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-2026/10

Système de contrôle d'accès XSecur'-Evo

Version 2.1

Paris, le 4/6/2026 | 23:18 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-2026/10

Nom du produit

Système de contrôle d'accès XSecur'-Evo

Référence/version du produit

Version 2.1

Catégorie de produit

Identification, authentification et contrôle d'accès

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

SYNCHRONIC
393 rue des Manets, ZAC des Champs Fleuris
76520 Franqueville Saint Pierre, France

Développeur

SYNCHRONIC
393 rue des Manets, ZAC des Champs Fleuris
76520 Franqueville Saint Pierre, France

Centre d'évaluation

LEXFO
17 Avenue Hoche
75008 Paris

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Autoprotection des coffrets
Sécurisation de la carte d'extension SAM-SE
Sécurisation du lecteur
Protection des échanges de données par le protocole SCP03
Protection des échanges de données par les protocoles SBus et SSCPv2
Protection des échanges de données par le protocole TLS (Serveur CA – Concentrateur)
Protection des *Firmwares*
Protection des données du concentrateur
Vérification des certificats
Authentification des équipements par le protocole RADIUS

Protection des échanges de données par le protocole TLS (Serveur CA – Poste client / Station d'encodage) Protection du logiciel Authentification des exploitants Gestion des droits applicatifs Cloisonnement des ressources du contrôle d'accès
Fonctions de sécurité non évaluées Sans objet
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 « Système de contrôle d'accès XSecur'-Evo, Version 2.1 » développé par SYNCHRONIC.

Ce produit est une solution de sécurisation d'accès physique via l'utilisation de technologies sans contact RFID 13,56 MHz suivant la norme ISO 14443-A.

La solution s'articule autour de deux ensembles communicants :

- le « **GAC** » (Gestion des Accès Contrôlés), composé des éléments suivants de l'infrastructure informatique :
  - le serveur CA, comprenant les logiciels et les bases de données de gestion/exploitation ;
  - l'autorité de certification (non fourni par SYNCHRONIC) ;
  - le serveur RADIUS (non fourni par SYNCHRONIC) ;
  - les postes clients ;
  - la station d'encodage de badges ;
  - la station de programmation SAM-SE ;
- l'« **UTL pour XSecur'-Evo** », composée des équipements terrain :
  - les concentrateurs d'accès de la gamme d'UTL pour XSecur'-Evo ;
  - les modules de portes sécurisés UTP-SEC-EVO ;
  - les lecteurs et lecteurs-claviers ;
  - les badges MIFARE® DESFire® EV2 / EV3 (natif ou applet sur JavaCard – p.ex. : JCOP 3, JCOP 4.5)

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

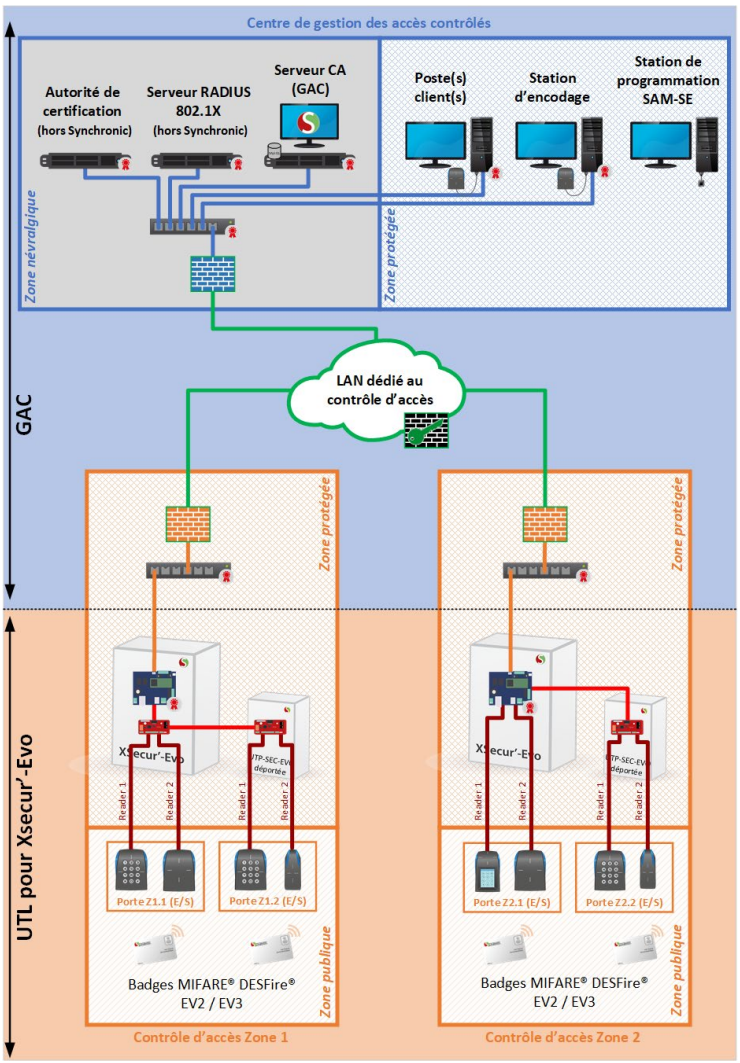


Figure 1 - Architecture Produit.

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*

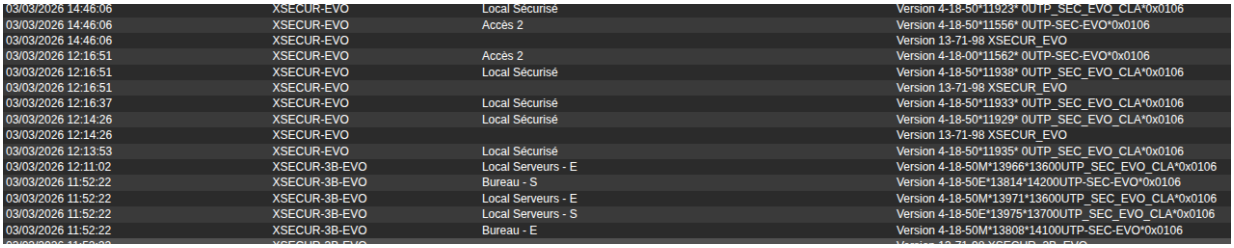
Produit	
Nom du produit	**Système de contrôle d'accès XSecur'-Evo**
Numéro de la version évaluée	**Version 2.1**

La version certifiée du produit peut être identifiée à partir de l'interface web et du XT Manager du GAC :

- pour le *firmware* Xpert (version 13-17-98) :

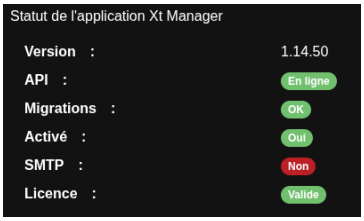
Firmware/modules	Activé	Information
Xpert	Oui	installé (V13-71-98)
Module iptablesd (Pare-feu)	Oui	installé (V01-36-00)
Module WEB	Oui	installé (V15-41-50)
Module MODBUS	Non	installé (V19-12-00)
Module XPE-RTC	Non	installé (V21-14-00)
Module TCP	Non	installé (V21-16-00)
Module CA	Non	non installé
Module TLS	Oui	installé (V02-37-50)
Module JANUS	Non	installé (V03-11-00)
Module Reseau Mobile	Non	installé (V21-07-00)
Module SNMP	Non	non installé
Module OSB	Non	non installé

- pour les modules UTP-SEC-EVO (version 4-18-50) :



03/03/2026 14:46:06	XSECUR-EVO	Local Sécurisé	Version 4-18-50*11923* 0UTP_SEC_EVO_CLA*0x0106
03/03/2026 14:46:06	XSECUR-EVO	Accès 2	Version 4-18-50*11556* 0UTP-SEC-EVO*0x0106
03/03/2026 14:46:06	XSECUR-EVO		Version 13-71-98 XSECUR_EVO
03/03/2026 12:16:51	XSECUR-EVO	Accès 2	Version 4-18-00*11562* 0UTP-SEC-EVO*0x0106
03/03/2026 12:16:51	XSECUR-EVO	Local Sécurisé	Version 4-18-50*11938* 0UTP_SEC_EVO_CLA*0x0106
03/03/2026 12:16:51	XSECUR-EVO		Version 13-71-98 XSECUR_EVO
03/03/2026 12:16:37	XSECUR-EVO	Local Sécurisé	Version 4-18-50*11933* 0UTP_SEC_EVO_CLA*0x0106
03/03/2026 12:14:26	XSECUR-EVO	Local Sécurisé	Version 4-18-50*11929* 0UTP_SEC_EVO_CLA*0x0106
03/03/2026 12:14:26	XSECUR-EVO		Version 13-71-98 XSECUR_EVO
03/03/2026 12:13:53	XSECUR-EVO	Local Sécurisé	Version 4-18-50*11935* 0UTP_SEC_EVO_CLA*0x0106
03/03/2026 12:11:02	XSECUR-3B-EVO	Local Serveurs - E	Version 4-18-50M*13966*13600UTP_SEC_EVO_CLA*0x0106
03/03/2026 11:52:22	XSECUR-3B-EVO	Bureau - S	Version 4-18-50E*13814*14200UTP-SEC-EVO*0x0106
03/03/2026 11:52:22	XSECUR-3B-EVO	Local Serveurs - E	Version 4-18-50M*13971*13600UTP_SEC_EVO_CLA*0x0106
03/03/2026 11:52:22	XSECUR-3B-EVO	Local Serveurs - S	Version 4-18-50E*13975*13700UTP_SEC_EVO_CLA*0x0106
03/03/2026 11:52:22	XSECUR-3B-EVO	Bureau - E	Version 4-18-50M*13808*14100UTP-SEC-EVO*0x0106

- pour le XT Manager du GAC (version 1.14.50) :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'autoprotection des coffrets ;
- la sécurisation de la carte d'extension SAM-SE ;
- la sécurisation du lecteur ;
- la protection des échanges de données par le protocole SCP03 ;
- la protection des échanges de données par les protocoles SBus et SSCPv2 ;
- la protection des échanges de données par le protocole TLS (Serveur CA – Concentrateur) ;
- la protection des *firmwares* ;
- la protection des données du concentrateur ;
- la vérification des certificats ;
- l'authentification des équipements par le protocole RADIUS ;
- la protection des échanges de données par le protocole TLS (Serveur CA – Poste client / Station d'encodage) ;
- la protection du logiciel ;
- l'authentification des exploitants ;
- la gestion des droits applicatifs ;
- le cloisonnement des ressources du contrôle d'accès.

1.2.4 *Configuration évaluée*

Le tableau ci-dessous explicite 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 Windows 11
	Applicatifs	XT Manager v1.14.50 ServeurUG TLS v5.33.0	
	Fonctions cryptographiques	XT Manager : OpenSSL 3.1 ServeurUG TLS : mbedTLS 3.6.5	
	Bases de données et annuaires		MySQL Server 8.4
UTL	Matériel	UTL : PCB XL02-v7 / XP02-v5a (Atmel ATSAMA5D44B-CU) UTP-SEC-EVO : PCB V10 (NXP Kinetis MK11DxxxxAVLK5, xxxx selon taille mémoire)	
	Système d'exploitation	UTL : v7-01-00 • Linux 6.6 (Microchip LTS) • Debian 12 UTP-SEC-EVO : sans OS	
	Applicatifs	UTL : Firmware Xpert 13-71-98 UTP-SEC-EVO : 4-18-50	
	Fonctions cryptographiques	UTL : mbedTLS 3.6.5 UTP-SEC-EVO : • mbedTLS 3.6.5 ; • mmCAU *library* 1.4	

	SAM	SAM-SE : PCB SAM V4 (NXP SE050C)	
Lecteurs	Lecteurs simples	SSCPv2 : Z18-Z22	
	Lecteurs-claviers	SSCPv2 : Z18-Z22	
Badges			DESFire EV3 : MF3D(H)x3 DESFire EV2 : MF3D(H)x2 (H selon format, x selon capacité) JCOP 4.5 sur P71D600

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 déployé dans un environnement de test (maquette préinstallée) dans les locaux du CESTI, par les ingénieurs de SYNCHRONIC.

2.2.1.3 Notes et remarques diverses

La configuration retenue pour la CSPN est telle qu'il n'est pas possible d'abaisser le niveau de sécurité une fois la solution déployée, des tests ont été effectués en ce sens dans l'analyse des fonctions de sécurité.

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 et de la gestion des lecteurs dans les modules UTP, ainsi que la partie Web du GAC.

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

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

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 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 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 « Système de contrôle d'accès XSecur'-Evo, Version 2.1 » 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 – Système de contrôle d'accès XSecur'-Evo, version 3.5, 2 février 2026.
[RTE]	Rapport technique d'évaluation : - Rapport Technique - Evaluation CSPN – Solution XSecur'-Evo, référence SYN20260330, version 2.2, 13 mai 2026.
[GUIDES]	Guides d'installation du produit : - Documentation Installateur - XSecur'-Evo, version 3.1, 11 février 2026 ; - Documentation Installateur - Synchronisation *Firmware*, version 1.1, 12 novembre 2020 ; - Documentation Installateur - Xt Manager, version 1.0, novembre 2024. Guides d'utilisation du produit : - Documentation Utilisateur - Xt Manager, version 1.3, novembre 2024 ; - Documentation Utilisateur - Xt Print, version 1.1, octobre 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, 12 juillet 2024. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 12 juillet 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 4.2, 18 mars 2025.
[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.