PREMIER MINISTRE
*Liberté*
*Égalité*
*Fraternité*

Agence nationale de la sécurité
des systèmes d'information

**Secrétariat général de la défense**
**et de la sécurité nationale**

# Rapport de certification
# ANSSI-CSPN-2025/11

## Solution SMI Server

### Version SMI Server 4.6, SM400 2.8.6, SM100+ 4.0.100

Paris, le 14/8/2025 | 18:31 CEST

Vincent Strubel

# 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-2025/11**

Nom du produit

**Solution SMI Server**

Référence/version du produit

**Version SMI Server 4.6, SM400 2.8.6, SM100+ 4.0.100**

Catégorie de produit

**Identification, authentification et contrôle d'accès**

Critère d'évaluation et version

**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**

Commanditaire

**FICHET TECHNOLOGIES**
23 route de Schwobscheim, B.P. 40285
67606 Sélestat Cedex, France

Développeur

**FICHET TECHNOLOGIES**
23 route de Schwobscheim, B.P. 40285
67606 Sélestat Cedex, France

Centre d'évaluation

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

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Protection des codes PIN et des identifiants des badges
Protection des données échangées entre le « Server » et le concentrateur SM400 (ou SM400-L)
Protection des données échangées entre le concentrateur SM400(-L) et le contrôleur SM100+
Sécurisation du contrôleur de portes SM100+
Sécurisation du concentrateur d'accès SM400 / SM400-L
Sécurisation des lecteurs claviers de la gamme ProStyl
Protection des clés
Authentification des opérateurs
Protection des mots de passe des opérateurs
Protection des communications

| |
|---|
| Protection de l'accès à la base de données<br>Définition des droits<br>Protection des événements<br>Génération des évènements du GAC<br>Protection de l'accès au mode *debug* des microcontrôleurs |
| Fonctions de sécurité non évaluées<br>Sans objet |
| Restriction(s) d'usage<br>Non |

# 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 cyber.gouv.fr.

## TABLE DES MATIERES

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « Solution SMI Server, Version SMI Server 4.6, SM400 2.8.6, SM100+ 4.0.100 » développé par FICHET TECHNOLOGIES.

Ce produit correspond à une solution intégrée pour une gestion centralisée de contrôle d'accès physique et est composé :

- d'une partie appelée « Server » intégrant les applications, les bases de données et les serveurs d'applications et de présentation, située en zone névralgique ;
- d'une partie appelée « SMI » intégrant les équipements de terrain : concentrateurs d'accès, contrôleurs de portes et lecteurs.

Le système est architecturé autour des équipements représentés sur la figure 1 ci-dessous et a pour objectif de filtrer les flux d'individus (usagers) autorisés ou non à pénétrer sur un site, un bâtiment ou des locaux.

Pour assurer les contrôles sur les accès, le système d'accès remplit les fonctions suivantes :

- Identification par badge RFID (sans contact) et authentification par code PIN ;
- Traitements des droits d'accès au niveau du contrôleur de portes (UTL) ;
- Automatisme d'accès (déverrouillage, séquencement d'opérations de contrôle de l'ouvrant, état de l'accès physique) ;
- La solution SMI Server peut être implantée dans différents secteurs tels que les Administrations, l'Industrie et le Tertiaire.

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

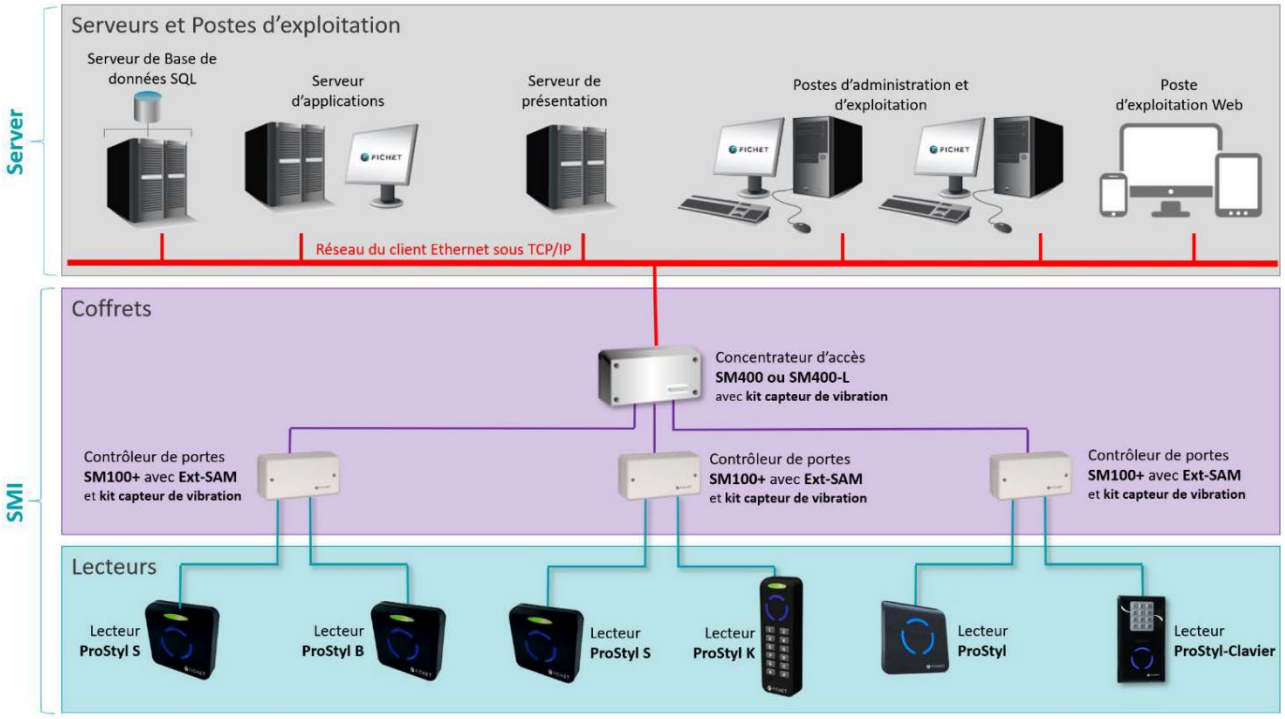



**Figure 1 - Architecture Produit.**

## 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 |

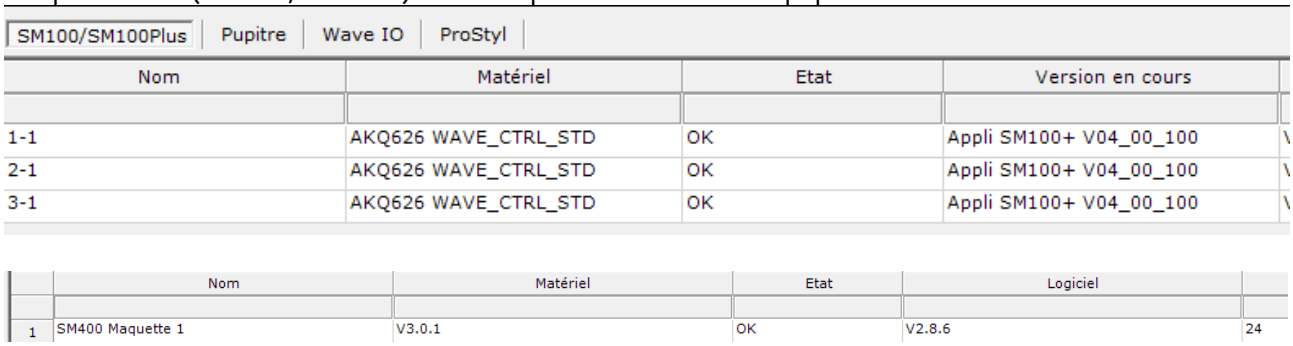
### 1.2.2 *Identification du produit*

| Produit | |
|---|---|
| Nom du produit | Solution SMI Server |
| Numéro de la version évaluée | Version SMI Server 4.6, SM400 2.8.6, SM100+ 4.0.100 |

La version certifiée du produit peut être identifiée de la manière suivante :

- pour le GAC (SMI Server) : depuis le menu général :

- pour l'UTL (SM400, SM100+) : dans la partie détails des équipements :




- pour les lecteurs : dans la partie Prostyl ou sur la face arrière de la carte électronique présent dans le lecteur.

### 1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection des codes PIN et des identifiants des badges ;
- la protection des données échangées entre le « Server » et le concentrateur SM400 (ou SM400-L) ;
- la protection des données échangées entre le concentrateur SM400(-L) et le contrôleur SM100+ ;
- la sécurisation du contrôleur de portes SM100+ ;
- la sécurisation du concentrateur d'accès SM400 / SM400-L ;
- la sécurisation des lecteurs claviers de la gamme ProStyl ;
- la protection des clés ;
- l'authentification des opérateurs ;
- la protection des mots de passe des opérateurs ;
- la protection des communications ;
- la protection de l'accès à la base de données ;
- la définition des droits ;
- la protection des évènements ;
- la génération des évènements du GAC ;
- la protection de l'accès au mode *debug* des microcontrôleurs.

### 1.2.4 *Configuration évaluée*

Le tableau ci-dessous décrit la configuration évaluée :

| Composants du système | | Inclus dans la cible de l'évaluation (TOE) | Non évalué (environnement de la TOE), supposé de confiance |
|---|---|---|---|
| GAC | Système d'exploitation | | Windows 10<br>Windows 11<br>Windows Server 2019<br>Windows Server 2022 |

| | | | |
|---|---|---|---|
| | Serveur d'applications | SMI Server 4.6 | |
| | Fonctions cryptographiques | .NET 4.8<br>LibCom 4.0.10 | |
| | Bases de données et annuaires | | SQL Server 2019<br>SQL Server 2022 |
| UTL | Système d'exploitation | SM400 / SM400-L : Ecos 3.0<br>SM100+ : Keil RTX 4.80 | |
| | Applicatifs | SM400(-L) : 2.8.6<br>SM100+ : 4.0.100 | |
| | Fonctions cryptographiques | OpenSSL 3.0.15<br>WPA supplicant 2.11<br>LibCom 4.0.10<br>Mongoose 7.12 | |
| | SAM | | SAM NXP AV2/AV3 |
| Lecteurs | Lecteurs simples | ProStyl S 1.1.6<br>ProStyl 1.1.6<br>ProStyl AVL 1.1.6<br>ProStyl B 1.8.9 | |
| | Lecteurs-clavier | Logiciel du clavier du ProStyl K : 1.0.6<br>Logiciel du lecteur du ProStyl K : 1.1.6<br>Logiciel du clavier du ProStyl-Clavier : 1.0.6<br>Logiciel du lecteur du ProStyl-Clavier : 1.1.6 | |
| Badges | | | DESFire EV2/EV3 |

# 2 L'évaluation

## 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-07].

## 2.2 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].

### 2.2.1 *Installation du produit*

#### *2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation*

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

#### *2.2.1.2 Description de l'installation et des non-conformités éventuelles*

Le produit est globalement simple à installer à l'aide des guides qui sont correctement détaillés.

#### *2.2.1.3 Notes et remarques diverses*

L'analyse de l'installation et de l'utilisation du produit n'a pas permis d'identifier de vulnérabilités potentielles.

### 2.2.2 *Analyse de la documentation*

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

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

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

### 2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

### 2.2.5 *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.

### 2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

#### *2.2.6.1 Liste des vulnérabilités connues*

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

#### *2.2.6.2 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 défini par la cible de sécurité [CDS].

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

#### *2.2.7.1 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.

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

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

#### *2.2.7.3 Notes et remarques diverses*

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

## 2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

## 2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées [GUIDES] doivent être suivies.

# 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 « Solution SMI Server, Version SMI Server 4.6, SM400 2.8.6, SM100+ 4.0.100 » 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], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

## 3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ *(Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | Cible de sécurité de référence pour l'évaluation :<br>- Cible de sécurité – Solution SMI Server - 2024, référence A0Y011, version 11, 23 janvier 2025.<br><br>Pour les besoins de publication, la cible de sécurité suivante a été fournie :<br>- Cible de sécurité – Solution SMI Server v4.6, référence A0Y011, version 12, 24 juillet 2025. |
| [RTE] | Rapport technique d'évaluation :<br>- Rapport Technique d'Evaluation CSPN – *Solution SMI Server – SMI-SERVER_2024,* référence OPPIDA/CESTI/2025/SMI-SERVER_2024/RTE, version 3.0, 24 juillet 2025. |
| [GUIDES] | Guide d'administration et d'installation du produit :<br>- Notice d'installation et de maintenance, référence A0I295E, mars 2022 ;<br>- Notice d'installation et de maintenance, référence A0I501G, mars 2022 ;<br>- Notice d'installation et de maintenance, référence A0I586E, mars 2022 ;<br>- Notice d'installation et de maintenance, référence A0I723A, juin 2025 ;<br>- Manuel de mise en conformité CSPN pour le produit SMI Server, référence A0U609, 2023.<br>- Chiffrement et Authentification des Communications, référence A0I542F, 2023. |

# ANNEXE B. Références liées 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, version 5.0, 12 janvier 2023.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, 6 mars 2024.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 6 mars 2024. |
| [CRY-P-01] | Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021. |
| [ANSSI Crypto] | Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020. |
| [SOG-IS Crypto] | *SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.2, janvier 2020. |
| [NOTE-07] | Note d'application - Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN, référence ANSSI-CSPN-NOTE-07, version 2.1, 7 juillet 2020. |
| [BSZ_CSPN] | *Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement*,version 2.0, mai 2024. |