Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2018/15

HID ActivID Push-based Authentication solution

Version ActivID Appliance v8.0 (FIXS1709016), HID Approve v2.0.3 (iOS), HID Approve v2.0.2 (Android)

Paris, le 9 juillet 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ 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-2018/15**
Nom du produit **HID ActivID Push-based Authentication solution**
Référence/version du produit **ActivID Appliance v8.0 (FIXS1709016), HID Approve v2.0.3 (iOS), HID Approve v2.0.2 (Android)**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **HID Global SAS** **26 avenue du Général de Gaulle** **92156 Suresnes Cedex**
Développeur **HID Global SAS** **26 avenue du Général de Gaulle** **92156 Suresnes Cedex**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B,** **78180 Montigny le Bretonneux, France**
Fonctions de sécurité évaluées **Communications sécurisées** **Vérification de l'opération par l'application cliente** **Vérification de l'opération par le serveur** **Stockage des clefs sur le terminal et sur le serveur** **Log des opérations effectuées et stockage sur le serveur**
Fonction(s) de sécurité non évaluées **Sans objet**
Restriction(s) d'usage **Oui (cf. §3.2)**

Préface

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 Premier ministre 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « HID ActivID Push-based Authentication solution, version ActivID Appliance v8.0 (FIXS1709016), HID Approve v2.0.3 (iOS), HID Approve v2.0.2 (Android) » développé par *HID GLOBAL*.

Ce produit vise à fournir aux utilisateurs d'applications web un moyen d'authentification unique sur terminaux mobiles.
Le produit met en œuvre la solution dite *ActivID* à travers les composants suivants:

- un serveur principal d'authentification (sous la forme d'une *appliance*, sur laquelle s'exécute le logiciel *ActivID Authentication Server*), qui gère la base d'utilisateurs et vérifie leur authentification ;
- une application mobile (iOS ou Android) « HID Approve » permettant à l'utilisateur de valider une authentification, de valider une opération effectuée (par exemple un virement bancaire), et de générer un mot de passe à utilisation unique ;
- un réseau de notification *push* supporté par les services *cloud* de Microsoft Azure ;
- une application cliente : il s'agit du service auquel l'utilisateur final souhaite s'authentifier (par exemple un site de gestion bancaire).

La figure ci-dessous explicite l'architecture du produit, et précise les composants faisant partie de la cible d'évaluation (blocs mis en couleur) ainsi que les communications évaluées entre ces composants (flèches mises en couleurs).

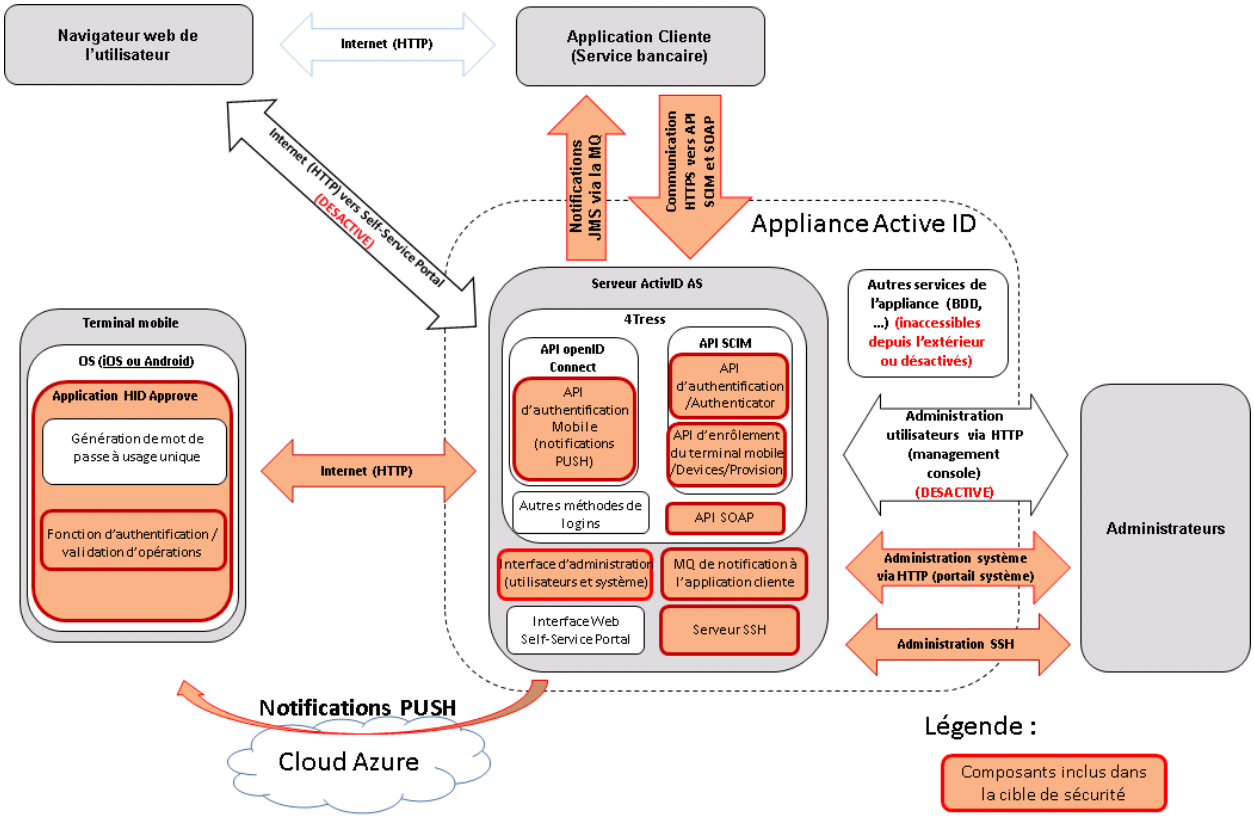

Figure 1 - Architecture Produit.

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

Nom du produit	HID ActivID Push-based Authentication solution
Numéro de la version évaluée	ActivID Appliance v8.0 (FIXS1709016), HID Approve v2.0.3 (iOS), HID Approve v2.0.2 (Android)

1.2.2.1. ActivID Appliance

Il est possible d'obtenir le numéro de version de l'ActivID Appliance *via* le panneau d'administration de l'interface Web, dans la catégorie *Troubleshooting*. La version est identifiée sous le numéro de build 8.0.0.571.

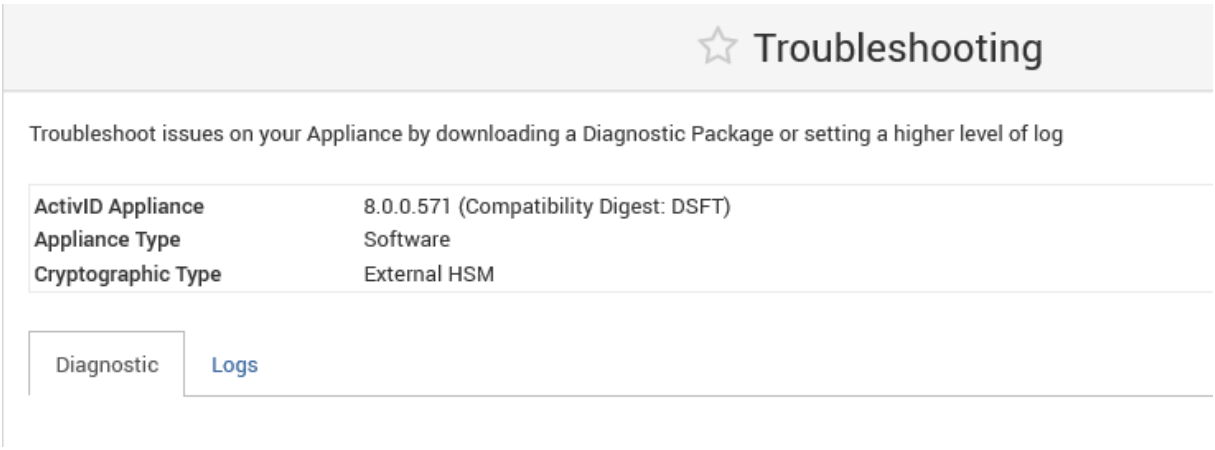

Figure 2 : identification de la version ActivID Appliance

Ce numéro correspond bien au patch FIXS1709016 tel qu'identifié dans sa documentation en ligne.

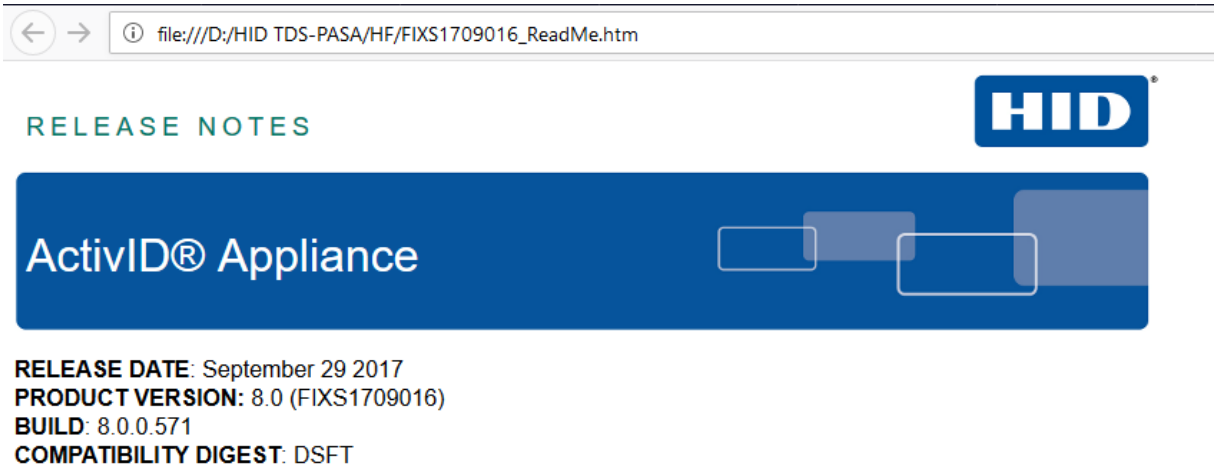

Figure 3 : identification du patch FIXS1709016

1.2.2.2. HID Approve (Android)

Pour récupérer la version de l'application HID Approve sur Android, il est nécessaire de la télécharger sur le Google Store. Une fois installée, la version est indiquée dans Paramètre > Applications > Approve.

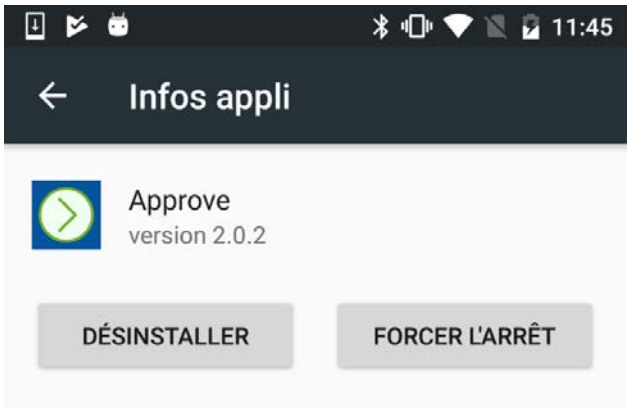

Figure 4 : identification de la version HID Approve Android

1.2.2.3. HID Approve (iOS)

Pour récupérer la version de l'application HID Approve sur iOS, il est nécessaire de la télécharger sur l'App Store.
Il est possible de voir son numéro de version à partir d'iTunes :

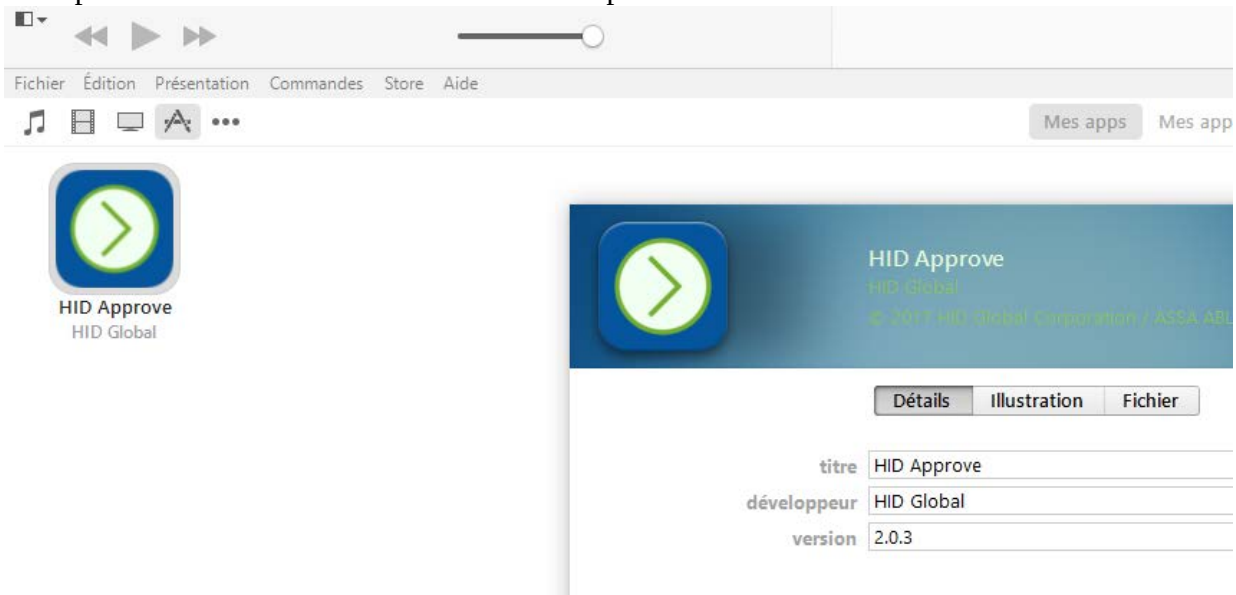

Figure 5 : Identification de la version HID Approve iOS

Une fois installée, la version de l'application est également indiquée sur le téléphone au chemin suivant :

- iOS 11 : Paramètres / Général / Stockage de l'iPad ;
- iOS 9 & iOS 10 : Paramètres / Général / Stockage local et iCloud / Gérer le stockage.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- les communications sécurisées ;
- la vérification de l'opération par l'application cliente[1] ;
- la vérification de l'opération par le serveur ;
- le stockage des clefs sur le terminal mobile et sur le serveur ;
- le log des opérations effectuées et stockage sur le serveur.

1.2.4. Configuration évaluée

La configuration évaluée met en œuvre deux téléphones de tests et une *Appliance* connectée à un HSM[2] réseau.

La plateforme de test est constituée des éléments suivants :

- Hyperviseur : Ubuntu 14, VMWare Workstation 12 ;
- OS de l'*Appliance* : *ORACLE* Linux Server 7.3, Kernel 4.1.12-103.3.8 ;
- Téléphone Android : Nexus 5, Android 6.0.1 ;
- Téléphone iOS : iPhone 6, iOS 10.3.3 ;
- HSM réseau : *THALES* nShield Connect 6000+.

[1] La « vérification de l'opération » est un mécanisme par lequel l'application client ou le serveur ActivID AS, avant d'effectuer une opération donnée, peuvent demander l'autorisation de l'utilisateur concerné. Cette autorisation se fait va une validation sur le terminal mobile.

[2] *Hardware Security Module*

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

L'installation de l'application HID Approve sur mobile est effectuée depuis le *store* correspondant à l'OS mobile visé.
La machine virtuelle correspondant à ActivID Appliance est ajoutée directement à un hyperviseur.

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

L'installation inclut :

- l'installation des applications mobiles ;
- l'installation d'ActivID Appliance, suivie de la migration des clefs de l'Appliance sur le HSM ;
- la configuration d'ActivID Appliance.

2.3.1.3. Durée de l'installation

Le temps total d'installation et de configuration est évalué entre 1 et 2 jours.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit.

2.3.3. Revue du code source (facultative)

L'évaluateur a eu accès au code source dans le cadre de la recherche de vulnérabilités.

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 potentielles connues ont été identifiées sur le produit, et les briques tierces qu'il utilise. Cependant, elles sont considérées comme non exploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

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 dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour l'identification des parties du code source implémentant les mécanismes cryptographiques.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur a identifié plusieurs points de configuration pouvant mener à un affaiblissement de la sécurité du système, qui donnent lieu à recommandations dans la section suivante.

2.3.8.2. Recommandations pour une utilisation sûre du produit

L'utilisateur du produit devra mettre en œuvre les mesures suivantes :

- l'administrateur doit changer le mot de passe *root* par défaut lors de l'installation ;
- l'administrateur doit désactiver les panneaux d'administration des domaines après installation ;
- l'administrateur doit mettre en place le mécanisme d'authentification par certificat pour l'accès SSH plutôt que par mot de passe.

Enfin, les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux guides fournis.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le CESTI a relevé que l'administrateur du produit aura besoin de l'assistance du développeur lors de l'installation et de la configuration du produit.

2.3.8.4. 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.
L'évaluateur a identifié un risque lié aux mots de passe sur téléphones iOS et Android. Pour cette raison, une restriction d'usage a été ajoutée au chapitre 3.2. Si cette restriction est respectée, l'évaluateur n'a pas relevé de vulnérabilité exploitable dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.5. Analyse du générateur d'aléas

Le produit utilise plusieurs générateurs d'aléa (pour la génération du *QR Code* d'enregistrement, ainsi que pour l'établissement de secrets partagés ou de vecteurs d'initialisation).
L'évaluateur a identifié un risque lié à la génération du *QR Code*. Pour cette raison, une restriction d'usage a été ajoutée au chapitre 3.2. Si cette restriction est respectée, l'évaluateur n'a pas relevé de vulnérabilité exploitable dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

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 « HID ActivID Push-based Authentication solution, version ActivID Appliance v8.0 (FIXS1709016), HID Approve v2.0.3 (iOS), HID Approve v2.0.2 (Android) » 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. 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 énoncées dans le présent rapport (voir 2.3.8.2).

En complément, l'évaluation a mis en avant des restrictions d'usage à respecter pour une utilisation sécurisé du produit décrites ci-après :

- l'administrateur doit configurer le produit de façon à limiter la durée des *QR codes* à une durée courte (24 heures ou moins) ;
- l'administrateur doit s'assurer que les utilisateurs des applications HID Approve sur (téléphones iOS comme Android) respectent une politique de mots de passe par défaut correspondant a minima à une force « moyenne » ainsi que préconisé par l'ANSSI (voir [MdP]).

Annexe 1. Références documentaires du produit évalué

[CDS]	*HID® ActivID Push-based Authentication solution Cible de sécurité CSPN* Référence : N/A ; Version : *1.1* ; Date : *juin 2017*
[RTE]	*Rapport Technique d'Evaluation CSPN AIPA - HID® ActivID Push-based Authentication solution* Référence : OPPIDA/CESTI/TDS PASA/RTE ; Version : 1.3 ; Date : *20 juin 2018*

Annexe 2. 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, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[MdP]	Note technique – Recommandations de sécurité relatives aux mots de passe, 5 juin 2012, ANSSI. https://www.ssi.gouv.fr/administration/guide/mot-de-passe/