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-2017/03

Gunnebo SMI
Version CSPN_01-01

Paris, le 2 mars 2017

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-2017/03

Nom du produit

Gunnebo SMI

Référence/version du produit

Version CSPN_01-01

Catégorie de produit

Identification, authentification et contrôle d'accès

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

Gunnebo Electronic Security

7 rue Paul Dautier

78140 Vélizy Villacoublay

France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B,

78180 Montigny le Bretonneux

France

Fonctions de sécurité évaluées

Communications sécurisées entre les composants

Chiffrement du PIN

Gestion des alarmes

Fonction(s) de sécurité non évaluées

Néant

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 le « Gunnebo SMI, version CSPN_01-01 » développé par *GUNNEBO ELECTRONIC SECURITY*.

Ce produit est une solution de contrôle d'accès physique. Il est composé de trois types d'équipements, à savoir :

- un lecteur de badges RFID, permettant la récupération des informations d'identification et éventuellement d'authentification[1] ;
- un contrôleur d'accès, commandant les mécanismes d'accès du site en fonction des données reçues des lecteurs ;
- un concentrateur d'accès, servant de passerelle de communication entre les contrôleurs et le serveur de gestion, situé dans le réseau client.

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

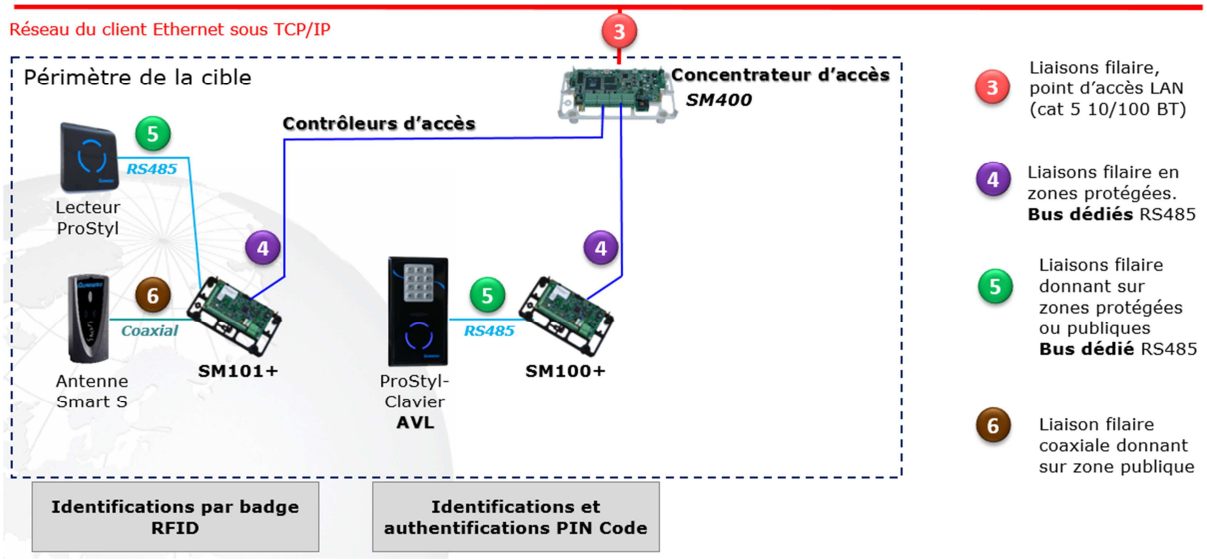

Figure 1 - Architecture Produit.

Pour initialiser et configurer le produit, l'utilisateur s'appuie sur une solution logicielle développée par *GUNNEBO ELECTRONIC SECURITY* appelée SMI Serveur[2]. Cette dernière, déployée dans un environnement physique à protéger, est en charge de générer, stocker et envoyer les données de configuration aux équipements. Elle sert également à gérer les alarmes remontées par les équipements.

[1] Utilisation d'un PIN dans ce cas.
[2] Cet élément est hors périmètre de l'évaluation.

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

Le produit Gunnebo SMI en version CSPN_01-01 comprend les éléments suivants :

- le concentrateur d'accès SM400 :
  - référence : A19914H ;
  - version matériel : V3.0.1 ;
  - version du logiciel : V2.3.5 ;

- le contrôleur d'accès SM100+ :
  - référence : A19A28J ;
  - version matériel : AKQ626 WAVE_CTRL_ETH ;
  - version du logiciel : Appli WaveCtrl V3_0_19 ;
  - version du bootloader : V3.0.5 ;

- le contrôleur d'accès SM101+ (correspond à un SM100+ équipé d'une antenne Smart S additionnelle) :
  - référence : A19A28J ;
  - version matériel : AKQ626 WAVE_CTRL_ETH ;
  - version du logiciel : Appli WaveCtrl V3_0_19 ;
  - version du bootloader : V3.0.5 ;

- le lecteur de badges ProStyl :
  - référence : A10512L ;
  - configuration matérielle : AKQ647 WR, version 1.0.0 ;
  - version du bootloader : BOOT WR V1_0_1, version 1.0.1 ;
  - version du logiciel : Appli WR V1_0_9, version 1.0.9 ;
  - configuration des lecteurs : WR Cfg Wiegand, version 0.1.1 ;

- le lecteur de badges ProStyl-Clavier :
  - référence : A10535A ;
  - configuration matérielle : AKQ647 WR, version 1.0.0 ;
  - version du bootloader : BOOT WR V1_0_1, version 1.0.1 ;
  - version du logiciel : Appli WR V1_0_9, version 1.0.9 ;
  - configuration des lecteurs : WR Cfg Wiegand, version 0.1.1.

La version certifiée du produit peut être identifiée à l'aide du logiciel suivant, exécuté sur le serveur :

- SMI Serveur, pour la récupération des configurations des SM400, SM100+ et SM101+.

Pendant l'évaluation, le développeur a également mis à disposition de l'évaluateur un logiciel interne SOP Tool. Il est à exécuter sur un ordinateur et permet la récupération des configurations des Lecteur ProStyl et Lecteur ProStyl-Clavier au travers d'une liaison série.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- les communications sécurisées entre les composants ;
- le chiffrement du PIN ;
- la gestion des alarmes.

1.2.4. Configuration évaluée

La configuration évaluée est celle décrite dans le document [MANUEL]. Cette configuration durcit la sécurité par défaut du produit en chiffrant la table des clés du SM100+ en mémoire et en augmentant le niveau de sécurité des communications.

La plateforme de test prise en compte dans le cadre de cette évaluation est la suivante :

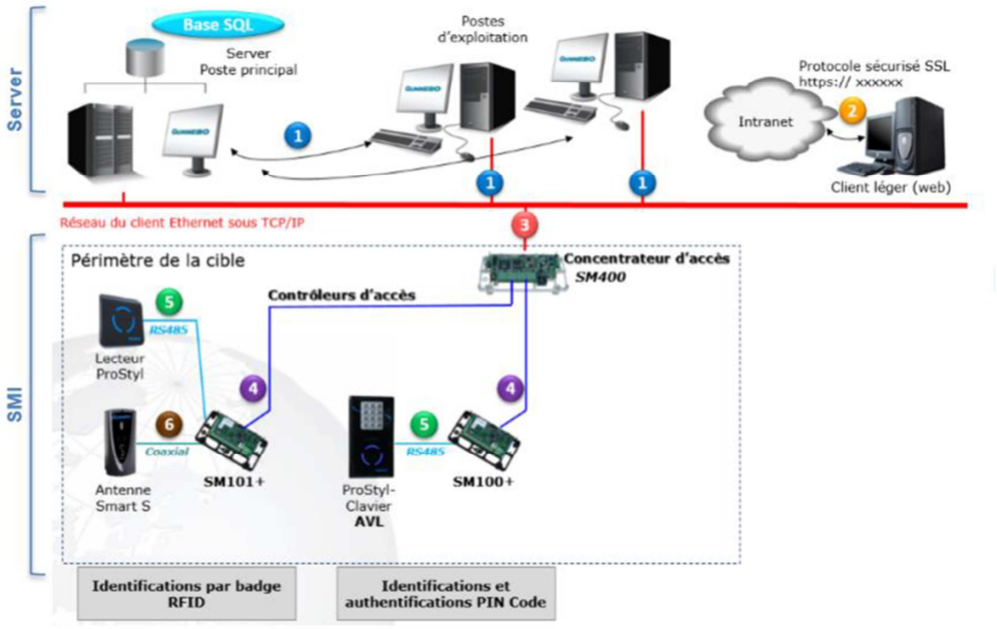

Figure 2 – Configuration évaluée.

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 *GUNNEBO ELECTRONIC SECURITY* 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

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit.
Il est à noter que le document [MANUEL] détaille les étapes nécessaires pour paramétrer le produit afin de retrouver la configuration évaluée en CSPN.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

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 du produit qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Des contacts ponctuels pour des demandes de précisions ou de dépannage ont été établis pendant l'évaluation.

2.3.8. Analyse de la facilité d'emploi et préconisations

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. Recommandations pour une utilisation sûre du produit

Les recommandations suivantes sont listées par l'évaluateur :

- les composants du produit et son environnement, ainsi que leurs câblages, doivent être protégés physiquement[1]. L'accès à ces éléments doit être réduit au strict minimum ;
- l'ensemble des processus de configuration, d'exploitation et de maintenance doit être régulièrement audités. Les intervenants doivent être correctement formés.

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

De l'avis du CESTI, une fois l'environnement déployé, le produit est relativement facile d'emploi. Une formation dédiée à la configuration du produit peut faciliter sa prise en main.

2.3.8.4. Notes et remarques diverses

L'architecture de déploiement doit être conçue avec précaution, en s'appuyant si nécessaire sur l'expertise de *GUNNEBO ELECTRONIC SECURITY*. Quant à l'installation du produit, des compétences minimales en électronique semblent nécessaires.

[1] Les lecteurs étant en zone publique, le niveau de sécurité physique peut être différent de celui des autres composants.

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.
Celle-ci a identifié des non-conformités au RGS, mais n'a pas permis de mettre en évidence de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le générateur d'aléas du produit n'a pas fait l'objet d'une analyse au titre de cette évaluation CSPN.

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 « Gunnebo SMI, version CSPN_01-01 » 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 1.2 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], appliquer le « Manuel de mise en conformité CSPN » ([MANUEL]) ainsi que les [GUIDES], et mettre en œuvre les recommandations énoncées dans le présent rapport (voir 2.3.8.2 et 2.3.8.4).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN SMI - Identification, authentification pour le contrôle des accès physiques* Référence : AOY002 ; Version : 4-2 ; Date : septembre 2016
[SPEC-CRY]	*Fournitures Cryptographiques* Référence : AOY003 ; Version : 05 ; Date : août 2016
[MANUEL]	*Manuel de mise en conformité CSPN* Référence : A0U565; Version : 01 ; Date : septembre 2016
[GUIDES]	*Chiffrement et authentification des communications – SMI Server* Référence : A0I542B *Guide de configuration SMI* Référence : A0U562A *Guide d'utilisation SMI* Référence : A0U563A
[RTE]	*Rapport Technique d'Evaluation CSPN GUNNEBO-SMI - Dispositif d'identification SMI* Référence : OPPIDA/CESTI/GUNNEBO-SMI/RTE/1.1 ; Version : 1.1 ; Date : 9 février 2017

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 (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 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/
[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_B_1), voir www.ssi.gouv.fr/.