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-2022/08

UTL pour XSecur'-Evo

Version 1.1

Paris, le 6 juillet 2022

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-2022/08**
Nom du produit **UTL pour XSecur'-Evo**
Référence/version du produit **Version 1.1**
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-St-Pierre, France
Développeur **SYNCHRONIC** 393 rue des Manets – ZAC des champs fleuris 76520 Franqueville-St-Pierre, France
Centre d'évaluation **TRUSTED LABS** 6 rue de la Verrerie – CS 20001 92197 Meudon Cedex, France
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 Protection des *Firmwares* Protection des données du concentrateur Vérification des certificats Authentification des équipements par le protocole RADIUS
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 www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « UTL pour XSecur'-Evo, Version 1.1 » développé par SYNCHRONIC.

Il est intégré aux équipements de terrain de la solution complète « XSecur'-Evo » de contrôle d'accès physique centralisé, articulée en deux sous-ensembles communicants :

- le système d'information de gestion des accès contrôlés (GAC), composé des éléments de l'infrastructure informatique de l'entreprise (serveur de base de données, serveur CA, serveur de certificats, serveur RADIUS, postes clients etc) ;
- l'« UTL pour XSecur'-Evo » (c'est-à-dire le produit évalué), composé des équipements de terrain :
    - les concentrateurs d'accès de la gamme d'UTL pour XSecur'-Evo ;
    - les modules de portes sécurisées UTP-SEC-EVO ;
    - les lecteurs et lecteurs/claviers ;
    - les badges MIFARE® DESFire® EV2.

L'« UTL pour XSecur'-Evo » utilise des technologies sans contact RFID ainsi que des claviers de saisie de codes PIN et s'interface avec le GAC via une liaison TCP/IP.

L'administration et l'exploitation de l'installation se fait à travers le GAC, tandis que l'UTL pour XSecur'-Evo permet de gérer les flux de personnes au sein des zones sensibles.

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

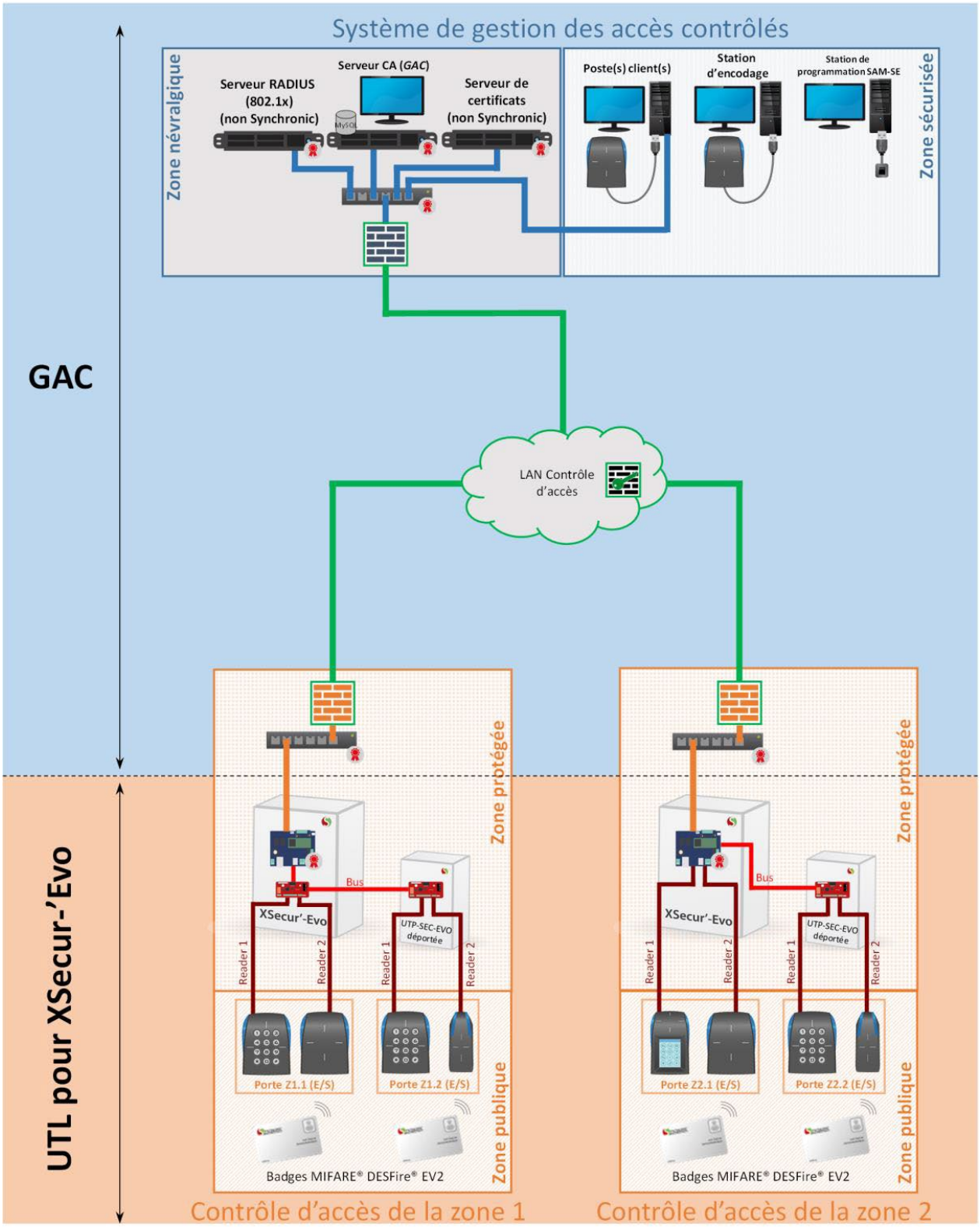

Figure 1 - Architecture du produit

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 pour XSecur'-Evo
Numéro de la version évaluée	Version 1.1 : Concentrateur XSecur'-Evo V13-44-51 Module UTP-SEC-EVO V4-08-00 Module TLS V2-29-00

La version certifiée des composants matériels du produit peut être identifiée par lecture de la version sérigraphiée sur les circuits imprimés des différentes cartes électroniques.

La version certifiée des composants logiciels du produit ainsi que la version des lecteurs peut être identifiée via l'application *Pack XPert Evolution* (via le menu « Fil de l'eau » puis « *Diagnostics* »).

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 ;
- la protection des *Firmwares* ;
- la protection des données du concentrateur ;
- la vérification des certificats ;
- l'authentification des équipements par le protocole RADIUS.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à la configuration générale « Mode durci » de Secur'Evolution pour le paramétrage du SAM-SE pour les lecteurs SSCPv2.

La plateforme de tests est constituée des éléments suivants :

- un PC qui implémente la partie Gestion des accès contrôlés (GAC) ;
- un Switch avec authentification RADIUS ;
- un Unité de Traitement Local (UTL) dans une armoire métallique intégrant :
    - une carte UGL XP02 d'Unité de Traitement de Porte (UTP) natif sur laquelle est connectée une carte mezzanine A5_SOCKET pour le concentrateur ;
    - une carte UTP-SEC-EVO ;
    - un Système de détection antieffraction ;
    - un système d'alimentation de secours par batterie.
- quatre lecteurs sans contact NFC (2 entrées et 2 sorties) avec une liaison utilisant le protocole SSCPv2 ;
- un ensemble de voyants et d'interrupteurs pour la simulation du fonctionnement de la porte.

L'installation a été réalisée en suivant les procédures et directives décrites dans [GUIDES].

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

Une plateforme de tests a été prêtée à l'évaluateur, qui a utilisé la documentation d'installation fournie par le développeur pour configurer le concentrateur XSecur'Evo et l'UTP en utilisant l'interface de maintenance en mode USB.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] 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.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit et fourni les résultats de l'analyse dans le rapport technique d'évaluation [RTE].

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 pour le niveau d'attaquant considéré et 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 pour le niveau d'attaquant considéré et 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

Les interfaces permettant de réaliser la configuration et les opérations de maintenance du produit sont intuitives et faciles à utiliser. Ces opérations nécessitent cependant un personnel préalablement formé sur les différents paramétrages.

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 « UTL pour XSecur'-Evo, Version 1.1 » 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 spécifié dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité UTL pour XSecur'-Evo, référence SYN-CIBLE-XSECUR-EVO-2.10, version 2.10, 11 mai 2022.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation VITAMINE - Synchronic (Norddalfjord), référence CP-2022-RT-515-1.1, version 1.1, 11 mai 2022.
[GUIDES]	Guides d'installation et configuration du produit : - Documentation Installateur XSecur'-Evo, version 2.1, 20 décembre 2021 ; - DU Secur'Evolution, version 2.2, 10 février 2020 ; - DI Synchronisation *Firmware*, version 1.1, 12 novembre 2020.

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 4.0, 3 mars 2022. 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 1.0, 7 juillet 2020.