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-2020/39

Evolynx-ITL

iPerflex V8.2.1a4

Fait le 25 novembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2020/39**
Nom du produit **Evolynx-ITL**
Référence/version du produit **iPerflex V8.2.1a4**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Secure systems & services** Bat C Le Millenium 180 rue René Descartes, CS 80339 13799 Aix-En-Provence Cedex 3
Développeur **Secure systems & services** Bat C Le Millenium 180 rue René Descartes, CS 80339 13799 Aix-En-Provence Cedex 3, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Protection des données échangées entre le serveur et le contrôleur ITL Protection des données échangées entre le contrôleur ITL et le contrôleur UED Protection en transmission du code PIN Sécurisation du contrôleur ITL Sécurisation du contrôleur UED Sécurisation du lecteur / Lecteur clavier
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. 3.2)

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 www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Evolynx-ITL, iPerflex V8.2.1a4 » développé par Secure Systems & services.

Ce produit est un ensemble de composants appartenant à une solution de contrôle d'accès physique.

La solution complète inclut les sous-systèmes suivants :

- des badges utilisés par les porteurs ;
- des lecteurs de badges :
    - lecteur simple STID (ARC-W33-A/PH5-7AD/1) ;
    - lecteur clavier physique STID (ARC-W33-B/PH5-7AD/1) ;
    - lecteur clavier tactile STID (ARC- W33-C/PH5-7AD/1).
- des équipements terrain, à savoir :
    - des unités de traitement local ITL embarquant une SAM *NXP SAM AV2* ;
    - des unités de contrôle d'accès UED ;
- des serveurs de base de données, d'application et de communication, ainsi que les postes d'exploitation associés ;
- un poste d'encodage SAM ;
- des composants de confiance externes pour l'authentification (serveur RADIUS et une PKI).

Seuls les ITL, les UED et les lecteurs de badges sont visés par ce rapport de certification : les autres composants sont hors-périmètre et n'ont pas été évalués.

La figure ci-dessous explicite l'architecture de la solution.

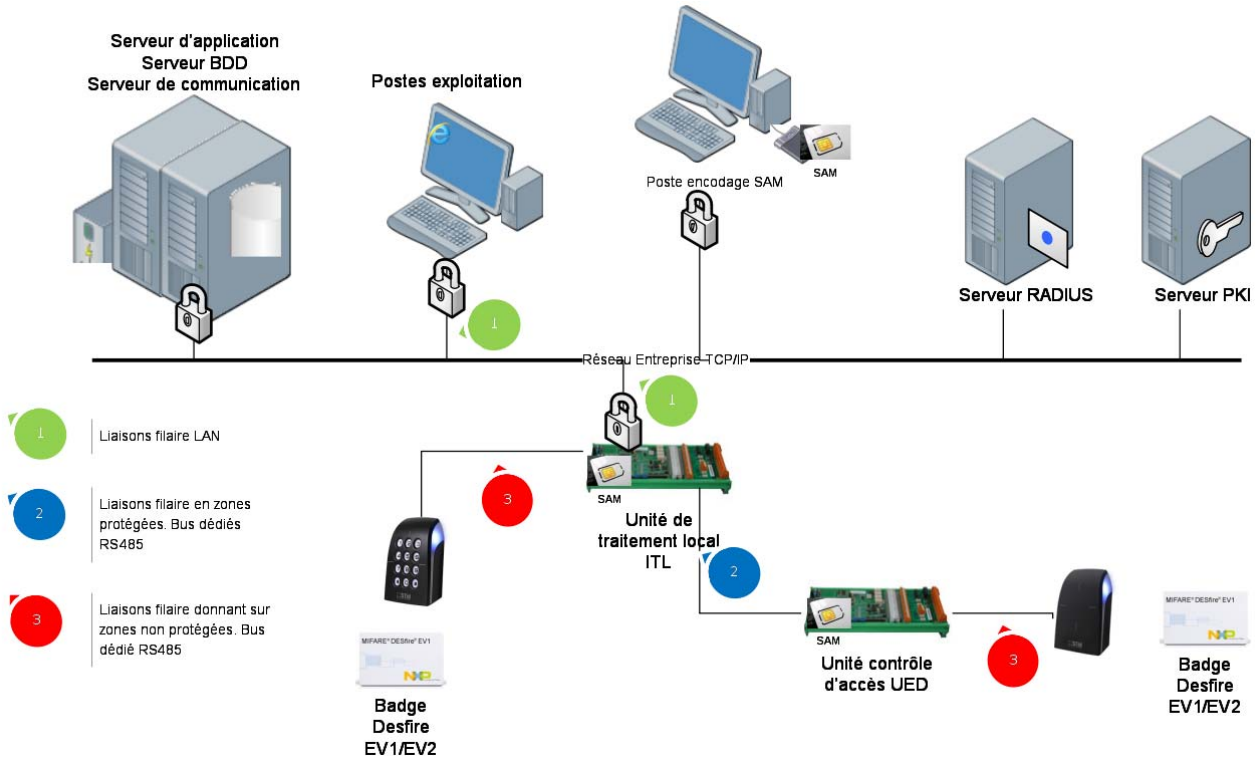

Figure 1 - Architecture Produit.

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	Evolynx-ITL
Numéro de la version évaluée	iPerflex V8.2.1a4

La version certifiée du produit peut être vérifiée dans le menu « À propos » de l'interface web :

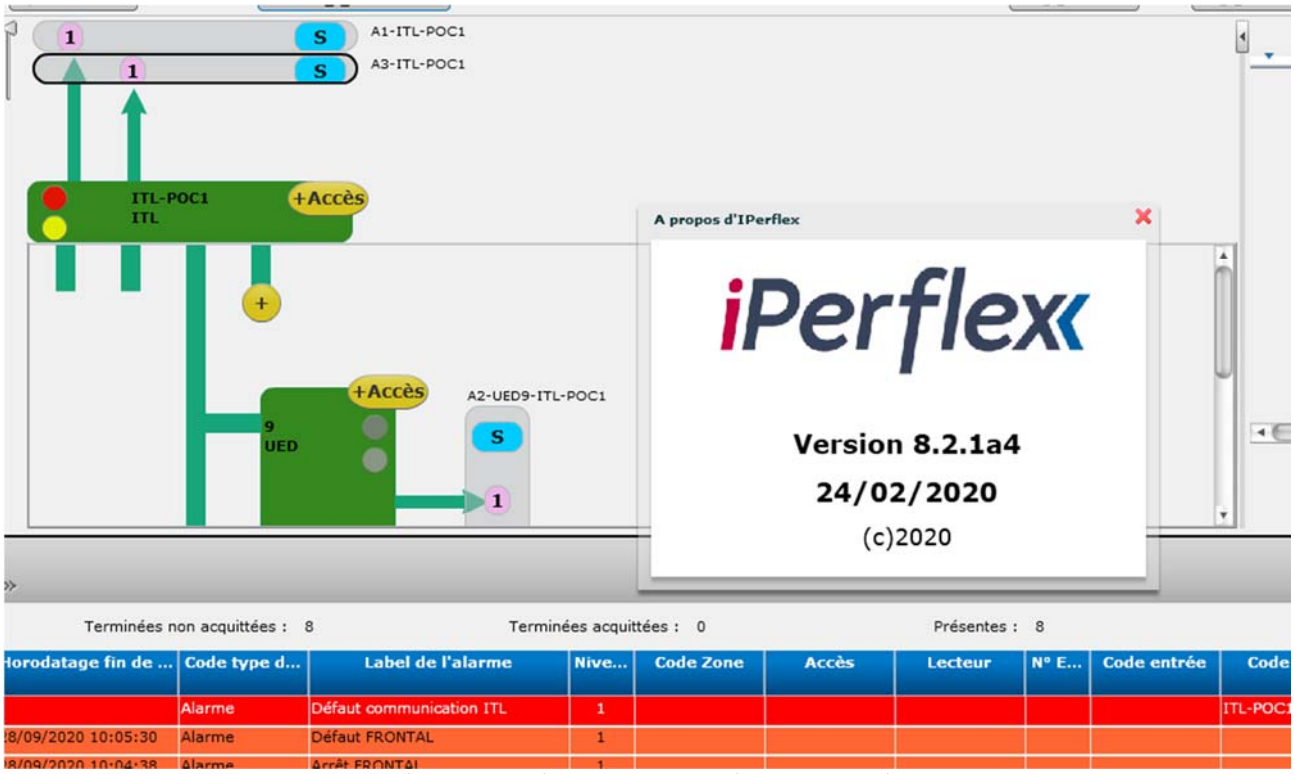

Figure 2 : Affichage de la version du produit

La version du firmware de l'ITL est la V8.2.0c. Elle peut être consultée soit depuis l'application web IPerflex (en cliquant sur l'ITL ou l'UED depuis l'explorateur de configuration), soit depuis la page d'accueil du serveur web embarqué de l'ITL.

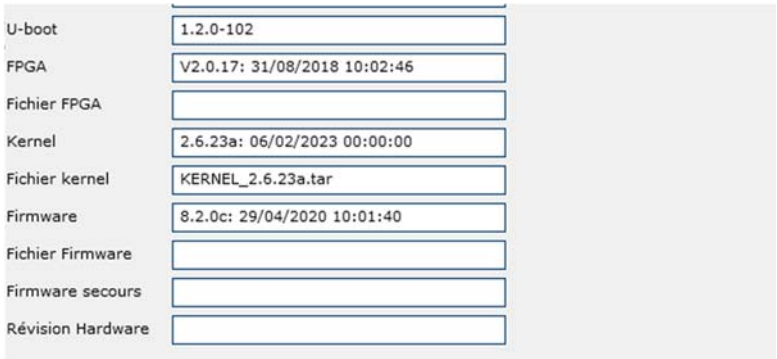

Figure 3 : Affichage de la version du firmware ITL depuis l'application web iPerflex

Figure 4 : Affichage de la version du firmware ITL depuis le serveur web embarqué

Les versions de lecteurs sont également consultables depuis l'application web IPerflex.

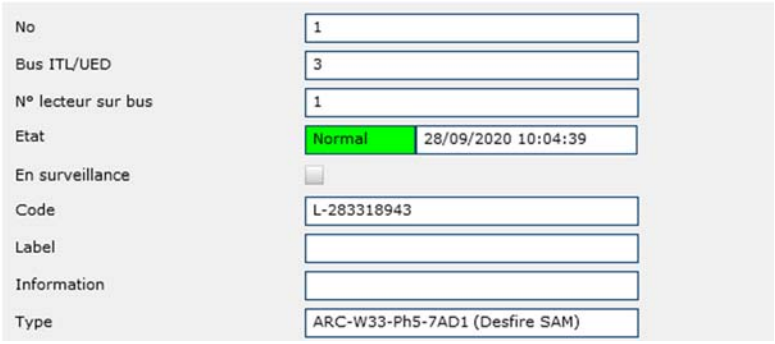

Figure 5 : Affichage de la version des lecteurs depuis l'application web iPerflex

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection des données échangées entre le serveur et le contrôleur ITL ;
- la protection des données échangées entre le contrôleur ITL et le contrôleur UED ;
- la protection en transmission du code PIN ;
- la sécurisation du contrôleur ITL ;
- la sécurisation du contrôleur UED ;
- la sécurisation du lecteur / lecteur clavier.

1.2.4 *Configuration évaluée*

La configuration évaluée, servant également de plateforme de tests, est une maquette constituée

- d'un serveur de gestion des accès iPerflex ;

- d'une station d'exploitation des SAM et de la solution iPerflex ;
- d'un serveur hébergeant Radius et une PKI ;
- d'un *switch* ;
- d'un contrôleur ITL ;
- d'une interface UED ;
- de trois lecteurs de proximité avec clavier et sans clavier (voir références au chapitre 1.1).

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. L'évaluation n'a pas intégralement suivi les exigences de la [NOTE-07], qui n'était pas encore applicable au moment de l'enregistrement du projet d'évaluation – ce point entre pour partie dans les recommandations et restrictions d'usage du produit, qui imposent un strict contrôle des accès physiques aux ITL (voir section 3.2). 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

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

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

Le produit est livré pré-installé par le développeur.

2.3.1.3 Durée de l'installation

Sans objet.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

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

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

2.3.3 *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.

2.3.4 *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 connues existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

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 pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.3.7 *Accès aux développeurs*

Sans objet.

2.3.8 *Analyse de la facilité d'emploi*

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 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.

2.3.8.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

Le produit a fait l'objet d'une analyse des mécanismes cryptographiques au titre de cette évaluation CSPN. Cette analyse n'a pas relevé de vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le produit a fait l'objet d'une analyse du générateur d'aléas au titre de cette évaluation CSPN. Cette analyse n'a pas relevé de vulnérabilité exploitable.

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 « Evolynx-ITL, version iPerflex V8.2.1a4 » 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les restrictions d'usage suivantes sans lesquelles le présent certificat n'est pas valide :

- les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées. En particulier, l'utilisateur doit s'assurer qu'il respecte :
    - l'hypothèse *Installation des ITL/UED*, afin d'interdire aux personnes non autorisées d'accéder physiquement à l'ITL,
    - les hypothèses relatives aux serveurs, ce qui nécessite impérativement de mettre en œuvre les recommandations du guide « Guide de sécurisation du Serveur Jboss sur l'infrastructure Evolynx » ;
- les utilisateurs doivent impérativement se conformer aux recommandation des documents [GUIDE], en particulier les recommandations du guide « Guide de sécurisation de l'infrastructure Evolynx – ITL ».

ANNEXE A. Références documentaires du produit évalué

[CDS]	Evolynx-NT-FR - Architecture cible de securité Référence : Evolynx-NT-FR ; Version : D ; Date : 28 janvier 2020.
[RTE]	Rapport Technique d'Évaluation CSPN - Secure System – Evolynx iPerflex Référence : OPPIDA/CESTI/Evolynx-ITL/RTE ; Version : 1.3 ; Date : 5 novembre 2020.
[GUIDE]	GS - Guides de spécification : • Configuration - Référence : EPF-SYS-1307-520-A-FR ; • Droits accès - Référence : EPF-SYS-1307-521-A-FR ; • Personnes,badges - Référence : EPF-SYS-1307-522-C-FR ; • Archivage mensuel - Référence : EPF-SYS-1309-523-B-FR. GU - Guides d'utilisation : • Gestion comptes utilisateurs – référence : EPF-SYS-1312-528-B-FR ; • Card Mapping – référence : EPF-SYS-1602-537-B-FR ; • Maintenance système - référence : sans - version : C – date : 4 avril 2018 ; • Guide de sécurisation de l'infrastructure Evolynx - ITL - référence : sans - version : B – date : 1 octobre 2020 ; • Security Module SAM - référence : sans - version : A – date : 12 janvier 2018 ; • Guide de sécurisation du Serveur Jboss sur l'infrastructure Evolynx – référence : sans – version : B – date : 6 novembre 2020. MI - Manuels d'installation : • Déploiement_PKI_win2012 – référence : sans ; • Manuel d'Installation - Installation Système iPerflex – référence : sans – version : S – date : 4 juin 2018 ; • Manuel d'installation – référence : EPF-HDW-1103-427-C-FR . MREF - Manuel de référence : • Sécurité informatique – référence EPF-SYS-1102-424-B-FR ; • Evolynx - MR - FR - Manuel de référence – référence : sans – version : E.

ANNEXE B. 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, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.
[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 1.0, 7 juillet 2020.