Cible de Sécurité CSPN

Security Center Synergis[MC]

Version 1.5

Genetec™

Table des matières

Historique des versions

Révision	Date	Rédacteurs	Commentaires
1.0	14 juin 2023	Jérôme Brodeur Sylvain Ouellet Damien DE LA HOZ	Version initiale
1.1	22 septembre 2023	Jérôme Brodeur	Précisions dans les hypothèses H6 et H7
1.2	27 octobre 2023	Jérôme Brodeur	• Précision dans H10 • Corrections dans FS2
1.3	22 août 2024	Jérôme BRODEUR Damien DE LA HOZ	• Mise à jour de la cible de sécurité à la suite des remarques de l'ANSSI • Prise en compte de la nouvelle base documentaire ANSSI
1.4	12 mai 2025	Jérôme BRODEUR Damien DE LA HOZ	Précision sur l'identification du produit
1.5	16 mai 2025	Jérôme BRODEUR Damien DE LA HOZ	Version pour publication

1 Introduction

1.1 Identification de la cible de sécurité

Ce document décrit la cible de sécurité relative à la solution de contrôle d'accès Synergis[MC] en vue de l'obtention d'une certification de sécurité de premier niveau (CSPN).

La présente Cible de Sécurité est établie dans le cadre de la méthodologie d'évaluation décrite dans :

- **ANSSI-CSPN-CER-P-01 Certification de sécurité de premier niveau v5.0 [ANSSI_CER_P_01],**
- **ANSSI-CSPN-NOTE-07 Méthodologie pour évaluation CSPN Contrôle d'accès V2.0 [ANSSI_NOTE_7].**

La Cible de Sécurité répond aussi bien au contenu qu'à la structure décrits dans :

- **ANSSI-CSPN-NOTE-09 Contenu et structure de la cible de sécurité CSPN v1.0 [ANSSI_NOTE_9],**
- **Profil de protection pour les Système de contrôle d'accès physique v1.0 [ANSSI_MOD_CDS].**

Ces documents sont disponibles publiquement sur le site de l'ANSSI.

1.2 Identification du produit

Fabricant	Genetec Inc.
Site du fabricant	https://www.genetec.com
Nom commercial du produit	Security Center Synergis[MC]
Référence	Security Center et Synergis[MC] Cloud Link (SY-CLOUDLINK-G2-312)
Version du produit	Security Center 5.12.2 Synergis[MC] Cloud Link 3.1.2 (Firmware 3.1.855.0)
Catégorie du produit[1]	Identification, authentification et contrôle d'accès

Note 1 : Selon l'annexe B : Porté d'agrément du document ANSSI-CSPN-AGR-P-01 Procédure d'agrément des centres évaluation en vue de la CSPN – v1.2

1.2.1 Procédure d'identification

L'identification des versions logicielles, matérielles et micrologicielles est décrite dans les guides :
[GEN_SCL_INS] *Guide d'installation du matériel Synergis[MC] Cloud Link*
[GEN_SC_ADMIN] *Guide de l'administrateur Security Center*

2 Argumentaire du produit

Cette section décrit le produit et son environnement d'utilisation. Lorsque cela est pertinent, chaque sous-section réfère aux recommandations du guide [ANSSI_PA_72], sous la forme : « Recommandations : Rxx ».

2.1 Description générale du produit

Le produit Security Center est la plateforme de sécurité unifiée de Genetec, unifiant le contrôle d'accès, la vidéoprotection ainsi que la reconnaissance automatique de plaque d'immatriculation (RAPI) sous un même produit. Il s'agit d'une solution dite « ouverte » qui offre l'option aux clients de choisir parmi plusieurs manufacturiers d'équipements compatibles. L'innovation et la cybersécurité sont les piliers fondateurs de la plateforme Security Center.

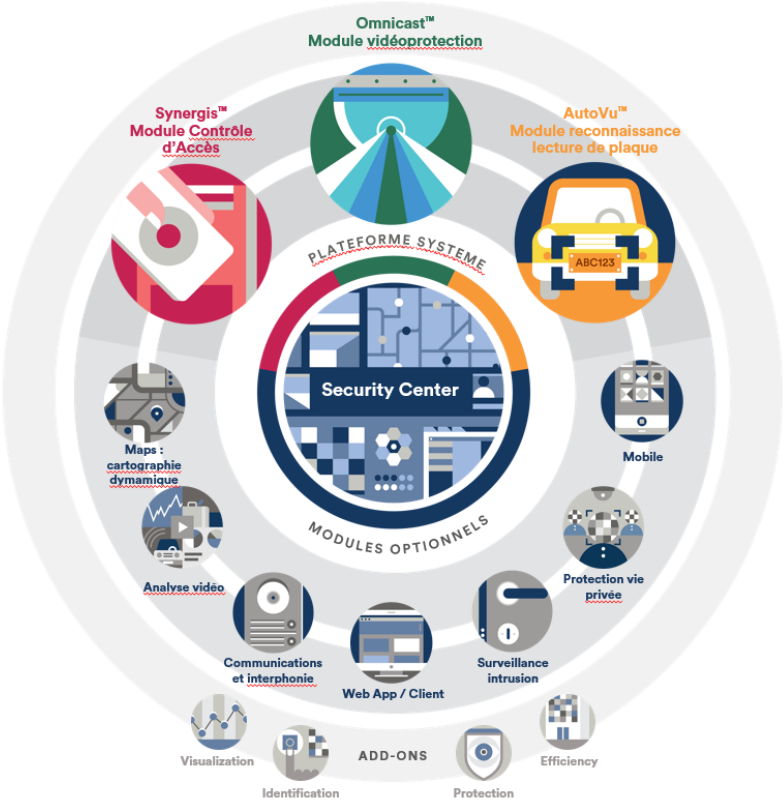

Figure 1 : Vue d'ensemble de la plateforme Security Center

Le produit Synergis[MC] est la composante de Security Center assurant les fonctions de contrôle d'accès physique sur réseau IP offrant une gestion centralisée en temps réel de secteurs sécurisés. La solution Synergis[MC] est compatible avec plusieurs manufacturiers de contrôleurs, lecteurs de porte et identifiants. Le tout repose sur une unité Synergis[MC] Cloud Link qui agit comme point d'interconnexion entre le serveur de Gestionnaire d'accès et les unités et les têtes de lecture.

Synergis[MC] est conçu sur la base d'une architecture ouverte et distribuée. Synergis[MC] peut prendre en charge plusieurs milliers de portes, de contrôleurs et de stations de gestions clientes. La solution est ainsi conçue pour pouvoir s'adapter à tout type de taille de site sur les différents marchés que sont le secteur industriel, le secteur tertiaire, le secteur bancaire, les infrastructures critiques ainsi que les centres de données.

Les titulaires de cartes d'accès disposent d'un badge personnel sans contact. Pour accéder à une zone sécurisée, ces derniers doivent présenter leur badge dans le champ magnétique d'une tête de lecture connectée au Synergis[MC] Cloud Link. L'accès au secteur est alors accordé ou refusé, selon les autorisations associées à l'identifiant.

Les secrets cryptographiques échangés entre la carte sans contact et le Synergis[MC] Cloud Link sont protégés en confidentialité et intégrité par la solution MIFARE® DESFire® EV2/EV3 proposée par NXP. La protection des échanges s'appuie sur des cartes MIFARE® SAM AV3 insérées dans les Synergis[MC] Cloud Link.

L'architecture CSPN de Synergis[MC] met en œuvre des têtes de lecture opérants sur bus sériel RS-485 en mode transparent, c'est-à-dire qu'elles relayent l'identifiant extrait du badge MIFARE® DESFire® EV2/EV3 à l'UTL Synergis[MC] Cloud Link sans participer au mécanisme cryptographique. De fait, les têtes de lecture ne disposent pas des clés cryptographiques protégeant les informations.

2.1.1 Composition de la solution

La composante contrôle d'accès Synergis[MC] de la plateforme Genetec[MC] Security Center peut être décomposée en trois : les serveurs du Système de Gestion des Accès Contrôlés (appelé GAC par la suite du présent document), les stations de travail et les équipements déployés sur le terrain pour contrôler les accès. Synergis[MC] évolue dans un écosystème de Systèmes d'Information (appelé SI par la suite du présent document) et repose sur d'autres éléments de sécurité que sont un système de synchronisation de temps, d'une infrastructure de gestion de clés (PKI) et d'un système d'authentification cryptographique des accès au réseau (protocole 802.1X).

Voir la section § 2.1.5 Description des éléments constitutifs de la solution.

a) Le GAC est constitué des éléments suivants :

- Le serveur de contrôle d'accès (Répertoire et Gestionnaire d'accès),
- Le serveur de base de données (SQL),

Inclus dans le périmètre de l'évaluation de la CSPN, à l'exception de la base de données SQL et de l'Operating System (OS) desdits serveurs.

b) Les stations de travail sont les suivantes :

- La station cliente de configuration : Genetec[MC] Security Center Config Tool,
- La station cliente opérationnelle : Genetec[MC] Security Center Security Desk
- La station cliente opérationnelle : Genetec[MC] Security Center WebApp (optionnelle),
- La station d'encodage des cartes MIFARE® SAM AV3

Exclues du périmètre de l'évaluation de la CSPN

c) Les équipements terrain sont :

- Le contrôleur intelligent (UTL) Synergis[MC] Cloud Link,
- Les cartes MIFARE® SAM AV3,
- Les modules d'entrées-sorties (voir liste en annexe § 8.1.2 Modules d'entrées-sorties);
- Les têtes de lecture SSCP®v2 avec/sans clavier PIN (voir liste en annexe § 8.1.1 Têtes de lecture),

Inclus dans le périmètre de l'évaluation de la CSPN, à l'exception des cartes MIFARE® SAM AV3

d) Les systèmes support connexes sont :

- Le système de gestion de synchronisation temps (exemple Serveur NTP),
- Le système d'authentification réseau (exemple : protocole 802.1x),
- L'infrastructure de gestion de clés (aussi appelée IGC ou PKI)

Exclus du périmètre de l'évaluation de la CSPN

2.1.2 Schéma d'architecture simplifié de la solution

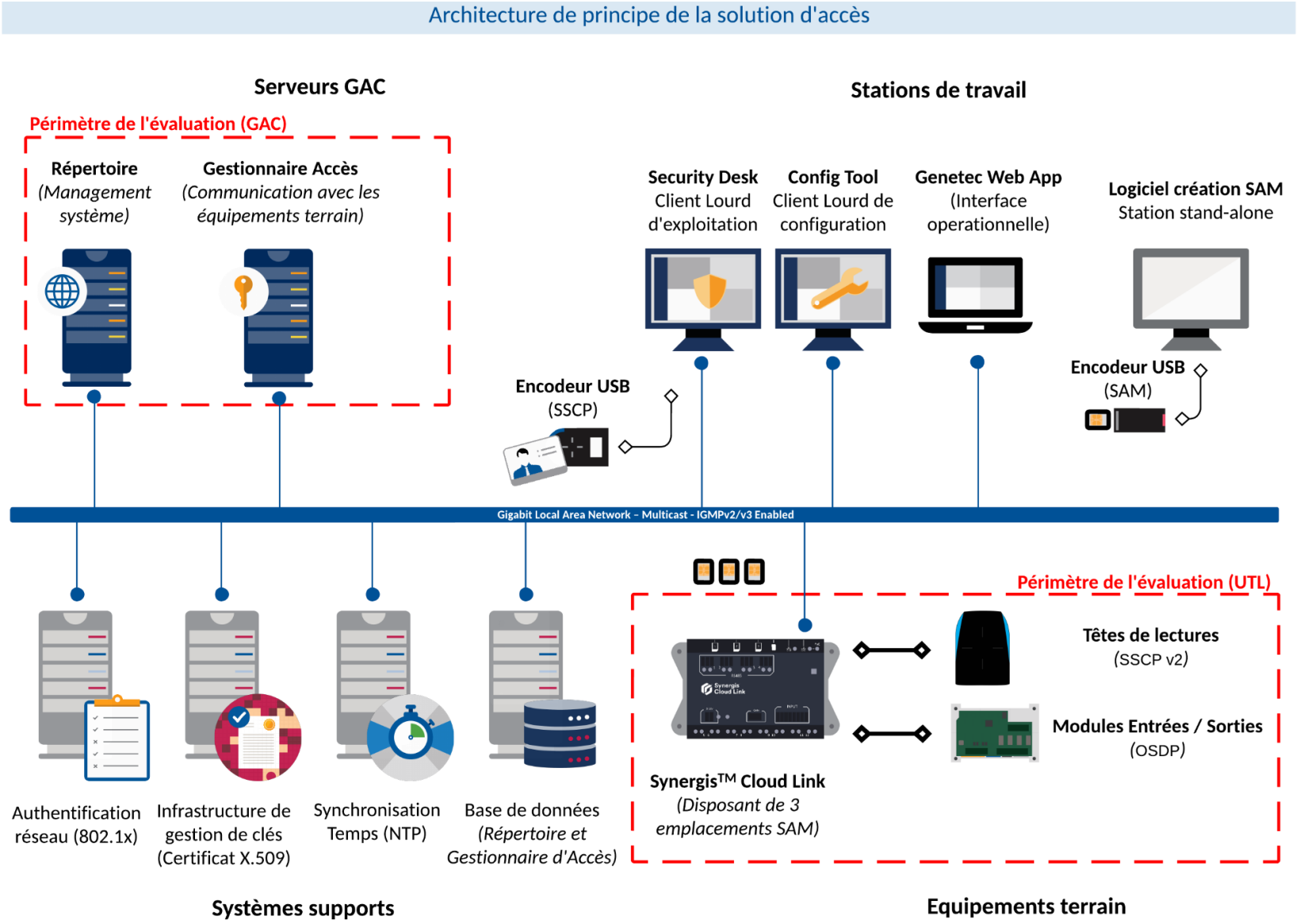

Figure 2 : Schéma d'architecture simplifié de la solution

2.1.3 Description fonctionnelle de la solution

La composante contrôle d'accès physique de la plateforme Security Center, nommée Synergis[MC], a pour objectif de filtrer les flux d'individus souhaitant évoluer à l'intérieur d'un site, d'un bâtiment ou d'un local. Pour cela les fonctionnalités suivantes sont assurées :

- Garantir l'unicité des titulaires de carte au sein de la base de données système et de consigner leurs informations relatives,
- Gérer les privilèges d'accès au travers des puissants concepts des Règles d'Accès et Groupe de Titulaires de Carte
- Consigner l'ensemble des évènements liés à l'activité des utilisateurs du système, selon la durée de rétention paramétrée.

Synergis[MC] est doté d'une architecture basée sur le serveur appelé Gestionnaire d'accès, qui gère les contrôleurs physiques de porte.

La description générale du fonctionnement de l'architecture de Synergis[MC] est résumée ci-après :

- Les configurations système sont enregistrées par le Répertoire.
- Le Répertoire transmet les configurations au Gestionnaire d'accès.
- Le Gestionnaire d'accès communique directement avec les contrôleurs intelligents (UTL) Synergis[MC] Cloud Link par TCP/IP.
- Le Gestionnaire d'accès envoie les horaires, les données de titulaires de cartes ainsi que les règles d'accès aux contrôleurs de porte intelligents (UTL) Synergis[MC] Cloud Link.
- Lorsqu'un titulaire de cartes présente son identifiant à un lecteur, le contrôleur intelligent (UTL) Synergis[MC] Cloud Link consulte la règle d'accès pour savoir s'il doit accorder ou refuser l'accès.
- Une fois que les contrôleurs intelligents (UTL) Synergis[MC] Cloud Link ont été synchronisés avec le Gestionnaire d'accès, ils peuvent fonctionner de façon autonome, même en cas de perte de connexion au Gestionnaire d'accès.
- Avec des configurations supplémentaires, un titulaire de cartes peut appartenir à un groupe de titulaires de cartes, ou une porte peut être intégrée à un secteur, et plusieurs horaires et règles peuvent être envoyés vers un contrôleur intelligent (UTL) Synergis[MC] Cloud Link.

Contrairement à d'autres solutions de contrôle d'accès, Synergis[MC] n'utilise pas de *codes d'autorisation* ou de *niveaux d'accès* pour accorder ou refuser l'accès. La logique de base utilisée par Synergis[MC] consiste plutôt à accorder ou refuser l'accès selon *des règles d'accès*.

Les règles d'accès s'articulent autour des trois Q :

- Qui (Qui peut passer - titulaires de cartes ou groupes de titulaires de cartes)
- Quoi (L'accès est accordé ou refusé)
- Quand (L'horaire d'application de la règle)

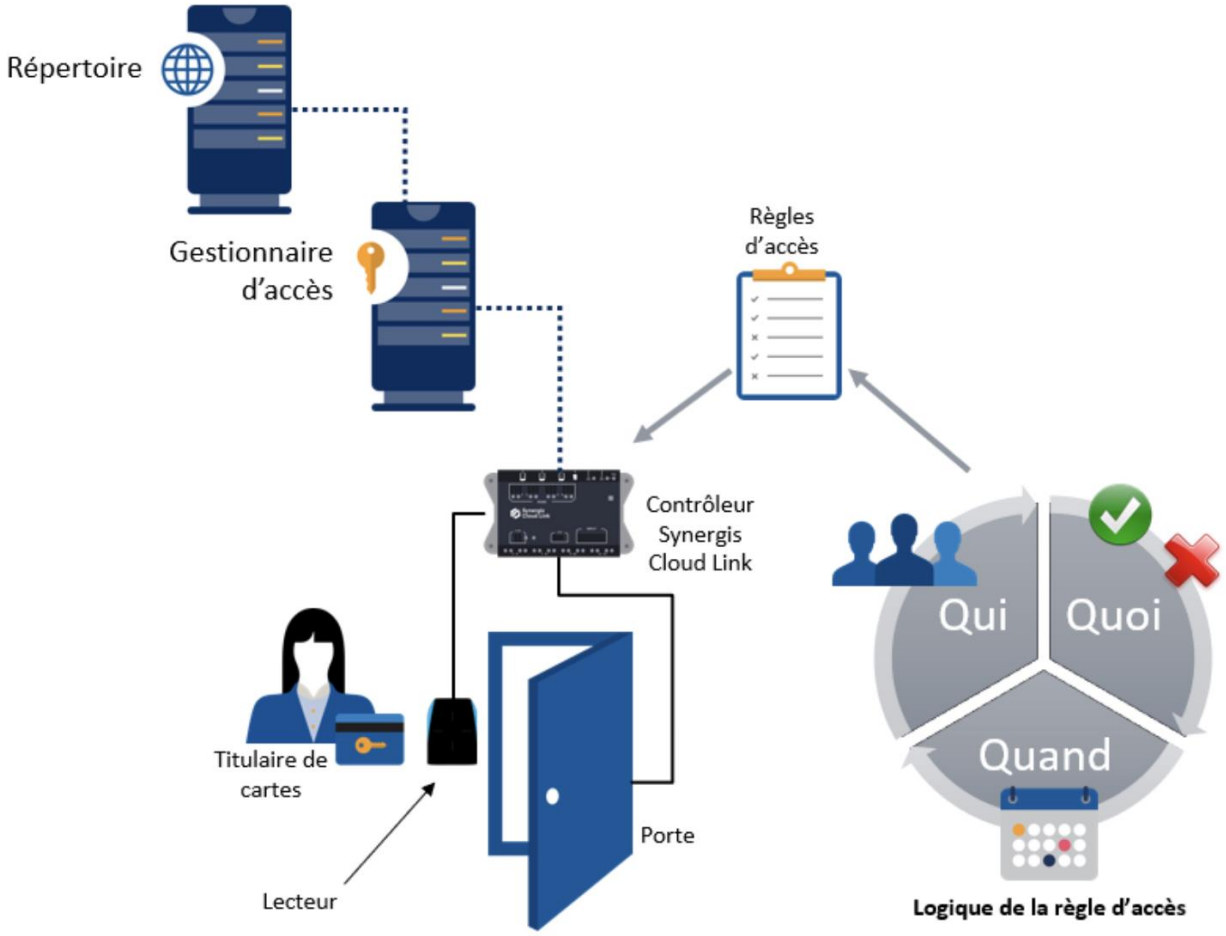

Figure 3 : Fonctionnement de Synergis[MC]

Le système de contrôle d'accès évolue dans un écosystème et repose sur des ressources décrites dans les paragraphes 2.1.1 Composition de la solution et 2.1.5 Description des éléments constitutifs de la solution :

Equipements du GAC :

- Serveur applicatif contrôle d'accès
- Serveur de base de données
- Serveur d'authentification réseau
- Serveur de Certificat
- Station d'exploitation et/ou d'encodage de badge MIFARE® DESFire® EV2/EV3
- Station d'encodage des cartes MIFARE® SAM AV3

Equipements terrain :

- Contrôleur Synergis[MC] Cloud Link
- Module d'entrées-sorties

- Lecteurs transparents
- Les cartes MIFARE® SAM AV3
- Les badges MIFARE® DESFire® EV2/EV3

2.1.4 Description des réseaux

Les équipements de contrôle d'accès peuvent présenter un niveau d'exposition accru dû à leur emplacement ce qui représente un point d'intrusion potentiel dans le système d'information de l'entité, notamment lorsque les réseaux supports et fédérateurs sont mutualisés avec d'autres composantes du système d'information de l'entité. Il convient ici de décrire les différents réseaux utilisés dans le système d'information contrôle d'accès, afin de mieux appréhender les risques, les enjeux et les recommandations associées.

Recommandations : R10, R10-, R11

Description des réseaux de terrain dédiés RS-485

Les réseaux terrain dédiés, aussi appelés liaisons filaires, constituent le câblage exclusif mis en place pour raccorder les têtes de lecture ainsi que les modules d'entrées-sorties aux contrôleurs intelligents (UTL) Synergis[MC] Cloud Link. Du fait de leur fonction, les têtes de lecture de contrôle d'accès sont situées à l'extérieur de la zone sécurisée et doivent être protégées. Leur accessibilité est un risque à considérer. Il est hautement recommandé que ces liaisons soient réalisées côté sécurisé de la zone et protégées physiquement à leur tour par des moyens en adéquation aux risques environnementaux.

Ces liaisons sont des liaisons électriques dédiées uniquement aux équipements du contrôle d'accès, répondant à la norme EIA-485 (souvent appelée RS-485), transportant des protocoles de communication standards et non-propriétaires eux-mêmes sécurisés lorsque les préconisations de mise en service sont appliquées. Ces protocoles sont le SSCP®v2 pour les liaisons têtes de lecture et l'OSDP[MC]v2 Secure Channel pour les liaisons modules entrées/sorties. Il convient ainsi de respecter la nature et les propriétés techniques de ces liaisons telles que spécifiées dans les standards afin d'assurer le bon fonctionnement et la pérennité de l'installation.

Les réseaux terrains sont inclus dans le périmètre de l'évaluation de la CSPN.

Recommandations : R12, R13, R14, R15, R15-

Description du réseau support

Le réseau support constitue le commutateur Ethernet TCP/IP sur lequel sont connectés les contrôleurs Synergis[MC] Cloud Link. Ce réseau étant la porte d'entrée pour la communication avec le ou les serveurs Security Center hébergeant le(s) Gestionnaire d'accès, il est essentiel de prendre toutes les précautions nécessaires pour sa protection. Le déploiement, la mise en œuvre et la maintenance de ce réseau support sont assurés par le client final ou une société tierce mandatée par le client final.

Le réseau support est exclu du périmètre de l'évaluation de la CSPN à l'exception de la connexion des contrôleurs Synergis[MC] Cloud Link.

Recommandations : R16, R17, R18, R19; R19-, R20, R21, R21-

Description du réseau fédérateur

Le réseau fédérateur désigne l'ensemble des équipements réseaux intervenant dans la mise en relation entre les réseaux support avec le réseau du centre de gestion. Il constitue de ce fait le réseau local Ethernet TCP/IP mettant en relation les serveurs Security Center hébergeant le Gestionnaire d'accès, le Répertoire, le serveur de certificats (X.509), le serveur d'authentification réseau (802.1x), les stations de travail hébergeant les applications clientes Genetec[MC] Security Desk, Genetec[MC] Config et Genetec[MC] WebApp.

Le déploiement, la mise en œuvre et la maintenance de ce réseau support sont assurés par le client final ou une société tierce mandatée par le client final.

Le réseau fédérateur support est exclu du périmètre de l'évaluation de la CSPN à l'exception de la connexion des contrôleurs Synergis[MC] Cloud Link, les serveurs hébergeant les Security Center et les stations de travail exécutant les clients Security Center.

Recommandations : R23, R24, R25, R26; R26-, R27, R27-, R28, R29, R29-

2.1.5 Description des éléments constitutifs de la solution

Système de Gestion des Accès Contrôlés (GAC)

Synergis[MC] Security Center permet d'enrôler les contrôleurs Synergis[MC] Cloud Link de les configurer; d'administrer l'intégralité des Titulaires de carte, de leurs privilèges ainsi que mener des tâches d'investigations concernant les entités concernées. Synergis[MC] Security Center représente ici le GAC. Il repose sur des ressources pouvant être des serveurs physiques ou virtuels opérant un système d'exploitation de type Windows et héberge une base de données de type SQL Express. Dans son expression la plus simple une seule ressource peut héberger l'ensemble des composantes applicatives et base de données. Pour des systèmes de grande envergure comptant des milliers de portes, il est recommandé d'utiliser une machine distincte pour chaque instance de serveur applicatif.

Le système de base de données est considéré comme étant supposé de confiance, celui-ci est plus amplement décrit dans la section: Le(s) serveur(s) de base de données SQL. Toutefois l'authentification et le chiffrement des données en transit impliquent la responsabilité du GAC.

Il est considéré que les serveurs hébergeant le GAC, sont :

- installés dans des locaux sécurisés (zone névralgique), dont l'accès à la ressource est contrôlé physiquement et informatiquement,
- dotés d'un antivirus réputé et éprouvé,
- à jour en termes de correctifs de sécurité

Uniquement lors des premières étapes du déploiement du GAC, un compte administrateur avec l'intégralité des droits et privilèges sur le système est requis. Ce compte peut être désactivé au profit de comptes administrateurs partiels, eux-mêmes synchronisés depuis un Fournisseur d'Identité (IdP) faisant ainsi bénéficier des politiques de MFA et de SSO mis en place par le client final.

Synergis[MC] repose essentiellement sur deux composants pour le fonctionnement du métier contrôle d'accès. Ces modules sont décrits ci-après.

Inclus dans le périmètre de l'évaluation de la CSPN

a) Répertoire (Directory)

Le Répertoire est la fonction principale qui identifie un système. Il gère toutes les configurations d'entités et réglages à l'échelle du système dans Security Center (titulaires de cartes, identifiants, portes, horaires, règles d'accès, etc.). Une seule instance est autorisée par système. Le serveur qui héberge le Répertoire est appelé le

serveur principal. Afin de proposer une haute disponibilité, Security Center propose un mécanisme de basculement et d'équilibrage de charge au niveau applicatif, sans devoir reposer sur un système tiers.

b) Gestionnaire d'accès (Access Manager)

Le Gestionnaire d'accès est la fonction qui gère les unités de contrôle d'accès du système. Il assure la mise à jour des réglages de contrôle d'accès Security Center sur les unités (en temps réel ou sur horaire) afin qu'elles puissent prendre des décisions de contrôle d'accès de manière autonome, qu'elles soient connectées ou non au Gestionnaire d'accès.

Le Gestionnaire d'accès consigne également les événements de contrôle d'accès dans la base de données à des fins d'investigation ou de maintenance. Tous les événements générés par les unités (accès accordé, accès refusé, porte ouverte, etc.) sont transmis par le Gestionnaire d'accès, par l'intermédiaire du Répertoire, aux composants concernés du système.
Plusieurs instances du Gestionnaire d'accès peuvent être créées au sein du système, pour offrir une redondance et augmenter l'extensibilité.

Stations de travail

Les administrateurs et les utilisateurs du système ont besoin de postes de travail sur lesquels s'exécutent les applications Config Tool et Security Desk de la plateforme Genetec[MC] Security Center.

Ces postes de travail doivent respecter :

- Les prérequis Genetec en accord avec leurs rôles au sein du système,
- La mise en place d'un antivirus éprouvé et l'application régulière de correctifs de sécurité.

Le respect d'une hygiène informatique stricte est d'autant plus crucial lorsque le système de contrôle d'accès est connecté à d'autres SI.

Exclu du périmètre de l'évaluation de la CSPN

Recommandations : R42, R79

a) Config Tool : Client Lourd de paramétrage de Genetec[MC] Security Center

Config Tool est l'interface utilisateur permettant la configuration de la plateforme Genetec[MC] Security Center, incluant la partie Synergis[MC]. Cette interface est organisée en tâches, regroupées en quatre catégories principales (tâches communes, contrôle d'accès, RAPI et vidéo). La disponibilité des tâches varie en fonction de la licence du système et des privilèges de l'utilisateur connecté au Config Tool. Des privilèges d'utilisateur sont associés à chaque tâche et à de nombreuses commandes dans Security Center. Enfin, les tâches peuvent être personnalisées et plusieurs tâches peuvent être effectuées en même temps.

Exclu du périmètre de l'évaluation de la CSPN

b) Security Desk : Client Lourd opérationnel de Genetec[MC] Security Center

Security Desk est l'interface utilisateur destinée à l'exploitation de la plateforme Genetec[MC] Security Center. Il fournit des processus cohérents à l'échelle d'Omnicast[MC], Synergis[MC], et AutoVu[MC], les principaux modules de

Security Center, destinés respectivement à la vidéosurveillance, au contrôle d'accès et à la reconnaissance automatique de plaques d'immatriculation (RAPI).

La conception centrée sur les tâches de Security Desk permet aux agents d'exploitation de contrôler et surveiller efficacement de nombreuses applications de sécurité et de sûreté. Au sein d'une interface unifiée, l'agent d'exploitation peut suivre les événements et les alarmes en temps réel, créer des rapports, contrôler l'état des portes et suivre les titulaires de cartes. Lorsqu'il est connecté à une Fédération[MC] de plusieurs systèmes, Security Desk permet de gérer la surveillance, la création de rapports et les alarmes sur des dizaines ou des centaines de sites.

Exclu du périmètre de l'évaluation de la CSPN

c) Encodage badge

La station d'encodage de badge peut être une station de travail exécutant le client Genetec[MC] Security Desk et muni d'un lecteur encodeur USB. Ces lecteurs sont en protocole SSCP®. Les bonnes pratiques de déploiement permettent de n'autoriser qu'une connexion chiffrée/signée à cet équipement avec un jeu de clé propre au client final. L'utilisateur connecté à cette station de travail doit être muni des privilèges adéquats, lui permettant de réaliser les missions d'encodage au sein de la plateforme Security Center. L'encodage du badge peut aussi être réalisé depuis un autre logiciel.

Exclu du périmètre de l'évaluation de la CSPN

d) Web App

Genetec[MC] Web App est un moyen unifié, mobile et axé sur les cartes de surveiller les entités et de générer des rapports depuis un navigateur Web.

Exclu du périmètre de l'évaluation de la CSPN

Équipements Terrain

a) Badge

Le badge MIFARE® DESFire® EV2/EV3 est le moyen pour le Titulaire de carte de s'identifier auprès du système via la tête de lecture. Ce moyen est réputé personnel et non cessible. Le badge est encodé soit par la tâche d'encodage native à la plateforme Security Center soit par une tierce partie. Cet encodage est réalisé selon la charte d'encodage propre au client final, il contient au minimum une application et un fichier en communication chiffrée afin de protéger l'identifiant privé.

Par définition le badge contient une partie des secrets du client et évolue en dehors des zones protégées, il est ainsi une cible potentielle d'attaque. Les meilleures pratiques de déploiement invitent le client à tirer pleinement profit des capacités sécuritaires proposées par le badge NXP (utilisation de plusieurs fichiers, mise en place de jeu de clé pour rotation périodique, diversification des clés, …). Ceci est réalisable grâce à une interface d'encodage de badge native à la plateforme Genetec[MC] Security Center qui est puissante et intuitive.

Exclu du périmètre de l'évaluation de la CSPN

Recommandations : R31, R32, R33, R34, R55, R56, R58,

b) Tête de lecture

Le contrôleur intelligent (UTL) Synergis[MC] Cloud Link supporte tous les lecteurs MIFARE® DESFire® répondant à la norme ISO/IEC 14443 et qui offrent le support du mode transparent sur le protocole SSCP®v2. Ces lecteurs établissent et gèrent le lien RFID avec le badge sans contact MIFARE® DESFire® EV2/EV3 au profit de l'UTL Synergis[MC] Cloud Link via une connexion sérielle sécurisée de type RS-485. Les lecteurs ne participent aucunement au protocole cryptographique (tête de lecture dite « transparente »).

La tête de lecture est dotée d'un témoin lumineux et sonore adaptés afin de notifier le titulaire de badge de l'état du lecteur et du statut de l'autorisation d'accès.

Lorsqu'il convient de durcir l'accès à une zone, il est possible d'ajouter un deuxième facteur permettant d'authentifier le Titulaire de Carte présentant le badge via la saisie d'un code PIN. La tête de lecture dotée d'un clavier numérique permettra cette opération. La saisie dudit code circule sur le canal filaire établi entre le lecteur et le contrôleur intelligents (UTL) Synergis[MC] Cloud Link. Pour plus de flexibilité, Security Center permet de gérer dynamiquement le comportement de la tête de lecture. Ainsi il est possible de passer la tête de lecture en Badge + PIN sur période horaire ou lorsque le contexte extérieur l'exige, ceci est aisément réalisable grâce à la fonction native Niveau de Risque.

Par définition, la tête de lecture est située côté non protégé de la zone sécurisée. De plus, bien qu'elle ne détienne aucune donnée sensible, le capteur d'autoprotection permet l'effacement de la clé d'appairage SSCP®v2.

Inclus dans le périmètre de l'évaluation de la CSPN

Recommandations : R36, R37, R66

c) Module d'entrées-sorties

Le module d'entrées-sorties est une carte électronique communiquant avec le contrôleur intelligent (UTL) Synergis[MC] Cloud Link via une liaison sérielle RS-485 et le protocole OSDP[MC]v2 Secure Channel. Cet équipement a pour seul objectif de gérer l'environnement de l'accès contrôlé au travers d'entrées analogiques supervisées et de sorties relais comme suit :

- Superviser l'état des entrées souvent reliées aux capteurs des portes (contact de position de la porte, capteurs de défaut de l'organe de verrouillage, bouton poussoir de sortie, déclencheur manuel de type boitier bris de glace vert, détecteurs de passage, etc.),

- Recevoir des ordres du contrôleur intelligent (UTL) Synergis[MC] Cloud Link pour les convertir en signaux de commande analogique à destination des organes de verrouillage (gâches, ventouse, serrure mécanique, verrou motorisée, porte automatique, barrière levante, etc.).

Le format compact de ce module ainsi que son contact d'autoprotection offre les atouts nécessaires lui permettant d'être installé au plus près de l'accès à contrôler sans introduire de contraintes physiques supplémentaires. Pour une plus grande flexibilité d'installation, il est aussi possible de centraliser les différents modules d'entrées-sorties au sein de locaux techniques. Quel que soit le choix d'emplacement, ce module doit être installé côté sécurisé de la zone à protéger, les liaisons filaires ne doivent pas être apparente ni facile d'accès.

Inclus dans le périmètre de l'évaluation de la CSPN

d) Contrôleur intelligent (UTL) Synergis[MC] Cloud Link

La cible de sécurité prévoit l'évaluation de la sécurité des fonctions de contrôle d'accès gérées par le contrôleur intelligent (UTL) Synergis[MC] Cloud Link. L'UTL Synergis[MC] Cloud Link s'intègre de manière transparente au sein de Security Center, et peut prendre des décisions de contrôle d'accès indépendamment du Gestionnaire d'accès.

Il est doté de 2 ports LAN, dont le premier permet une alimentation via POE IEEE 802.3af ou 802.3at Type 1 (Classe 2 6,49 W). En matière de réseautique, le contrôleur intelligent (UTL) Synergis[MC] Cloud Link communique avec le Gestionnaire d'accès via le protocole TLS1.2/1.3) et supporte l'authentification réseau (802.1x) via une infrastructure dédiée à cet effet (hors périmètre de la solution et de la présente évaluation).

Le contrôleur intelligent (UTL) Synergis[MC] Cloud Link propose une architecture unique sur le marché du contrôle d'accès. Il est doté de 12 bus sériel RS-485 permettant de transporter au choix l'un du protocole SSCP®v2 pour le raccordement des lecteurs transparents et du protocole OSDP[MC]v2 pour le raccordement des modules entrées/sorties selon la liste de compatibilités décrites dans le présent document en § 8.1 Tableau de références des équipements.

Il dispose aussi de trois emplacements pour carte MIFARE® SAM AV3 permettant d'optimiser le nombre de lectures de badge successives et rapprochées dans le temps. Les secrets propres au client et relatifs à la lecture des badges (Clés de Lecture) ne sont jamais connus par le contrôleur intelligent (UTL) Synergis[MC] Cloud Link. En effet, les cartes MIFARE® SAM AV3 sont créées par une station de création autonome et indépendante de la solution Genetec[MC] Security Center. Ces cartes SAM sont programmées pour ne jamais divulguer leur contenu. Ce maintien du plus haut niveau de sécurité assure ainsi leur déploiement et leur manipulation par des tiers.

Cet équipement se présente sous forme d'un boitier physique (cf. figure suivante). Son format compact et léger (500g) permet son installation dans un coffret à l'aide des trous de fixation ou sur un rail DIN à l'aide du support de fixation pour rail DIN (en option).

L'appareil comprend quatre entrées (supervisées ou numériques) pouvant être utilisées pour surveiller les événements externes du système de contrôle d'accès, tels que l'ouverture et/ou l'arrachement du coffret via capteur d'autoprotection de ce dernier, le défaut de source d'alimentation primaire, le défaut de batterie etc.

Le contrôleur intelligent (UTL) Synergis[MC] Cloud Link est installé côté protégé de la zone sécurisée dans un coffret lui-même verrouillé par des moyens en adéquation avec le niveau de sécurité exigé.

Figure 4 : L'UTL Genetec[MC] Synergis[MC] Cloud Link (modèle SY-CLOUDLINK-G2-312)

L'UTL assure en toute autonomie les fonctionnalités suivantes :

- Le pilotage en mode transparent de la tête de lecture (SSCP®v2), la communication avec le badge MIFARE® DESFire® EV2/EV3 et sa mise en relation avec la carte NXP SAM AV3 afin d'établir la clé de session utilisée pour la transaction concernée. Le calcul de cette clé est réalisé sans intervention du contrôleur intelligent (UTL) Synergis[MC] Cloud Link, assurant ainsi le fait que le contrôleur intelligent (UTL) Synergis[MC] Cloud Link ne connait jamais les secrets.
- Détention de la base de données contenant l'extrait de la politique de contrôle d'accès associée à un point d'accès ou une zone sécurisée.
- Détention des puissantes logiques de contrôle d'accès, telles que sas, antiretour, escorte visiteur, Double-badgeage, règle de deuxième personne, etc. Ceci au sein de ces propres lecteurs ou en interaction avec d'autres contrôleurs Synergis[MC] Cloud Link (via l'activation du Peer-to-Peer).
- Enregistrement des évènements de sécurité (perte réseau, tentative d'effraction, …) et gestion dynamique en fonction des situations suivantes :
    - Transmission des évènements en temps réel auprès du Gestionnaire d'accès lorsque la liaison entre les deux acteurs est opérationnelle.
    - Rétention jusqu'à 5 000 000 évènements en cas de coupure réseau avec le Gestionnaire d'accès.

Inclus dans le périmètre de l'évaluation de la CSPN

Recommandations : R12, R13, R14, R15, R16, R17, R19, R20, R38, R39, R40, R41, R60, R62, R80, R81, R82, R84

Serveurs connexes

a) Le(s) serveur(s) de base de données SQL

Le Répertoire (Directory) et le Gestionnaire d'accès de Genetec[MC] Security Center reposent sur une base de données pour consigner l'ensemble des entités, des équipements terrains, leurs paramètres associés ainsi que l'horodatage de l'ensemble des évènements associés. La base de données supportée par le système est Microsoft SQL (cf *Guide de la configuration requise pour Security Center* [GEN_SC_CSR]). Lorsque le déploiement suit le *Guide de renforcement de Security Center* [GEN_SC_HG], la communication avec ces bases de données est par défaut sécurisée et authentifiée. Le chiffrement de la base de données est supporté par la solution Security Center et est fortement encouragé dans le guide [GEN_SC_HG].

Lors de l'installation du logiciel Security Center, Genetec propose le déploiement d'une base SQL Express, il est aussi possible de déporter ladite base de données dans une infrastructure existante dédiée indépendante proposant un niveau de haute disponibilité. La base de données est supposée installée dans des locaux sécurisés et dont l'accès à la ressource requiert une authentification préalable.

Exclu du périmètre de l'évaluation de la CSPN

b) L'infrastructure de gestion de clés : serveur de certificats

L'infrastructure de gestion des clés a pour objectif de créer, délivrer, vérifier les certificats à destination des équipements sur le réseau Ethernet. Ceci afin de chiffrer et signer les protocoles TLS sur lesquels reposent l'ensemble des communications Ethernet TCP/IP de la solution Genetec[MC] Security Center Synergis[MC]. Les équipements du système Synergis[MC] proposent par défaut des certificats autosignés. Le *Guide de renforcement de Security Center* [GEN_SC_HG] encourage soit de signer des certificats par une PKI, soit de charger des certificats issus d'une autorité de certification connue et de confiance.

Cette infrastructure relève de la responsabilité du client final et/ou de son mandataire.

Exclu du périmètre de l'évaluation de la CSPN

Recommandations : R53, R54

c) Le système d'authentification réseau

L'authentification réseau est un mécanisme d'authentification des équipements réseaux. Celui-ci intervient en complément de l'infrastructure de gestion de clés. Il a pour objectif d'authentifier les équipements réseaux, leur attribuer une configuration réseau valide en fonction des politiques d'adressages établies par le client final ou son mandataire. Ainsi seuls les équipements réseaux, encore appelés Supplicant (serveurs, stations de travail, contrôleurs, etc.) sont autorisés à communiquer sur le réseau à accès contrôlé (réseaux fédérateurs et supports).

Ce système relève de la responsabilité du client final et/ou de son mandataire.

Exclu du périmètre de l'évaluation de la CSPN

Recommandations : R18, R19, R20 et *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux*.

Outils Annexe

a) Logiciel de création de cartes MIFARE® SAM AV3

Les clés protégeant les informations contenues sur les badges MIFARE® DESFire® (soit minimalement la clé de lecture de l'application contenant l'identifiant du titulaire de carte) sont stockées dans des cartes MIFARE® SAM AV3 pour un niveau de sécurité accru.

Conséquemment, un outil doit être utilisé pour configurer les cartes MIFARE® SAM AV3 employées pour protéger les secrets du client final. Nous assumons que les cartes MIFARE® SAM AV3 sont déjà configurées et sont réputées de confiance, elles n'entrent pas ainsi dans le périmètre de la présente évaluation. Genetec recommande l'usage d'un outil autonome pour être déployé sur des stations de travail indépendantes et isolées du réseau Ethernet.

La configuration des cartes MIFARE® SAM AV3 est nécessaire pour obtenir la configuration la plus sécurisée possible du contrôleur Synergis[MC] Cloud Link. En effet, aucun paramètre permettant aux cartes MIFARE® SAM AV3 de communiquer les clés maitresses n'est autorisé. Le concept de clé maître/esclave n'est pas exploité et aucune clé « DESFire® » n'est contenue en mémoire du contrôleur intelligent (UTL) Synergis[MC] Cloud Link. Une fois la clé de session calculée entre le badge et la carte MIFARE® SAM, il est éventuellement possible d'activer son stockage dans le contrôleur intelligent (UTL) Synergis[MC] Cloud Link pour la fin de la transaction. Ceci permet d'optimiser l'utilisation des ressources SAM dans des déploiements à grande échelle.

Exclu du périmètre de l'évaluation de la CSPN

b) Logiciel de création de SKB

Dans le cas où des lecteurs reposants sur le protocole SSCP®v2 sont utilisés, il peut être nécessaire de créer des Secure Key Bundles (SKB) à partir de badges MIFARE® DESFire® vierges.

Le cas échéant, Genetec recommande l'emploi de l'application SECard fournie par STid.

Exclu du périmètre de l'évaluation de la CSPN

2.2 Description de l'environnement d'utilisation du produit

En réponse aux besoins sécuritaires grandissants du marché de contrôle d'accès physique, les industriels font continuellement évoluer les communications depuis le badge, moyen d'identification et d'authentification utilisé par le titulaire de carte, jusqu'au contrôleur intelligent (UTL) Synergis[MC] Cloud Link qui prend la décision d'autoriser l'accès ou de refuser l'accès.

Ceci est réalisé au travers de plusieurs moyens :

- L'évolution de la communication entre la puce du badge et l'antenne RFID du lecteur,
- L'évolution de la communication entre l'électronique du lecteur et celle du contrôleur intelligent (UTL) Synergis[MC] Cloud Link,
- La mise en place d'une communication chiffrée de bout en bout au travers de lecteur transparent.

2.2.1 Communication badge - lecteur

La communication entre le puce du badge et l'antenne RFID a évoluée d'une lecture d'un simple numéro public, lisible en clair une fois le badge présent devant un champ électromagnétique; à un identifiant privé, protégé dans une zone mémoire du badge, accessible après authentification mutuelle. Ainsi des mécanismes cryptographiques ont été introduits au fil des années avec l'apparition d'algorithmes de chiffrement puissants, non propriétaires et largement utilisés dans le monde informatique et bancaire.

La mise en place de mécanismes d'autoprotections au niveau du lecteur est une des réponses de la part des manufacturiers de lecteurs afin de protéger le secret en effaçant les données sensibles sur tentative d'intrusion sur la tête de lecture. De plus, il est possible d'augmenter le niveau de sécurité en déportant le secret en zone protégée, sujet abordé ci-après dans la section 2.2.3 Communication lecteur transparent.

Dans la présente évaluation, la solution de contrôle d'accès Synergis[MC] Cloud Link repose uniquement sur l'utilisation de badges MIFARE® DESFire® EV2/EV3. Ce support permet le chiffrement des transactions en AES-128 ainsi que l'utilisation de la diversification des clés contenues dans le badge suivant les standards en vigueur. Ceci aura pour effet de « générer » une clé propre et unique à chaque support badge. La norme préconisée est NXP AN-10922. Au fur et à mesure des évolutions de la puce NXP MIFARE® DESFire®, l'introduction de nouvelles possibilités de communication avec la puce sont désormais possible.

Recommandations : R36, R55, R56, R56-

2.2.2 Communication lecteur - contrôleur

La communication entre le lecteur et le contrôleur intelligent (UTL) Synergis[MC] Cloud Link s'effectue au moyen d'une liaison filaire électrique sérielle dédiée, connue sous le nom de RS-485. Elle permet de véhiculer l'information de manière sécurisée via le protocole de communication ouvert et non propriétaire qu'est le SSCP®v2.

Les documents de déploiement [GEN_SCL_INS], [GEN_SCL_CFG], [GEN_SCL_INT] guident les utilisateurs dans les meilleures pratiques pour la mise en sécurité complète de ces liaisons.

Lorsque la situation le requiert, la tête de lecture peut se voir dotée d'un clavier numérique afin d'authentifier le titulaire de carte. Le code personnel saisi est ainsi protégé en intégrité et en confidentialité lors du transit sur le canal de communication RS-485.

Recommandations : R37

2.2.3 Communication lecteur transparent

La combinaison des 2 communications susmentionnées constitue une communication chiffrée de bout en bout entre le badge et le contrôleur intelligent (UTL) Synergis[MC] Cloud Link avec la tête de lecture comme élément réalisant l'authentification sur le canal filaire et le canal sans fil. Par définition le lecteur se situe dans la zone non protégée, introduisant ainsi une faiblesse sécuritaire dans la chaine de communication. Malgré les mécanismes de protection évoqués précédemment, cette configuration est désormais déconseillée par l'*ANSSI guide recommandations sécurisation systèmes contrôle accès physique et vidéoprotection-v2.1* [ANSSI_PA_72].

En introduisant le concept de lecteur transparent et à l'exception du Proximity Check, la tête de lecture ne participe plus aux mécanismes cryptographiques lors des transactions avec la puce NXP MIFARE® DESFire® et les secrets sont déportés au niveau du contrôleur intelligent (UTL) Synergis[MC] Cloud Link en zone sécurisée. Ce dernier communique directement avec la puce NXP MIFARE® DESFire® sans modification de la part de la tête de lecture, pilotant ainsi les mécanismes d'authentification et de chiffrement. Cette configuration est recommandée par *l'ANSSI guide recommandations sécurisation systèmes contrôle accès physique et vidéoprotection-v2.1* [ANSSI_PA_72]. Le Proximity Check est détaillé dans la section 2.3.1 Utilisation du badge seul.

L'architecture mise en œuvre dans le cadre de l'évaluation CSPN est celle correspondant à la configuration type n°1 : Lecteur Transparent, authentification de bout en bout. Le lecteur ne possède aucune clé cryptographique nécessaire à la lecture de la puce NXP MIFARE® DESFire®. Ces clés sont stockées et sécurisées dans les cartes Secure Access Module (MIFARE® SAM AV3) hébergées sur le contrôleur Synergis[MC] Cloud Link.

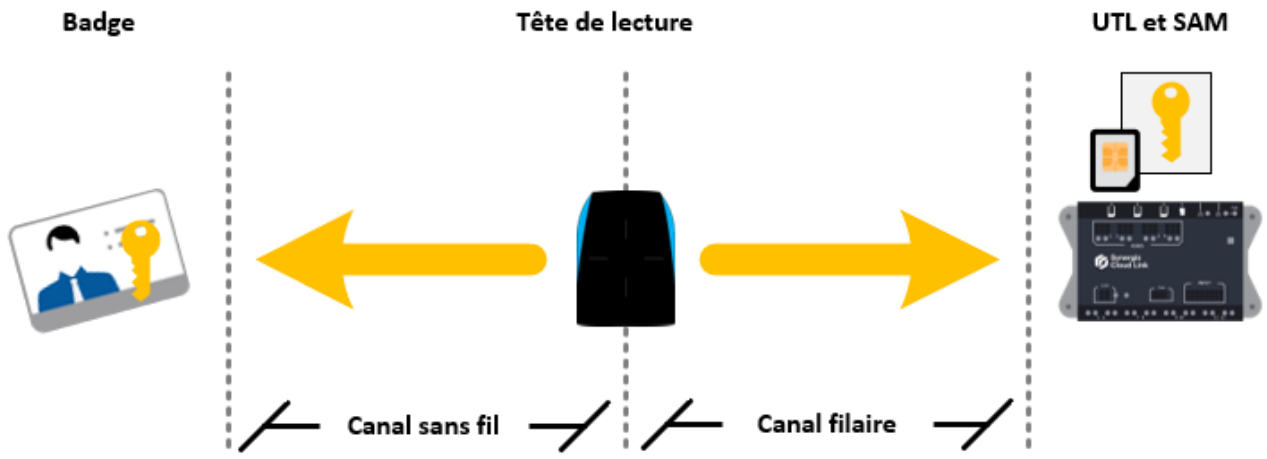

Figure 5 : Configuration type n°1

Dans le cas où une authentification multi facteur est utilisée (usage d'un code PIN par exemple), il est nécessaire de protéger le second facteur échangé entre le dispositif rattaché à la tête de lecture et l'UTL. Pour cela un secret détenu par les deux équipements est nécessaire.

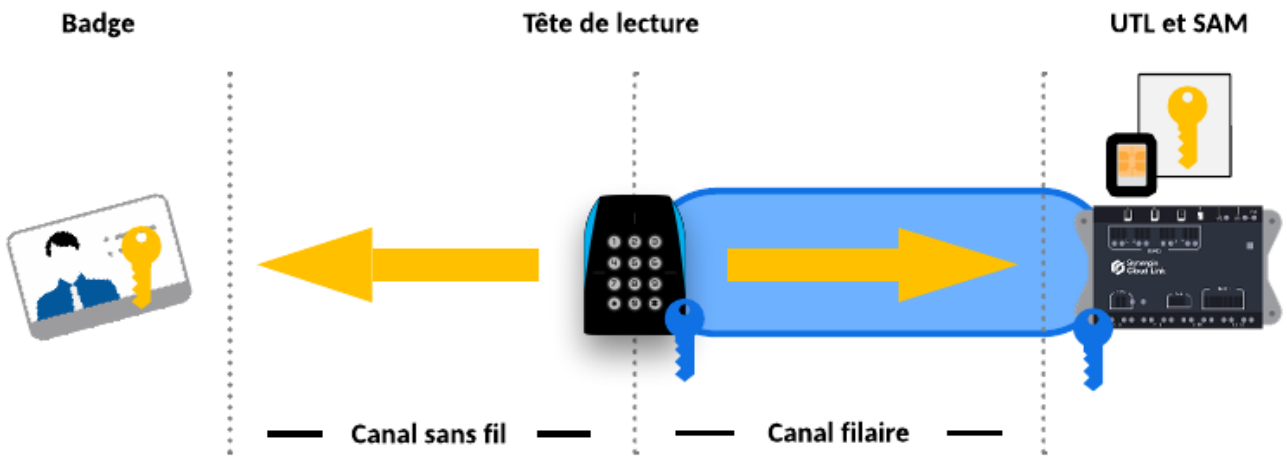

Figure 6 : Configuration type n°1 – cas d'une authentification multi facteur.

Recommandations : R41

2.3 Description de l'utilisation courante du produit

Dans le présent cadre d'évaluation CSPN de la solution, l'utilisation est exclusivement basée sur des badges MIFARE® DESFire® EV2/EV3. Ces badges sont considérés être configurés et prêt à l'emploi. Ledit encodage peut être réalisé par la tâche d'encodage native dans la plateforme Security Center soit par une application tierce. Seul l'identifiant privé contenu dans le fichier de l'application contrôle d'accès est utilisé pour l'authentification auprès du lecteur. Il est vivement conseillé l'usage de la diversification des clés de l'application suivant la norme NXP AN-10922.

Deux usages sont communément envisagés par les titulaires de carte. L'utilisation du badge seul ou bien l'utilisation du badge suivi de la saisie d'un code PIN au sein de la même tête de lecture, cette dernière doit être dotée d'un clavier numérique. Les deux usages sont décrits de manière plus détaillée ci-après.

2.3.1 Utilisation du badge seul

Le titulaire de carte souhaitant accéder à la zone sécurisée, présente son badge adéquatement devant la tête de lecture. Le champ magnétique active la puce du badge et l'identifie comme étant de la famille MIFARE® DESFire®. Après sélection de l'application contrôle d'accès au sein du badge, s'initie alors une phase d'authentification mutuelle pilotée par le contrôleur intelligent (UTL) Synergis[MC] Cloud Link, suivi par la vérification de proximité du badge (Proximity Check) par le lecteur. En fonction de la charte d'encodage du badge, la lecture ou le calcul de son UID entre dans le mécanisme d'authentification. Le contrôleur intelligent (UTL) Synergis[MC] Cloud Link consulte le module SAM disponible afin de lui faire calculer la clé de session propre à cette transaction. Ainsi à aucun instant le contrôleur intelligent (UTL) Synergis[MC] Cloud Link n'a connaissance de la clé maitresse. À la suite du déchiffrement de l'identifiant, le contrôleur intelligent (UTL) Synergis[MC] Cloud Link prendra la décision d'autoriser ou de refuser l'accès en fonction des privilèges du titulaire de carte. L'intégralité des évènements de cette lecture d'identifiant est transmise au Gestionnaire d'accès pour consignation dans les journaux d'activités des entités concernées (porte, secteur, titulaire de carte…). En cas d'impossibilité de communication avec le Gestionnaire d'accès, le contrôleur intelligent (UTL) Synergis[MC] Cloud Link gardera en mémoire ces évènements jusqu'à pouvoir le joindre, et ce dans la limite de ses capacités de rétention d'évènements.

Par ailleurs, il est pertinent de préciser que le contrôleur intelligent (UTL) Synergis[MC] Cloud Link détient la configuration DESFire® qui pilote la lecture de l'identifiant dans l'application du badge. La flexibilité de la solution permet de paramétrer plusieurs configurations DESFire® au sein de la même tête de lecture afin de lui faire lire successivement différentes applications. Il est aussi possible d'assigner des configurations DESFire différentes à chaque lecteur du même contrôleur intelligent (UTL) Synergis[MC] Cloud Link afin d'utiliser des clés de lecture différentes en fonction du niveau de sécurité attendu au sein du site à protéger.

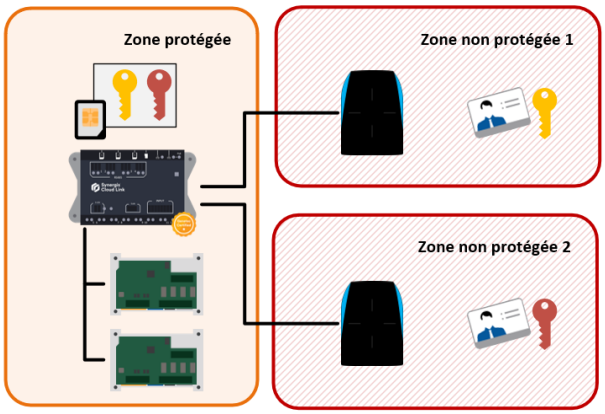

Figure 7 : Différentiation des clés maîtresses selon le niveau de protection attendu des zones

Recommandations : R58

2.3.2 Utilisation du badge puis d'un code PIN

Lorsque la situation le demande, il est possible d'augmenter le niveau de sécurité de l'accès contrôlé. Ceci est réalisable via une tête de lecture dotée d'un clavier numérique. Ainsi l'identification et l'authentification du badge sont réalisées comme décrit dans le précédent paragraphe, à cela vient s'ajouter l'authentification du titulaire de carte via son code PIN.

Ainsi après présentation du badge, le titulaire de carte est invité par un jeu de LED de la tête de lecture, à saisir son code PIN dans un délai imparti. Ce délai peut être paramétré individuellement pour chaque tête de lecture et peut être augmenté dans le cas d'un titulaire de carte identifié comme une personne à mobilité réduite. Dans le cas du match entre l'identifiant badge et du code PIN, le contrôleur intelligent (UTL) Synergis[MC] Cloud Link prendra la décision d'autoriser ou de refuser l'accès en fonction des privilèges du titulaire de carte.

La flexibilité de la plateforme Security Center permet de définir facilement le comporte Badge + Code PIN du lecteur de manière définitive ou de manière dynamique (en fonction d'une période horaire ou sur activation d'un niveau de risque).

Dans les cas où un titulaire de carte est forcé à débloquer une porte, la capacité à déclencher une alarme de manière non évidente peut aider à garantir la sécurité des salariés. Le code PIN de contrainte accordera l'entrée tout en générant un événement « Code PIN de contrainte saisi », cet événement sera utilisé pour déclencher des actions/alarme sur le système GAC.

2.4 Description des dépendances logicielles et matérielles

2.4.1 Dépendance logicielle

Pour que la solution évaluée fonctionne de manière optimale; il est important de respecter la configuration logicielle minimale requise (voir [GEN_SC_CSR] *Guide de la configuration requise pour Security Center*).

Parmi les dépendances, la solution évaluée nécessite :

- Système d'exploitation,
- Moteur de base de données (Microsoft SQL Express est fourni avec l'installateur Security Center),
- Navigateur web.

2.4.2 Dépendance matérielle

La solution évaluée repose sur 2 dépendances matérielles que sont le Badge NXP MIFARE DESFire EV2/EV3 ainsi que le NXP MIFARE SAM AV3.

2.5 Description des bibliothèques tierces

Voir dossier COTS, fourni séparément.

2.6 Description des utilisateurs du GAC

Il est important d'identifier les différents utilisateurs et leurs rôles associés. Les acteurs susceptibles d'intervenir sur le système peuvent être classés en différents rôles. Les paragraphes suivants décrivent chacun de ces acteurs. Selon la situation, plusieurs rôles peuvent être assurés par les mêmes individus.

Recommandations : R8, R9

A1 – Titulaire de carte

Une entité *titulaire de cartes* représente un individu autorisé à pénétrer et à quitter des secteurs sécurisés en fonction de ses identifiants (généralement des cartes d'accès), et dont les activités peuvent être surveillées. Ils correspondent au « Qui » dans le cadre d'une règle d'accès et peuvent ainsi être soit un collaborateur, un employé ou un prestataire.

La fiche de profil du titulaire de carte peut se voir définir une date d'activation, une date d'expiration ainsi que des attributs tels que l'escorte visiteur, être soumis à antiretour, etc.

Recommandations : R68, R69, R70, R72, R73, R74

A2 – Visiteur

Une entité *visiteur* est un individu au même titre qu'un titulaire de carte, toutefois ce dernier peut se voir attribuer l'obligation d'être escorté par un titulaire de carte disposant de ce privilège. Il est ainsi possible de renforcer la sécurité de certains secteurs en obligeant l'accompagnement des visiteurs par un hôte désigné. Un hôte doit présenter son identifiant après le visiteur dans un certain délai pour que l'accès soit accordé à l'ensemble des personnes.

Recommandations : R71

A3 – Agent d'exploitation

Un Agent d'exploitation est une entité *utilisateur* de la plateforme Security Center avec un jeu de privilège lui permettant d'accéder aux fonctions d'Opération et d'Investigation de l'application client Security Desk ou Genetec[MC] Web App afin d'assurer ces missions. Le jeu de privilèges peut être confié directement au profil concerné ou hérité d'un groupe d'utilisateur. Ces tâches sont souvent composées de :

- Gestion des Titulaires de Carte et/ou des privilèges d'accès
- Surveillance et/ou Investigation de l'activité du site
- Enrôlement / Encodage d'identifiant MIFARE® DESFire®

A4 – Agent technique

Un Agent technique est une entité *utilisateur* de la plateforme Security Center avec un jeu de privilèges lui permettant d'accéder potentiellement aux applications Security Desk et Config Tool. L'objectif de ce type d'utilisateur est de déployer, paramétrer, dépanner et maintenir le système. Il aura de ce fait aussi accès aux équipements du contrôle d'accès tels que les lecteurs, les contrôleurs etc. Parmi les agents techniques nous pouvons catégoriser les différentes classes suivantes :

a) Intégrateur

Cet acteur réceptionne les équipements fournis par Genetec, et les met en service. Il est responsable de l'installation physique des composantes matérielles du système (serveurs, UTLs, lecteurs de badge, etc.) et de la configuration initiale des entités logiques (portes, secteurs sécurisés, horaires, règles d'accès, etc.).

Il a pour mission d'effectuer le choix des solutions pour les accessoires matériel (PNG, lecteurs, cartes).

Il est formé par Genetec afin d'être labélisé.

Il est temporairement Administrateur avant de livrer le système au client final.

b) Installateur

L'acteur a délégation de l'intégrateur pour l'installation des équipements dans les locaux du client final.

c) Chargé de Maintenance

Cet acteur se voit confier les tâches dédiées à la maintenance et au dépannage des composantes matérielles du système. L'agent d'exploitation lui affecte typiquement une carte avec des accès restreints pour la durée de la maintenance. Le chargé de maintenance règle les problèmes physiques (tels que les problèmes de portes, d'UTL, etc…).

Il n'y a pas obligatoirement de lien avec l'Intégrateur.

Recommandations : R80, R81, R82, R83, R84

A5 – Administrateur

Un Administrateur est une entité *utilisateur* de la plateforme Security Center avec un jeu de privilèges souvent élevés, lui permettant d'accéder potentiellement aux applications Security Desk et Config Tool. Cet acteur est chargé des tâches de création et configuration des entités requises pour modéliser le système. Il convient de différentier :

- Les administrateurs applicatifs, qui effectuent les opérations de maintenance sur les applications,
- Les administrateurs techniques, qui effectuent les opérations de maintenance sur les systèmes d'exploitation.

Recommandations : R75, R77, R78, R78-, R79

A6 – Approvisionnement

L'UTL est par définition une Appliance. Celle-ci est approvisionnée par un réseau d'utilisateur (livreur, revendeur). Ces utilisateurs n'ont théoriquement pas accès physiquement à l'UTL sans briser le scellé de l'emballage contenant l'Appliance. Il appartient aux utilisateurs de type Agent Technique de vérifier l'intégrité physique des emballages avant tout déploiement.

2.7 Description du périmètre de l'évaluation

Tableau récapitulatif de l'évaluation

L'évaluation concerne les éléments du système de contrôle d'accès physique listés dans le tableau ci-dessous :

Catégorie du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE)	
			Supposé de confiance	Est un attaquant potentiel
GAC	Système d'exploitation[1] (version en vigueur Microsoft Windows selon [GEN_SC_CSR])		X	
	Applicatifs (Voir § 1.2 Identification du produit)	X		
	Fonctions cryptographiques (Voir [GEN_CRYPTO])	X		
	Base de données[1] (version en vigueur SQL Server selon [GEN_SC_CSR])		X	
UTL	Système d'exploitation	X		
	Applicatifs (Voir § 1.2 Identification du produit)	X		
	Fonctions cryptographiques (Voir [GEN_CRYPTO])	X		
	Module entrées – sorties (Voir § 8.1.2 Modules d'entrées-sorties)	X		
	SAM AV3		X	
Têtes de lecture	Lecteurs simples (Voir § 8.1.1 Têtes de lecture)	X		
	Lecteurs / clavier (Voir § 8.1.1 Têtes de lecture)	X		
Badges DESFire EV2/EV3			X	

Le périmètre de l'évaluation est représenté au chapitre 2.1.2 Schéma d'architecture simplifié de la solution, en Figure 2.

Note 1 : Les mises à jour à caractère sécuritaire doivent être appliquées.

Schéma de composition et d'implantation des équipements GAC et terrain

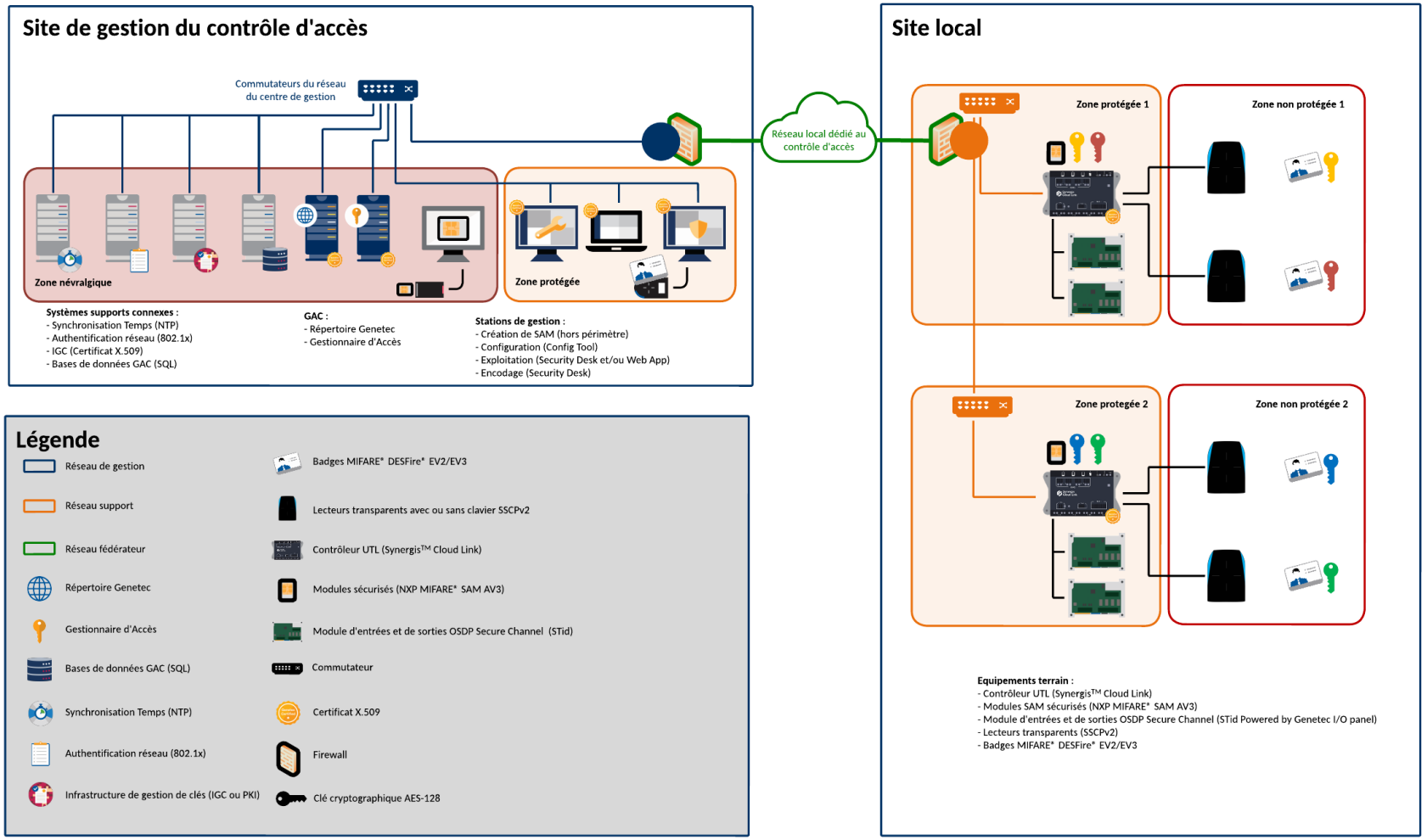

Figure 8 : Schéma de composition et d'implantation des équipements

3 Hypothèses sur l'environnement du produit

3.1 Hypothèses sur l'environnement physique

H1 – Installation physique

- L'utilisateur final de la solution s'assure que l'installation physique des équipements de la solution de contrôle d'accès est conforme aux préconisations d'installation décrites dans le guide d'installation [GEN_SCL_INS] ainsi qu'aux guides des manufacturiers de lecteurs.
- Les règles de l'art sont respectées pour les liaisons filaires entre les différents équipements terrain de la solution. Il est possible de citer, de manière non exhaustive :
    - Le passage de câble en zone protégée
    - L'usage de protections mécaniques pour lesdits passages de câble
    - L'identification explicite des liaisons
    - Le respect des distances (longueurs maximales des liaisons, les distances minimales entre les liaisons de différentes natures …)

H2 – Locaux sécurisés

- Les locaux qui hébergent les serveurs du GAC et les UTLs sont sous accès contrôlés et strictement limités aux personnels habilités.
    - Serveurs : Il est supposé que le ou les serveurs sont installés dans des locaux sécurisés physiquement et logiquement (zone névralgique) afin de ne laisser accès aux ressources qu'aux personnes habilitées et formées à l'administration de la solution.
    - Stations de travail : les postes d'exploitation de la solution sont supposés être localisés dans des lieux sécurisés dont l'accès est protégé et restreint aux seuls utilisateurs mandatés et formés à l'usage de la solution.
    - L'UTL *Synergis[MC] Cloud Link* et les accessoires connexes : sont installés en zone sécurisée à l'intérieur d'armoires métalliques verrouillables et dotés de capteurs d'ouverture et d'arrachement permettant d'identifier une autoprotection du coffret, en conformité au guide d'installation [GEN_SCL_INS], par des personnes formées et certifiées par Genetec. Les UTL sont elles-mêmes protégées dans une enveloppe physique ne laissant aucun accès à l'électronique.

3.2 Hypothèses sur les intervenants

H3 – Confiance envers le personnel

- L'équipement est administré et opéré par des personnels non hostiles, formés et responsables identifiés au sein de l'entité (client final). Nous pouvons citer ici des Administrateurs, des Agents techniques ainsi que des Agents d'exploitation. (Voir § 2.6 Description des utilisateurs du GAC).
- L'exploitation des journaux d'évènements du système sont régulièrement consulté par les opérateurs et les administrateurs.
- La mise à la clé des cartes SAM, des lecteurs SSCPv2, des modules entrées-sorties OSDPv2 et des badges est effectuée en protégeant les secrets, dans un environnement sécurisé; maitrisé par du personnel de confiance. Pour cela suivre le guide de déploiement [GEN_ANSSI_CSPN].

3.3 Hypothèses sur l'environnement technique

H4 – Réseaux sécurisés

- Les réseaux de communication TCP/IP sont réalisés, maintenus et gérés par le client selon les règles de sécurité en vigueur. Au travers d'une analyse de risque ces règles sont déterminées en adéquation avec l'exposition aux attaques du réseau.
- Les mises à jour sécuritaires sont appliquées régulièrement.
- L'accès au réseau est authentifié cryptographiquement par une solution reposant sur le protocole 802.1x.
- Le cloisonnement logique au sein d'un réseau support est réalisé en associant les UTL aux zones par niveau de protection.
- La désactivation des ports non utilisés sur les commutateurs réseau est réalisée.
- Les flux sont filtrés entre les différents réseaux (support, de gestion).

H5 – Bases de données sécurisées

- Les bases de données utilisées par le GAC sont réalisées, maintenues et gérées par le client selon les règles de sécurité en vigueur.
- Les mises à jour sécuritaires sont appliquées régulièrement.
- Les données sont protégées en transit et au repos selon les recommandations du *Guide de renforcement de Security Center* [GEN_SC_HG].
- Les bases de données sont réputées saines et fiables.

H6 – Badges sécurisés NXP MIFARE® DESFire®

- Le badge assure la confidentialité et l'intégrité de ses éléments secrets. Ils ont déjà été évalués a minima critères communs EAL5+ et sont conformes aux niveaux de sûreté ANSSI [ANSSI_PA_72].
- Les éléments secrets qui garantissent l'authenticité des badges ne doivent pas être exportés hors du périmètre de contrôle du client final.
- Les sources d'aléas utilisées par les badges sécurisés sont supposées de confiance et conformes aux exigences ANSSI [ANSSI_PA_079] et [ANSSI_PG_083].

H7 – Cartes NXP MIFARE® SAM AV3

- Les cartes MIFARE® SAM AV3 assurent la confidentialité et l'intégrité de ses éléments secrets. Elles ont déjà été évaluées a minima critères communs EAL6+
- Les éléments secrets qui garantissent l'authenticité des badges ne doivent pas être exportés hors du périmètre de contrôle du client final.
- Les sources d'aléas utilisées par les badges sécurisés sont supposées de confiance et conformes aux exigences ANSSI [ANSSI_PA_079] et [ANSSI_PG_083].

H8 – Mise en oeuvre d'une source de temps NTP

- L'ensemble des équipements, des stations de travail, des serveurs, des UTLs sont synchronisés par la même source de temps NTP.
- Cette source de temps est réputée fiable et de confiance.

H9 – Sécurité des postes clients et serveurs

- Les postes clients et les serveurs du GAC sont installés et configurés selon les recommandations des *Guide d'installation et de mise à jour de Security Center* [GEN_SC_INS] et *Guide de renforcement de Security Center* [GEN_SC_HG]. Ils sont exempts de logiciels malveillants, sont protégés par un antivirus éprouvé et les correctifs de sécurités sont appliqués et sont à jour.

H10 – Sécurité des secrets stockés dans la puce centrale

- Les fusibles de la puce centrale sont en lecture seule et les valeurs ne peuvent pas être modifiées.
- Les clés sont protégées en intégrité et confidentialité.
- La génération de clé est conforme aux exigences ANSSI [ANSSI_PA_079] et [ANSSI_PG_083].

H11 – Périphériques sériels

- Les lecteurs de carte et les modules d'entrées-sorties sont de confiance et conformes par rapport aux recommandations de l'ANSSI [ANSSI_PA_72]. Voir en annexe du document Mécanismes cryptographiques [GEN_CRYPTO].

H12 – Modules désactivés

- La désactivation des modules consignés comme devant l'être par la présente cible de sécurité est assurée par l'utilisateur.

H13 – Serveurs d'authentification

- L'utilisateur s'assure que les serveurs connexes hors de la cible d'évaluation utilisés pour authentifier les utilisateurs de la solution sont réputés fiables et configurés correctement.
- L'utilisateur s'assure que les serveurs connexes hors de la cible d'évaluation utilisés pour authentifier les équipements réseaux sont réputés fiables et configurés correctement.

H14 – Documentation d'administration et d'opération

- L'utilisateur se conforme aux préconisations de déploiement et d'usage opérationnel fournis par le constructeur au travers des guides et notices mis à disposition.

4 Biens sensibles

4.1 Inventaire des biens sensibles

Ce tableau liste les biens sensibles et leur besoin de protection (**D**isponibilité**, C**onfidentialité, **I**ntégrité, **A**uthenticité) :

Bien sensible	D	C	I	A
B1 – Les droits d'accès des titulaires de cartes		✔	✔	
B2 – Configuration système			✔	✔
B3 – Échanges entre les UTL et le GAC		✔	✔	✔
B4 – Échanges entre la tête de lecture et l'UTL		✔	✔	✔
B5 – Mécanisme d'authentification des utilisateurs			✔	✔
B6 – Secrets de connexion		✔	✔	✔
B7 – Micrologiciel (*firmware*)			✔	✔
B8 – Logiciel(s)			✔	✔
B9 – Gestion des privilèges utilisateurs			✔	
B10 – Fonction de journalisation	✔			
B11 – Journaux d'évènements et historique de configuration			✔	✔

5 Description des menaces

5.1 Interfaces d'attaque

Cette section liste les attaques possibles tout au long de la chaine du système de contrôle d'accès. Le schéma ci-dessous illustre chaque point d'accès d'un attaquant.

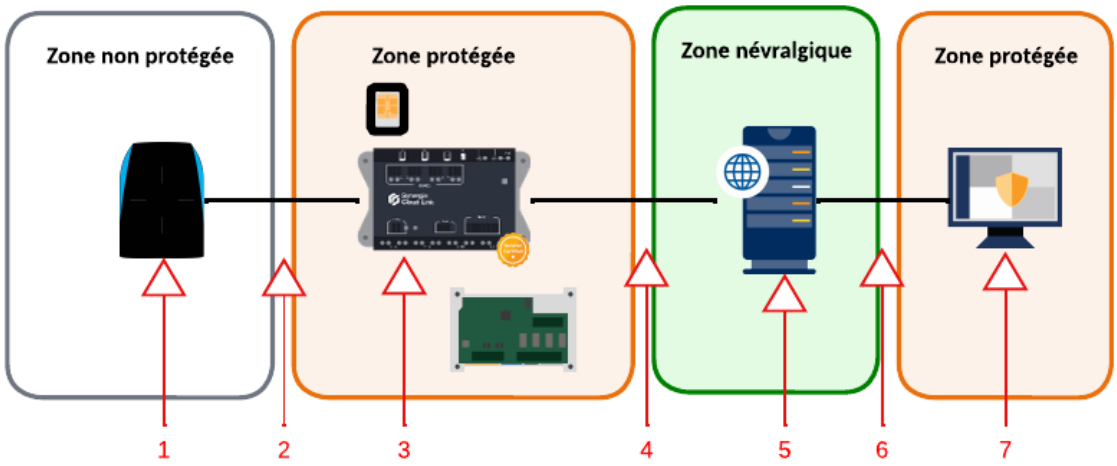

Figure 9 : Schéma simplifié de la chaine de la solution contrôle d'accès

1- **(I1)** Attaquant situé dans une zone non-protégée, ayant accès uniquement à la tête de lecture
2- **(I2)** Attaquant ayant accès la liaison RS-485 entre la tête de lecture et l'UTL
3- **(I3)** Attaquant situé dans la zone protégée, ayant accès physique à l'UTL et/ou aux modules de portes
4- **(I4)** Attaquant ayant accès au réseau support (entre le GAC et l'UTL)
5- **(I5)** Attaquant situé dans la zone névralgique, ayant accès au GAC
6- **(I6)** Attaquant ayant accès au réseau fédérateur (entre le GAC et la station d'exploitation)
7- **(I7)** Attaquant situé dans la zone protégée, ayant accès à l'application d'opération ou de configuration

5.2 Menaces

M1 - Déni de service

L'attaquant parvient à effectuer un déni de service sur la TOE en effectuant une action imprévue ou en exploitant une vulnérabilité.

M2 - Corruption du micrologiciel (*firmware*)

L'attaquant parvient à injecter et faire exécuter un micrologiciel (*firmware*) corrompu sur la TOE, ou y injecter du code et l'exécuter.

L'attaquant peut également réussir à substituer une mise à jour corrompue à une mise à jour légitime. Un utilisateur pourra alors tenter d'installer cette mise à jour dans la TOE par des moyens légitimes.

M3 - Corruption du logiciel

L'attaquant parvient à modifier, de manière temporaire ou permanente le logiciel du GAC, ou bien l'attaquant réussit à y exécuter du code illégitime.

M4- Vol d'identifiants

L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.

M5 - Contournement de l'authentification

L'attaquant parvient à s'authentifier au GAC / à l'UTL sans avoir l'identifiant et le mot de passe (secrets de connexion).

L'attaquant contourne les mécanismes de sécurité pour être considéré comme un titulaire de badge légitime sans avoir de badge authentique.

M6 - Contournement de la politique de droits

L'attaquant parvient à obtenir des droits qui ne lui sont pas normalement dévolus. L'attaquant peut également tenter d'installer une version légitime du micrologiciel (firmware) sans en avoir le droit.

M7 - Corruption des journaux d'évènements

L'attaquant parvient à supprimer ou modifier une entrée dans les journaux d'évènements locaux sans y avoir été autorisé par la politique de droits.

L'attaquant parvient à modifier une entrée de journal distant émise par la TOE sans que le destinataire ne puisse s'en rendre compte.

L'attaquant parvient à supprimer une émission de journalisation distante sans que le destinataire ne puisse s'en rendre compte.

M8 – Altération / Compromission des flux

L'attaquant parvient à modifier des échanges entre la TOE et un composant externe ou interne à celle-ci sans que cela ne soit détecté.

Pour les flux requérant la confidentialité, l'attaquant parvient à récupérer des informations en interceptant des échanges entre la TOE et un composant externe ou interne à celle-ci.

M9 – Corruption / Compromission de données au repos

L'attaquant parvient à modifier des données, sans en avoir le droit, en exploitant une faille de la TOE.

L'attaquant parvient à exploiter une faille dans la TOE pour accéder à des informations auxquelles il ne devrait pas avoir accès.

6 Description des fonctions du produit

6.1 Fonctions métiers

FM1 - Gestion des règles d'accès

Security Center repose sur le concept de règles d'accès pour la gestion des privilèges d'accès. C'est une entité qui définit une liste de titulaires de cartes auxquels un accès est accordé ou refusé en fonction d'un horaire. Les règles d'accès peuvent être appliquées aux secteurs sécurisés et aux portes d'entrée et de sortie, ou aux secteurs de détection d'intrusion pour l'armement et le désarmement.

FM2 - Notification des événements et des alarmes aux l'utilisateurs du système

En tant qu'utilisateur du système vous pouvez surveiller les événements en temps réel, tels que ceux liés aux accès ou aux personnes, et y répondre à l'aide de la tâche *Surveillance* du Security Desk. Lors de la surveillance des événements, vous surveillez les entités qui déclenchent ces événements.

La gestion unifiée des alarmes permet d'escalader les événements de votre système de sécurité pour déclencher automatiquement des alarmes, ce qui permet aux opérateurs de visualiser les alarmes en temps réel et de réagir rapidement et efficacement.

Les alarmes sont affichées dans la tâche de *Surveillance des alarmes* par ordre de priorité (celle-ci est évaluée à chaque fois qu'une nouvelle alarme est reçue). L'alarme la plus prioritaire est affichée dans la tuile n° 1, suivie de la deuxième dans la tuile n° 2, et ainsi de suite. Lorsque deux alarmes ont la même valeur de priorité, la priorité est donnée à la plus récente. Dans Security Center, vous pouvez classer la file d'attente des alarmes de la plus ancienne à la plus récente ou de la plus récente à la plus ancienne.

FM3 - Pilotages des accès

Pour déverrouiller une porte ou modifier les horaires de verrouillage et de déverrouillage, vous pouvez utiliser le widget Porte pour contrôler l'accès aux portes. Le widget *porte* est activé lorsqu'une entité *porte* est affichée dans la tuile sélectionnée ou depuis la tâche Cartes.

FM4 - Interface de paramétrage

Config Tool est l'application d'administration utilisée pour gérer tous les utilisateurs du Security Center, effectuer la configuration de la sécurité et configurer toutes les entités du Security Center telles que les zones, les portes, les horaires, les titulaires de cartes et les dispositifs matériels. Config Tool fournit également plusieurs rapports permettant aux administrateurs et aux utilisateurs autorisés de visualiser les événements historiques basés sur l'activité de l'entité, les pistes d'audit qui montrent l'historique des modifications apportées par l'utilisateur à une entité, l'activité de santé, les statistiques et l'inventaire du matériel.

FM5 – Historiques d'Activité et Historiques de Configuration

Security Center comprend deux rapports permettant de suivre les activités des utilisateurs et les changements de configuration. Il s'agit respectivement des rapports d'Historiques d'activité et d'Historique de configuration, qui sont générés par les tâches du même nom dans Security Desk ou Config Tool. L'accès aux rapports d'audit et d'activité est limité à l'aide d'un privilège qui peut être activé ou désactivé pour tout utilisateur du Security Center.

Historiques d'Activité

L'Historiques d'Activité est un rapport qui montre les actions effectuées par n'importe quel utilisateur sur le système. Il peut s'agir d'acquitter des alarmes, de générer des rapports, de se connecter, de se déconnecter, imprimer un badge, encoder une carte, définir un mode de lecteur ...

Les tentatives infructueuses sont consignées dans le rapport d'activité, par exemple les mauvaises combinaisons de nom d'utilisateur et de mot de passe. L'utilisateur et le poste de travail source sont indiqués, ainsi que la raison de l'échec de la connexion.

Historiques de Configuration

Le rapport sur l'historique de Configuration permet de suivre les modifications apportées à la configuration du système, de savoir qui les a effectuées, à quel moment et sur quels paramètres de l'entité (valeurs avant et après). Le rapport est utile si vous constatez que les propriétés d'une entité ont changé et que vous devez déterminer qui a effectué ces changements et quand. Si vous demandez une mise à jour pour une entité (par exemple, les privilèges d'un utilisateur), vous pouvez vérifier si les changements ont été effectués à partir de Config Tool. Les pistes d'audit enregistrent les changements de configuration des bases de données de rôles.

FM6 – Port de découverte des UTL

Un port de découverte est utilisé par le système pour répertorier les UTL lors de leur enrôlement sur le GAC ainsi qu'à signaler leur présence. Ce port de découverte est personnalisable par Gestionnaire d'Accès.

6.2 Fonctions de sécurité

FS1 – Protection des communications IP

Communications avec le GAC

Toutes les communications au GAC (applications clients, Gestionnaire d'accès, serveurs GAC) se font sur des canaux sécurisés par TLS. Au niveau de l'authentification, voir FS12 – Authentification des usagers au GAC.

Communications avec l'UTL

La protection des communications IP s'appuie sur le protocole Transport Layer Security (TLS) qui permet de garantir intégrité et confidentialité des communications entre deux entités sur un réseau. Une authentification mutuelle est réalisée entre le GAC et l'UTL. Un mécanisme anti brute-force est en place sur l'authentification client avec délais exponentiels.

Configuration

L'UTL supporte les versions TLS v1.2 et TLS v1.3, avec suites ciphers sélectionnées. Toute demande de connexion selon une version antérieure à 1.2 sera rejetée. Les configurations respectent les recommandations décrites dans le document [ANSSI_TLS].

Voir aussi ces sections du document Mécanismes cryptographiques [GEN_CRYPTO] :

- *UTL - Protocoles TLS et suites cryptographiques acceptées*
- *Certificats de l'UTL*
- *Communications entre le GAC et l'UTL*
- *Communication entre les UTLs (peer-to-peer)*

FS2 – Contrôle des données entrantes de l'UTL

Interfaces Ethernet

L'UTL restreint au strict minimum les services exposés. Voir *Contrôle des données entrantes – UTL*, de Mécanismes cryptographiques [GEN_CRYPTO].

Interfaces RS-485

Les interfaces RS-485 sont utilisées pour connecter l'UTL aux périphériques sériels, tels les lecteurs de badges et les modules d'entrées-sorties.

Le canal peut être configuré en mode chiffré + signé, suivant les spécificités du protocole SSCPv2, pour le déploiement des têtes de lecture avec/sans clavier; et suivant les spécificités du protocole OSDPv2 pour les modules d'entrées-sorties permettant la gestion de l'environnement des portes.

Dans les deux cas, le matériel qui est la source des données (badge ou lecteur) doit être authentifié à l'UTL; dans le cas contraire les données sont rejetées.

Dans le cas d'une interface non attribuée ni à un lecteur ni à une porte, aucune écoute n'est appliquée (pas de polling fait par l'UTL).

Interface SD

L'interface SD est désactivée de manière permanente sur l'UTL Synergis[MC] Cloud Link.

FS3 – Mises à jour sécurisées de l'UTL

Les paquets de mise à jour du micrologiciel de l'UTL sont protégés en intégrité. La vérification de l'intégrité assure qu'aucun code étranger ne s'exécute sur l'UTL.

La rétrogradation du micrologiciel (*firmware downgrade*) n'est pas possible.

Voir section *Mise à jour du micrologiciel de l'UTL* de [GEN_CRYPTO].

FS4 – Durcissement du système d'exploitation de l'UTL

Différentes mesures aident à réduire la surface d'attaque ou l'impact :

- L'application sur l'UTL s'exécute avec un compte usager aux privilèges limités;
- L'image contient le minimum de composants;
- L'application réside dans une partition en lecture seule (*read-only*), dont la signature est validée. Voir FS7 – Amorce sécurisée de l'UTL (Secure boot).

FS5 – Utilisation de la technologie *MIFARE® DESFire®*

Les communications avec les badges se font avec des lecteurs en mode transparent en utilisant le protocole *MIFARE® DESFire® EV2/EV3*, ce qui protège les secrets cryptographiques et empêche de cloner les badges.

Voir *Communication entre le badge et l'UTL* dans [GEN_CRYPTO].

L'UTL utilise des cartes NXP SAM AV3 pour stocker les secrets cryptographiques impliqués dans les communications avec les badges. L'isolation des secrets dans les cartes SAM amovibles facilite la gestion de la fin de vie des UTLs.

Voir *Communication entre l'UTL et la SAM* dans [GEN_CRYPTO].

FS6 – Protections des communications sérielles avec l'UTL

Ces mécanismes de sécurité sont en supplément à l'hypothèse *H1 – Installation physique*, au sujet des fils RS-485 non accessibles à partir des zones non protégées. Les interfaces électriques des modules d'entrées-sorties ne peuvent être protégées que physiquement.

Sécurisation du lien entre périphérique sériel et UTL

La communication entre les périphériques sériels et l'UTL est protégée en confidentialité. Voir la section *Sécurisation de la communication avec les périphériques sériels* dans [GEN_CRYPTO].

L'UTL assure une authentification mutuelle avec le périphérique sériel, de même qu'une protection en confidentialité et intégrité. Les clés maîtresses sont programmées de manière sécurisée lors de la phase de mise en service (voir § Mise à la clé de la section H3 – Confiance envers le personnel).

Stockage des biens

Pour les lecteurs STid, Genetec recommande de configurer les lecteurs de sorte que les clés ne soient pas stockées en mémoire persistante (voir [GEN_ANSSI_CSPN]). Les lecteurs *STid* sont munis d'un accéléromètre pouvant servir à effacer les clés lors de l'arrachement.

FS7 – Amorce sécurisée de l'UTL (*Secure boot*)

Une série de validations assurent que l'UTL exécute seulement des micrologiciels signés par Genetec. Voir *Amorce sécurisée* dans [GEN_CRYPTO].

FS8 – Chiffrement de l'exportation des configurations de l'UTL

Les configurations de l'UTL peuvent être exportées pour ensuite être chargées sur une unité de remplacement. Des mécanismes cryptographiques sont en place pour protéger les données en intégrité et en confidentialité, basé sur un mot de passe spécifié par l'usager. Voir *Chiffrement de l'exportation des configurations* dans [GEN_CRYPTO].

FS9 – Forcer le changement du mot de passe par défaut de l'UTL

Le portail web de l'UTL force l'usager à changer le mot de passe par défaut lors de la première utilisation. Autrement, l'UTL est inutilisable.

L'UTL accepte seulement les mots de passe de complexité élevée (*password strength meter*).

Il n'existe aucune façon de réinitialiser le mot de passe sans aussi effacer les données utilisateur.

Genetec recommande de choisir des mots de passe différents et complexes pour chaque UTL [GEN_SC_HG]. Il est attendu que l'entropie contenue dans ces mots de passes soit conforme aux politiques de sécurité du client final.

FS10 – Protection de l'accès administrateur au système d'exploitation de l'UTL (*root*)

Le mot de passe de l'administrateur du système d'exploitation de l'UTL est protégé. Voir *Protection du mot de passe de l'administrateur du système d'exploitation (root)* dans [GEN_CRYPTO].

FS11 - Chiffrement des données utilisateur sur l'UTL

La partition utilisateur de l'UTL est chiffrée par la couche matérielle par une clé unique dérivée d'une clé aléatoire gravée lors de la production dans les fusibles de la puce centrale.

Les données ne sont lisibles par aucun autre système que celui de l'UTL. Ceci protège les données contre une attaque où la puce mémoire serait répliquée ou arrachée, puis liée à un autre système. L'hypothèse *H2 – Locaux sécurisés* implique que l'UTL est protégé physiquement. Le chiffrement des données utilisateur est présent dans une approche de défense en profondeur.

Voir les détails dans la section *Chiffrement des données utilisateur* de [GEN_CRYPTO].

FS12 – Authentification des usagers au GAC

Toutes les communications au GAC (applications clients, Gestionnaire d'accès, serveurs GAC) se font sur des canaux sécurisés par TLS.

L'authentification des usagers du GAC est réalisée de deux façons.

La première repose sur l'utilisation d'un identifiant et d'un mot de passe entrés dans l'application client et envoyés au GAC sur le canal TLS.

La deuxième solution repose sur un fournisseur d'identité de confiance, dans quel cas le fournisseur d'identité peut demander différents types d'identifiants (mots de passe, jetons de sécurité, vérifications biométriques, etc.) pour créer une protection multicouche contre les accès illicites. Également appelé authentification à plusieurs facteurs. Voir *Communications avec le GAC* dans [GEN_CRYPTO].

FS13 – Gestion des privilèges des usagers du GAC

Le GAC offre un mécanisme de gestion de privilèges permettant de définir les opérations permises à chaque usager. De plus, le mécanisme de partitions permet de segmenter le système et configurer quel usager aura accès à quelle partie. Voir [GEN_SC_ADMIN].

FS14 – Protection des bases de données du GAC

Les communications avec la base de données sont chiffrées. Voir *À propos du chiffrement des communications entre les bases de données et les services Genetec[MC]* dans le *Guide de renforcement de Security Center* [GEN_SC_HG].

FS15 – Protection contre les attaques par relais

L'interface de l'UTL permet à l'administrateur de définir les variables seuils pour l'authentification des badges (seuil *Proximity Check* en µs). Si le délai est dépassé, la communication au badge est interrompue, l'accès est refusé et une entrée de journalisation est créée.

FS16 – Logiciel du GAC intègre et authentique

Genetec publie les condensats des fichiers d'installation du GAC, permettant la validation de l'intégrité et de l'authenticité de l'installation et des mises à jour du logiciel du GAC.

Les binaires du logiciel du GAC sont signés par Genetec avec un certificat émis par une autorité de certification (Certificate Authority).

FS17 – Protection en disponibilité de la fonction de journalisation

Les évènements sont transférés des UTLs au GAC en direct, pour stockage en base de données. Lors de perte de connexion temporaire, les UTLs accumulent en local les évènements, transmis au GAC sur reconnexion. Les évènements sont horodatés. L'horloge du GAC et des UTLs sont synchronisées.

7 Matrices de couverture

7.1 Menaces et biens sensibles

	B1 – Droits d'accès des titulaires de cartes	B2 – Configuration système	B3 – Échanges entre les UTL et le GAC	B4 – Échanges entre la tête de lecture et l'UTL	B5 – Mécanisme d'authentification des utilisateurs	B6 – Secrets de connexion	B7 – Micrologiciel (firmware)	B8 – Logiciel(s)	B9 – Gestion des privilèges utilisateurs	B10 – Fonction de journalisation	B11 – Journaux d'évènements
M1 – Déni de service										**D**	
M2 – Corruption du micrologiciel (firmware)							**I A**				
M3 – Corruption du logiciel								**I A**			
M4 – Vol d'identifiants						**C I**					
M5 – Contournement de l'authentification					**I A**	**I A**					
M6 – Contournement de la politique de droits									**I**		
M7 – Corruption des journaux d'évènements											**I A**
M8 – Altération / Compromission des flux			**C I A**	**C I A**							
M9 – Corruption / Compromission de données au repos	**C I**	**I A**				**I A**					

7.2 Fonctions de sécurité

		M1 Déni de service	M2 Corruption du micrologiciel (firmware)	M3 Corruption du logiciel	M4 Vol d'identifiants	M5 Contournement de l'authentification	M6 Contournement de la politique de droits	M7 Corruption des journaux d'évènements	M8 Altération/ Compromission des flux	M9 Corruption/Compromission de données au repos
FS1	Protection des communications IP			✔	✔	✔		✔	✔	
FS2	Contrôle des données entrantes de l'UTL		✔							✔
FS3	Mises à jour sécurisées de l'UTL		✔							
FS4	Durcissement du système d'exploitation de l'UTL		✔			✔		✔		
FS5	Utilisation de la technologie MIFARE® DESFire®				✔				✔	
FS6	Protections des communications sérielles avec l'UTL								✔	
FS7	Amorce sécurisée de l'UTL (Secure boot)		✔							
FS8	Chiffrement de l'exportation des configurations de l'UTL									✔
FS9	Forcer le changement du mot de passe par défaut de l'UTL					✔				
FS10	Protection de l'accès administrateur au système d'exploitation de l'UTL (root)		✔					✔		✔
FS11	Chiffrement des données utilisateur sur UTL									✔
FS12	Authentification des usagers au GAC				✔					
FS13	Gestion des privilèges des usagers du GAC						✔			
FS14	Protection des bases de données du GAC				✔			✔		✔
FS15	Protection contre les attaques par relais					✔				
FS16	GAC intègre et authentique			✔						
FS17	Protection en disponibilité de la fonction de journalisation	✔								

8 Annexes

8.1 Tableau de références des équipements

8.1.1 Têtes de lecture

La solution Synergis[MC] Cloud Link est compatible avec l'ensemble des lecteurs SSCP®v2 supportant le mode transparent. Plus spécifiquement, les références ci-dessous ont été présentées lors de l'évaluation CSPN.

Manufacturier	Référence	Description	Protocole	Micrologiciel
STid	ARCT-W33-APH5-7ADx 	Lecteur format standard	SSCP V2	22
STid	ARC-W33-APH5-7ADx 	Lecteur format standard	SSCP V2	21
STid	ARC1-W33-yPH5-7ADx 	Lecteur format étroit	SSCP V2	22
STid	ARC-W33-BPH5-7ADx 	Lecteur / clavier format standard	SSCP V2	21

La mention :

- x sur les références des lecteurs STid correspond à la couleur de la coque de la tête de lecture. La couleur habituelle est noire (code couleur 1) et éventuellement blanche (code couleur 2).
- y sur la référence des lecteurs Stid correspond au type de bornier pour le raccordement de la liaison RS-485. y peut prendre la valeur A (pour un câble moulé) ou B (pour un câble bornier).

8.1.2 Modules d'entrées-sorties

Manufacturier	Référence	Description	Protocole	Micrologiciel
STid	STid I/O panel 8/8	8 entrées supervisées 8 sorties relais	OSDP	1.0

8.2 Table des figures

8.3 Références

Référence	Titre	Version
[ANSSI_TLS]	Recommandations de sécurités relatives à TLS	1.2
[ANSSI_PA_72]	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection	2.1
[ANSSI_PA_079]	Guide de sélection d'algorithmes cryptographiques	1.0
[ANSSI_PG_083]	Guide des mécanismes cryptographiques	2.04
[ANSSI_CER_P_01]	Certification de Sécurité de Premier Niveau des produits des technologies de l'information	5.0
[ANSSI_MOD_CDS]	Document de travail : système de contrôle d'accès physique	1.0
[ANSSI_NOTE_7]	Méthodologie pour évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN	2.0
[ANSSI_NOTE_9]	Contenu et structure de la cible de sécurité CSPN	1.0
[GEN_ANSSI_CSPN]	Configurer Genetec[MC] Security Center et le Synergis[MC] Cloud Link pour conformité ANSSI CSPN	1.3
[GEN_CRYPTO] (1)	Mécanismes cryptographiques	1.3
[GEN_SC_ADMIN]	Guide de l'administrateur Security Center	5.12
[GEN_SC_CSR]	Guide de la configuration requise pour Security Center	5.12
[GEN_SC_HG]	Guide de renforcement de Security Center	5.12
[GEN_SC_INS]	Guide d'installation et de mise à jour de Security Center	5.12.2.0
[GEN_SCL_CFG]	Guide de l'administrateur Synergis[MC] Cloud Link	3.1.2
[GEN_SCL_INS]	Guide d'installation du matériel Synergis[MC] Cloud Link	2024-07-16
[GEN_SCL_INT]	Guide d'intégration Synergis[MC] Softwire	11.5.2

Note 1 : diffusion sous accord de confidentialité

8.4 Glossaire

Terminologie	Description
AES	Advanced Encryption Standard, algorithme de chiffrement symétrique
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Config Tool	Interface client de Security Center dédiée à la configuration du contrôle d'accès
CSN	Card Serial Number, numéro de série public et unique à chaque badge (aussi appelé UID : Unique IDentifier)
CSPN	Certification de Sécurité de Premier Niveau, aussi appelée « Visa de Sécurité de l'ANSSI », est une des certifications délivrées par l'ANSSI pour des produits des technologies de l'information
GAC	Système de Gestion des Accès Contrôlés
Gestionnaire d'accès	Le Gestionnaire d'accès gère et surveille les unités de contrôle d'accès du système.
Identifiant	Type d'entité qui représente une carte de proximité, exigé pour accéder à un secteur sécurisé. Un identifiant ne peut être affecté qu'à un titulaire à la fois
IdP	Fournisseur d'identité en authentification
IGC	Infrastructure de Gestion de Clés, est une infrastructure permettant la gestion de certificats (aussi appelé PKI pour Public Key Infrastructure)
MFA	Méthode d'authentification forte par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification
MIFARE® DESFire®	Marque déposée par NXP Semiconductors concernant des cartes à puce sans contact reposant sur des standards tels que ISO 14443. La gamme DESFire® une version spéciale de la plateforme NXP SmartMX. Elle existe en version, dans le présent document les version EV2 et EV3 sont les versions ciblées.
NTP	Network Time Protocol est un protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.
NXP	NXP est un fabricant de semi-conducteurs, fondé en 1967 sous le nom de Philips. Elle est issue d'une scission de la division semi-conducteurs de Philips.
OSDP[MC]v2	Open Supervised Device Protocol version 2 est une norme de communication de contrôle d'accès développée par la Security Industry Association (SIA). Protocole utilisé pour la communication avec les modules d'entrées-sorties. La version 2 permet l'activation du Secure Channel, sécurisant ainsi la communication RS-485.
Périphériques sériels	Têtes de lecture et/ou modules d'entrées-sorties reliés à une UTL par une connexion sérielle de type RS-485 répondant à la norme EIA-485
PIN	Personal Identification Number, numéro d'identification personnel. C'est le code numérique personnel réservé au Titulaire de cartes en tant que deuxième facteur d'authentification.
PKI	Public Key Infrastructure, est une infrastructure permettant la gestion de certificats (aussi appelé IGC pour Infrastructure de Gestion de Clés)
PNG	Passage non-gardé, accès, un système de portillon d'accès automatiques permettant de contrôler les accès de personnes, et parfois l'unicité de passage
POE	Power over Ethernet,ou l'alimentation électrique par câble Ethernet, est la technologie qui utilise les câbles Ethernet RJ45 pour alimenter en électricité les équipements
Point d'accès	Un point d'accès est un point d'entrée (ou de sortie) d'un secteur physique pour lequel le passage peut être surveillé et soumis à des règles d'accès. Il s'agit généralement d'un côté de porte ou d'un étage d'ascenseur.

Porte	Type d'entité qui représente une barrière physique. Il peut s'agir d'une porte, mais aussi d'une grille, d'un tourniquet ou de tout autre passage contrôlable. Chaque porte a deux côtés, appelés Entrée et Sortie par défaut. Chaque côté est un point d'accès (entrée ou sortie) à un secteur sécurisé.
Règle d'accès	Type d'entité qui définit une liste de titulaires de cartes auxquels un accès est accordé ou refusé en fonction d'un horaire. Une règle d'accès peut être affectée à un point d'accès ou à un secteur sécurisé.
Répertoire	Le Répertoire identifie un système Security Center. Il gère toutes les configurations des entités et les paramètres du système.
RS-485	Type de liaison électrique permettant la connexion via un bus répondant à la norme EIA-485 véhiculant des protocoles de type SSCP®v2 ou OSDP[MC]v2
SAM	Secure Access Module
Secteur sécurisé	Entité secteur qui représente un site physique auquel l'accès est contrôlé. Un secteur sécurisé est constitué de portes de périmètre (portes servant à pénétrer et à quitter le secteur) et de restrictions d'accès (règles régissant l'accès au secteur).
Security Center	Plateforme logicielle embarquant la composante contrôle d'accès
Security Desk	Interface client de Security Center dédiée à l'exploitation du contrôle d'accès
Serveur	Type de ressource qui représente un ordinateur sur lequel le service Genetec Server est installé. Les entités Serveur sont créées automatiquement à l'installation du logiciel Security Center Server sur un ordinateur, et lorsque l'ordinateur est connecté au serveur principal du système. Le serveur principal est celui qui héberge le Répertoire.
Softwire	Synergis[MC] Softwire est le micrologiciel (*firmware*) dans le contrôleur Synergis[MC] Cloud Link
SQL	SQL est un langage informatique normalisé servant à exploiter des bases de données relationnelles.
SSCP®v2	Smart Secure Common Protocol version 2, protocole de communication utilisé par les têtes de lecture. Ce protocole est de facto sécurisé entre les équipements.
SSO	Single Sign-On. Méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification.
Synergis[MC]	Security Center Synergis[MC] est le système de contrôle d'accès (SCA) sur IP qui renforce la sécurité physique de votre organisation ainsi que votre capacité à réagir aux menaces.
TOE	Target of evaluation
Titulaire de cartes	Type d'entité qui représente un individu autorisé à pénétrer et à quitter des secteurs sécurisés en fonction de ses identifiants, et dont les activités peuvent être surveillées.
TLS	Transport Layer Security, c'est un protocole de Sécurité de la couche de transport Ethernet TCP/IP. Les version 1.2 et 1.3 sont les versions ciblées dans le présent document.
Utilisateur	Type d'entité qui identifie une personne qui utilise les applications Security Center et définit ses droits et privilèges au sein du système. Les utilisateurs peuvent être créés manuellement ou importés depuis Active Directory.
UTL	Unité de Traitement Local (également connue sous le nom d'unité de contrôleur)
WebAPP	Genetec[MC] Web App est l'application Web qui donne aux utilisateurs un accès à Security Center via un navigateur.

FIN DU DOCUMENT :

Cible de Sécurité CSPN - Version 1.5

Security Center Synergis[MC]