



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-2018/21

Synergis Cloud Link

Version HW : SY-CLOUDLINK-312-CSPN / SW : 10.7.411.8 (2018-04-18)

Paris, le 25 septembre 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

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



<i>Référence du rapport de certification</i>	ANSSI-CSPN-2018/21
<i>Nom du produit</i>	Synergis Cloud Link
<i>Référence/version du produit</i>	Version HW : SY-CLOUDLINK-312-CSPN / SW : 10.7.411.8 (2018-04-18)
<i>Catégorie de produit</i>	Identification, authentification et contrôle d'accès
<i>Critères d'évaluation et version</i>	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
<i>Commanditaire</i>	GENETEC Inc. 2280 Boulevard Alfred-Nobel Montréal, Québec HAS 2A4
<i>Développeur</i>	GENETEC Inc. 2280 Boulevard Alfred-Nobel Montréal, Québec HAS 2A4
<i>Centre d'évaluation</i>	THALES (TCS – CNES) 290 allée du Lac, 31670 Labège, France
<i>Fonctions de sécurité évaluées</i>	Protection des communications IP Contrôle des données entrantes Protections du Firmware Protections des données (UTL) Durcissement du système d'exploitation Utilisation de la technologie MIFARE DESFire Protections du lecteur et des communications avec l'UTL
<i>Fonction(s) de sécurité non évaluées</i>	Sans objet
<i>Restriction(s) d'usage</i>	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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT EVALUE	7
1.2.1. <i>Catégorie du produit</i>	7
1.2.2. <i>Identification du produit</i>	7
1.2.3. <i>Fonctions de sécurité</i>	8
1.2.4. <i>Configuration évaluée</i>	9
2. L’EVALUATION	10
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 du produit</i>	10
2.3.2. <i>Analyse de la documentation</i>	10
2.3.3. <i>Revue du code source (facultative)</i>	10
2.3.4. <i>Analyse de la conformité des fonctions de sécurité</i>	10
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
3. LA CERTIFICATION	13
3.1. CONCLUSION	13
3.2. RESTRICTIONS D’USAGE.....	13
ANNEXE 1. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 2. REFERENCES A LA CERTIFICATION.....	15

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Synergis Cloud Link, version HW : SY-CLOUDLINK-312-CSPN / SW : 10.7.411.8 (2018-04-18) » développé par *GENETEC INC.*. Ce produit est un ensemble de composants appartenant à une solution de contrôle d'accès physique.

Le produit évalué inclut

- l'Unité de Traitement Local (UTL) Synergis CloudLink version HW : SY-CLOUDLINK-312-CSPN / SW : 10.7.411.8 (2018-04-18);
- les lecteurs/claviers de modèles :
 - o HID iClass SE R10¹, SE R40², SE RK40³ et SE R95A Decor⁴ ;
 - o STid ARC-W33-A/PH5-7AD/y⁵, ARC-W33-B/PH5-7AD/y⁶, ARC-W33-C/PH5-7AD/y⁷, ARC1-W33-X/PH5-7AD/1⁸ et LXS-W33-E/PH5-7AD/y⁹.

Le produit évalué interagit avec :

- un gestionnaire d'accès (*Access Manager*) ;
- un répertoire et des outils de configuration (*Directory* et *Config Tool*) ;
- des badges d'accès MIFARE® DESFire ;
- les mécanismes d'ouverture de porte (représentés en vert sur la figure 1 ci-après).

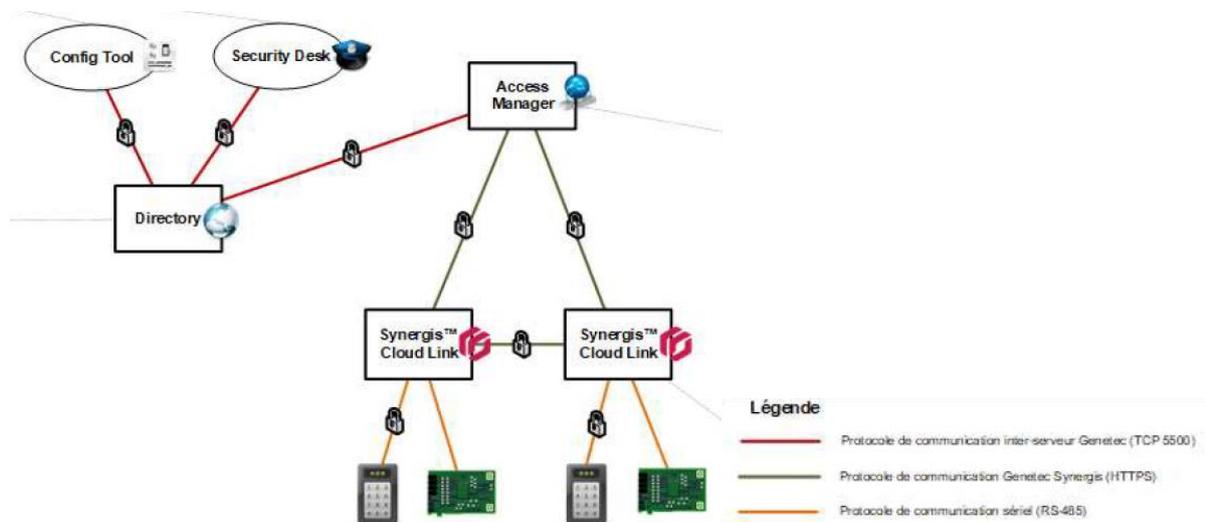


Figure 1 - Environnement du produit évalué

¹ OSDP, modèles 900NMPNEKMA0J0 et 900NMPTEKMA0J0

² OSDP, modèles 920NMPNEKMA0J0 et 920NMPTEKMA0J0

³ OSDP, modèles 921NMPNEKMA0J1 et 921NMPTEKMA0J1

⁴ OSDP, modèle 95ANMPTEWMA0J0

⁵ SSCPv2, modèle ARC-A

⁶ SSCPv2, modèle ARC-B

⁷ SSCPv2, modèle ARC-C

⁸ SSCPv2, modèle ARC-1

⁹ SSCPv2, modèle LXS

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

<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"/>	6 – identification, authentification et contrôle d'accès
<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 du produit

Nom du produit	Synergis Cloud Link
Numéro de la version évaluée	HW : SY-CLOUDLINK-312-CSPN / SW : 10.7.411.8 (2018-04-18) Utilisé en conjonction avec les lecteurs : - HID iClass SE R10 ¹ , SE R40 ² , SE RK40 ³ et SE R95A Decor ⁴ ; - STid ARC-W33-A/PH5-7AD/y ⁵ , ARC-W33-B/PH5-7AD/y ⁶ , ARC-W33-C/PH5-7AD/y ⁷ , ARC1-W33-X/PH5-7AD/1 ⁸ et LXS-W33-E/PH5-7AD/y ⁹ .

¹ OSDP, modèles 900NMPNEKMA0J0 et 900NMPTEKMA0J0

² OSDP, modèles 920NMPNEKMA0J0 et 920NMPTEKMA0J0

³ OSDP, modèles 921NMPNEKMA0J1 et 921NMPTEKMA0J1

⁴ OSDP, modèle 95ANMPTEWMA0J0

⁵ SSCPv2, modèle ARC-A

⁶ SSCPv2, modèle ARC-B

⁷ SSCPv2, modèle ARC-C

⁸ SSCPv2, modèle ARC-1

⁹ SSCPv2, modèle LXS

L'identification de la version matérielle des UTLs est possible par examen de l'étiquette :



Figure 2 : Version matérielle

La version du logiciel (nommé *Softwire*) peut être obtenue en se rendant sur l'onglet « Mise à niveau de Softwire » depuis l'interface web d'administration du Synergis Cloud link, accessible via le port 443 (https) de l'UTL :

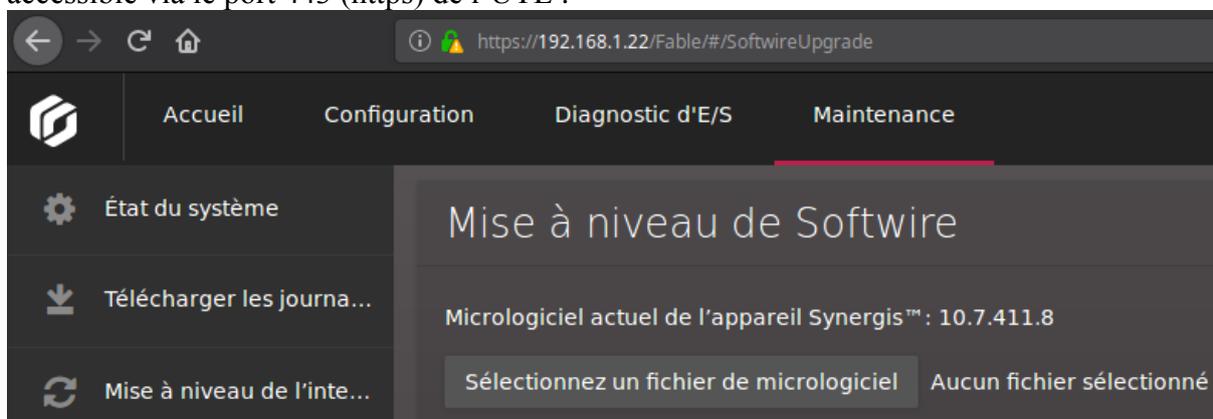


Figure 3 : Version logicielle

L'identification des lecteurs de badge se fait par lecture de l'étiquette située à l'intérieur du lecteur. Cela ne peut donc se faire que lors de l'installation ou de la maintenance.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- protection des communications IP ;
- contrôle des données entrantes ;
- protections du Firmware ;
- protections des données (UTL) ;



- durcissement du système d'exploitation ;
- utilisation de la technologie MIFARE DESFire ;
- protections du lecteur et des communications avec l'UTL.

1.2.4. Configuration évaluée

Les tests de cette évaluation ont été menés sur une maquette, et non des portes réelles (l'accès physique a été simulé). La maquette met en œuvre les lecteurs/claviers identifiés au paragraphe 1.1.

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

Sans objet.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

L'installation du produit a été effectuée avec l'aide des équipes du développeur. En conséquence, la sécurité de l'installation n'est pas rigoureusement testée par l'évaluateur, ce qui donne lieu à des restrictions d'emploi (voir §3.2).

2.3.1.3. Durée de l'installation

Sans objet.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

Aucune vulnérabilité relative à la documentation n'a été relevée par l'évaluateur.

2.3.3. Revue du code source (facultative)

Le code source du produit n'a pas été fourni pour l'évaluation.

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**

Des vulnérabilités potentielles connues ont été identifiées sur le produit, et les briques tierces qu'il utilise. Cependant, elles sont considérées comme non exploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

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 prévu et pour le niveau d'attaquant considéré.

2.3.7. **Accès aux développeurs**

Un entretien avec les développeurs a été effectué afin d'installer la TOE.

2.3.8. **Analyse de la facilité d'emploi et préconisations**

2.3.8.1. **Cas où la sécurité est remise en cause**

Sans objet.

2.3.8.2. **Recommandations pour une utilisation sûre du produit**

Le présent rapport de certification ne se prononce pas sur la résistance de l'UTL à une attaque physique – il est donc impératif que les UTLs soient installés et manipulés en zone non hostile, par des personnels compétents et de confiance. Ce point constitue une restriction d'usage (voir section 3.2).

Plus généralement, les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées.

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

Le CESTI a relevé que l'administrateur du produit aura besoin de recourir à un installateur certifié par le développeur lors de l'installation et de la configuration du produit.

2.3.8.4. **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 au titre de cette évaluation CSPN. L'évaluateur n'a pas relevé de vulnérabilité exploitable, dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

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 œuvre 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 « Synergis Cloud Link, version HW : SY-CLOUDLINK-312-CSPN / SW : 10.7.411.8 (2018-04-18) » 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 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]. La sécurité du produit est fortement dépendante de sa bonne installation et de sa bonne configuration initiale, qui ne sont pas garanties par l'évaluation du produit. Il est donc impératif que ces phases soient réalisées par des intégrateurs compétents et de confiance. Par ailleurs, le présent rapport de certification ne se prononce pas sur la résistance des UTLs à une attaque physique – il est donc impératif que les concentrateurs d'accès soient installés et manipulés en zone non hostile, par des personnels compétents et de confiance.

Annexe 1. Références documentaires du produit évalué

[CDS]	<i>Synergis CloudLink – Cible de sécurité CSPN</i> Référence : SY-CLOUDLINK-312-CSPN ; Version : 1.1 ; Date : 16 août 2018
[RTE]	<i>Rapport Technique d’Evaluation CSPN Synergis Cloud Link</i> Référence : SCL_CSPN_RTE ; Version : 2.0 ; Date : 31 août 2018 Et son annexe <i>Analysis of Cryptographic Mechanisms Synergis Cloud Link</i> Référence : SCL_CRY ; Version : 1.0 ; Date : 2 juillet 2018

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 www.ssi.gouv.fr.</p>
[MdP]	<p>Note technique – Recommandations de sécurité relatives aux mots de passe, 5 juin 2012, ANSSI.</p> <p>https://www.ssi.gouv.fr/administration/guide/mot-de-passe/</p>