du Token Winkeo FIDO2

2.4. Description des hypothèses sur l'environnement

Hypothèse 1 sur Le porteur final :

- Le porteur est de confiance ;
- Il préserve le secret de son code PIN, et ne le saisit pas dans des conditions où celui-ci est directement observable d'un utilisateur extérieur ;
- Il n'installe pas de programme malveillant sur son ordinateur ou destiné à débloquer l'utilisation administrateur de l'équipement.

Hypothèse 2 sur le Fabricant :

- Le fabricant est de confiance, il fournit un Token conformes aux spécifications ;
- Une clé privée d'attestation (clé de groupe) est utilisée par un nombre de Tokens suffisamment important pour garantir la non-traçabilité d'une personne, le nombre suffisant de Tokens est indiqué dans le Guide d'administration du Token [20] ;
- Il existe un processus d'import du certificat d'attestation entre le fabricant et l'autorité de certification.

Hypothèse 3 sur l'autorité de certification :

- Il existe un processus garantissant la transmission de la clé publique d'attestation du fabricant vers l'autorité de certification, ce processus est décrit dans le Guide d'administration du Token [20] ;
- Il existe un processus garantissant l'intégrité et l'authenticité lors de l'import du certificat d'attestation de l'autorité de certification vers le fabricant, ce processus est décrit dans le Guide d'administration du Token [20] ;
- Le certificat d'attestation (format X509) fourni par l'autorité de certification et installé par le fabricant est considéré authentique et intègre.

Hypothèse 4 sur le protocole FIDO (U2F et FIDO2)

- Le protocole FIDO ne comporte pas de vulnérabilité fonctionnelle liée à sa conception, aucun mécanisme ne permet la mise à jour du protocole une fois que le Token est sur le terrain.

Hypothèse 5 sur la Cryptographie

- Les algorithmes du catalogue cryptographique du SOGIS ne présentent pas de vulnérabilité connue.

Hypothèse 6 sur les Logiciels FIDO fournis par l'OS de l'ordinateur :

- Les logiciels FIDO fournis par l'OS et utilisés par le produit à évaluer sont supposés de confiance : leur intégrité est garantie et en particulier ils ne sont ni infectés, ni corrompus par des logiciels malveillants ;
- En cas de gestion de la saisie du code PIN par l'OS, il est supposé garantir la confidentialité de la saisie et de son envoi au produit à évaluer.

Hypothèse 7 sur les Serveurs FIDO :

- L'agent d'enregistrement des Serveurs FIDO est de confiance et demande l'enregistrement d'utilisateurs dont les identifiants FIDO ont été dûment vérifiés ;
- Les Serveurs FIDO utilisés par les fournisseurs de service sont de confiance et envoient des requêtes d'authentification légitimes.

2.5. Description des dépendances

Pour fonctionner correctement, le produit à évaluer est dépendant de l'ensemble des éléments de son environnement indiqués au paragraphe 2.3. Il utilise le protocole CTAPHID qui lui permet d'être reconnu par l'OS comme un périphérique FIDO. La saisie du code PIN est aussi gérée par l'OS comme défini dans FIDO2 [15].

2.6. Description des utilisateurs typiques

Les utilisateurs susceptibles d'interagir avec le produit à évaluer sont les suivants :

- Porteur final : c'est l'utilisateur final du Token qui est autorisé à l'utiliser pour réaliser l'authentification avec le serveur FIDO ;
- Administrateur du Token, il est en charge d'acheter auprès du Fabricant et de diffuser aux utilisateurs finaux les Tokens, c'est lui qui est responsable des Tokens et qui définit les paramètres de pré-personnalisation ;
- Fabricant : Il fabrique et pré-personnalise le Token ;
- Navigateur Web : une application exécutée sur le poste de travail de l'utilisateur qui agit au nom d'un utilisateur dans un système client-serveur. Il établit un canal de communication TLS avec le serveur d'applications. Il prend en charge les API JavaScript FIDO U2F et FIDO2 utilisées pour les opérations d'enregistrement et de signature ;
- Attaquant : le principal objectif de l'attaquant est d'accéder au Token ou aux services du Token de manière à lui permettre de contourner son utilisation légitime. Il le fait par exemple en essayant d'acquérir des informations secrètes (biens sensibles) stockées sur le Token.

2.7. Description du périmètre de l'évaluation

L'évaluation porte sur l'intégralité des fonctionnalités du Token FIDO2 : applications Winkeo U2F et Winkeo FIDO2, logiciel embarqué qui supporte les fonctions génériques aux deux applications Winkeo U2F et Winkeo FIDO2, le Secure Element certifié par l'ANSSI [10] MS6003 rev C et son connecteur USB à l'exclusion du Mode off-line (utilisant l'extension hmacSecret) de l'application Winkeo FIDO2 : mode de fonctionnement « off-line »

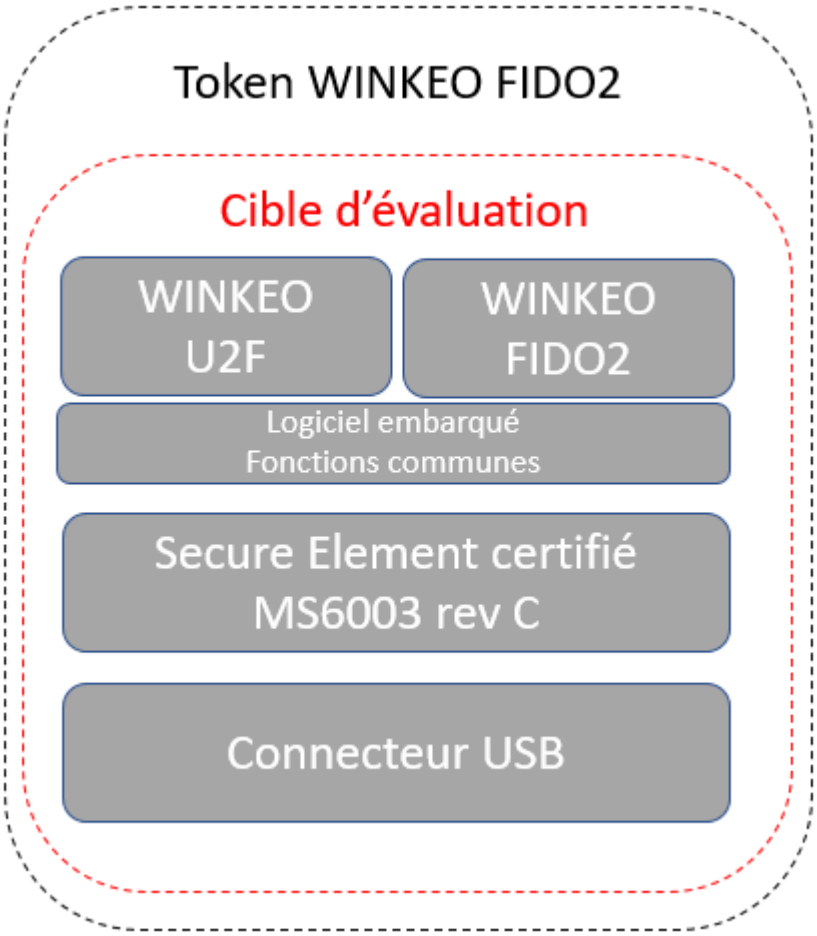

Figure 2 : cible d'évaluation

3. Description de l'environnement technique de fonctionnement

3.1. Protocoles FIDO

Le but de ce chapitre est de décrire les commandes des protocoles FIDO qui interagissent avec les biens primaires du Token.

Protocole FIDO U2F

Enregistrement (commande U2F REGISTER)

Le Token reçoit : Un identifiant d'application (Application Parameter)
Le Token effectue alors les opérations suivantes :

- Il crée une paire de clés du Credential (Credential Private Key, Credential Public Key) ;
- Il calcule le Credential Id en utilisant l'Application Parameter et des informations relatives à la paire de clés du Credential.

Le Token retourne :

- Le Credential Id (Key Handle);
- La clé publique du Credential (Credential Public Key) ;
- Une signature calculée avec l'Attestation Private Key permettant au serveur FIDO d'authentifier le Credential Id et la Credential Public Key ;
- Le certificat d'attestation (Attestation Certificate) permettant au serveur FIDO d'authentifier l'Attestation Private Key.

Authentification (commande U2F_AUTHENTICATE)

Le Token reçoit :

- Un identifiant d'application (Application Parameter) ;
- Un Credential Id.

Le Token effectue alors les opérations suivantes :

- Il vérifie l'authenticité du Credential Id ;
- Il identifie la Credential Private Key associée au Credential Id.

Le Token retourne :

- Un compteur de signature ;
- Une signature calculée avec la Credential Private Key (cette signature pouvant être vérifiée par le serveur FIDO en utilisant la Credential Public Key retournée par la commande U2F_REGISTER).

Protocole FIDO2

Le Token supporte :

- Les options clientPIN et residentKey ;
- L'extension hmacSecret (cette extension est hors du périmètre de la cible d'évaluation).

Les paragraphes suivants décrivent les fonctionnalités principales des commandes FIDO2. Le lecteur pourra se référer à la spécification FIDO2 [15] pour plus de détails.

Enregistrement (commande authenticatorMakeCredential)

Le Token reçoit :

- Un identifiant d'application (rpId) ;
- Optionnellement, une information de vérification du PIN (pinAuth) ;
- Optionnellement, une information indiquant que l'option « residentKey » est activée, le nombre maximum de clés disponibles et leur mode de gestion (dont leur suppression par reset) est indiqué dans le Guide d'utilisation du Token [21].

Le Token effectue alors les opérations suivantes :

- Optionnellement, il vérifie l'authenticité du paramètre pinAuth en utilisant le PIN Token ;
- Il crée une paire de clés du Credential (Credential Private Key, Credential Public Key) ;
- Optionnellement, si l'option "residentKey" est activée, il stocke les données utilisateur du Credential en mémoire persistante.

Le Token retourne :

- Le Credential Id ;
- Un compteur de signature ;
- La clé publique du Credential (Credential Public Key) ;
- Une signature calculée avec l'Attestation Private Key permettant au serveur FIDO d'authentifier le Credential Id et la Credential Public Key ;
- Le certificat d'attestation (Attestation Certificate) permettant au serveur FIDO d'authentifier l'Attestation Private Key.

Authentification (commande authenticatorGetAssertion)

Le Token reçoit :

- Un identifiant d'application (rpId) ;
- Optionnellement, une information de vérification du PIN (pinAuth) ;
- Optionnellement, une liste de Credential Ids autorisés (allowList).

Le Token effectue alors les opérations suivantes :

- Si la liste des Credential Ids autorisés est non vide : Il identifie comme candidats les Credential Ids de cette liste qui sont associés au rpId ;
- Sinon : Il identifie comme candidats parmi les Resident Keys les Credential Ids associés au rpId ;
- Optionnellement, il vérifie l'authenticité du paramètre pinAuth en utilisant le PIN Token ;
- Il demande la présence utilisateur (attente d'un appui sur le bouton de présence).
- Il sélectionne le premier candidat et, en utilisant sa Credential Private Key associée, il signe des données incluant en particulier son Credential Id et le rpIdHash (SHA-256 du rpId).

Le Token retourne :

- Le Credential Id ;
- Un compteur de signature ;
- La clé publique du Credential (Credential Public Key) ;
- Une signature calculée avec la Credential Private Key permettant au serveur FIDO d'authentifier le Credential Id et la Credential Public Key.

Note : Si plusieurs candidats ont été identifiés, les candidats suivants sont obtenus à l'aide de la commande authenticatorGetNextAssertion.

Gestion du PIN client (commande authenticatorClientPIN)

La commande authenticatorClientPIN comprend les sous-commandes suivantes :

- Obtention du compteur d'essais restants (getRetries) ;
- Détermination d'un secret partagé (getKeyAgreement) ;
- Initialisation du code PIN (setPIN) ;
- Modification du code PIN (changePIN) ;
- Obtention du PIN Token (getPINToken).

Lorsque le Token sort de fabrication, le code PIN n'est pas initialisé. La sous-commande setPIN permet alors de l'initialiser.
Son compteur d'essais (Client PIN Try Counter) est positionné initialement à 8. Il est remis à cette valeur à chaque vérification réussie du code PIN.
Sa valeur est décrémentée à chaque essai incorrect. Lorsqu'il atteint 0, le code PIN est bloqué. Seule une remise à zéro du Token peut permettre de donner une nouvelle valeur au code PIN.
Note : le PIN est rattaché au Token.

A chaque mise sous tension, le Token génère :

- Un PIN Token aléatoire, éventuellement utilisé ultérieurement dans les commandes authenticatorMakeCredential et authenticatorGetAssertion ;
- Une paire de clés Authenticator Key Agreement Private Key et Authenticator Key Agreement Public Key dont la clé privée est aléatoire.

Détermination d'un secret partagé (sous-commande getKeyAgreement)

Le Token retourne :

- La clé publique Authenticator Key Agreement Public Key.

Le secret partagé Shared Secret est utilisé dans la plupart des commandes FIDO2 pour effectuer une authentification, un chiffrement ou un déchiffrement.

Initialisation du code PIN (sous-commande setPIN)

Une sous-commande getKeyAgreement est préalablement exécutée.
Le Token reçoit :

- Une clé publique permettant de calculer le Shared Secret (keyAgreement) ;
- La Client PIN Value chiffrée avec le Shared Secret (newPinEnc) ;
- Une information d'authentification (pinAuth) calculée avec le Shared Secret ;
- Le token effectue alors les opérations suivantes :
- Il calcule le Shared Secret en utilisant l'Authenticator Key Private Key et la clé publique qu'il a reçue ;
- Il vérifie pinAuth en utilisant le Shared Secret ;
- Il déchiffre newPinEnc en utilisant le Shared Secret ;
- Il stocke le Client PIN Value en mémoire persistante et initialise son compteur d'essais à 8.

Le Token retourne : OK.

Changement du code PIN (sous-commande changePIN)

Une sous-commande getKeyAgreement est préalablement exécutée.
Le Token reçoit :

- Une clé publique permettant de calculer le Shared Secret (keyAgreement) ;
- Le hachage de l'ancienne Client PIN Value chiffré avec le Shared Secret (pinHashEnc) ;
- La Client PIN Value chiffrée avec le Shared Secret (newPinEnc) ;
- Une information d'authentification (pinAuth) calculée avec le Shared Secret.

Le Token effectue alors les opérations suivantes :

- Il rejette la sous-commande si le Client PIN est bloqué ;
- Il calcule le Shared Secret en utilisant l'Authenticator Key Private Key et la clé publique qu'il a reçue ;
- Il vérifie pinAuth en utilisant le Shared Secret ;
- Il décrémente le Client PIN Try Counter ;
- Il déchiffre pinHashEnc en utilisant le Shared Secret pour obtenir le haché du PIN à vérifier et le compare avec le haché du PIN courant : Si la comparaison réussit :
- Il positionne le Client PIN Try Counter à sa valeur maximale 8 ;
- Il déchiffre newPinEnc en utilisant le Shared Secret ;
- Il stocke le nouveau Client PIN Value en mémoire persistante.

Le Token retourne : OK.

Obtention du PIN Token (sous-commande getPINToken)

Une sous-commande getKeyAgreement est préalablement exécutée.
Le Token reçoit :

- Une clé publique permettant de calculer le Shared Secret (keyAgreement) ;
- Le hachage de la Client PIN Value chiffré avec le Shared Secret (pinHashEnc).

Le Token effectue alors les opérations suivantes :

- Il calcule le Shared Secret en utilisant l'Authenticator Key Private Key et la clé publique qu'il a reçue ;
- Il déchiffre pinHashEnc en utilisant le Shared Secret et le compare le PIN reçu avec le PIN courant : Si la comparaison réussit, le Client PIN Try Counter est mis à sa valeur maximale (8), sinon il est décrémenté.
- Il stocke le Client PIN Value en mémoire persistante et initialise son compteur d'essais à 8.

Le Token retourne : Le PIN Token chiffré avec le Shared Secret.

Remise à zéro (commande authenticatorReset)

A réception de cette commande, le Token effectue les opérations suivantes :

- Il attend que l'utilisateur appuie sur le bouton de présence pendant une durée d'environ 10 secondes ;
- Lorsque l'appui sur le bouton de présence est effectué, il efface :
  - Toutes les clés privées FIDO U2F ;
  - Le compteur de signature FIDO U2F (il est remis à zéro) ;
  - Toutes les clés privées FIDO2 et les éventuelles « Resident Keys » associées ;
  - Le compteur de signature FIDO2 (il est remis à zéro) ;
  - Le PIN FIDO2.

3.2. Matériel compatible ou dédié

Aucune contrainte matérielle particulière si ce n'est que le matériel doit disposer d'un port USB pour pouvoir accepter la connexion avec le Token.

3.3. Système d'exploitation

Il n'y a pas de contraintes techniques particulières sur les systèmes d'exploitation.

3.4. Navigateur

La plupart des web browsers supportent nativement les spécifications FIDO2. Les spécifications FIDO2 ont été acceptées par le W3C (forum de standardisation du Web). Les web browsers sont aussi en charge de créer une session TLS entre eux et service Web ciblé.

3.5. Serveurs FIDO

Dans le but de garantir l'interopérabilité, les serveurs FIDO doivent être certifiés fonctionnellement par le schéma de certification de la FIDO Alliance.

3.6. Relying Party (service web)

Aucune contrainte matérielle particulière si ce n'est que le service web doit disposer d'un serveur FIDO.

4. Description des biens sensibles que le produit à évaluer doit protéger

Biens sensibles à protéger	Biens attachés à l'application	Emplacement	Confidentialité	Intégrité	Authenticité	Référence du Bien
Attestation Private Key	FIDO U2F et FIDO2	NVM (Flash sécurisée)	Oui	Oui	Oui	B1
Signature Count	FIDO U2F et FIDO2	NVM (Flash sécurisée)	Non	Oui	Non	B2
Credential Private Keys	FIDO U2F et FIDO2	NVM (Flash sécurisée)	Oui	Oui	Oui	B3
Credential ID	FIDO U2F et FIDO2	RAM sécurisée	Non	Oui	Non	B4
Client PIN Try Counter	FIDO 2	NVM (Flash sécurisée)	Non	Oui	Non	B5
Client Pin Value (LEFT(SHA-256(PIN))	FIDO 2	NVM (Flash sécurisée)	Oui	Oui	Non	B6
Resident Keys	FIDO 2	NVM (Flash sécurisée)	Non	Oui	Non	B7
Pin Token	FIDO 2	RAM sécurisée	Oui	Oui	Non	B8
Authenticator Agreement Key (private key)	FIDO 2	RAM sécurisée	Oui	Oui	Oui	B9
Attestation Certificate	FIDO U2F et FIDO2	NVM (Flash sécurisée)	Non	Oui	Oui	B10

Tableau 1 : Biens sensibles à protéger

4.1. Description des menaces

L'identification de ces menaces résulte de l'analyse des biens à protéger par la cible d'évaluation et de la méthode d'utilisation de la cible d'évaluation dans son environnement opérationnel.

Menaces	Description	Biens concernés
M1 – Token malveillant	L'attaquant convainc les utilisateurs d'utiliser un Token mis en œuvre de manière malveillante. Le faux Token n'implémente aucune mesure de sécurité appropriée et est capable de violer tous les objectifs de sécurité des protocoles FIDO U2F et FIDO2.	Tous
M2 – Compromis de clé privée	Un attaquant réussit à extraire la clé privée d'un utilisateur pour une utilisation dans un contexte différent. Si la clé privée est compromise, un attaquant est capable de violer tous les objectifs de sécurité de FIDO. L'attaquant pourrait se faire passer pour l'utilisateur avec un Token cloné et a un accès non autorisé à la partie utilisatrice.	B1, B3, B9
M3 – Accès physique au Token	L'attaquant pourrait amener l'authentificateur dans un laboratoire afin d'utiliser la clé d'authentification (par exemple en contournant la vérification de l'utilisateur et en connaissant la partie utilisatrice liée à cette clé). Si cette attaque physique réussit, l'attaquant pourrait se faire passer pour l'utilisateur. L'attaquant peut introduire une situation de faible entropie pour récupérer une clé de signature ECDSA (ou extraire autrement la clé Uauth.priv).	B1, B3, B4, B7, B9,
M4 – Faux Token	Un attaquant est capable d'extraire la clé privée d'attestation du Token, par exemple en neutralisant les contre-mesures physiques en laboratoire. L'attaquant peut violer les propriétés attestables en créant un Token matériel ou logiciel malveillant qui se présente comme un Token légitime.	B1, B10
M5 – Attaque d'algorithme de signature	L'attaquant met en place une attaque pour déjouer la robustesse et la conformité des implémentations des algorithmes de signature du Token.	B4, B5
M6 – Abus de fonctionnalité	Il peut être possible pour un attaquant d'abuser de la fonctionnalité de Token en envoyant des commandes avec des paramètres invalides ou des commandes non valides au Token. Cela pourrait conduire à une extraction de clé potentielle.	B1, B3, B4, B7, B9
M7 – Prédiction de nombres aléatoires	Il peut être possible pour un attaquant d'accéder à des informations permettant la prédiction des données RNG. Cela peut conduire à la situation de compromission de clé.	B3, B9
M8 – Restauration du Firmware	L'attaquant peut être en mesure d'installer une version précédente et potentiellement boguée du Firmware. Cela peut conduire à des attaques réussies d'abus de fonctionnalité.	Tous

M9 – Falsification	Un attaquant peut tenter de modifier les communications interceptées afin de se faire passer pour l'utilisateur légitime et de se connecter à la partie utilisatrice.	B1, B3, B4, B7, B9
M10 – Clonage	Un attaquant clone le Token et utilise le Token cloné pour se connecter à la partie de confiance en tant qu'utilisateur légitime.	B1, B4, B10
M11 – Violation de la vie privée	Un attaquant est capable de tracer les connexions à deux comptes différents grâce aux informations échangées entre le Token et deux parties de confiance sur le même Token, violant ainsi la confidentialité de la vie privée de l'utilisateur.	B3, B4
M12 – Fuite d'informations	Un attaquant peut exploiter des informations provenant de la TOE lors de son utilisation afin de divulguer des clés confidentielles stockées sur le Token ou / et échangées entre la TOE et la partie utilisatrice. La fuite d'informations peut être inhérente au fonctionnement normal ou causée par l'attaquant. Des fuites d'informations peuvent se produire via des canaux cachés (canaux auxiliaires). Les attaques de canal latéral typiques incluent la mesure de la consommation d'énergie (puissance différentielle / analyse électromagnétique) pendant l'utilisation opérationnelle ou pour forcer activement la fuite par injection de défaut (analyse différentielle de défaut).	Tous
M13 – Falsification physique	Un attaquant peut effectuer un sondage physique de la TOE afin de divulguer / reconstruire les clés. Un attaquant peut modifier physiquement le Token afin d'altérer ses fonctionnalités de sécurité (partie matérielle et logicielle). La falsification physique peut être focalisée directement sur la divulgation ou la manipulation de matériaux clés. Des techniques couramment utilisées dans l'analyse des défaillances de circuits intégrés et les efforts de rétro-ingénierie de circuits intégrés peuvent être utilisées. Avant cela, les mécanismes de sécurité du matériel et les caractéristiques de mise en page doivent être identifiés. La modification peut entraîner la désactivation d'une fonction de sécurité. Les changements de circuits ou de données peuvent être permanents ou temporaires.	Tous
M14 – Attaque par force brute	L'attaquant connaît la valeur de l'identifiant du Credential ID et effectue une attaque par force brute pour tenter de deviner la clé privée associée. Un autre chemin d'attaque peut être réalisé lorsque l'utilisateur est loin du clavier, des logiciels malveillants peuvent essayer d'effectuer une récupération de clé ou effectuer une attaque par force brute sur la clé pour générer des réponses malveillantes.	B3 et B4
M15 – Déni de services en ligne	Un attaquant met en place un logiciel malveillant permettant de présenter plusieurs fois une mauvaise valeur du PIN utilisateur dans le but de bloquer l'utilisation du Token lors d'une transaction en ligne.	B2, B5, B6, B8
M16 – Vol du Token	L'attaquant vole physiquement le Token et l'utilise de façon illégitime.	Tous
M17 – Usurpation d'identité en ligne	Un attaquant met en place un faux site internet reproduisant les éléments visuels d'un site légitime et met en place un server FIDO non légitime. Il demande au porteur final du Token de créer le Credential ID fourni par le	B3 et B4

	serveur FIDO non légitime et utilise le résultat pour présenter le résultat du Credential ID légitime signé par le Token au site internet légitime.	

Tableau 2 : Description des menaces

4.2. Description des fonctions de sécurité du produit à évaluer

Fonctions de sécurité fournies par le produit à évaluer (dénommés ci-dessous : SFR)
Les deux applications Winkeo U2F et Winkeo FIDO2 utilisent les mêmes SFR.

	SFR	Description
SFR – 1	Fonction de sécurité d'intégrité basée sur une signature AES-CMAC.	Cette fonction de sécurité est fournie par le logiciel embarqué (fonctions communes). Elle est utilisée par les applications Winkeo FIDO U2F et FIDO2, elle garantit l'intégrité des biens sensibles du token tels que les "Attestation Private Key FIDO U2F", "Attestation Private Key FIDO2", "Credential Private Keys FIDO U2F", "Credential IDs FIDO U2F", "Signature Count FIDO U2F", "Credential Private Keys FIDO2", "Credential IDs FIDO2", "Signature Count FIDO2", "Client Pin Try Counter FIDO2", "Client Pin Value FIDO2", "Resident Keys FIDO2", "Pin Token FIDO2" et "Authenticator Agreement Private Key FIDO2".
SFR – 2	Fonction de sécurité de confidentialité basée sur un chiffrement AES-CBC.	Cette fonction de sécurité est fournie par le logiciel embarqué (fonctions communes). Elle est utilisée par l'application Winkeo FIDO2. Elle garantit la confidentialité du bien sensible "Client Pin Value FIDO2".
SFR – 3	Fonction de génération des clés symétriques de confiance.	Cette fonction de sécurité est fournie par le logiciel embarqué (fonctions communes). Elle est utilisée par les applications Winkeo FIDO U2F et FIDO2 pour générer les clés symétriques (AES) nécessaires aux fonctions de sécurité d'intégrité et de confidentialité des biens sensibles.
SFR – 4	Fonction de confidentialité de la Flash fournie par la puce Wisekey [9] certifiée par l'ANSSI [10] en utilisant les guides de sécurité de la puce et par le logiciel embarqué (fonctions communes.	Cette fonction de sécurité est fournie par la puce Wisekey MS6003 Rev C - Certifiée [10] et par le logiciel embarqué (fonctions communes). Elle permet de garantir la confidentialité des données stockées dans la zone FLASH de la puce tels que les "Attestation Private Key FIDO U2F", "Attestation Private Key FIDO2", "Credential Private Keys FIDO U2F" et "Credential Private Keys FIDO2".
SFR – 5	Fonction de confidentialité de la Flash fournie par la puce Wisekey [9] certifiée par l'ANSSI [10] en utilisant les guides de sécurité de la puce et par le logiciel embarqué (fonctions communes.	Cette fonction de sécurité est fournie par la puce Wisekey MS6003 Rev C - Certifiée [10] et par le logiciel embarqué (fonctions communes). Elle permet de garantir la confidentialité des données stockées dans la zone RAM de la puce tels que le "Pin Token FIDO2" et "Authenticator Agreement Private Key FIDO2"

SFR – 6	Fonction de sécurité de création d'un nombre aléatoire permettant la création de clés privées de confiance en confidentialité, intégrité et authenticité.	Cette fonction de sécurité est fournie par la puce Wisekey MS6003 Rev C - Certifiée [10] et par le logiciel embarqué (fonctions communes - post-traitement) . Elle permet de générer des nombres aléatoires d'entropie conforme à l'AIS 31 et au RGS (Génération de clés)
SFR – 7	Fonction de génération des clés asymétriques de confiance.	Cette fonction de sécurité est fournie par le logiciel embarqué (fonctions communes). Elle est utilisée par les applications Winkeo FIDO U2F et FIDO2 pour générer les clés symétriques (AES) nécessaires pour garantir l'intégrité et la confidentialité des biens sensibles stockés en FLASH et en RAM.
SFR – 8	Fonction de sécurité permettant la « Tamper Resistance » aux attaques physiques de haut niveau.	Cette fonction de sécurité est fournie par la puce Wisekey MS6003 Rev C - Certifiée [10] et par le logiciel embarqué (fonctions communes). Elle permet de détecter et déjouer les attaques physiques (par canaux auxiliaires ou injection de fautes) dans le but de protéger les biens sensibles de la TOE.
SFR – 9	Fonction de sécurité d'authentification fournie par l'implémentation des protocoles FIDO U2F et FIDO2 incluant l'enrôlement et la remise à l'état initial du Token.	Cette fonction de sécurité est fournie par les protocoles FIDO2 et U2F. Elle permet de garantir l'intégrité et l'authenticité des processus d'enregistrement, d'authentification et de remise à l'état initial du Token.
SFR – 10	Fonction de sécurité permettant la vérification de la présence d'un utilisateur.	Cette fonction de sécurité est fournie par le Token et plus précisément par le bouton de présence utilisateur. Elle permet de vérifier la présence physique de l'utilisateur lors d'opérations sensibles (enregistrement, authentification, reset du token).
SFR – 11	Fonction de sécurité permettant la suppression des commandes du bootloader pendant le processus de pré-personnalisation.	Cette fonction de sécurité est fournie par la puce Wisekey MS6003 Rev C - Certifiée [10] et par le logiciel embarqué (fonctions communes). Elle permet d'effacer le code (situé en FLASH) du bootloader de la puce servant au chargement du logiciel embarqué en FLASH pendant le processus de pré-personnalisation.

Tableau 3 : Fonction de sécurité (SFR)

4.3. Synthèse de couverture des menaces

		SFR 1	SFR 2	SFR 3	SFR 4	SFR 5	SFR 6	SFR 7	SFR 8	SFR 9	SFR 10	SFR 11
Menaces	**Biens concernés**											
M1 – Token malveillant	**Tous**									*		
M2 - Compromis de clé privée	**B1, B3, B9**	*			*		*	*	*			
M3 – Accès physique au Token	**B1, B3,B4, B7, B8 ,B9,**	*	*		*	*	*	*	*			
M4 – Faux Token	**B1, B10**	*			*	*			*	*		
M5 – Attaque d'algorithme de signature	**B4, B5**									*		
M6 – Abus de fonctionnalité	**B1, B3, B4, B7, B9**	*			*		*	*	*	*		
M7 – Prédiction de nombres aléatoires	**B3, B9**	*			*		*					
M8 – Restauration du Firmware	**Tous**											*
M9 – Falsification	**B1, B3, B4, B7, B9**	*			*	*	*	*	*	*		
M10 – Clonage	**B1, B4, B10**	*			*	*				*		
M11 – Violation de la vie privée	**B3, B4**	*			*					*		
M12 – Fuite d'informations	**Tous**			*	*	*	*	*	*	*		
M13 – Falsification physique	**Tous**	*	*	*	*	*	*	*	*	*		*
M14 – Attaque par force brute	**B3, B4**	*			*		*	*		*		
M15 – Déni de services en ligne	**B2, B5, B6, B8**				*					*	*	
M16 – Vol du Token	**Tous**									*		
M17 – Usurpation d'identité en ligne	**B3, B4**	*			*		*	*		*		

Tableau 4 : Synthèse de couverture des menaces

FIN DU DOCUMENT