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-2025/12

EvolynxNG

Version supervision 2024.2 ; Version firmware ITL/UED : 8.3.2a

Paris, le 14/8/2025 | 18:30 CEST

Vincent Strubel

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-2025/12

Nom du produit

EvolynxNG

Référence/version du produit

Version supervision 2024.2 ; Version firmware ITL/UED : 8.3.2a

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
Bât C LE MILLENIUM, 180 rue René Descartes, CS80339
13799 Aix-en-Provence Cedex 3, France

Développeur

SECURE SYSTEMS & SERVICES
Bât C LE MILLENIUM, 180 rue René Descartes, CS80339
13799 Aix-en-Provence Cedex 3, 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 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
Protection des données échangées entre le poste opérateur et le serveur d'application
Protection des données échangées entre la base de données et les applications
Protection des connexions opérateurs

Protection des privilèges opérateurs Protection des données sensibles stockées dans la base de données Protection du mot de passe d'accès à la base de données Protection de l'intégrité des *firmware* ITL/UED Protection du démarrage des ITL/UED ainsi que de l'intégrité des *flash*
Fonctions de sécurité non évaluées Non
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

1.1 Présentation du produit

Le produit évalué est « EvolynxNG, Version supervision 2024.2 ; Version firmware ITL/UED : 8.3.2a » développé par SECURE SYSTEMS & SERVICES.

Ce produit est une solution de sûreté adaptée aux infrastructures multi-sites et permettant de gérer de façon centralisée les droits d'accès physique d'une population.

La solution est composée des éléments suivants :

- un GAC, composé des éléments suivants :
  - serveur de base de données ;
  - serveur web ;
  - serveur d'application ;
  - frontal de communication.
- des équipements de terrains, constitués de :
  - une ITL32 (UTL) ;
  - une UED (unité de contrôle d'accès) ;
  - des lecteurs de badges Stid DESFire (référence ARC-W33x /PH5-7AD) ;
  - des badges DESFire EV2/EV3.

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

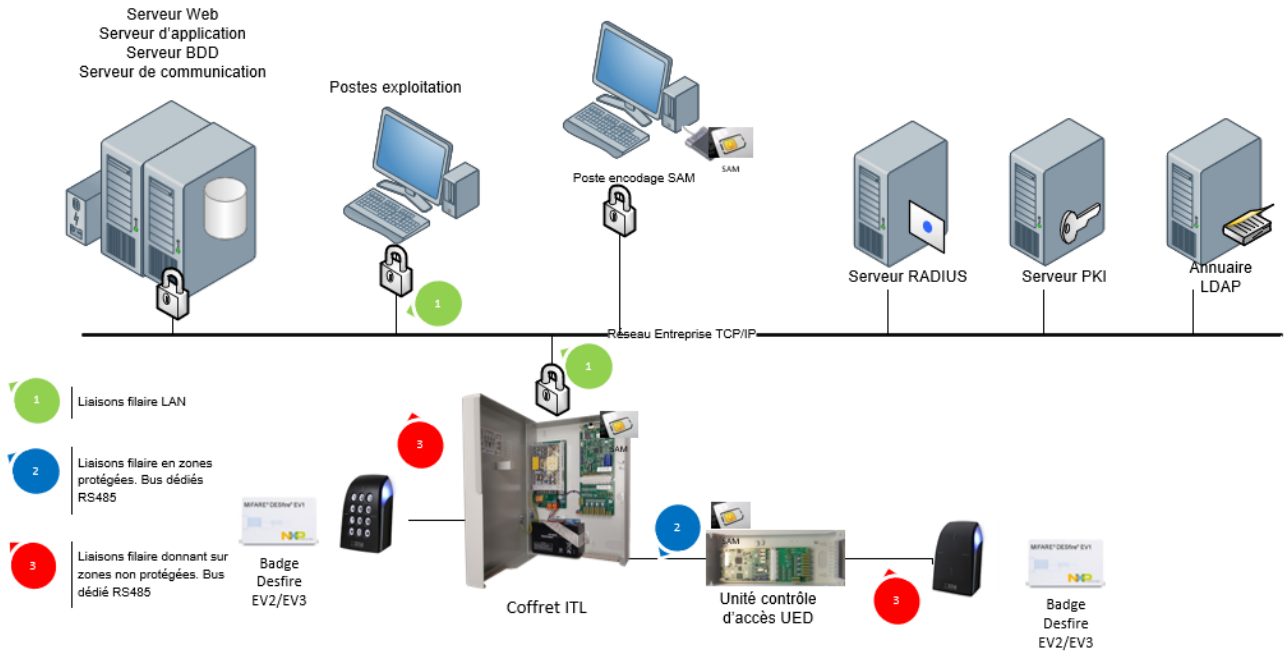


Figure 1 - Architecture Produit.

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*

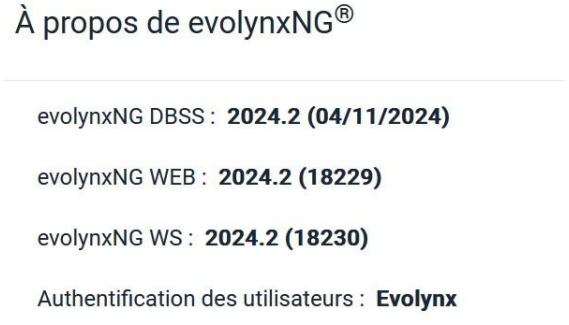
☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☒	**6**	**identification, authentification et contrôle d'accès**
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	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*

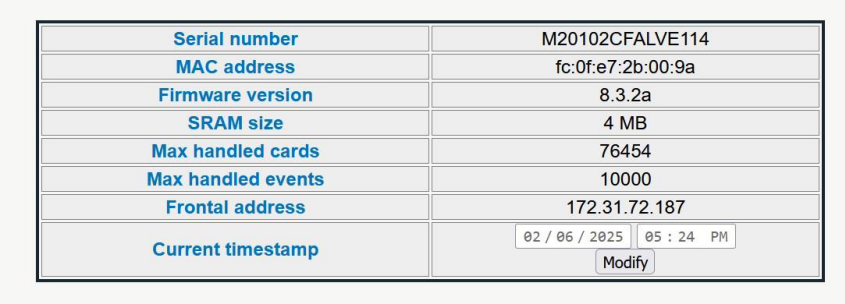
Produit	
Nom du produit	EvolynxNG
Numéro de la version évaluée	Version supervision 2024.2 ; Version firmware ITL/UED : 8.3.2a

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

- pour le GAC : depuis l'interface web de l'application EvolynxNG :



- pour l'ITL : depuis son interface web :



Serial number	M20102CFALVE114
MAC address	fc:0f:e7:2b:00:9a
Firmware version	8.3.2a
SRAM size	4 MB
Max handled cards	76454
Max handled events	10000
Frontal address	172.31.72.187
Current timestamp	02 / 06 / 2025 05 : 24 PM Modify

- pour les lecteurs : les versions des *firmware* peuvent être retrouvées sur l'interface web de l'application EvolynxNG, dans l'onglet « Configuration » puis « lecteurs ».

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 ;
- la protection des données échangées entre le poste opérateur et le serveur d'application ;
- la protection des données échangées entre la base de données et les applications ;
- la protection des connexions opérateurs ;
- la protection des privilèges opérateurs ;
- la protection des données sensibles stockées dans la base de données ;
- la protection du mot de passe d'accès à la base de données ;
- la protection de l'intégrité des *firmware* ITL/UED ;
- la protection du démarrage des ITL/UED ainsi que de l'intégrité des *flash*.

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		Windows Server 2022
	Applicatifs	Serveur Apache Serveur Wildfly Serveur d'application EvolynxNG Frontal de communication	
	Base de données	Oracle	

	Fonctions cryptographiques	OpenSSL (serveur Apache, frontal de communication) OpenJDK (serveur Wildfly)	
	Annuaires		Active Directory
ITL	Système d'exploitation	Linux microship	
	Applicatifs	*Firmware* *Appweb*	
	Fonctions cryptographiques	OpenSSL MbedTLS Librairies AES, SHA, HMAC soft Dialogue ITL/UED	
	SAM		SAM NXP AV3
UED	Système d'exploitation	Linux microship	
	Applicatifs	*Firmware*	
	Fonctions cryptographiques	OpenSSL Librairies AES, SHA, HMAC soft Dialogue ITL/UED	
	SAM		SAM NXP AV3
Lecteurs	Lecteurs simples	Stid réf. ARCW33APH57AD1	
	Lecteurs-clavier	Stid réf. ARCW33BPH57AD1 ARCW33CPH57AD1	
Badges			DESFire EV2/EV3

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

Le produit a été installé par le CESTI dans ses locaux.

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 des mécanismes cryptographiques ainsi que de certains éléments 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.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

Les mécanismes cryptographiques suivants n'ont pas été analysés car ils sont implémentés par un composant tiers :

- Oracle *NNES (Native Network Encryption Security)* ;
- Oracle *TDE (Transparent Data Encryption).*

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 « EvolynxNG, Version supervision 2024.2 ; Version firmware ITL/UED : 8.3.2a » 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].

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 evolynxNG, référence Evolynx-CS-FR- Cible de sécurité evolynxNG – F, version F, 5 novembre 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cible de sécurité evolynxNG, référence Evolynx-CS-FR- Cible de sécurité evolynxNG – G, version G, 30 juillet 2025.
[RTE]	Rapport technique d'évaluation : - Titre du Rapport Technique d'Evaluation CSPN - EvolynxNG, référence OPPIDA/CESTI/2025/Evolynx/RTE, version 1.2, 24 juillet 2025.
[GUIDES]	Guide d'installation du produit : - Guide d'installation EvolynxNG, référence EvolynxNG-MI-FR - Guide installation-2024.2-A.pdf, version A, 4 novembre 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 5.0, 6 mars 2024. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 6 mars 2024.
[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 2.1, 13 février 2025.
[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.