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-2025/05

Security Center Synergis

Version Security Center Synergis 5.12.2, Synergis Cloud Link 3.1.2 (Firmware 3.1.855.0)

Paris, le 27 Mai 2025

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

Vincent STRUBEL

[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-2025/05

Nom du produit

Security Center Synergis

Référence/version du produit

Version Security Center Synergis 5.12.2, Synergis Cloud Link 3.1.2 (Firmware 3.1.855.0)

Catégorie de produit

Identification, authentification et contrôle d'accès

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

GENETEC EUROPE
4-8 rue Daru
75008 Paris

Développeur

GENETEC EUROPE
4-8 rue Daru
75008 Paris

Centre d'évaluation

THALES / CNES
290, allée du Lac
31670 Labège, France

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Protection des communications IP
Contrôle des données entrantes de l'UTL
Mises à jour sécurisées de l'UTL
Durcissement du système d'exploitation de l'UTL
Utilisation de la technologie MIFARE® DESFire®
Protections des communications sérielles avec l'UTL
Amorce sécurisée de l'UTL (Secure boot)
Chiffrement de l'exportation des configurations de l'UTL
Forcer le changement du mot de passe par défaut de l'UTL
Protection de l'accès administrateur au système d'exploitation de l'UTL (root)

Chiffrement des données utilisateur sur UTL Authentification des usagers au GAC Gestion des privilèges des usagers du GAC Protection des bases de données du GAC Protection contre les attaques par relais GAC intègre et authentique Protection en disponibilité de la fonction de journalisation
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. 3.2)

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 « Security Center Synergis, Version Security Center Synergis 5.12.2, Synergis Cloud Link 3.1.2 (Firmware 3.1.855.0) » développé par GENETEC EUROPE.

Ce produit est une composante de la plateforme de sécurité unifiée Security Center de GENETEC assurant les fonctions de contrôle d'accès physique et offrant une gestion centralisée en temps réel de secteurs sécurisés.

Le produit Security Center Synergis permet de contrôler et superviser l'accès physique aux locaux d'une entreprise aux personnes munies d'un badge légitime et d'un code PIN.

Le produit évalué est composé des éléments suivants :

- le serveur « *Security Center* Synergis » permettant la gestion des accès (GAC) ;
- les clients *Security Desk, Config Tool* et Genetec *Web App* permettant d'accéder au serveur GAC de manière déportée ;
- quatre types de têtes de lecture (lecteurs de badge simple ou clavier) ;
- des modules « Synergis *Cloud Link* » (UTL) autorisant ou non l'accès utilisateur ;
- des modules d'entrée-sortie.

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

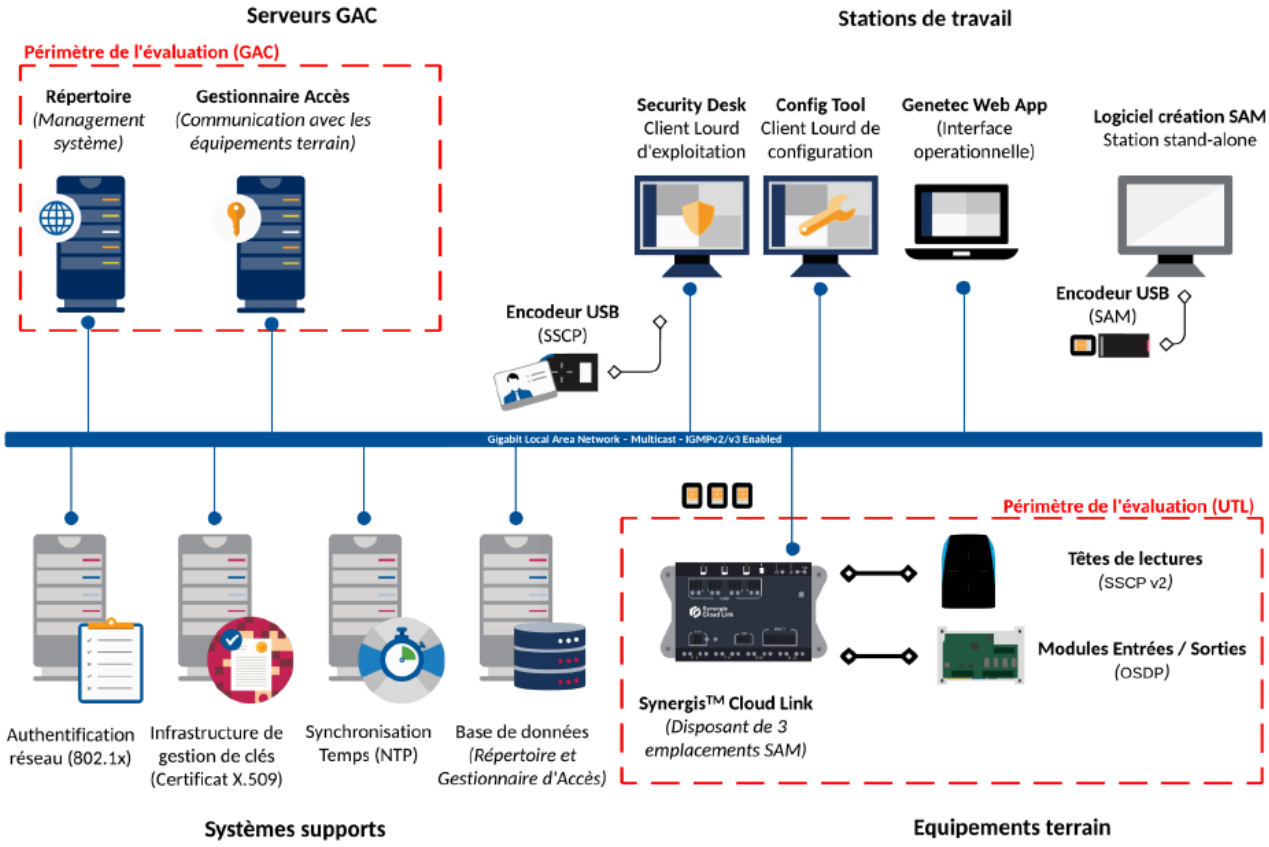

Figure 1 - Architecture Produit.

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	Security Center Synergis
Numéro de la version évaluée	Version Security Center Synergis 5.12.2, Synergis Cloud Link 3.1.2 (Firmware 3.1.855.0)

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

- Pour le GAC *(Security Center* Synergis*)* : dans l'onglet « A propos » de la page d'accueil ;
- Pour l'UTL (Synergis *Cloud Link*) : dans le Security Desk, l'onglet « Maintenance > Etat du système > Unité » affiche la version du microgiciel et de Synergis *Softwire* ;
- Pour les têtes de lecture : dans le Security Desk, l'onglet « Maintenance > Etat du système > Moniteur > Unités de contrôle d'accès > Unité » affiche la version des lecteurs.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection des communications IP ;
- le contrôle des données entrantes de l'UTL ;
- les mises à jour sécurisées de l'UTL ;
- le durcissement du système d'exploitation de l'UTL ;
- l'utilisation de la technologie MIFARE® DESFire® ;
- la protection des communications sérielles avec l'UTL ;
- l'amorce sécurisée de l'UTL *(Secure boot)* ;
- le chiffrement de l'exportation des configurations de l'UTL ;
- le forçage du changement du mot de passe par défaut de l'UTL ;
- la protection de l'accès administrateur au système d'exploitation de l'UTL (root) ;
- le chiffrement des données utilisateur sur UTL ;
- l'authentification des usagers au GAC ;
- la gestion des privilèges des usagers du GAC ;
- la protection des bases de données du GAC ;
- la protection contre les attaques par relais ;
- la garantie d'intégrité et d'authenticité du GAC ;
- la protection en disponibilité de la fonction de journalisation.

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 Enterprise LTSC Version 1809
	Applicatifs	*Security Center* 5.12.2 *(Directory and Access Manager)*	*Security Center 5.12.2 (Security Desk , Config Tool)*
	Fonctions cryptographiques	.NET Framework 4.8	
	Bases de données et annuaires		SQL *Server* 2022
UTL	Système d'exploitation	Linux kernel 5.15	
	Applicatifs	Synergis *Cloud Link* 3.1.2 : - Microgiciel version 3.1.855 - Synergis *Softwire* version 11.5.1584.0	
	Fonctions cryptographiques		
	Module entrée-sortie	STid version 1.0.31	
	SAM		MIFARE SAM AV3
Têtes de lecture	Lecteurs simples	STid réf. ARCT-W33-APH5-7ADx, *firmware* version 22 STid réf. ARC-W33-APH5-7ADx, *firmware* version 21 STid réf. ARC1-W33-yPH5-7ADx, *firmware* version 22	

	Lecteurs-clavier	STid réf. ARC-W33-BPH5-7ADx, *firmware* version 21	
Badges			MIFARE 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 système doit être installé et configuré par un prestataire de confiance agréé par le développeur. Les éléments critiques (UTLs, serveur GAC) sont placés dans des zones sûres (protégées en accès physique) et les modules de porte sont placés à l'intérieur du local protégé.

2.2.1.3 Notes et remarques diverses

Sans objet.

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.

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 pour le niveau d'attaquant considéré et 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

Les risques identifiés lors de l'évaluation entraînent des recommandations pour l'utilisateur (voir chapitre 3.2).

2.2.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté mais sa mise en œuvre est complexe.

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 [ANA_CRY].

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 n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence 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 « Security Center Synergis, Version Security Center Synergis 5.12.2, Synergis Cloud Link 3.1.2 (Firmware 3.1.855.0) » 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], notamment :

- L'installation du produit doit se faire selon le guide « Configurer Genetec Security Center et le Synergis Cloud Link pour conformité ANSSI CSPN », qui détaille divers aspects de la sécurisation et de la configuration opérationnelle.

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 : - Cible de sécurité CSPN Security Center Synergis, version 1.4, 12 mai 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cible de sécurité CSPN Security Center Synergis, version 1.5, 16 mai 2025.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN *Genetec Synergis CSPN 2024,* référence GNT2_CSPN_RTE_FR_1.4, version 1.4, 12 mai 2025.
[ANA_CRY]	Rapport d'expertise cryptographique : - *Analysis of Cryptographic Mechanisms* Genetec Synergis CSPN 2024*,* référence GNT2_CRY, version 1.2, 7 mai 2025.
[GUIDES]	Guides d'utilisation, d'administration et d'installation du produit : - *Security Center Installation and Upgrade Guide*, version 5.12.2.0, 9 juillet 2024 ; - *Security Center Hardening Guide*, version 5.12, 4 avril 2024 ; - *Security Center Administrator Guide,* version 5.12, 19 avril 2024 ; - *Security Center User Guide*, version 5.12, 2 juillet 2024 ; - Configurer Genetec Security Center et le Synergis Cloud Link pour conformité ANSSI CSPN, version 1.3.

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. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[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.
[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 2.0, 23 novembre 2023.
[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.