PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de certification
ANSSI-CSPN-2025/02

UTL SCAiP PoE avec lecteurs transparents

Version UTL fV2005, version Lecteurs fV2003

Paris, le 25 Avril 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 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-2025/02**
Nom du produit **UTL SCAiP PoE avec lecteurs transparents**
Référence/version du produit **Version UTL fV2005, version Lecteurs fV2003**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **FDI MATELEC** 110, rue Pierre-Gilles de Gennes 49300 Cholet, France
Développeur **FDI MATELEC** 110, rue Pierre-Gilles de Gennes 49300 Cholet, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Accord de reconnaissance applicable fixed time certification Ce certificat est reconnu dans le cadre du [BSZ_CSPN]
Fonctions de sécurité évaluées Protection des données échangées entre le Serveur et l'UTL Sécurisation de l'UTL Protection des données échangées entre l'UTL et les lecteurs Protection du code PIN Sécurisation du lecteur Sécurisation des mises à jour *firmware* Sécurisation contre les attaques relais Protection des attaques par déni de service
Fonctions 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 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

1.1 Présentation du produit

Le produit évalué est « UTL SCAiP PoE avec lecteurs transparents, Version UTL fV2005, version Lecteurs fV2003 » développé par FDI MATELEC.

Ce produit est intégré aux équipements de terrain de la solution complète de gestion centralisée de contrôle d'accès physique « SCAiP », qui est elle-même composée :

- d'une partie « Serveur » intégrant les applications, les bases de données et le serveur de terrain ;
- d'une partie « Matériel » intégrant les équipements de terrain : UTL, lecteurs, claviers et badges MIFARE DESFire.

Le présent certificat porte uniquement sur l'UTL et les lecteurs.

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

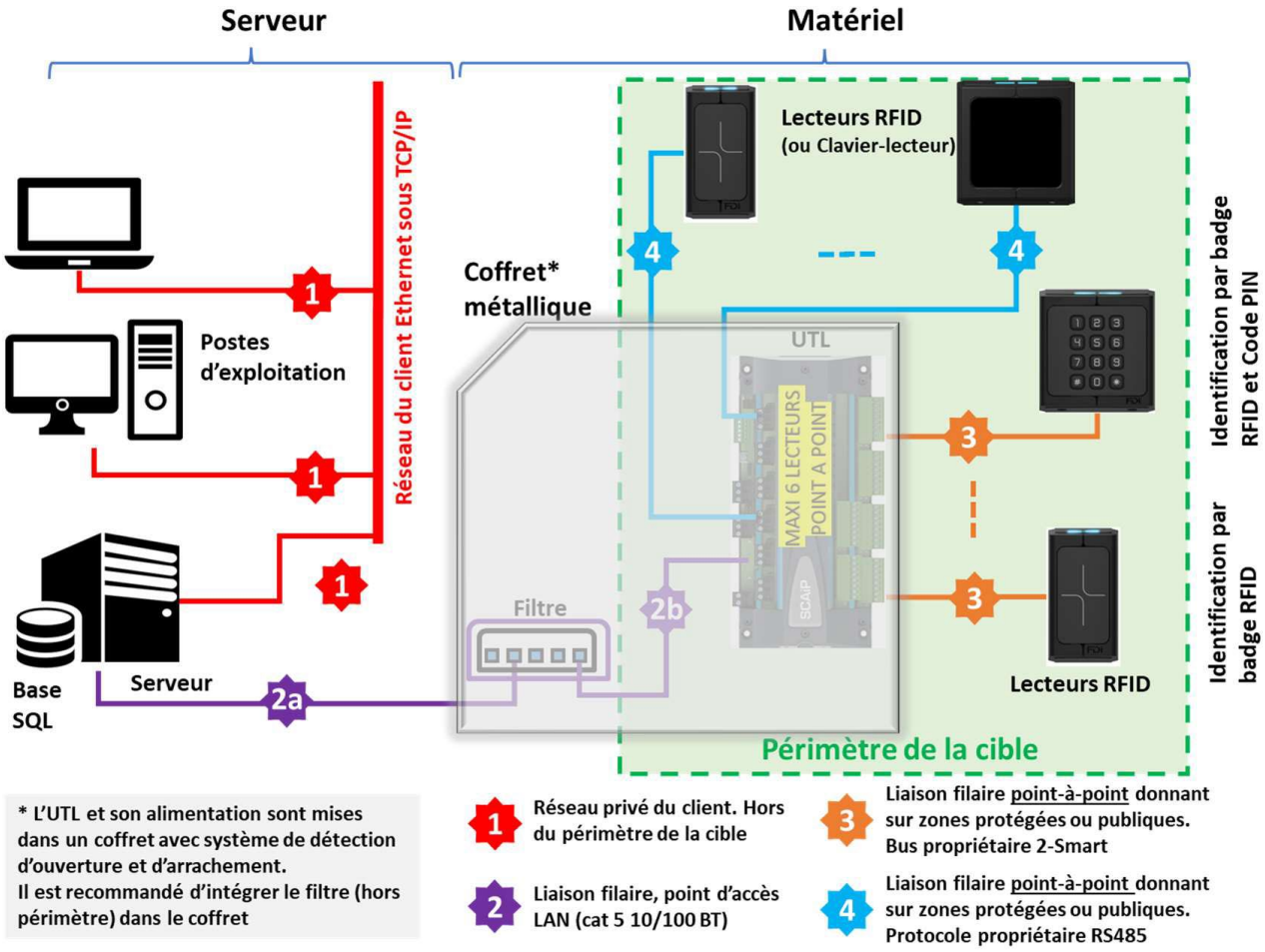

Figure 1 - Architecture Produit.

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	UTL SCAiP PoE avec lecteurs transparents
Numéro de la version évaluée	Version UTL fV2005, version Lecteurs fV2003

Le produit est commercialisé sous trois marques différentes (FDI, Castel et Golmar) avec des composants et une version de *firmware* similaires.

L'UTL et les lecteurs portent leurs identifiants sur l'envers ou le bas du boîtier.

Leur version certifiée peut être identifiée via le serveur web.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection des données échangées entre le Serveur et l'UTL ;
- la sécurisation de l'UTL ;
- la protection des données échangées entre l'UTL et les lecteurs ;
- la protection du code PIN ;
- la sécurisation du lecteur ;
- la sécurisation des mises à jour du *firmware* ;
- la sécurisation contre les attaques relais ;
- la protection contre les attaques par déni de service.

1.2.4 *Configuration évaluée*

Le tableau ci-dessous décrit la configuration évaluée :

Composants du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE), supposé de confiance
GAC	Système d'exploitation		Linux Ubuntu 22.04
	Applicatifs		Propriétaire, version logicielle 01.19.00
	Fonctions cryptographiques		TLS 1.3, SHA-256, RSA-2048, RSA-PSS
	Bases de données et annuaires		MariaDB 10.6.16
UTL	Système d'exploitation	FreeRTOS 10.5.1 LTS	
	Applicatifs	Propriétaire version logicielle fV2025 Référence XX-125-906 (XX = FD pour FDI, CA pour Castel, GE pour Golmar)	
	Fonctions cryptographiques	TLS 1.3, SHA-256, AES, ECDSA, HMAC-SHA256, RSA-2048, RSA-PSS, CMAC, HKDF-SH384	
	SAM	NXP MIFARE SAM AV3 MF4SAM3X84	
Lecteurs simples (P40 , P80) et lecteurs-clavier (PK80)	Applicatifs	Propriétaire version logicielle fV2023 Référence XX-020-924/925/926 (XX = FD pour FDI, CA pour Castel, GE pour Golmar)	
	Fonctions cryptographiques	CMAC, HKDF-SHA384, AES	
	SAM	Aucun	
Badges			MIFARE DESFire EV3

La plateforme de test est constituée de deux maquettes préinstallées et prêtes à l'emploi du produit pour la marque FDI.

Chaque maquette est composée de :

- un lecteur de badge de type P40 ;
- un lecteur de badge de type P80 ;
- un lecteur de badge de type PK80 ;
- un bouton poussoir de sortie libre associé à chaque lecteur de badge ;
- un coffret métallique protégé par un tamper et un système basé sur des accéléromètres ;
- une UTL intégrée dans le coffret métallique ;
- un dispositif de filtrage (pare-feu) intégré dans le coffret métallique (hors périmètre) ;
- un switch avec filtrage MAC directement connecté à l'UTL (hors périmètre) ;
- un serveur (hors périmètre).

Pour les deux maquettes, le matériel suivant a également été fourni :

- quatre badges de type Mifare DESFIRE EV3 (hors périmètre) ;
- un poste d'exploitation (hors périmètre).

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-07].

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.

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

Les deux maquettes préinstallées et prêtes à l'emploi du produit ont été mises en route par le développeur aux côtés de l'évaluateur.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

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

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

2.2.4 *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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

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 inexploitables dans le contexte défini par la cible de sécurité [CDS].

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

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

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 a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

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.

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 « UTL SCAiP PoE avec lecteurs transparents, Version UTL fV2005, version Lecteurs fV2003 » 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], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- Le certificat généré pour le serveur web doit avoir un *Common Name* correspondant au nom de domaine pour lequel il est utilisé.

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 : - Cible de sécurité CSPN – SCAiP PoE avec lecteurs transparents, version 3.6, 3 avril 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cible de sécurité CSPN – SCAiP PoE avec lecteurs transparents, version 3.7, 8 avril 2025.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN *SCAiP* , référence OPPIDA/CESTI/CSPN/2024/LIBELLULE2/RTE, version 4.0, 3 avril 2025.
[GUIDES]	Guide d'utilisation, d'administration et d'installation du produit : - Plan de l'architecture de tests CSPN, référence « Architecture test CSPN V2.pdf » ; - Manuel utilisateur, référence *« iPassan Manager user manual FR*.pdf » ; - Notice simplifiée pour la mise en place d'un site ANSSI, référence *« Notice IPassan manager FR* – ANSSI simplifié - V2.1.pdf », version 2.1.

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.
[NOTE-07]	Note d'application - Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN, référence ANSSI-CSPN-NOTE-07, version v2.0, 23 novembre 2023.
[BSZ_CSPN]	*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.