



**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-2025/01

**HP Endpoint Security Controller (EpSC)
Platform Hardware Root of Trust**

NPCX499HA1BX et NPCD324HA0DX

Paris, le 30 Mars 2025

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

Vincent STRUBEL

[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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CSPN-2025/01
Nom du produit	HP Endpoint Security Controller (EpSC) Platform Hardware Root of Trust
Référence/version du produit	NPCX499HA1BX et NPCD324HA0DX
Catégorie de produit	Matériel et logiciel embarqué
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	HP INC. 14 rue de la Verrerie, 92190 Meudon, France
Développeur	NUVOTON TECHNOLOGY ISRAEL LTD. P.O. Box 12347 Herzliya B, 4673324 Israel
Centre d'évaluation	CEA - LETI 17 avenue des martyrs 38054 Grenoble Cedex 9, France
Accord de reconnaissance applicable	
Ce certificat est reconnu dans le cadre du [BSZ_CSPN]	
Fonctions de sécurité évaluées	Protection de l'intégrité basée sur la ROM Protection de l'intégrité de l'extension de la ROM Vérification de l'authenticité du code du <i>Firmware</i> Protection de l'intégrité basée sur une mémoire OTP Protection pour la confidentialité Disponibilité du mécanisme d'authentification du code au démarrage
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 cyber.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	7
1.2.1	Catégorie du produit	7
1.2.2	Identification du produit.....	7
1.2.3	Fonctions de sécurité.....	8
1.2.4	Configuration évaluée	8
2	L'évaluation.....	9
2.1	Référentiels d'évaluation	9
2.2	Travaux d'évaluation	9
2.2.1	Installation du produit.....	9
2.2.2	Analyse de la documentation.....	9
2.2.3	Revue du code source (facultative).....	10
2.2.4	Analyse de la conformité des fonctions de sécurité	10
2.2.5	Analyse de la résistance des mécanismes des fonctions de sécurité	10
2.2.6	Analyse des vulnérabilités (conception, construction, etc.)	10
2.2.7	Analyse de la facilité d'emploi	10
2.3	Analyse de la résistance des mécanismes cryptographiques	11
2.4	Analyse du générateur d'aléa.....	11
3	La certification	12
3.1	Conclusion.....	12
3.2	Recommandations et restrictions d'usage	12
3.3	Reconnaissance du certificat.....	12
ANNEXE A.	Références documentaires du produit évalué	13
ANNEXE B.	Références liées à la certification	14

1 Le produit

1.1 Présentation du produit

Le produit évalué est « HP Endpoint Security Controller (EpSC) Platform Hardware Root of Trust, NPCX499HA1BX et NPCD324HA0DX » développé par NUVOTON TECHNOLOGY ISRAEL LTD..

Ce produit est un microcontrôleur, au format *Very Thin Profile Fine-Pitch Ball Grid Array* (144-Pin VFBGA), 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. Pour cela, le produit « *HP Endpoint Security Controller (EpSC)* » 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.

La figure ci-dessous explicite l'architecture du produit. (Figure 1 de la cible de sécurité [CDS])

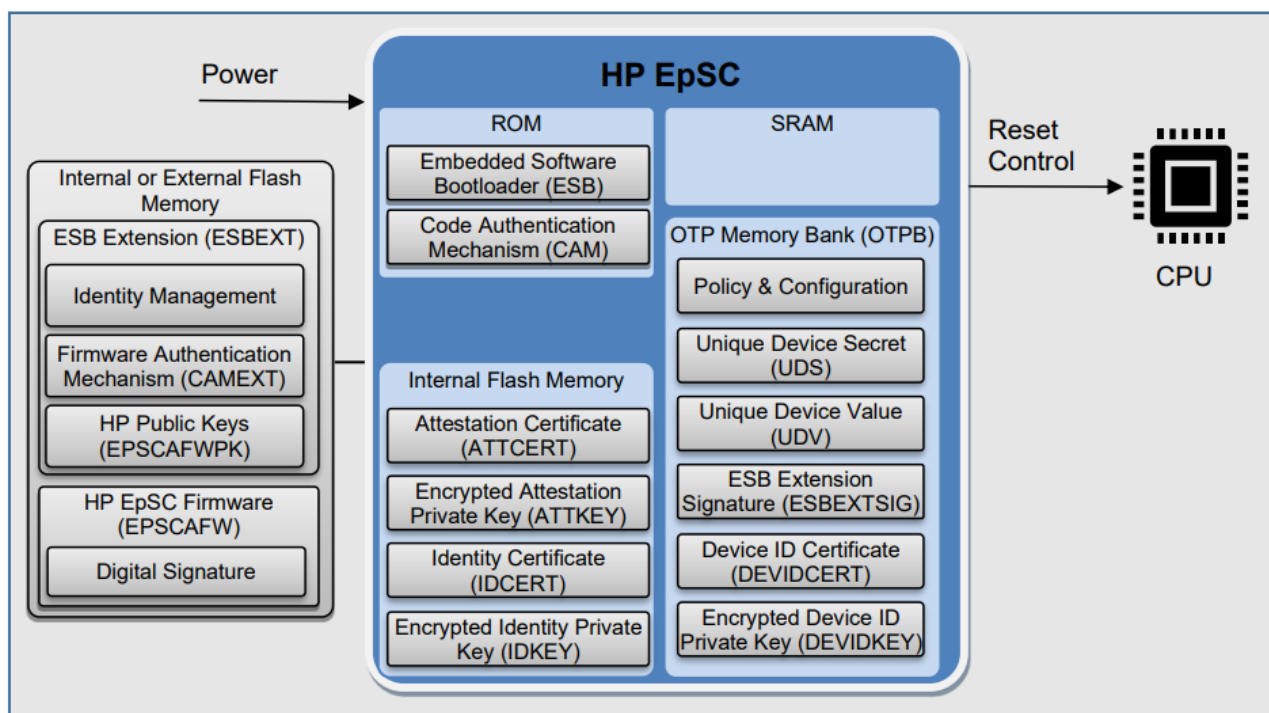


Figure 1 - Architecture Produit.

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

Produit	
Nom du produit	HP Endpoint Security Controller (EpSC) Platform Hardware Root of Trust
Numéro de la version évaluée	NPCX499HA1BX et NPCD324HA0DX

La version certifiée du produit peut être identifiée de la manière suivante :

- lecture du numéro de version (BX ou DX) écrit sur la puce ;
- lecture de la sortie de la fonction BOOTER_GetROMVer (0x00000629) indiquant la version de la ROM.

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la protection de l'intégrité basée sur la ROM ;
- la protection de l'intégrité de l'extension ROM ;
- la vérification de l'authenticité du code du *firmware* ;
- la protection de l'intégrité basée sur une mémoire *One-Time-Programmable* (OTP) ;
- les mécanismes de protection de la confidentialité des secrets du produit ;
- la disponibilité du mécanisme d'authentification du code qui assure que le composant EpSC est alimenté en premier et démarre avant le CPU.

1.2.4 Configuration évaluée

La configuration évaluée correspond aux puces NPCX499HA1BX et NPCD324HA0DX intégrées dans deux cartes d'évaluation fournies par le développeur.

Les plateformes de tests sont constituées des éléments suivants :

- la puce NPCX499HA1BX (ou NPCD324HA0DX) ;
- de LED indiquant l'alimentation, le succès ou l'échec du démarrage du *firmware* ;
- un accès au *SPI* partagé ;
- un accès au *SPI* privé.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-01].

2.2 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].

2.2.1 Installation du produit

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

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.

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

L'environnement d'évaluation a été fourni par le développeur sous forme d'une carte d'évaluation prête à l'emploi. L'évaluateur ne peut donc pas se prononcer sur cet aspect de l'évaluation.

2.2.1.3 Notes et remarques diverses

Néant.

2.2.2 Analyse de la documentation

L'évaluateur a eu accès aux documents [DOC_DEV] dans le cadre de cette évaluation.

2.2.3 Revue du code source (facultative)

L'évaluateur a revu le code source de l'intégralité des fonctions de sécurité du produit mentionnées au paragraphe 1.2.3.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

L'évaluateur a effectué une revue du code source et estime que le code est clairement organisé et correctement documenté.

2.2.4 Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 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.

2.2.6 Analyse des vulnérabilités (conception, construction, etc.)

2.2.6.1 Liste des vulnérabilités connues

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

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitable pour le niveau d'attaquant considéré.

2.2.7 Analyse de la facilité d'emploi

2.2.7.1 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.

2.2.7.2 Avis d'expert sur la facilité d'emploi

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

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit ne comporte pas de générateur d'aléa entrant dans le périmètre d'évaluation.

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 Endpoint Security Controller (EpSC) Platform Hardware Root of Trust, NPCX499HA1BX et NPCD324HA0DX » 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].

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (Beschleunigte Sicherheitszertifizierung ou Certification de sécurité accélérée).



ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - <i>CSPN Security Target HP Endpoint Security Controller (EpSC) Platform Hardware Root of Trust NPCX499HA1 and NPCD324HA0</i>, référence EpSC24 CSPN Security Target, version 1.2, 20 juin 2024.
[RTE]	Rapport technique d'évaluation : - <i>CSPN Evaluation Technical Report - HPSSHW_NBDT24_A0</i>, référence LETI.CESTI.ECSIO24.RT.001, version 1.1, 30 septembre 2024.
[GUIDES]	<i>EpSC24 BootLoader Cryptographic Design Document</i> , version 1.1, 4 avril 2024.

ANNEXE B. Références liées 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, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0, 6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[BSZ_CSPN]	<i>Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI, référence bsz_cspn_mutual_recognition_agreement, version 2.0, mai 2024.</i>