Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2018/20

Xsecur'

Version UG V13-20-00 / UTP-Sec V2-10-00 / TLS V2-20-00

Paris, le 1er octobre 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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-2018/20

Nom du produit

Xsecur'

Référence/version du produit

Version UG V13-20-00 / UTP-Sec V2-10-00 / TLS V2-20-00

Catégorie de produit

Identification, authentification et contrôle d'accès

Critères 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

Développeur

Synchronic
393 rue des manets, ZAC des champs fleuris
76520 Franqueville St Pierre

Centre d'évaluation

Oppida
4-6 avenue du vieil étang, Bâtiment B,
78180 Montigny le Bretonneux, France

Fonctions de sécurité évaluées

Protection du concentrateur XSecur'
Protection du lecteur
Protection de l'ID Privé
Protection des échanges de données entre le concentrateur XSecur' et le lecteur
Protection des échanges de données entre le concentrateur XSecur' et le Serveur CA

Fonction(s) 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 Premier ministre 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Xsecur', version UG V13-20-00 / UTP-Sec V2-10-00 / TLS V2-20-00 » développé par *SYNCHRONIC*. Ce produit est un ensemble de composants appartenant à une solution de contrôle d'accès physique.
Le produit évalué inclut, comme l'indique la figure ci-après :

- le concentrateur d'accès XSecur' version UG V13-20-00 / UTP-Sec V2-10-00 / TLS V2-20-00 ;
- le lecteur/clavier STid ARC-W33-B-PH5-7AD (référence TCLDS-485 dans le schéma ci-dessous).

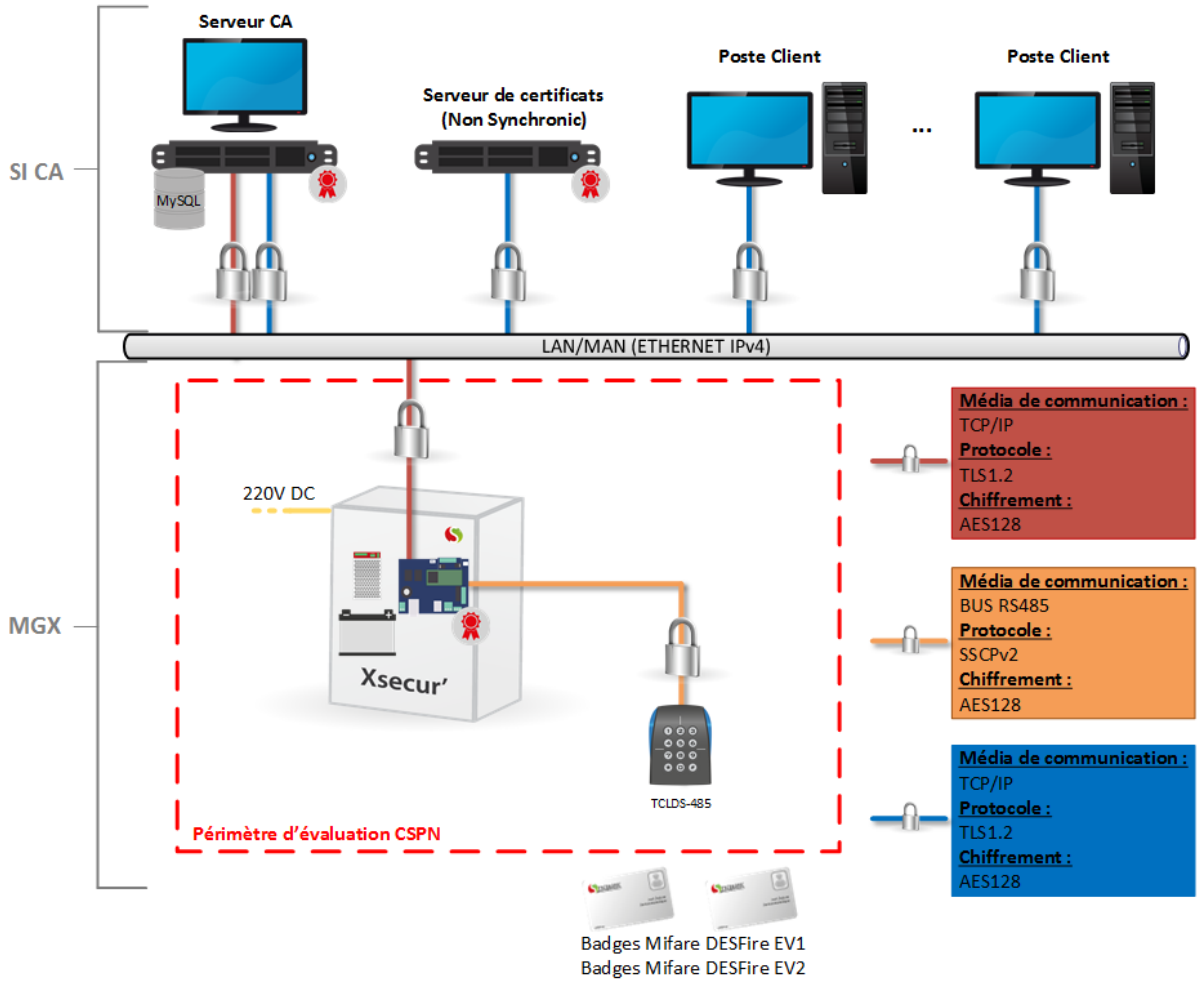

Figure 1 - Environnement du produit évalué

Le produit évalué interagit avec une partie intitulée « SI CA », composée :

- d'un serveur de certificats et d'un serveur CA hébergeant les bases de données et les logiciels de gestion/exploitation ;
- de postes clients.

Le produit impose l'utilisation de badges d'accès MIFARE® DESFire EV1 ou EV2.

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

Nom du produit	Xsecur'
Numéro de la version évaluée	Concentrateurs XSecur' incluant les versions logicielles UG V13-20-00 / UTP-Sec V2-10-00 / TLS V2-20-00 Utilisé en conjonction avec les lecteurs de badge STid de modèle ARC-W33-B-PH5-7AD.

L'identification du produit évalué est possible au travers de l'interface dite « fil de l'eau » :

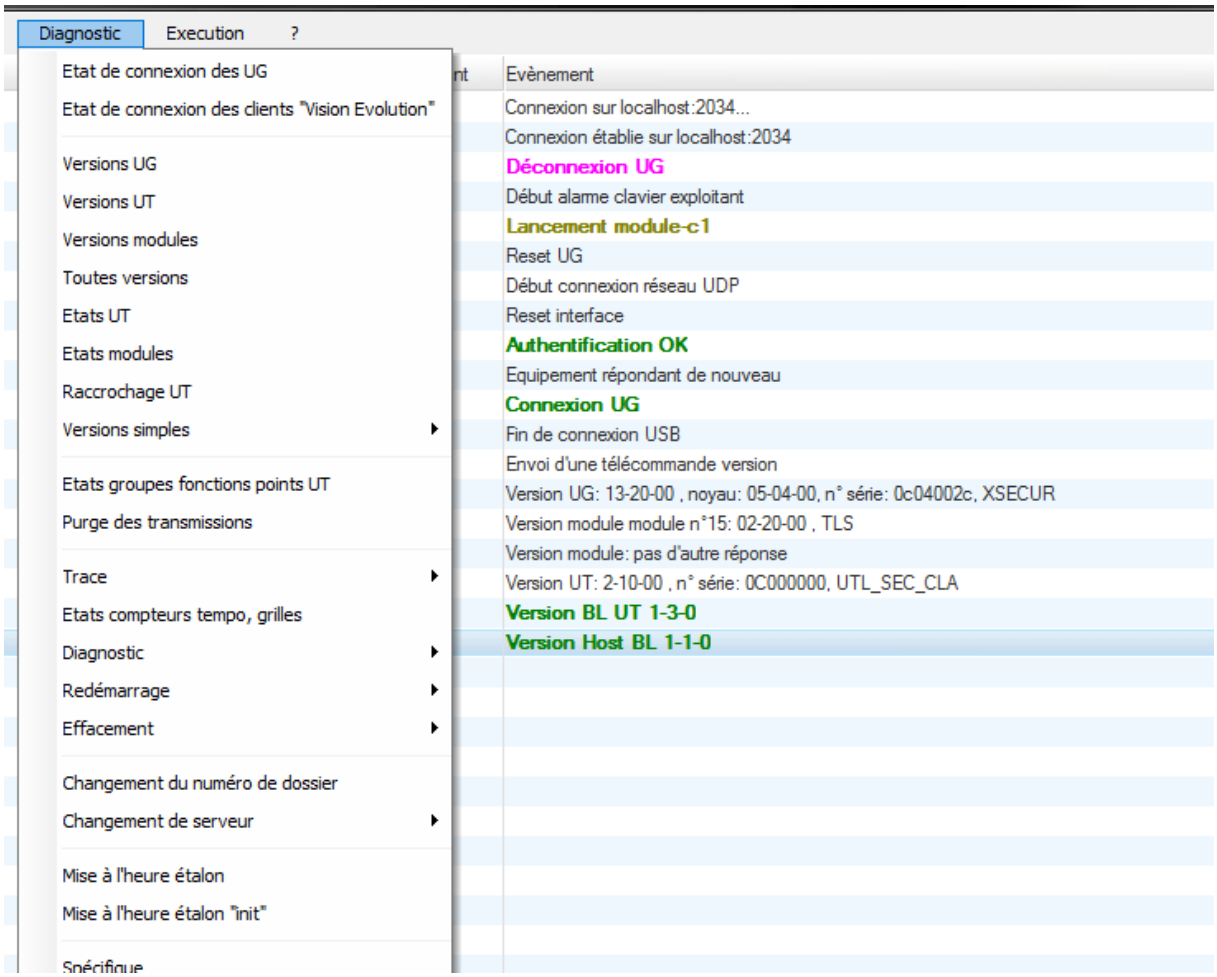

Figure 2 : Interface « fil de l'eau »

Il suffit ensuite de sélectionner les commandes relatives aux versions dans le menu déroulant :

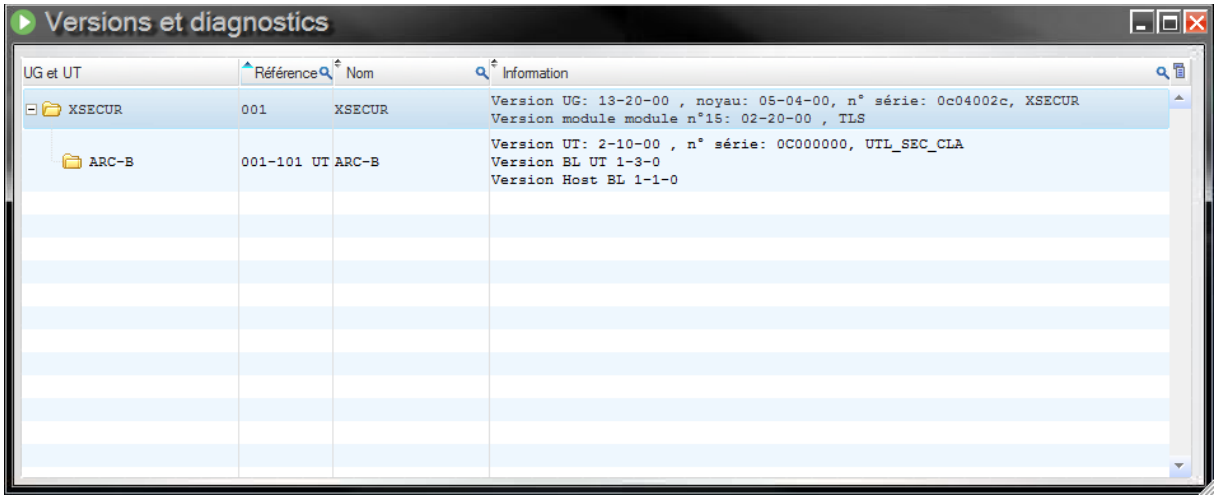

Figure 3 : Versions de l'UG et de l'UTL

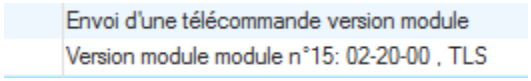

Figure 4 : Version du module TLS

L'identification des lecteurs de badge se fait par lecture de l'étiquette située à l'intérieur du lecteur. Cela ne peut donc se faire que lors de l'installation ou de la maintenance.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- protection du concentrateur XSecur' ;
- protection du lecteur ;
- protection de l'ID Privé ;
- protection des échanges de données entre le concentrateur XSecur' et le lecteur ;
- protection des échanges de données entre le concentrateur XSecur' et le Serveur CA.

1.2.4. Configuration évaluée

Le développeur indique une compatibilité de ses UTLs avec l'ensemble des équipements 7AD du fabricant STid, dans la section 2.6.2 de [CDS].
Cependant, le présent rapport ne certifie que la configuration évaluée du produit, mettant exclusivement en œuvre des lecteurs STid de modèle ARC-W33-B-PH5-7AD.
Les tests de cette évaluation ont été menés sur une maquette, et non des portes réelles (l'accès physique a été simulé).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. 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

Sans objet.

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

L'installation du produit a été effectuée avec l'aide des équipes du développeur. En conséquence, la procédure d'installation n'a pas été rigoureusement testée par l'évaluateur, ce qui donne lieu à des restrictions d'emploi (voir §3.2).

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

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit. Néanmoins, une formation dédiée reste recommandée, ainsi qu'indiqué au paragraphe 2.3.1.2.

2.3.3. Revue du code source (facultative)

L'évaluateur a eu accès au code source dans le cadre de l'analyse des mécanismes cryptographiques.

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 potentielles connues ont été identifiées sur le produit, et les briques tierces qu'il utilise. Cependant, elles sont considérées comme non exploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

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 dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.3.7. Accès aux développeurs

Un entretien avec les développeurs a été effectué afin d'installer la TOE.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

Sans objet.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Le présent rapport de certification ne se prononce pas sur la résistance des concentrateurs à une attaque physique – il est donc impératif que les concentrateurs d'accès soient installés et manipulés en zone non hostile, par des personnels compétents et de confiance. Ce point constitue une restriction d'usage (voir section 3.2).
Plus généralement, les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le CESTI a relevé que l'administrateur du produit aura besoin de l'assistance du développeur lors de l'installation et de la configuration du produit.

2.3.8.4. Notes et remarques diverses

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

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. L'évaluateur n'a pas relevé de vulnérabilité exploitable, dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.5. Analyse du générateur d'aléas

L'évaluateur n'a pas relevé de vulnérabilité exploitable, dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré, concernant les générateurs d'aléa mis en œuvre par le produit.

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 « Xsecur', version UG V13-20-00 / UTP-Sec V2-10-00 / TLS V2-20-00 » 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. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1 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].
La sécurité du produit est fortement dépendante de sa bonne installation et de sa bonne configuration initiale, qui ne sont pas garanties par l'évaluation du produit. Il est donc impératif que ces phases soient réalisées par des intégrateurs compétents et de confiance.
Par ailleurs, le présent rapport de certification ne se prononce pas sur la résistance des UTLs à une attaque physique – il est donc impératif que les concentrateurs d'accès soient installés et manipulés en zone non hostile, par des personnels compétents et de confiance.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité – XSECUR'* Référence SYN-CIBLE-XSECUR ; Version : 1.05 ; Date : 19 juillet 2018
[RTE]	*Rapport Technique d'Evaluation CSPN XSECUR'* Référence : OPPIDA/CESTI/ XSECUR/RTE ; Version : 2.2 ; Date : 14 septembre 2018

Annexe 2. 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, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 7 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.