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-2021/15

## S4W

### version 3.10.41.100

Paris, le 27 juillet 2021

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

La reproduction de ce document sans altération ni coupure est autorisée.

| |
|---|
| Référence du rapport de certification<br>**ANSSI-CSPN-2021/15** |
| Nom du produit<br>**S4W** |
| Référence/version du produit<br>**version 3.10.41.100** |
| Catégorie de produit<br>**Automate programmable industriel** |
| Critère d'évaluation et version<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)** |
| Commanditaire<br>**LACROIX-SOFREL**<br>2, rue du Plessis<br>35770 Vern-Sur-Seiche |
| Développeur<br>**LACROIX-SOFREL**<br>2, rue du Plessis<br>35770 Vern-Sur-Seiche |
| Centre d'évaluation<br>**AMOSSYS**<br>11 rue Maurice Fabre<br>35000 Rennes |
| Fonctions de sécurité évaluées<br>Gestion des entrées malformées<br>Stockage sécurisé des secrets<br>Authentification sécurisée sur les interfaces d'administration et d'exploitation<br>Politique de droits<br>Signature du logiciel<br>Intégrité et confidentialité de la configuration<br>Intégrité des commandes du mode de fonctionnement<br>Communications sécurisées<br>Intégrité du journal local<br>Intégrité du journal déporté<br>Intégrité des paramètres de la ToE |
| Fonctions de sécurité non évaluées<br>Néant |
| Restriction(s) d'usage<br>Oui |

**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 « S4W, version 3.10.41.100 » développé par LACROIX-SOFREL.

Ce produit est un « Poste Local de Télégestion » (ou RTU), permettant de surveiller et contrôler, à distance, les installations techniques réparties sur les réseaux d'eau potable et d'assainissement.

Les S4W acquièrent, traitent et transmettent les données des différents organes de captage de ces ouvrages (états de marche et d'arrêt, défauts, mesures de niveau et de pression, taux de chlore, comptages, température, …). Ils enregistrent les événements qui se produisent sur l'installation.

Un réseau de télégestion est doté d'un « Poste Central de Télégestion » (SCADA, …) qui a pour rôle de centraliser les données acquises par les S4W sur les différentes installations. Ainsi, le Poste Central de Télégestion permet au personnel d'exploitation d'obtenir une vue globale du fonctionnement de ses installations.

Ce type de produit se rapproche d'un Automate Programmable Industriel (API), mais a ses spécificités.

Tout d'abord, à la différence d'un API, le S4W est préprogrammé, il ne nécessite donc pas de programme particulier fourni par l'utilisateur pour assurer les services d'acquisition, de traitement, d'archivage des entrées/sorties et des communications. Il suffit de configurer les services. Il peut, néanmoins, accepter un programme d'automatisme écrit par l'utilisateur pour compléter les services déjà existants.

Enfin, les modes d'utilisation et d'installation sont également différents :

- un API est installé dans une usine, et sa portée de communication se limite à un réseau IP local ;
- un RTU fonctionne sur un réseau distribué : il s'installe sur des sites géographiquement isolés (château d'eau, réservoir, station de pompage, poste de relèvement, …) et communique à distance avec des postes centraux de télégestion ou des utilisateurs. De plus, le RTU peut être amené à communiquer sur un réseau public (Internet) sur différents supports (cellulaire ou ADSL).

## 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*

La version du produit S4W peut être obtenue à l'aide de S4W-Tools. La procédure est la suivante :
- s'authentifier sur S4W-Tools ;
- se rendre dans l'onglet « Réseau » ;
- cliquer sur le S4W dont on souhaite récupérer le numéro de version.

Le numéro de version s'affiche dans le volet de droite dans la catégorie « logiciel ».

### 1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :
- la gestion des entrées malformées ;
- le stockage sécurisé des secrets ;
- l'authentification sécurisée sur les interfaces d'administration et d'exploitation ;
- la politique de droits ;
- la signature du logiciel ;
- l'intégrité et confidentialité de la configuration ;
- l'intégrité des commandes du mode de fonctionnement ;
- les communications sécurisées ;
- l'intégrité du journal local ;
- l'intégrité du journal déporté ;
- l'intégrité des paramètres de la TOE.

### 1.2.4 *Configuration évaluée*

L'évaluateur a eu accès à une TOE en configuration « de développement » et une TOE en configuration « de production ».

La plateforme d'évaluation est composée des postes suivants :
- des postes distants, hébergés sur un serveur ESXi :
  - un serveur SG4000 pour le lien VPN avec la TOE ;
  - un poste S4-Manager permettant l'administration à distance de la TOE ;
  - un poste central de télégestion PCWin2 ;
  - un serveur syslog distant ;
  - un poste S4-View, S4W-Tools et S4-Key pour l'exploitation et l'administration de la TOE ;

- un poste d'exploitation et d'administration S4-View et S4W-Tools ;
- une TOE (S4W) en mode « production », telle qu'elle est normalement déployée ;
- une TOE en mode « développement », exposant notamment un service SSH qui n'est normalement pas présent.

Afin de représenter le déploiement réel, deux réseaux ont été mis en place. D'un côté, un site distant hébergeant des postes de télégestion et de supervision et de l'autre un réseau IP industriel sur lequel se situent les TOE.

# 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 B.

## 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*

L'installation a suivi la documentation fournie par le développeur.

#### *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*

Le développeur a fourni une plateforme déjà fonctionnelle. L'installation a consisté à configurer le pare-feu en coupure du serveur ESXi, à installer le réseau local et à déployer les certificats électroniques nécessaires au bon fonctionnement des machines.

#### *2.3.1.3 Durée de l'installation*

Une journée.

#### *2.3.1.4 Notes et remarques diverses*

Sans objet.

### 2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] lors de l'évaluation. L'évaluateur a relevé que cette documentation renseignait efficacement sur l'implémentation des fonctions de sécurité mises en œuvre.

### 2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source des mécanismes cryptographiques du produit. 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*

L'évaluateur a relevé des non-conformités sur les fonctions de sécurité testées, mais aucune n'a été considérée comme entraînant un problème de sécurité dans le contexte d'utilisation du produit.

### 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 publiques existent sur le produit ou ses briques tierce partie, mais aucune n'a été considérée par l'évaluateur comme exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

#### *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 du produit et pour le niveau d'attaquant considéré.

### 2.3.7 *Analyse de la facilité d'emploi*

#### *2.3.7.1 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.

#### *2.3.7.2 Avis d'expert sur la facilité d'emploi*

La prise en main et la maintenance du serveur pour un administrateur sont détaillées dans la documentation.

Dans le cas d'un client, il n'a pas été observé de situations où une mauvaise manipulation mettrait à mal la sécurité du produit.

#### *2.3.7.3 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 selon le référentiel [RGS] au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de vulnérabilité exploitable pour le niveau d'attaquant visé.

## 2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé selon le référentiel [RGS].

L'analyse n'a pas identifié 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 « S4W, version 3.10.41.100 » 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].

De manière générale, l'utilisateur doit garder en mémoire que l'évaluation ne garantit pas la robustesse du produit face à une attaque locale – il est donc impératif que l'utilisateur s'assure de la protection physique des équipements S4W (voir H.Local ToE et H.Local autres S4W dans le document [CDS]).

La clé privée associée au certificat électronique de la TOE, écrite en usine, n'est plus lisible ni modifiable par la suite. De plus, la possession du certificat client d'un S4W légitime permettrait à un attaquant potentiel de menacer d'autres équipements. Pour cette raison, si un équipement venait tout de même à être compromis par une attaque locale, il serait nécessaire pour l'utilisateur de changer toute la TOE.

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | Cible de sécurité CSPN S4W<br>Référence : S4-CSPN-CibleDeSécurité.docx ;<br>Version : 1.32 Publique ;<br>Date : 11 juin 2021. |
| [RTE] | Rapport technique d'évaluation CSPN Produit S4W - version v3.10.41.100<br>Référence : CSPN-RTE-S4W-DR ;<br>Version : 2.01 ;<br>Date : 1 juin 2021. |
| [GUIDES] | S4G-PL_DSF_Utilisateurs ;<br>Version : 3.20 ;<br>S4G-PL_DSL_Utilisateurs ;<br>Version : 3.31 ;<br>S4G-PL_DSF_Sécurité ;<br>Version : 3.40 ;<br>S4G-PL_DSF_EcoSystèmes ;<br>Version : 3.20 ;<br>S4G_DSL_Securite ;<br>Version : 3.20. |

# ANNEXE B. 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.<br><br>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.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018.<br><br>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. |