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-2020/03

SYRIUS-2P2L-IP-EXT
Version 1660f

Paris, le 9 juin 2020

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-2020/03**
Nom du produit **SYRIUS-2P2L-IP-EXT**
Référence/version du produit **Version 1660f**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire / Développeur **Elsylog** **10-12 rue Marcel Paul** **Parc d'activités Les Berges de Seine 3** **95070 Bezons** **France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B** **78180 Montigny le Bretonneux** **France**
Fonctions de sécurité évaluées **Protection des échanges entre la tête de lecture et l'UTL** **Protection des échanges entre l'UTL et le serveur SYRACUSE** **Protection contre l'arrachement de l'UTL** **Détection d'ouverture de la tête de lecture** **Protection contre l'arrachement de la tête de lecture** **Protection du firmware**
Fonction(s) de sécurité non évaluées **Sans objet**
Restriction(s) d'usage **Non**

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 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le'UTL (Unité de Traitement Local) « SYRIUS-2P2L-IP-EXT, version 1660f » développé par *ELSYLOG*.

Ce produit appartient à l'ensemble de composants constituant la solution de contrôle d'accès physique SYRACUSE 6.01.01. Il permet notamment l'interprétation des flux depuis ou vers des têtes de lecture. Ces dernières sont chargées de transmettre à l'UTL les informations d'identification de badges *DESFIRE*. Deux modèles de tête de lecture *STID* ont été pris en compte dans le cadre de cette évaluation : ARCW33APH57AD1 et ARCW33BPH57AD1.

L'UTL *SYRIUS* est équipée d'une carte SAM AV2 de *NXP* permettant la gestion et la sécurisation des clés cryptographiques utilisées dans le cadre des communications avec le badge, ainsi que celles nécessaires à la communication avec le serveur *SYRACUSE*.

La figure ci-dessous explicite l'architecture du système SYRACUSE.

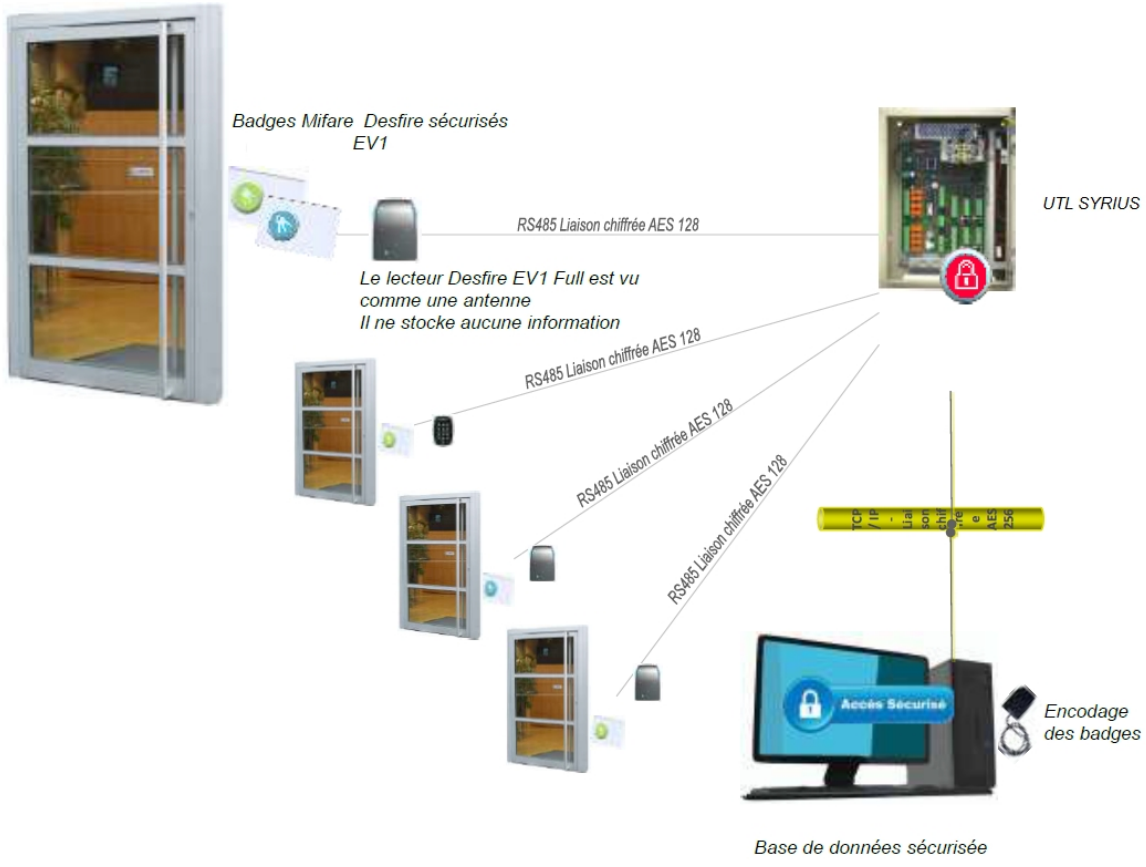

Figure 1 - Architecture du système SYRACUSE.

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	SYRIUS-2P2L-IP-EXT
Numéro de la version évaluée	1660f
Numéro de version de SYRACUSE	6.01.01
Têtes de lectures utilisées	ARCW33APH57AD1 ARCW33BPH57AD1

La version certifiée du produit peut être identifiée dans le logiciel *SYRACUSE* via le menu Commande / Intervention Lecteurs / Consultation.

La version du logiciel *SYRACUSE* est accessible dans « À propos ».

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- la protection des échanges entre la tête de lecture et l'UTL ;
- la protection des échanges entre l'UTL et le serveur *SYRACUSE* ;
- la protection contre l'arrachement de l'UTL ;
- la détection d'ouverture de la tête de lecture ;
- la protection contre l'arrachement de la tête de lecture ;
- la protection du *firmware* de l'UTL.

1.2.4. Configuration évaluée

La configuration évaluée correspond :
- à l'unité de traitement logique SYRIUS-2P2L-IP-EXT en version 1660f ;

- aux têtes de lecture *STID* : ARCW33APH57AD1 et ARCW33BPH57AD1 ;
- à un poste d'administration hébergeant le logiciel de gestion SYRACUSE.

La carte SAM dans l'UTL, le serveur SYRACUSE, le poste d'exploitation et le badge *DESFIRE* ne font pas partie du périmètre d'évaluation.

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

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

L'environnement d'évaluation a été fourni par Elsylog sous forme de maquette prête à l'emploi. L'évaluateur ne peut donc pas se prononcer sur cet aspect de l'évaluation.

2.3.1.3. Durée de l'installation

Sans objet.

2.3.1.4. Notes et remarques diverses

Néant.

2.3.2. Analyse de la documentation

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

2.3.3. Revue du code source (facultative)

L'évaluateur a revu le code source lié aux implémentations des fonctions cryptographiques du produit ainsi que le code de l'UTL dédié à la communication avec les lecteurs. L'analyse a été effectuée manuellement. 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

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.3.6.2. 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.

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs afin de comprendre et d'analyser les mécanismes cryptographiques du produit.

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

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur.

2.3.8.3. Notes et remarques diverses

L'interface du logiciel d'administration *SYRACUSE* est claire et facile d'accès.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit hors protection et gestion des clés cryptographiques ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

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 oeuvre 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 « SYRIUS-2P2L-IP-EXT, version 1660f » 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].

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN V1.4* UTL « SYRIUS-2P2L-IP-EXT version 1660f » Version :1.4 ; *Date : 13 février 2020.*
[RTE]	*Rapport Technique d'Évaluation CSPN CASSYR - SYRACUSE* Référence : OPPIDA/CESTI/CASSYR/RTE/1.3 ; Version : 1.3 ; *Date : 12 février 2020.*
[GUIDES]	*Installation Syracuse Version* Référence : ELS-MOI-2019-0002-0. *Installation des services Syracuse* Référence : ELS-MOI-2019-0003-1. *Configuration CSPN* Manuel de mise en configuration répondant aux critères liés à la CSPN. *Diagnostic* Manuel de diagnostic.

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, 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.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.