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-2017/22

HP Sure Start Hardware Root of Trust version A2, embarqué sur les puces

NPCE586HA2MX

NPCE586HA2BX

NPCE576HA2YX

Paris, le 25 septembre 2017

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-2017/22**
Nom du produit **HP Sure Start Hardware Root of Trust**
Référence/version du produit **Version A2**
Catégorie de produit **Matériel et logiciel embarqué**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **HP Inc.** **20 quai du Point du Jour** **92100 Boulogne Billancourt** **France**
Développeur **HP Inc.** **20 quai du Point du Jour** **92100 Boulogne Billancourt** **France**
Centre d'évaluation **CEA - LETI** **17 rue des martyrs** **38054 Grenoble Cedex 9** **France**
Fonctions de sécurité évaluées **Protection en intégrité des données** **Mécanisme de vérification de l'intégrité et l'authenticité** **Maintien de la TOE dans un état sécurisé**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage **Non**

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 le « HP Sure Start Hardware Root of Trust version A2 », embarqué sur les puces NPCE586HA2MX, NPCE586HA2BX et NPCE576HA2YX, et développé par *HP INC.*.

Ce produit est un microcontrôleur destiné à être utilisé dans des équipements de la marque HP, tels que des PC ou des imprimantes. Cet élément est présent sur la carte mère et intervient au moment d'un démarrage de l'équipement. Lors de cette étape, le produit va procéder à une vérification du BIOS avant que ce dernier ne soit chargé par le CPU[1]. Pour cela, le produit « HP Sure Start Hardware Root of Trust » va d'abord récupérer dans une mémoire flash dédiée le code du *firmware* du BIOS, récupérer les clés cryptographiques stockées en mémoire interne au produit, puis vérifier l'intégrité et l'authenticité de ce *firmware*. Si le résultat est positif, alors le produit permet au *CPU* de démarrer les opérations. Dans le cas contraire, le signal *reset* est émis vers le *CPU*, et l'équipement ne démarre pas. Afin de récupérer de cette erreur, une seconde mémoire flash, utilisée comme stockage de secours, permet la recopie du *firmware* vers la première unité de stockage. Le *firmware* nouvellement copié est ensuite vérifié au prochain démarrage.

Le produit peut se présenter sous la forme de trois boîtiers de circuit intégré (*packaging* en anglais) différents, à savoir :

- *Thin Quad Flat Package* (TQFP), dont la référence est NPCE586HA2MX ;
- *Ball Grid Array* (BGA), dont la référence est NPCE586HA2BX ;
- *Quad Flat No-leads* (QFN), dont la référence est NPCE576HA2YX.

La figure ci-dessous explicite l'architecture du produit.

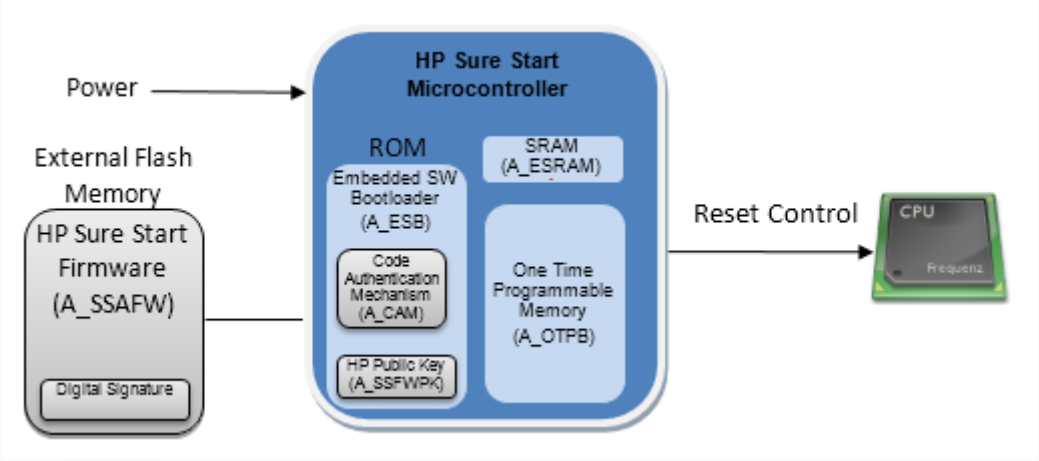

Figure 1 - Architecture produit.

[1] *Central Processing Unit* – unité central de traitement

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	HP Sure Start Hardware Root of Trust
Numéro de la version évaluée	NPCE586HA2MX NPCE586HA2BX NPCE576HA2YX
Version de la ROM	A2

Les versions évaluées du produit peuvent être identifiées par la lecture des informations écrites sur chacune des puces :

- NPCE586HA2MX ;
- NPCE586HA2BX ;
- NPCE576HA2YX.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la protection en intégrité des données par stockage en *Read-Only-Memory* (ROM) et en *Electrically Erasable Programmable Read-Only-Memory* (EEPROM) avec fusible ;
- le mécanisme de vérification de l'intégrité et de l'authenticité du *firmware* du BIOS ;
- à chaque redémarrage, le maintien, par conception, de l'équipement utilisateur dans un état sécurisé.

1.2.4. Configuration évaluée

Le produit est soudé sur la carte mère du PC. Quant aux mémoires flash, les *sockets* sont soudés sur la carte mère, mais les unités de stockages sont amovibles.

Le PC HP ainsi équipé représente la plateforme de test.

Pour les besoins de l'évaluation, seule la version NPCE586HA2MX a été évaluée. Le CESTI a en effet conclu que ce modèle, dans cette version, était représentatif des trois produits qui font l'objet de cette certification, et que les différences de *packaging* n'ont aucun impact sur la sécurité du produit évalué, comme cela a été confirmé dans le rapport de maintenance ([M01]) précédemment émis.

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 a été adaptée conformément à la procédure [MAI] pour tenir compte des travaux déjà effectués sur une précédente version du produit, certifiée sous la référence ANSSI-CSPN-2017/04 ([CER]).

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

Il n'y a pas d'installation, ni de paramétrage du produit. Il suffit de démarrer l'équipement pour que le produit rentre en phase d'utilisation.

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

L'environnement d'évaluation a été fourni par *HP INC.* sous forme d'un PC prêt à l'emploi. L'évaluateur ne peut donc pas se prononcer sur cet aspect de l'évaluation.

2.3.1.3. Durée de l'installation

Sans objet.

2.3.1.4. Notes et remarques diverses

Néant.

2.3.2. Analyse de la documentation

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

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et estime que le code est clairement organisé et correctement commenté, permettant une bonne compréhension du comportement de chacune des fonctions.

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

L'analyse du code source a permis de mettre en avant une potentielle faiblesse. Cependant, les tests menés par l'évaluateur ont mis en évidence que cette vulnérabilité n'était pas exploitable dans les conditions d'utilisation et pour le niveau d'attaquant visé.

2.3.7. Accès aux développeurs

Sans objet.

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 n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Aucune recommandation particulière n'est formulée par l'évaluateur.

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

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

2.3.8.4. 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. Celle-ci n'a pas identifié de non-conformité au [RGS] ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas.

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 « HP Sure Start Hardware Root of Trust version A2 » embarqué sur les puces NPCE586HA2MX, NPCE586HA2BX et NPCE576HA2YX 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].

Annexe 1. Références documentaires du produit évalué

[CDS]	*CSPN Security Target HP Sure Start HW Root of Trust NPCE5x6HA2* Référence : HPSSHW v1.5 ; Version : 1.5 ; Date : *mars 2017*
[RTE]	*Evaluation Technical Report « full »* Référence : LETI.CESTI.SUR.ETR_full– v2.0 – 03/07/2017 ; Version : 2.0 ; Date : *3 juillet 2017*
[CER]	*Rapport de certification ANSSI-CSPN-2017/04 HP Sure Start Hardware Root of Trust, en version A0, embarqué sur la puce NPCE586HA0MX* Référence : ANSSI-CSPN-2017/04 ; Version : 1.0 ; Date : *16 mars 2017*
[M01]	*Rapport de maintenance ANSSI-CSPN-2017/04-M01* *HP Sure Start Hardware Root of Trust version A0, embarqué sur les puces NPCE586HA0BX et NPCE576HA0YX* Référence : ANSSI-CSPN-2017/04-M01 ; Version : 1.0 ; Date : *3 septembre 2017*

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 (CSPN) 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.
[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.
[MAI]	Maintien de la confiance : continuité de l'assurance, version 1.0, référence ANSSI-CSPN-MAI-P-01 du 16 septembre 2014.
[NOTE-21]	Note d'application - Méthodologie pour l'évaluation d'une gamme de produits, référence ANSSI-CC-NOTE-21/1.0 du 1er février 2017.