



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-2018/12**

### **Gunnebo SMI Version CSPN\_01-02**

*Paris, le 15 octobre 2018*

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

Guillaume POUPARD  
[ORIGINAL SIGNE]



## 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 présumées 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](mailto:certification@ssi.gouv.fr)

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

<i>Référence du rapport de certification</i>	<b>ANSSI-CSPN-2018/12</b>
<i>Nom de la gamme de produits</i>	<b>Gunnebo SMI</b>
<i>Référence/version de la gamme de produits</i>	<b>Version CSPN_01-02</b>
<i>Catégorie de la gamme de produits</i>	<b>Identification, authentification et contrôle d'accès</b>
<i>Critères d'évaluation et version</i>	<b>CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)</b>
<i>Commanditaire</i>	<b>Gunnebo Electronic Security</b> 7 rue Paul Dautier 78140 Vélizy Villacoublay France
<i>Développeur</i>	<b>Gunnebo Electronic Security</b> 7 rue Paul Dautier 78140 Vélizy Villacoublay France
<i>Centre d'évaluation</i>	<b>Oppida</b> 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux France
<i>Fonctions de sécurité évaluées</i>	<b>Communications sécurisées entre les composants</b> <b>Chiffrement du PIN</b> <b>Gestion des alarmes</b>
<i>Fonction(s) de sécurité non évaluées</i>	<b>Néant</b>
<i>Restriction(s) d'usage</i>	<b>Oui (cf. §3.2)</b>

# 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LES PRODUITS.....</b>	<b>6</b>
1.1. PRESENTATION DES PRODUITS .....	6
1.2. DESCRIPTION DE LA GAMME DE PRODUITS EVALUES .....	7
1.2.1. <i>Catégorie des produits</i> .....	7
1.2.2. <i>Identification de la gamme de produits</i> .....	7
1.2.3. <i>Fonctions de sécurité</i> .....	9
1.2.4. <i>Configuration évaluée</i> .....	9
<b>2. L’EVALUATION .....</b>	<b>10</b>
2.1. REFERENTIELS D’EVALUATION .....	10
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L’EVALUATION .....	10
2.3. TRAVAUX D’EVALUATION .....	10
2.3.1. <i>Installation de la gamme de produits</i> .....	10
2.3.2. <i>Analyse de la documentation</i> .....	10
2.3.3. <i>Revue du code source (facultative)</i> .....	11
2.3.4. <i>Analyse de la conformité des fonctions de sécurité</i> .....	11
2.3.5. <i>Analyse de la résistance des mécanismes des fonctions de sécurité</i> .....	11
2.3.6. <i>Analyse des vulnérabilités (conception, construction, etc.)</i> .....	11
2.3.7. <i>Accès aux développeurs</i> .....	11
2.3.8. <i>Analyse de la facilité d’emploi et préconisations</i> .....	11
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES .....	12
2.5. ANALYSE DU GENERATEUR D’ALEAS.....	12
<b>3. LA CERTIFICATION .....</b>	<b>13</b>
3.1. CONCLUSION.....	13
3.2. RESTRICTIONS D’USAGE.....	13
<b>ANNEXE 1. REFERENCES DOCUMENTAIRES DES PRODUITS EVALUES.....</b>	<b>14</b>
<b>ANNEXE 2. REFERENCES A LA CERTIFICATION.....</b>	<b>15</b>

# 1. Les produits

## 1.1. Présentation des produits

Les produits évalués correspondent à ceux de la gamme nommée « Gunnebo SMI, version CSPN\_01-02 » développée par *GUNNEBO ELECTRONIC SECURITY*.

Cette gamme offre des solutions de contrôle d'accès physique. Elle est composée de trois types d'équipements, à savoir :

- des lecteurs de badges RFID<sup>1</sup>, permettant la récupération des informations d'identification et éventuellement d'authentification<sup>2</sup> ;
- des contrôleurs d'accès, commandant les mécanismes d'accès du site en fonction des données reçues des lecteurs ;
- des concentrateurs 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 de la gamme de produits.

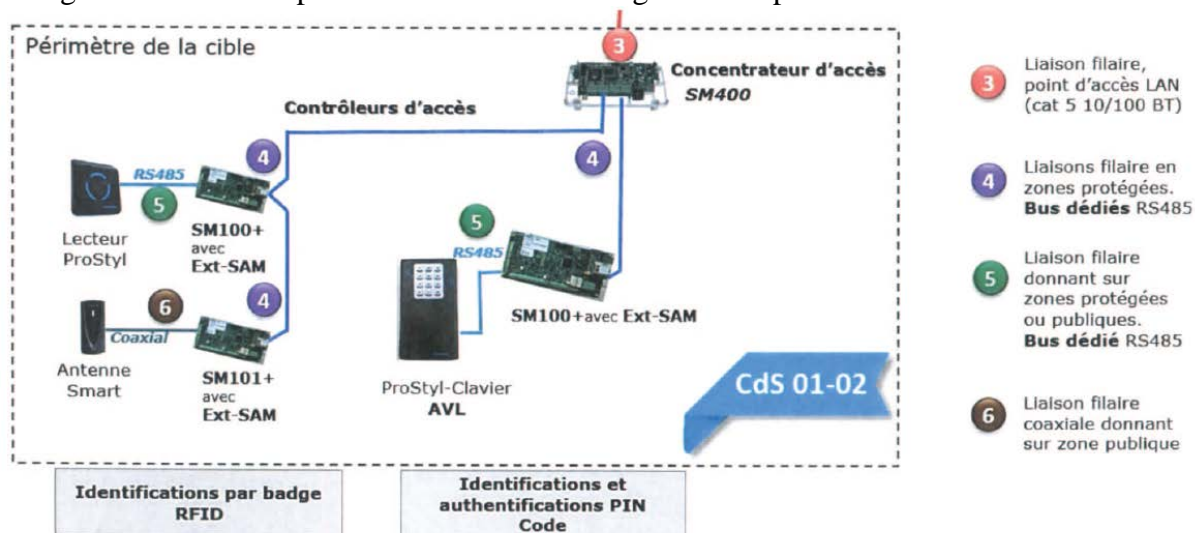


Figure 1 - Architecture Produits.

Pour initialiser et configurer ces produits, l'utilisateur doit s'appuyer sur une solution logicielle, développée par *GUNNEBO ELECTRONIC SECURITY*, appelée *SMI Server*<sup>3</sup>. Cette dernière, déployée dans l'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.

<sup>1</sup> *Radio-Frequency IDentification*.

<sup>2</sup> Utilisation d'un code PIN dans ce cas.

<sup>3</sup> Cet élément est hors périmètre de l'évaluation.

## 1.2. Description de la gamme de produits évalués

La cible de sécurité [CDS] définit les produits évalués, leurs fonctionnalités de sécurité évaluées et leurs environnements d'exploitation.

### 1.2.1. Catégorie des produits

<input type="checkbox"/>	1 – détection d'intrusions
<input type="checkbox"/>	2 – anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3 – pare-feu
<input type="checkbox"/>	4 – effacement de données
<input type="checkbox"/>	5 – administration et supervision de la sécurité
<input checked="" type="checkbox"/>	<b>6 – identification, authentification et contrôle d'accès</b>
<input type="checkbox"/>	7 – communication sécurisée
<input type="checkbox"/>	8 – messagerie sécurisée
<input type="checkbox"/>	9 – stockage sécurisé
<input type="checkbox"/>	10 – environnement d'exécution sécurisé
<input type="checkbox"/>	11 – terminal de réception numérique ( <i>Set top box, STB</i> )
<input type="checkbox"/>	12 – matériel et logiciel embarqué
<input type="checkbox"/>	13 – automate programmable industriel
<input type="checkbox"/>	99 – autre

### 1.2.2. Identification de la gamme de produits

Plusieurs produits sont identifiés pour cette évaluation, composant ainsi la gamme de produits « Gunnebo SMI, version CSPN\_01-02 ».

#### 1.2.2.1. Produits de référence

Pour les besoins de l'évaluation, et conformément à la [NOTE-21], l'intégralité des tests ont été déroulés sur les produits de référence. Le CESTI a en effet conclu que les produits mentionnés ci-après étaient représentatifs de la gamme de produits :

- le concentrateur d'accès SM400 :
  - o référence : A19914 ;
  - o version matériel : V3.0.1 ;
  - o version du logiciel : V2.3.5.
  
- les contrôleurs d'accès de référence SM100+ et SM101+ (correspondant à un SM100+ équipé d'une antenne Smart S additionnelle) :
  - o références : A19A28 et A19A44 ;
  - o version matériel : AKQ626 WAVE\_CTRL\_ETH ;
  - o version du logiciel : Appli WaveCtrl V3\_1\_0 ;
  - o version du bootloader : V3.0.5.
  
- le lecteur de badges ProStyl :
  - o référence : A10512 ;
  - o configuration matérielle : AKQ647 WR, version 1.0.0 ;
  - o version du bootloader : BOOT WR V1\_0\_1, version 1.0.1 ;
  - o version du logiciel : Appli WR V1\_0\_12, version 1.0.12 ;
  - o configuration des lecteurs : WR Cfg Wiegand, version 0.1.1.

- le lecteur de badges ProStyl-Clavier :
  - o référence : A10535 ;
  - o configuration matérielle : AKQ647 WR, version 1.0.0 ;
  - o version du bootloader : BOOT WR V1\_0\_1, version 1.0.1 ;
  - o version du logiciel : Appli WK V1\_0\_3, version 1.0.3 ;
  - o configuration des lecteurs : WR Cfg Wiegand, version 0.1.1.

#### 1.2.2.2. Produits déclinés

Les produits suivants, déclinés à partir des produits de référence, font partie de la gamme certifiée au titre de [NOTE-21] :

- le contrôleur d'accès SM101+E correspondant à un contrôleur d'accès SM100+ équipé d'une antenne Smart E additionnelle,
  - o référence : A19A46 ;
  - o version matériel : AKQ626 WAVE\_CTRL\_ETH ;
  - o version du logiciel : Appli WaveCtrl V3\_1\_0 ;
  - o version du bootloader : V3.0.5 ;
  - o antenne Smart E de référence : A19993.
- le contrôleur d'accès SM102+E correspondant à deux contrôleurs d'accès SM100+ chacun équipé d'une antenne Smart E additionnelle
  - o référence : A19A36 ;
  - o version matériel : AKQ626 WAVE\_CTRL\_ETH ;
  - o version du logiciel : Appli WaveCtrl V3\_1\_0 ;
  - o version du bootloader : V3.0.5 ;
  - o antenne Smart E de référence : A19993.
- le contrôleur d'accès SM102+S correspondant à deux contrôleurs d'accès SM100+ chacun équipé d'une antenne Smart S additionnelle
  - o référence : A19A35 ;
  - o version matériel : AKQ626 WAVE\_CTRL\_ETH ;
  - o version du logiciel : Appli WaveCtrl V3\_1\_0 ;
  - o version du bootloader : V3.0.5 ;
  - o antenne Smart S de référence : A19664.
- le lecteur de badges ProStyl à visser :
  - o référence : A10532 ;
  - o configuration matérielle : AKQ647 WR, version 1.0.0 ;
  - o version du bootloader : BOOT WR V1\_0\_1, version 1.0.1 ;
  - o version du logiciel : Appli WR V1\_0\_11, version 1.0.12 ;
  - o configuration des lecteurs : WR Cfg Wiegand, version 0.1.1.
- le lecteur de badges ProStyl AVL
  - o référence : A10523 ;
  - o configuration matérielle : AKQ647 WR, version 1.0.0 ;
  - o version du bootloader : BOOT WR V1\_0\_1, version 1.0.1 ;
  - o version du logiciel : Appli WR V1\_0\_11, version 1.0.12 ;
  - o configuration des lecteurs : WR Cfg Wiegand, version 0.1.1.



Les versions des produits peuvent être vérifiées :

- en interrogeant directement les produits au travers du réseau ;
- pour les concentrateurs et les lecteurs, à l'aide du logiciel *SMI Server*, exécuté sur le serveur, qui permet également la récupération de leurs configurations ;
- pour le lecteur ProStyl et le lecteur ProStyl-Clavier, à l'aide du logiciel interne du développeur *SOP Tool* qui permet également la récupération de leurs configurations.

### 1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées de la gamme des produits sont :

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

### 1.2.4. Configuration évaluée

La configuration évaluée est celle décrite dans le document [MANUEL]. Cette configuration utilise le kit d'extension *Secure Access Module (SAM)* (référence A19A98) pour les contrôleurs d'accès SM100+, SM101+ et SM102+, ainsi qu'une SAM *NXP* de type *MIFARE AV2* permettant le stockage des clés du contrôleur.

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

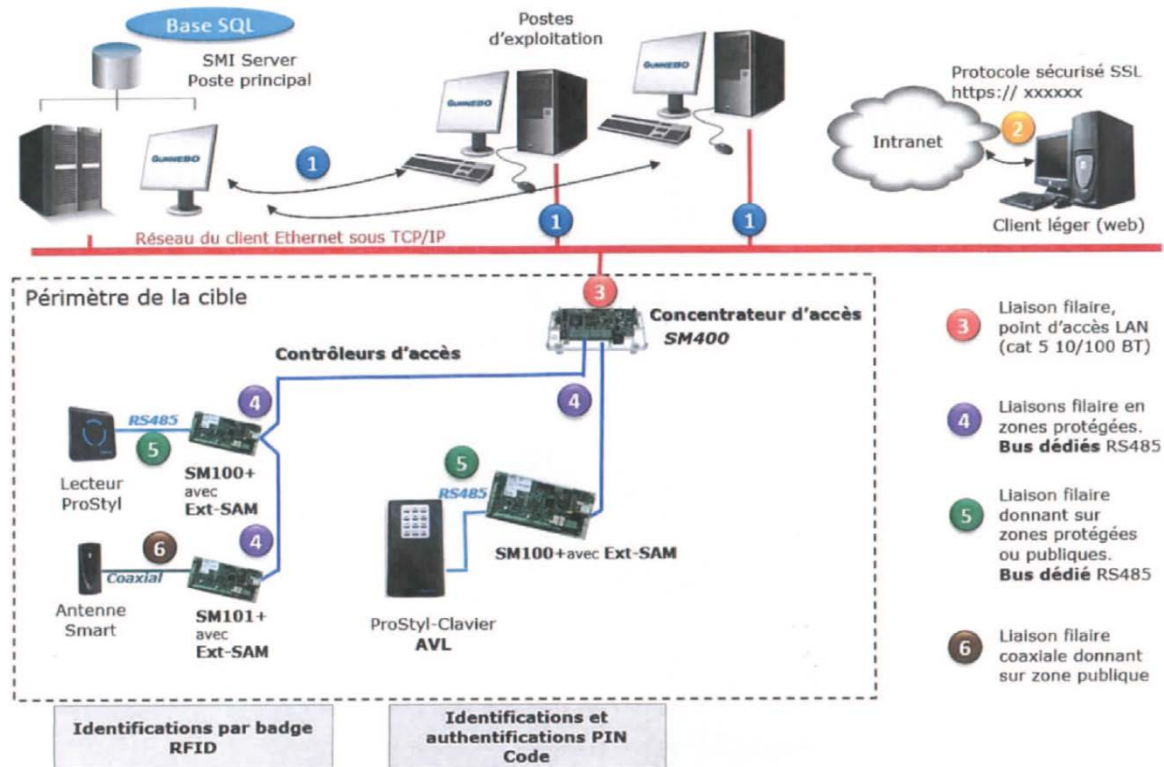


Figure 2 - Configuration évaluée.

## 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 a été adaptée conformément à la procédure [NOTE-21], seuls les tests ayant une adhérence aux caractéristiques distinguant les produits de la gamme ont été joués par le CESTI sur les produits déclinés. Il a également été pris en compte des travaux déjà effectués sur une précédente version du produit, certifiée sous la référence ANSSI-CSPN-2017/03 ([CER]).

### 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 de la gamme de produits

##### 2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

La gamme de produits a été évaluée 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 de la gamme de produits.

Il est à noter que le document [MANUEL] détaille les étapes nécessaires pour paramétrer la gamme de produits 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 de la gamme de produits 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 de la gamme de produits 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 à la gamme de produits, ni dans son implémentation, qui puisse remettre en cause la sécurité de cette gamme.

### **2.3.7. Accès aux développeurs**

Sans objet.

### **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 de la gamme de produits**

Aucune recommandation particulière n'est formulée par l'évaluateur. Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

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

De l'avis du CESTI, une fois l'environnement déployé, les produits sont relativement faciles d'emploi. Une formation dédiée à la configuration de la gamme de produits 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 de la gamme de produits, des compétences minimales en électronique semblent nécessaires.

## **2.4. Analyse de la résistance des mécanismes cryptographiques**

Les mécanismes cryptographiques mis en œuvre par la gamme de produits 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 de la gamme de produits 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 la gamme de produits « Gunnebo SMI, version CSPN\_01-02 » 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 la gamme de produits spécifiée au chapitre 1.2 du présent rapport de certification.

L'utilisateur des produits certifiés 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 2.3.8.4).

## Annexe 1. Références documentaires des produits évalués

[CDS]	<i>Cible de sécurité CSPN SMI - Identification, authentification pour le contrôle des accès physiques</i> Référence : AOY004 ; Version : 01 ; Date : juin 2017.
[RTE]	<i>Rapport Technique d'Évaluation CSPN SMI CSPN_01-02 - Gunnebo SMI</i> Référence : OPPIDA/CESTI/SMI CSPN_01-02/RTE/1.2 ; Version : 1.2 ; Date : 17 août 2018.
[GUIDES]	<i>Chiffrement et authentification des communications – SMI Server</i> Référence : A0I542B  <i>Guide de configuration SMI</i> Référence : A0U562  <i>Guide d'utilisation SMI</i> Référence : A0U563
[MANUEL]	<i>Manuel de mise en conformité CSPN</i> Référence : A0U581 ; Version : 1.2.
[CER]	<i>Rapport de certification ANSSI-CSPN-2017/03 Gunnebo SMI</i> Version CSPN_01-01 Référence : ANSSI-CSPN-2017/03 Version 1.0 ; Date : 2 mars 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]	<p>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 07 avril 2014.</p> <p>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.</p> <p>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014.</p> <p>Documents disponibles sur <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>
[RGS]	<p>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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>
[NOTE-21]	<p>Note d'application - Méthodologie pour l'évaluation d'une gamme de produits, référence ANSSI-CC-NOTE-21/1.0 du 1<sup>er</sup> février 2017.</p>