Synergis™ Cloud Link

Cible de Sécurité CSPN
Version 1.1

Solutions innovatrices

Genetec

Table des matières

0 Références

0.1 Traçabilité du document

Révision	Date	Rédacteur	Commentaires
1.0	23 avril 2018	Louis-Martin CÔTÉ	Version initiale
1.1	16 août 2018	Louis-Martin CÔTÉ	Révision finale

0.2 Documentation

0.2.1 Documentation applicable

Références	Titre	Version	Date
[ANSSI_RGS]	Référentiel Général de Sécurité (ANSSI)	2.0	13 Juin 2014
[ANSSI_CSPN_Note1]	Méthodologie pour l'évaluation en vue d'une évaluation CSPN	2.0	23 avril 2014
[ANSSI_CTRL_ACC]	Sécurité des technologies sans contact pour le contrôle des accès physiques	1.0	19 novembre 2012

0.2.2 Documentation de référence

Références	Titre	Version	Date
[GEN_SCL_INS]	Guide d'installation du matériel *Synergis Cloud Link*	3.0	13 mai 2016
[GEN_SCL_QS]	Guide de démarrage rapide *Synergis Cloud Link*	3.1	28 mars 2018
[GEN_SCL_CFG]	Guide de configuration de l'appareil *Synergis*	10.7	28 mars 2018
[GEN_SCL_INT]	Guide d'intégration *Synergis Softwire*	10.7	4 avril 2018
[GEN_SC_ADMIN]	Guide de l'administrateur *Security Center*	5.7 SR2	20 avril 2018
[GEN_SD_USER]	Guide de l'utilisateur de *Security Desk*	5.7 SR2	13 avril 2018
[GEN_SC_INS]	Guide d'installation et de mise à niveau de *Security Center*	5.7 SR2	20 avril 2018
[GEN_SC_HG]	Guide de renforcement de *Security Center 5.7 SR2*	1.4	12 mars 2018
[GEN_ANSSI_CSPN]	Guide de mise en route pour conformité ANSSI CSPN	1.0	16 avril 2018
[GEN_SYAN_SAM]	Configurer les cartes *MIFARE SAM AV2* pour utilisation avec le *Synergis Cloud Link*	1.0	13 avril 2018

[GEN_CRYPTO]	Mécanismes cryptographiques	1.0	23 avril 2018
[ANSSI_TLS]	Recommandations de sécurités relatives à TLS	1.1	19 août 2016
[STID_SSCP]	Protocole de communication *SSCP V2 RS485 (7AD)*	1.3	26 novembre 2015
[SIA_OSDP]	Open Supervised Device Protocol (OSDP)	2.1.6	mai 2014
[NXP_P5DF081]	*MIFARE Secure Access Module* SAM AV2	3.5	9 octobre 2014

1 Introduction

1.1 Identification de la cible de sécurité

Ce document décrit la cible de sécurité relative à l'UTL *Synergis Cloud Link* (modèle SY-CLOUDLINK-312-CSPN) en vue de l'obtention d'une certification de sécurité de premier niveau (CSPN) dans la catégorie 6 : identification, authentification et contrôle d'accès.

1.2 Identification du produit

Référence de la Cible d'évaluation	SY-CLOUDLINK-312-CSPN
Constructeur	Genetec
Version matérielle	1
Version logicielle / Date	10.7.411.8 (2018-04-18)
Domaine d'utilisation	Contrôle d'accès

1.3 Glossaire

Entité	Les entités sont les composants de base de *Security Center*. Tout ce qui requiert une configuration est représenté par une entité. Les entités peuvent représenter un objet physique, comme une caméra ou une porte, ou une notion abstraite, comme une alarme, un horaire, un utilisateur, un rôle, un module externe ou un composant logiciel.
Serveur	Type d'entité 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 rôle *Répertoire*.
Rôle	Un rôle est un module logiciel qui effectue une tâche particulière au sein de *Security Center*. Les rôles doivent être affectés à un ou plusieurs serveurs pour exécution. Vous pouvez affecter des rôles pour l'archivage vidéo, pour la gestion des unités de contrôle d'accès, ou pour synchroniser les utilisateurs *Security Center* avec votre système d'annuaire d'entreprise, etc.
Identifiant	Type d'entité qui représente une carte de proximité, un modèle biométrique ou un code PIN exigé pour accéder à un secteur sécurisé. Un identifiant ne peut être affecté qu'à un titulaire à la fois
Titulaire de cartes	Type d'entité qui 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.
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.
SAM	*Secure Access Module*
UTL	Unité de Traitement Local
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.

Secteur	Type d'entité qui représente un concept ou un lieu physique (pièce, étage, bâtiment, site, etc.) utilisé pour le regroupement logique des entités du système.
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).
Zone	Type d'entité qui surveille un ensemble d'entrées et déclenche des événements en fonction de leurs états. Ces événements peuvent servir à contrôler des relais de sortie.

1.4 Informations relatives aux brevets

Le mode d'opération dit "transparent" des lecteurs de badge *MIFARE DESFire* est soumis aux brevets suivants :

1. United States, 6575360, Device and method for personalizing chip cards
2. United States, 7853789, Method and system for establishing a communications pipe between a personal security device and a remote computer system

2 Argumentaire du produit

2.1 Description fonctionnelle du système de contrôle d'accès

2.1.1 Fonctionnalités du système

Le produit *Security Center*™ est une plateforme de sécurité unifiée de Genetec, permettant le contrôle d'accès, la vidéo-protection ainsi que la reconnaissance automatique de plaque d'immatriculation (RAPI).

Le produit *Synergis*™ 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.

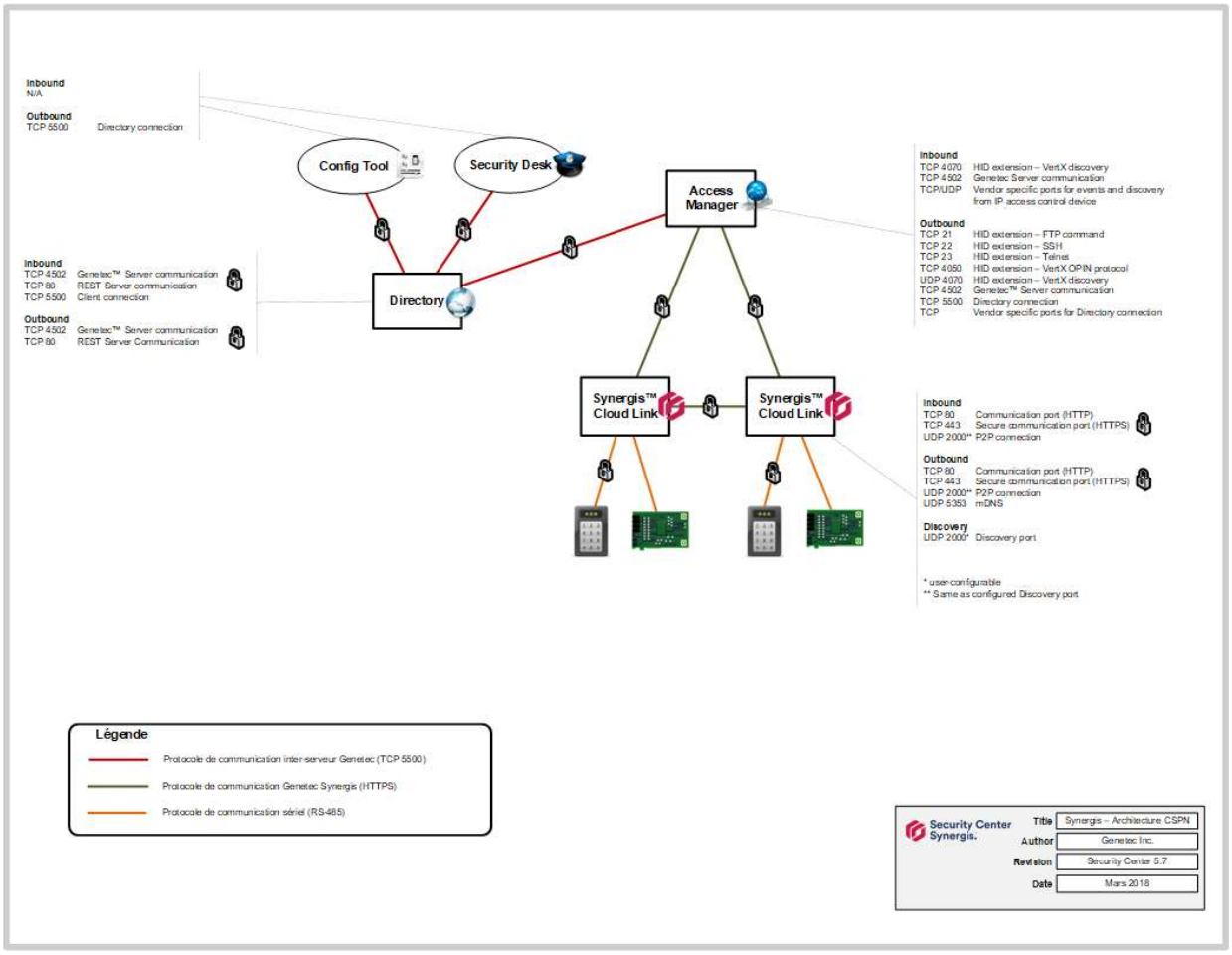

Figure 1 : La solution Synergis de Genetec

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'un lecteur de badge connecté à une Unité de Traitement Local (UTL) *Synergis Cloud Link*. L'accès au secteur est alors accordé ou refusé, selon les autorisations associées à l'identifiant obtenu par le lecteur du badge.

Figure 2 : L'Unité de Traitement Local Synergis CloudLink de Genetec (SY-CLOUDLINK-312-CSPN)

La solution *Synergis* propose deux procédures d'accès :

- Présentation simple du badge
- Présentation du badge avec confirmation par code PIN

Protection du canal radio de la carte sans contact

Afin de renforcer le niveau de sécurité offert par la solution, les secrets cryptographiques échangés entre la carte sans contact et l'UTL sont protégés en confidentialité et intégrité par la solution *MIFARE DESFire* proposée par NXP. La protection des échanges est confiée à des cartes *MIFARE SAM* intégrées dans les UTL. Afin de garantir une réactivité optimale même en période de forte charge, chaque UTL *Synergis* Cloud Link peut accueillir jusqu'à trois cartes SAM.

Lecteur de badge en mode transparent

L'architecture CSPN de *Synergis* met en œuvre des lecteurs de badges opérant sur bus sériel RS-485 en mode transparent, c'est-à-dire qu'ils relayent l'identifiant extrait du badge *MIFARE DESFire* à l'UTL *Synergis Cloud Link* sans le décrypter. De fait, les lecteurs ne disposent pas des clés cryptographiques protégeant les informations contenues dans le badge, ce qui minimise considérablement la surface d'attaque de la solution *Genetec Synergis*.

Boîtiers *Synergis Cloud Link* en mode interconnecté (mode *Peer-to-Peer*)

Le mode *peer-to-peer* est un mode de communication entre plusieurs UTL associées à un même serveur « Access Manager ». Il permet la réalisation de fonctions avancées telles que la gestion des « zones entrées/sorties » (fonctionnalité *lockdown* par exemple) ou l'anti retour global (fonctionnalité d'*anti passback*), indépendamment de la disponibilité du serveur.

Cette fonction est également utile en cas de catastrophe majeure pour assurer la résilience du système, en cas de perte de la salle serveur suite à une explosion ou un incendie par exemple.

2.1.2 Initialisation du système

L'initialisation d'un système *Genetec Synergis* est effectuée en quatre phases :

a) Déploiement des serveurs applicatifs (Security Center, SQL, etc.)

Au minimum, trois serveurs applicatifs doivent être déployés :

- Le serveur principal du système *Security Center* (rôle répertoire)
- Le serveur de contrôle d'accès du système *Security Center* (rôle gestionnaire d'accès)
- Le serveur de base de données SQL

Pour un système de taille restreinte, ces trois serveurs applicatifs peuvent coexister sur la même machine, physique ou virtuelle. Toutefois, 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. Il convient de noter au passage que, bien que le répertoire puisse gérer un nombre illimité d'UTLs, de portes et de titulaires de cartes, chaque rôle « Gestionnaire d'accès » supporte un maximum de 2000 portes, ou 100 UTL *Synergis Cloud Link* (selon la première limite atteinte).

Références :

- [GEN_SC_INS] *Guide d'installation de Security Center*
- [GEN_SC_ADMIN] *Guide de l'administrateur Security Center*, chapitre 29, pp. 595-603

b) Configuration des entités physiques (composantes matérielles)

La configuration des entités physiques se déroule en deux étapes.

Dans un premier temps, il faut initialiser chacune des UTL *Synergis Cloud Link* mise en œuvre dans le système. Cette opération doit être effectuée par un administrateur via le portail de configuration de l'UTL.

Les principaux éléments de configuration de l'UTL sont :

- Propriétés réseau
- Propriétés des ports RS-485 (lecteurs de badges *MIFARE DESFire* et interfaces de portes)

Si des lecteurs à clavier sont utilisés, il est conseillé de sécuriser le canal de communication RS-485 selon les recommandations du document [GEN_ANSSI_CSPN] afin de protéger adéquatement les codes PIN.

Dans un second temps, il faut enrôler les UTL *Synergis Cloud Link* sous un gestionnaire d'accès. Cette opération est réalisée par un Administrateur au moyen du logiciel de configuration *Security Center Config Tool*.

Références :

- [GEN_SCL_CFG] *Guide de configuration de l'appareil Synergis*, chapitre 3 (pp. 14-40)
- [GEN_SCL_INT] *Guide d'intégration Synergis Softwire*, chapitres 8 (pp. 109-120), 11 (pp. 149-156) et 14 (pp. 184-197)
- [GEN_ANSSI_CSPN] *Guide de mise en route pour conformité ANSSI CSPN*

c) *Configuration des entités logiques (portes, titulaires de cartes, règles d'accès, etc.)*

A ce stade, l'administrateur doit configurer les entités logiques du système. Cette configuration s'effectue également au moyen du logiciel de configuration *Security Center Config Tool*.

Le tableau suivant contient la liste des entités logiques constituant un système de contrôle d'accès *Genetec Synergis* :

Icône	Entité	Description
	Gestionnaire d'accès (rôle)	Rôle assurant la gestion des contrôleurs de porte sur le système.
	Unité de contrôle d'accès	Contrôleur de porte auquel est associé un lecteur.
	Porte	Barrière physique contrôlée par une unité de contrôle d'accès.
	Ascenseur	Cabine d'ascenseur unique.
	Règle d'accès	Logique utilisée pour savoir s'il faut accorder l'accès ou non.
	Secteur sécurisé	Emplacement physique auquel l'accès est contrôlé par des *règles d'accès* et d'autres comportements de contrôle d'accès, comme l'antiretour, les sas, la règle de superviseur présent, la règle de deuxième personne, etc.
	Titulaire de cartes	Personne possédant un identifiant.
	Groupe de titulaires de cartes	Groupe de titulaires de cartes partageant des caractéristiques communes.
	Identifiant	Preuve d'identité, comme une carte, un code PIN, un scan biométrique, etc.
	Modèle de badge	Modèle d'impression de badges personnalisé pour les identifiants des utilisateurs.
	Horaire	Plage de dates et heures.
	Partition	Groupe d'entités du système, visibles seulement par un groupe d'utilisateurs.
	utilisateur	Personne utilisant les applications de Security Center.
	Groupe d'utilisateurs	Groupe d'utilisateurs partageant des caractéristiques communes.

Figure 3 : Liste des entités constituant un système de contrôle d'accès Genetec Synergis

L'une des deux entités logiques de base de tout système de contrôle d'accès *Synergis* est la porte. C'est à la porte que l'administrateur associe les ressources matérielles qui contrôlent le passage (lecteur, verrou, capteur de contact, etc.).

Afin de faciliter la gestion des systèmes, il est possible de regrouper des portes dans des entités logiques de plus haut niveau, appelées *secteurs sécurisés*. Les règles d'accès peuvent alors être appliquées par secteurs, plutôt que d'avoir à leur associer de longues listes de portes individuelles. La notion de secteur sécurisé est nécessaire à la mise en œuvre de certaines fonctions plus avancées du système, comme par exemple le comptage des personnes, l'accompagnement de visiteurs, l'accès sous contrainte et la gestion de l'antiretour et des sas.

L'autre entité logique à la base du fonctionnement du système *Synergis* est le *titulaire de cartes*. Le titulaire de cartes est une personne possédant au moins un identifiant. Tout comme les portes qui peuvent être regroupées en secteurs, les titulaires de cartes peuvent être regroupés au moyen d'entités logiques abstraites, appelées *groupes de titulaires de cartes*. À la différence des portes, des secteurs et des groupes de titulaires de cartes, les titulaires de cartes et les identifiants peuvent être créés par un utilisateur du système (et non seulement par les administrateurs) au moyen du logiciel *Security Desk*.

Enfin, l'administrateur doit définir les règles d'accès du système. Une règle d'accès est une entité logique 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*.

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)

Synergis n'autorise pas directement l'accès à une carte ou à un identifiant. Il accorde ou refuse l'accès en fonction des titulaires de cartes eux-mêmes.

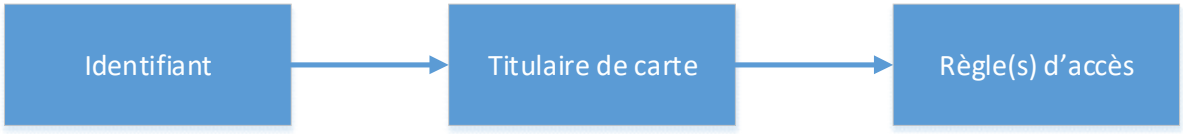

Figure 4 : Chaînage Identifiant / Titulaire / Règle(s)

Cette différence subtile mais fondamentale de la logique appliquée comporte un avantage notable en cas de cartes perdues ou volées : il n'est pas nécessaire de modifier les règles d'accès envoyées aux contrôleurs de porte. Si un nouvel identifiant est associé à un titulaire de cartes, l'ancienne règle reste valable.

Références :

- [GEN_SC_ADMIN] *Guide de l'administrateur Security Center*, chapitres 31,32 et 33 (pp. 616-702)
- [GEN_SD_USER] *Guide de l'utilisateur de Security Desk*, chapitres 16 et 17 (pp. 250-315)

d) Mise à la clé (sécurisation de la chaîne MIFARE DESFire)

La dernière étape d'initialisation du système *Synergis* est appelée mise à la clé. Le but de cette étape est la sécurisation de la chaîne *MIFARE DESFire* protégeant les identifiants contenus dans les badges portés par les titulaires de cartes.

Cette étape survient typiquement à la toute fin de la mise en service initiale du système. Elle consiste principalement à :

- Installer les cartes SAM dans les ports des UTLs *Synergis Cloud Link* prévus à cet effet
- Charger les fichiers de configuration *MIFARE DESFire* sur les UTLs *Synergis Cloud Link*
- Charger les fichiers de configuration *MIFARE DESFire* sur les postes d'encodage de badges

Les opérations de chargement sont réalisées et supervisées à partir de *Security Center*™.

2.1.3 Phase opérationnelle

Une fois le système *Genetec Synergis* mis en service, les utilisateurs du système en charge de la production (aussi appelés opérateurs) peuvent commencer à gérer et superviser les demandes d'accès au moyen du logiciel *Security Center Security Desk*.

a) Déclaration d'un titulaire de carte

La déclaration d'un nouveau titulaire de carte se fait à partir de la tâche « Gestion des titulaires de cartes » du *Security Desk*.

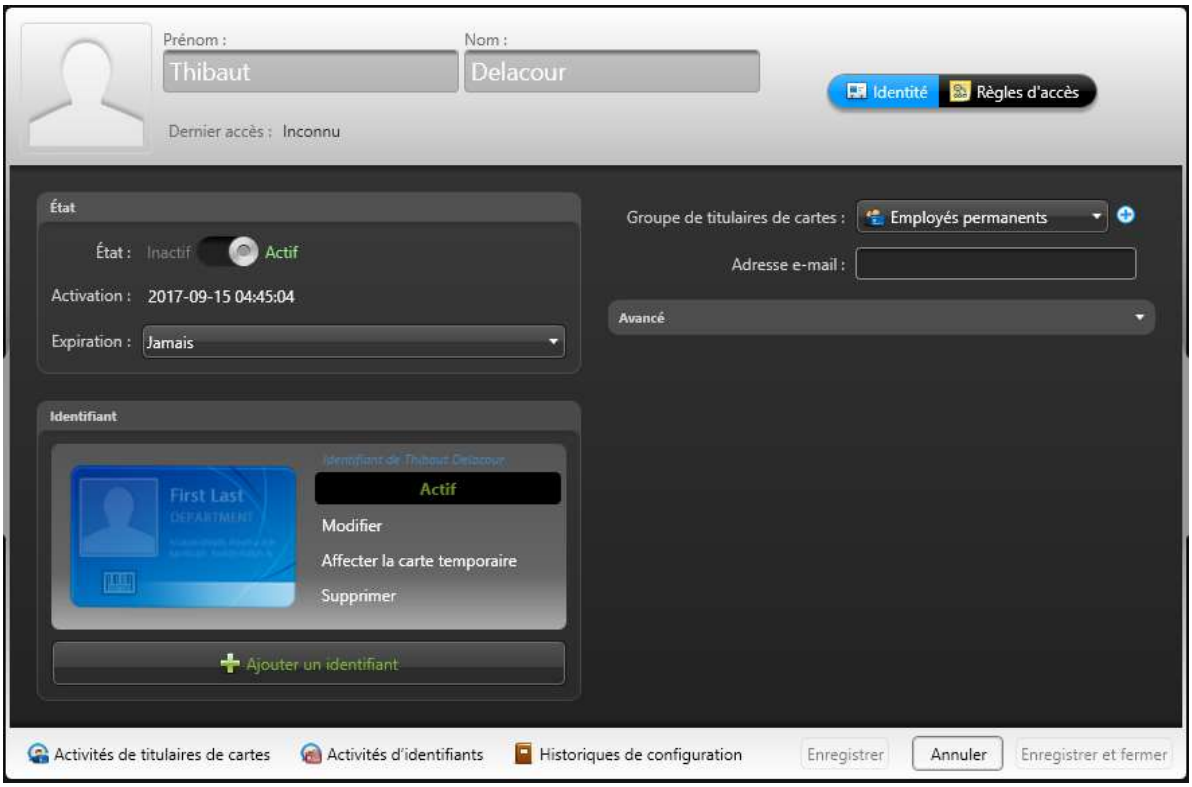

Figure 5 : Le panneau « Gestion des titulaires de cartes » du logiciel Security Desk

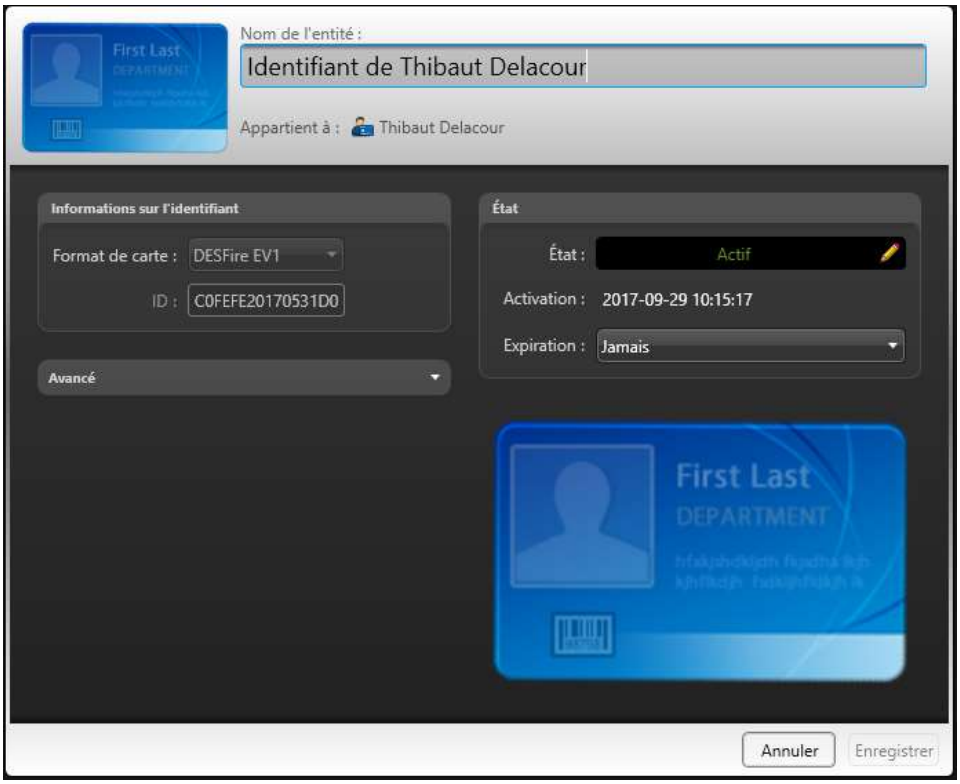

Figure 6 : Obtention de la valeur de l'identifiant d'un porteur de badge

En plus de permettre la saisie des informations permettant d'identifier le titulaire de carte (nom, prénom, photo), cette interface permet également de définir un ou plusieurs identifiants qui lui seront associés.

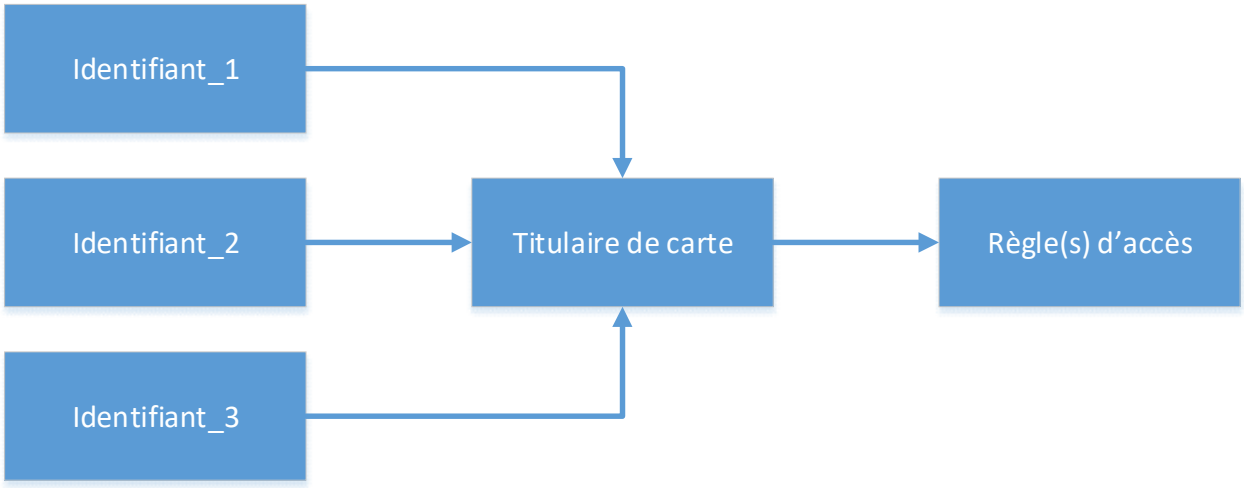

Figure 7 : Chaînage de plusieurs identifiants avec un titulaire de carte

b) *Révocation d'un titulaire de carte*

Security Desk permet également la révocation de l'accès à un titulaire de carte du système. La révocation peut s'appliquer soit à l'un des identifiants associés au titulaire de carte (comme par exemple dans le cas d'un badge perdu ou volé), soit au titulaire de carte lui-même (comme par exemple dans le cas d'une fin de contrat).

c) *Gestion des incidents et niveaux de risque*

Lorsqu'un utilisateur du système *Synergis* est témoin d'une situation qu'il convient de documenter, il peut la signaler en tant qu'incident. Les événements et entités (portes, titulaires de cartes, etc.) peuvent être joints à un rapport d'incident en tant qu'information complémentaire.

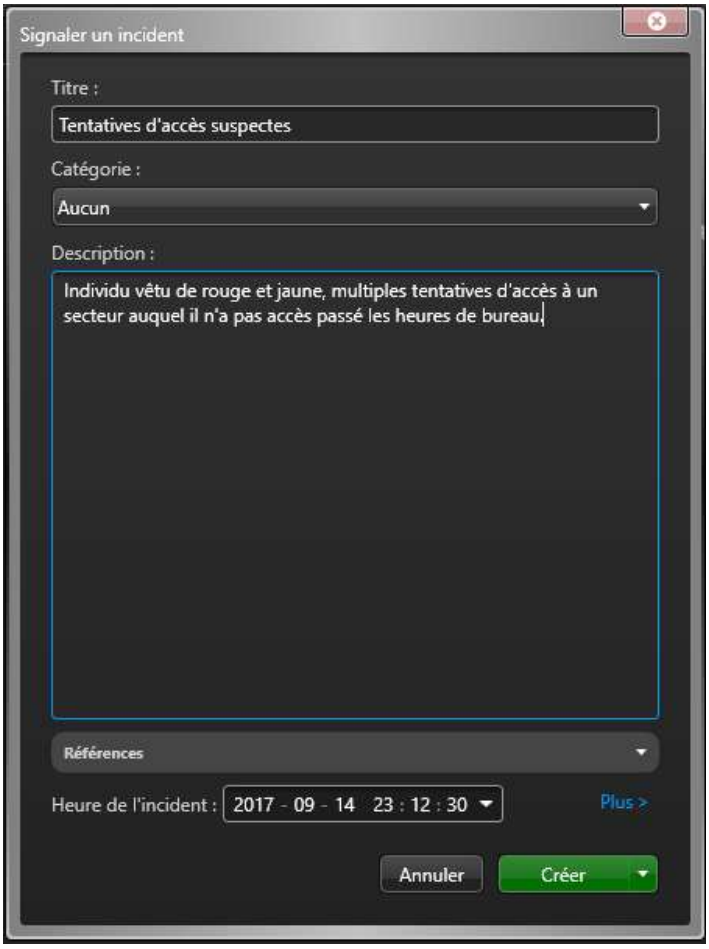

Figure 8 : Le panneau « Gestion des incidents » du logiciel Security Desk

Les utilisateurs du système peuvent aussi rechercher, analyser et modifier les incidents signalés avec le rapport Incidents, disponible dans la liste des tâches du *Security Desk*.

En cas d'événement critique durant la surveillance du système (incendie, fusillade, etc.), l'opérateur peut également modifier l'état du système global ou seulement celui d'un des secteurs, par le biais de niveaux de risque.

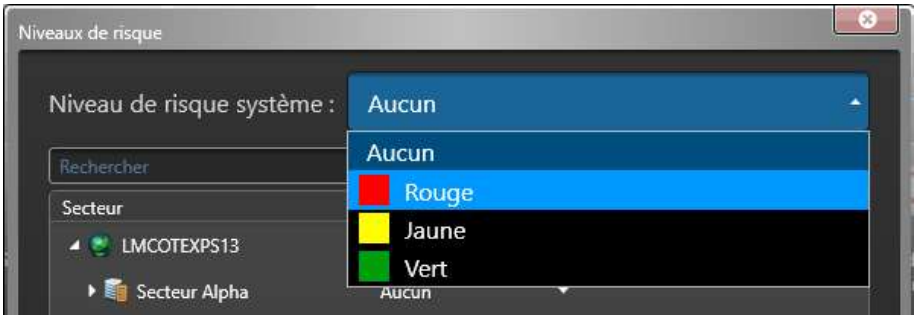

Figure 9 : Affectation du niveau de risque sur incident

Il incombe à l'administrateur de définir les différents niveaux de risques du système et leurs effets sur le comportement du système (par exemple : ignorer les horaires de verrouillage, déclencher une alarme, sécuriser complètement un périmètre, etc.). L'opérateur ne peut qu'appliquer un des niveaux de risques prédéfinis par l'administrateur.

Référence :

- [GEN_SD_USER] Guide de l'utilisateur de *Security Desk*, chapitre 27 (pp. 434-445)

2.2 Architecture opérationnelle du système de contrôle d'accès

2.2.1 Présentation générale

Le système de contrôle d'accès *Genetec Synergis*, fait partie de la solution de sécurité unifiée *Genetec Security Center*. Il repose sur une architecture ouverte et distribuée. Le fonctionnement général du système se décrit comme suit :

- Les configurations système sont enregistrées par le serveur Répertoire (*Directory*).
- Le serveur Répertoire transmet les configurations au serveur Gestionnaire d'accès (*Access Manager*).
- Le serveur Gestionnaire d'accès communique directement avec les UTL (*Controller*) par TCP/IP.
- Le serveur Gestionnaire d'accès envoie les horaires, les données de titulaires de cartes ainsi que les règles d'accès aux UTL.
- Lorsqu'un titulaire de cartes présente son identifiant à un lecteur, l'UTL consulte la règle d'accès pour savoir s'il doit accorder ou refuser l'accès.
- Une fois que les UTL ont été synchronisées avec le Gestionnaire d'accès, elles peuvent fonctionner de façon autonome, même en cas de perte de connexion au Gestionnaire d'accès.

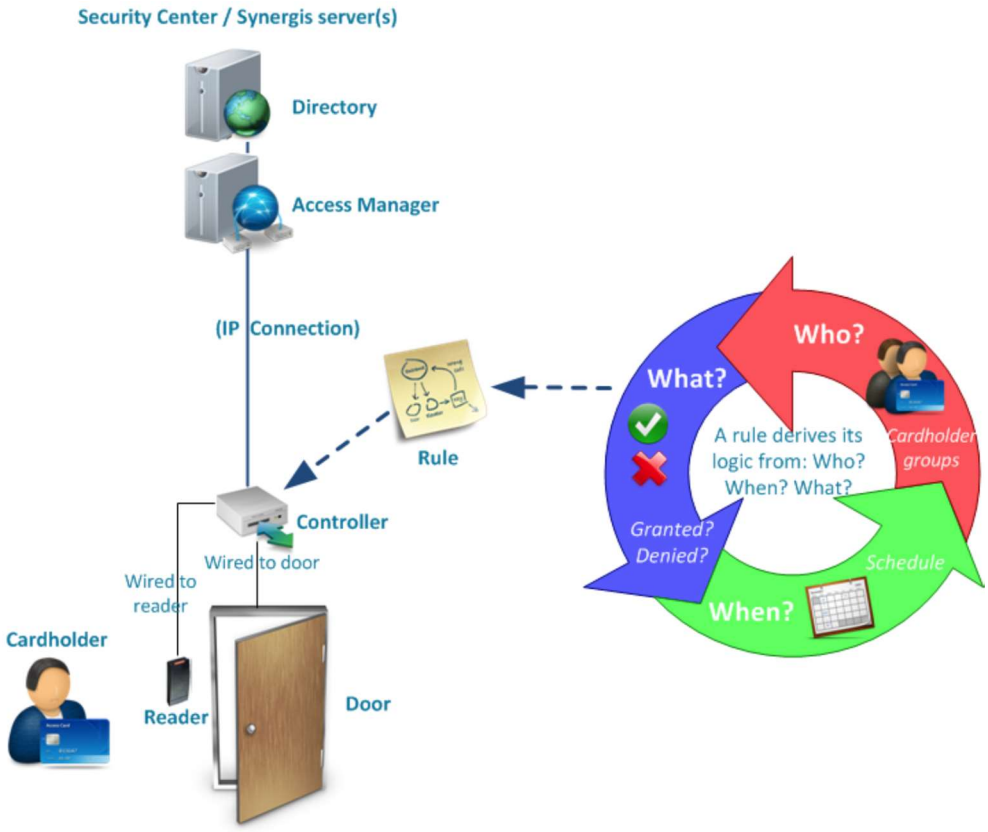

Figure 10 : Architecture Genetec Security Center

2.2.2 Composants logiciels

a) ***Rôle Répertoire (Directory)***

Le Répertoire est le rôle principal 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 de ce rôle est autorisée par système. Le serveur qui héberge le rôle Répertoire est appelé le serveur principal.

b) ***Rôle Gestionnaire d'accès (Access Manager)***

Le Gestionnaire d'accès est le rôle 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 rôle Répertoire, aux composants concernés du système.

Plusieurs instances de ce rôle peuvent être créées au sein du système.

c) Logiciel de configuration (Genetec Config Tool)

Config Tool est l'interface utilisateur permettant la configuration de la plateforme *Genetec Security Center*. 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.

d) Logiciel d'exploitation (Genetec Security Desk)

Security Desk est l'interface utilisateur destiné à l'exploitation de la plateforme *Genetec 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 opérateurs de contrôler et surveiller efficacement de nombreuses applications de sécurité et de sûreté. Au sein d'une interface unifiée, l'opérateur peut suivre les événements et les alarmes en temps réel, créer des rapports, contrôler l'état des portes et suivre les titulaires de cartes ou encore visionner les flux vidéo en temps réel ou enregistrés. Lorsqu'il est connecté à une Fédération 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.

e) Logiciel de production de cartes SAM

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 SAM pour un niveau de sécurité accru.

Conséquemment, un outil doit être utilisé pour configurer les SAM employées pour protéger les secrets du client final.

L'application SAM Manager de la société *Islog* est recommandée par Genetec.

f) Logiciel de production de badges SKB pour configuration des lecteurs STid

Dans le cas où des lecteurs *STid* sont utilisés, il peut être nécessaire de créer des *Secure Key Bundles* à partir de badges *MIFARE DESFire* vierges.

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

2.2.3 Composants matériels

a) Serveurs

Il faut au minimum une machine (physique ou virtuelle) pour héberger les trois serveurs applicatifs composant au minimum un système *Synergis*.

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.

b) Postes 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 Security Center*.

Ces postes de travail n'ont pas de contrainte technique particulière.

c) UTL

Le nombre de lecteurs supportés par chaque UTL *Synergis Cloud Link* varie en fonction du protocole de communication employé par les lecteurs RS-485 (toujours en mode transparent).

Protocole RS-485	Nombre maximal de lecteurs par UTL Synergis Cloud Link
OSDP (version 2.1.6 et plus)	44
SSCP (version 2.0 et plus)	22

d) Interfaces de portes

Ces boitiers d'interface reçoivent des ordres de l'UTL et les convertissent en signaux de commande analogique à destination des équipements terminaux (gâches, boutons poussoirs, détecteurs de passage, etc.).

e) Lecteurs de badges MIFARE DESFire (RS-485, mode transparent)

La solution *Genetec Synergis* supporte tous les lecteurs *MIFARE DESFire* répondant à la norme ISO/IEC 14443 et qui offrent le support du mode transparent. Ces lecteurs établissent et gèrent le lien radio avec la carte sans contact au profit de l'UTL *Synergis Cloud Link* via une connexion sérielle RS-485.

f) Encodeurs de badges MIFARE DESFire (USB)

Ces encodeurs permettent l'encodage de badges *MIFARE DESFire* à partir d'un poste de travail *Security Desk* via une connexion USB.

Seul le modèle ARC-W35-G/PH5-5AA/y du fabricant *STid* est actuellement supporté (avril 2018).

2.3 Rôle de la cible d'évaluation dans le système

La cible de sécurité prévoit l'évaluation de la sécurité des fonctions de contrôle d'accès gérées par Unité de Traitement Local UTL : l'équipement dédié à la vérification contrôle d'accès est le module *Synergis Cloud Link*. Cet appareil de contrôle d'accès intelligent compatible *PoE* de Genetec Inc. prend en charge un éventail de modules d'interface tiers sur IP et RS-485. *Synergis 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.

Cet équipement se présente sous forme d'un boitier physique (cf. figure suivante).

Figure 11 : L'UTL Synergis Cloud Link de Genetec (modèle SY-CLOUDLINK-312-CSPN)

Il effectue les fonctionnalités suivantes :

- 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.
- Collection de l'identifiant d'un badge
- Émission de la commande d'ouverture du point d'accès concerné
- Enregistrement des évènements de sécurité (perte réseau, tentative d'effraction, …)

3 Description de la cible d'évaluation

3.1 Acteurs et rôles

Les intervenants sur le système d'architecture réseau mis en place autour de la cible d'évaluation ainsi que les acteurs qui interviennent sur le *Synergis Cloud Link* se répartissent en une organisation de six rôles. Les paragraphes suivants décrivent ces informations.

3.1.1 Administrateur

Cet acteur est chargé des tâches de création et configuration des entités requises pour modéliser le système.

La plateforme de sécurité unifiée *Genetec Security Center* lui fournit une interface utilisateur pour configurer le contrôle d'accès et, si applicable, la vidéosurveillance et la RAPI (reconnaissance automatique de plaques d'immatriculation).

L'accès à l'application *Config Tool* se fait par réseau, via un *login*.

3.1.2 Utilisateur (Opérateur)

Cet acteur se voit confier des tâches d'exploitation liées aux opérations quotidiennes et d'investigation permettant de rechercher des informations dans les bases de données de *Security Center* ou des systèmes fédérés.

La plateforme de sécurité unifiée *Genetec Security Center* lui fournit une interface utilisateur pour surveiller, rapporter et gérer les événements et alarmes de contrôle d'accès et, si applicable, de vidéosurveillance et de RAPI (reconnaissance automatique de plaques d'immatriculation).

L'accès à l'application *Security Desk* se fait par réseau, via un login.

3.1.3 Titulaire de carte

Cet acteur 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.

3.1.4 Chargé de Maintenance

Cet acteur se voit confier les tâches dédiées à la maintenance et au dépannage des composantes matérielles du système. L'opérateur lui affecte une carte avec un profil 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.

3.1.5 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 HW (PNG, lecteurs, cartes).

Il est formé par Genetec afin d'être labélisé.

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

3.1.6 Installateur

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

3.2 Cycle de vie du produit

Le cycle de vie du produit décrit l'évolution de ses différents états en fonction des opérations qu'il subit.

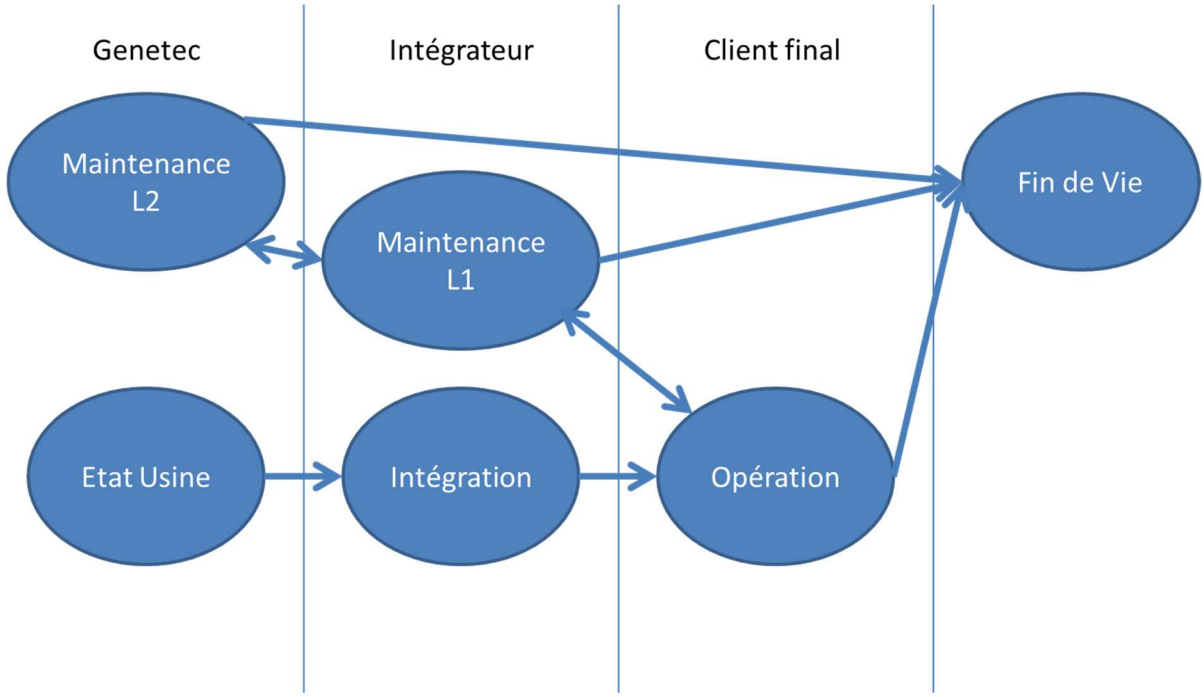

Figure 12 : Cycle de vie de l'UTL

3.2.1 État Usine : Fabrication et configuration initiale en usine

La dernière étape de fabrication de l'UTL est appelée « imagement ». C'est à ce moment que la mémoire flash de l'UTL est chargée avec les différentes composantes logicielles (système d'exploitation Windows embedded, plateforme .NET, *Softwire*).

Après l'installation de l'OS réalisée, celui-ci est configuré de manière durcie (désactivation de l'autorun, configuration Firewall Windows) pour garantir le maintien du produit dans un état sûr pour l'utilisateur final (qui n'a pas accès directement à la configuration de l'OS). De la même manière, il est à noter qu'une configuration « durcie » du BIOS est réalisée à cette étape (désactivation du boot sur clé USB par exemple) et que le mot de passe d'accès au BIOS n'est pas fourni à l'utilisateur final.

Enfin, c'est à cette étape que le certificat auto-signé destiné à sécuriser le canal TLS et le mot de passe unique du compte administrateur de Windows sont générés.

3.2.2 Intégration : Livraison à l'intégrateur et configuration destinée au client final

Genetec livre l'UTL à l'un de ses intégrateurs certifiés. L'intégrateur agit comme administrateur de première instance du système *Synergis*. C'est lui qui procède à l'installation et la configuration des serveurs applicatifs et qui procède à la configuration des entités physiques.

Lors de cette étape, l'intégrateur injecte les éléments de configuration matérielle dans l'UTL : configuration réseau, paramètres des portes, des relais, des capteurs de passage ainsi que ceux des lecteurs de badges.

3.2.3 Opération : Livraison au client final

Étape à laquelle l'intégrateur livre le système au client final. Le client final met son système à la clé. La clé est générée soit par le client final soit par l'intégrateur pour le compte et l'usage exclusif du client final.

Au moment de la mise en service du système, l'intégrateur cède ses droits d'administrateur au client final.

Le client final procède à la configuration des entités logiques (titulaires de cartes, droits d'accès, secteurs, etc).

3.2.4 Maintenance L1

Maintenance de premier niveau prise en charge par l'intégrateur. Ces travaux permettent de déterminer si les pannes rencontrées sont liées à la configuration du produit ou à une défaillance matérielle.

Un effacement du produit est réalisable par intervention sur les commutateurs DIP.

3.2.5 Maintenance L2

Maintenance de deuxième niveau prise en charge par Genetec. Ces travaux visent à vérifier le bon fonctionnement de l'UTL et d'y apporter les correctifs matériels ou logiciels nécessaires afin de procéder à sa remise en service.

3.2.6 Fin de vie

Il n'y a pas de procédure spécifique pour la gestion de fin de vie du produit de la part de Genetec. Le client final ou l'intégrateur est responsable de disposer adéquatement de ses équipements selon ses propres politiques de sécurité.

3.3 Périmètre physique

Le périmètre physique de la cible d'évaluation est composé d'un UTL et d'un lecteur de badges connectés entre eux.

3.3.1 UTL

Le boitier SY-CLOUDLINK-312-CSPN, composé d'une carte mère et une carte fille.

Figure 13 : UTL Synergis Cloud Link (modèle SY-CLOUDLINK-312-CSPN)

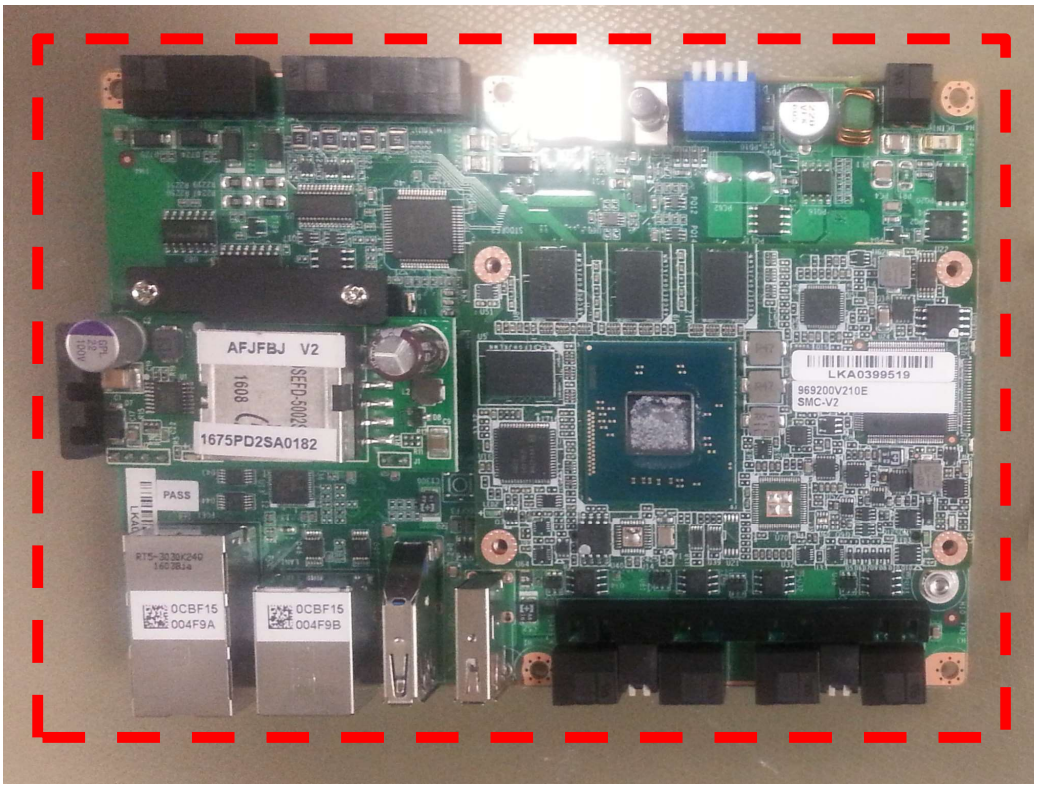

Figure 14 : Périmètre physique de la cible d'évaluation (carte mère)

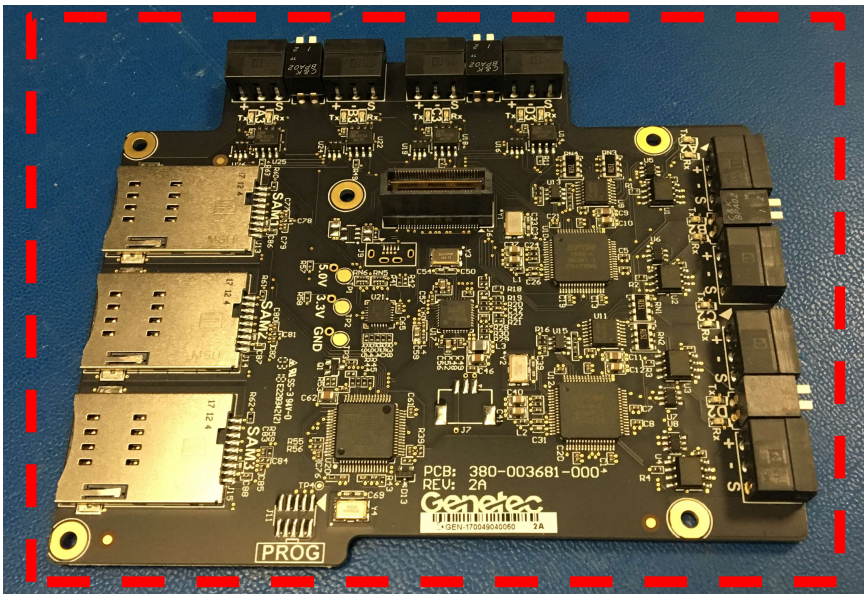

Figure 15 : Périmètre physique de la cible d'évaluation (carte fille)

Le périmètre physique de la cible d'évaluation est celui indiqué par les tirets rouges.

Interfaces matérielles

Les interfaces physiques de cette cible d'évaluation sont représentées ci-dessous :

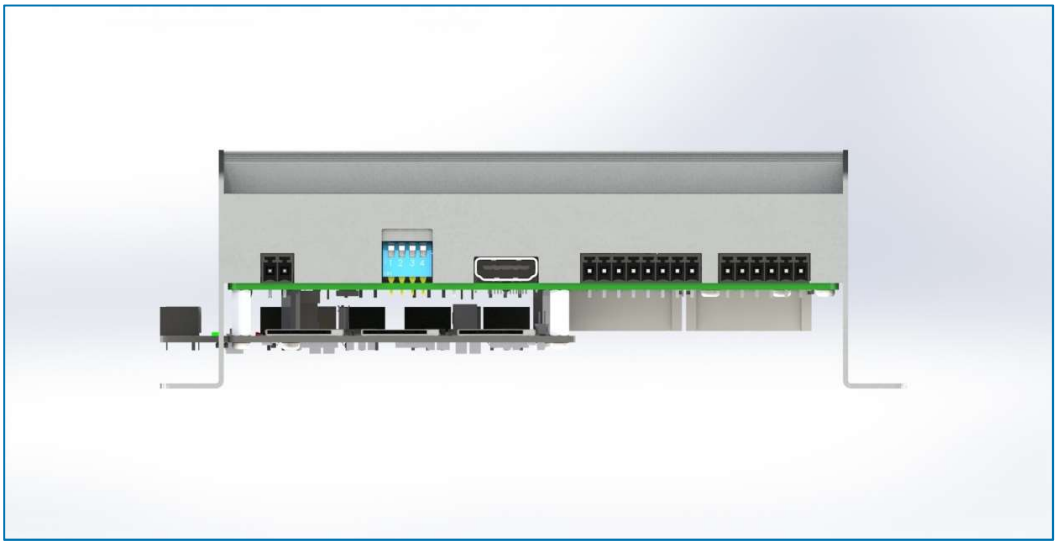

Figure 16 : Interfaces physiques

L'UTL possède des interfaces RS-485, USB, Ethernet, des LED d'état, une alimentation 12V, des codes de commande avec les commutateurs DIP et des ports de surveillance :

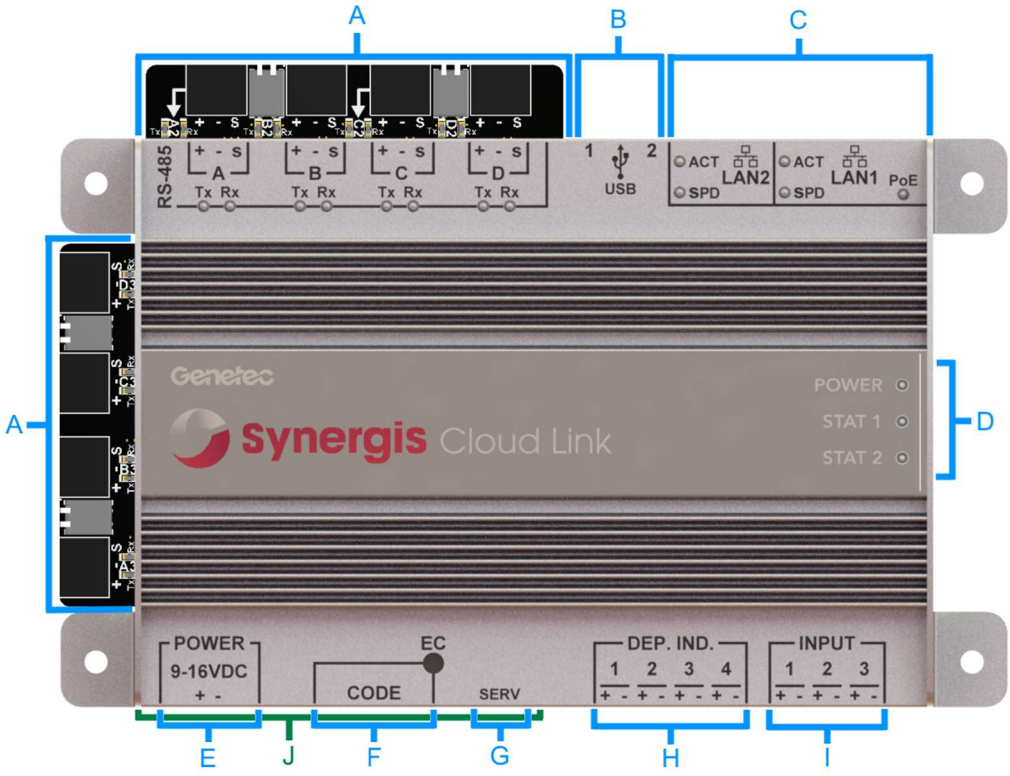

Figure 17 : Identification des interfaces physiques

A	RS-485 : Ports de communication pour protocoles sériels • Quatre ports intégrés sur la carte mère • Huit ports supplémentaires sur la carte fille SCLM-308
B	USB1 / USB2 Pour une utilisation lors de la maintenance.
C	LAN1 / LAN2 Deux ports LAN Ethernet sont fournis pour la connexion au réseau IP.
D	LEDs d'état *Synergis*
E	Alimentation
F	Code avec les commutateurs DIP
G	Port de service
H	Connecteur de LEDs déportées
I	Entrées de surveillance (non-fonctionnels)
J	Trois fentes pour cartes MIFARE SAM

3.3.2 Lecteur

La solution *Genetec Synergis* supporte tous les lecteurs *MIFARE DESFire* répondant à la norme ISO/IEC 14443 et qui offrent le support du mode transparent. Ces lecteurs établissent et gèrent le lien radio avec la carte sans contact au profit de l'UTL *Synergis Cloud Link* via une connexion sérielle RS-485.

Concernant le lien avec le badge, étant utilisés en mode transparent, les lecteurs n'interagissent pas avec la couche de sécurité qui protège les identifiant contenus dans la carte sans contact.

Ce mode de fonctionnement est celui préconisé dans [ANSSI_CTRL_ACC] pour l'architecture n°1 désignée comme « hautement recommandée ».

En supplément, des modèles de lecteurs avec clavier existent pour le support d'une authentification forte basée sur le PIN.

Les modèles suivants sont approuvés par Genetec à cette date (avril 2018):

- HID iClass SE R10 (OSDP, modèles 900NMPNEKMA0J0 et 900NMPTEKMA0J0)
- HID iClass SE R40 (OSDP, modèles 920NMPNEKMA0J0 et 920NMPTEKMA0J0)
- HID iClass SE RK40 (OSDP, modèles 921NMPNEKMA0J1 et 921NMPTEKMA0J1)
- HID iClass SE R95A Decor (OSDP, modèle 95ANMPTEWMA0J0)
- STid ARC-W33-A/PH5-7AD/y (SSCPv2, modèle ARC-A)
- STid ARC-W33-B/PH5-7AD/y SSCPv2, modèle ARC-B)
- STid ARC-W33-C/PH5-7AD/y (SSCPv2, modèle ARC-C)
- STid ARC1-W33-X/PH5-7AD/1 (SSCPv2, modèle ARC-1)
- STid LXS-W33-E/PH5-7AD/y (SSCPv2, modèle LXS)

Interfaces matérielles

Les interfaces matérielles d'un lecteur de badges transparent sans clavier sont le port RS-485 et le capteur RF. Pour un lecteur avec clavier, celui-ci est une interface externe supplémentaire.

3.4 Périmètre logique

3.4.1 UTL

Le périmètre logique de la cible de sécurité est composé de l'ensemble des modules logiciels de l'UTL en dehors de ceux embarqués sur les modules matériels SAM (OS Windows 7 Embedded); bien que l'OS en tant que brique logique ne soit pas inclus dans le périmètre logique de la cible de sécurité, la configuration de celui-ci est intégrée au périmètre. Au final, le périmètre considéré il est délimité par les tirets rouges sur le schéma ci-dessous :

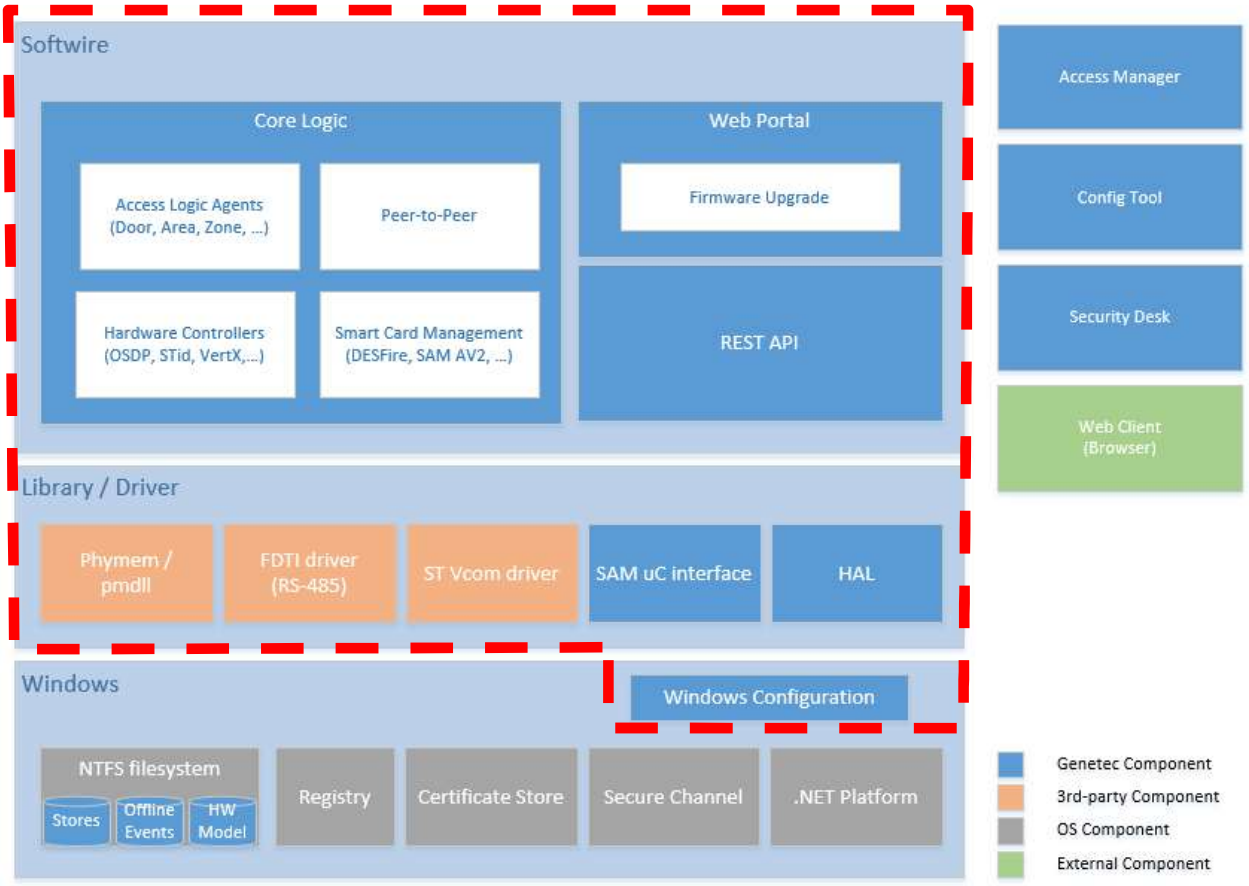

Figure 18 : Architecture applicative de la cible d'évaluation

Les interfaces logiques sont celles présentées au travers des ports externes : RS-485 (interfaces avec lecteurs et portes), USB et code avec commutateurs DIP (interfaces pour l'agent de maintenance), ports ethernet (interfaces avec le serveur *Access Manager* et avec autres UTLs), port de service (sortie HDMI pour maintenance seulement).

3.4.2 Lecteur

Le périmètre logique de la cible d'évaluation inclus de plus les méthodes impliquées dans le fonctionnement du système UTL-lecteur (e.g. authentification, mécanisme type *heartbeat*, etc.), les méthodes de traitement des codes PIN des titulaires de cartes entrés au clavier ainsi que les méthodes de transfert des commandes *MIFARE* vers l'UTL.

Les interfaces logiques sont donc celles présentées à l'UTL via le port RS-485 et celles présentées aux badges des titulaires via le capteur sans contact.

3.5 Dépendances de la cible d'évaluation par rapport à des matériels, logiciels et/ou des microprogrammes

La cible d'évaluation doit être portée sur le système d'exploitation *Windows 7 Embedded* pour assurer le fonctionnement de l'application *Softwire* (*Firmware* du *Synergis Cloud Link*).

La gestion du canal TLS, entre l'UTL et le serveur *Access Manager,* et la protection des certificats associés sont pris en charge par les services *Secure Channel* et *Certificate Store* du système d'exploitation *Windows*.

3.6 Environnement opérationnel en phase d'exploitation

Les UTL sont placées dans un local sécurisé à accès contrôlé et restreint.

L'accès physique à l'équipement n'est pas autorisé.

L'installation est décrite dans le guide [GEN_SCL_INS]. Elle se fait nominalement dans une armoire fermée à clé, disposant d'une source d'énergie de secours (batteries), conformément au schéma suivant :

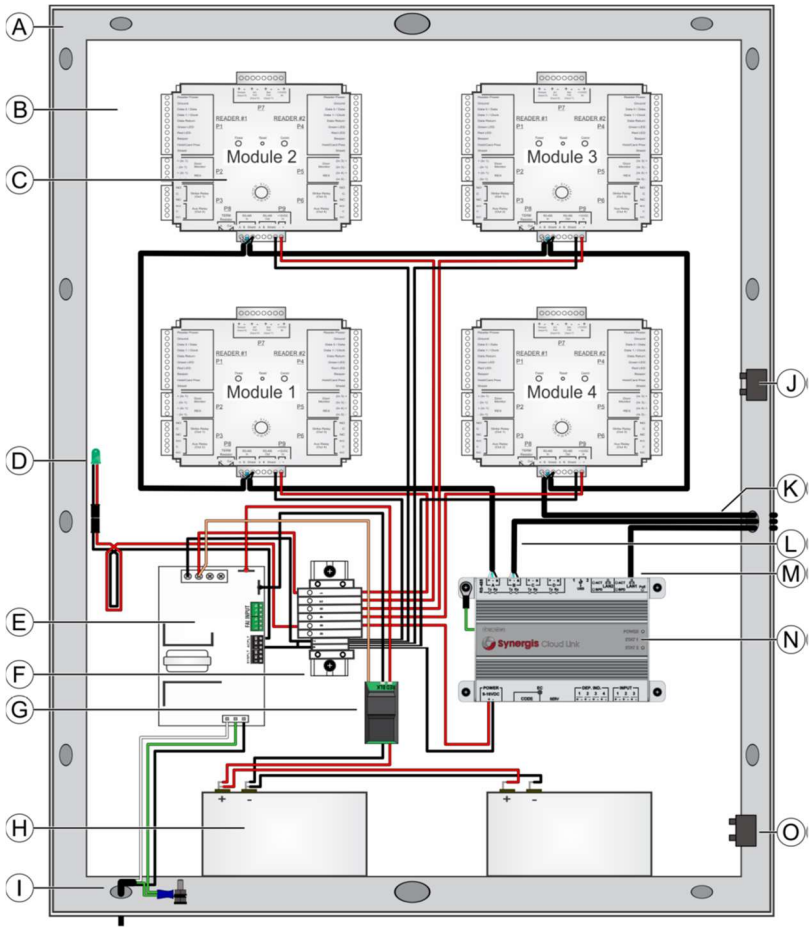

Figure 19 : Installation physique de l'UTL en armoire protégée

4 Problématique de sécurité

4.1 Biens sensibles

4.1.1 Biens essentiels

Le tableau suivant identifie les biens essentiels manipulés par la cible d'évaluation avec leurs besoins de sécurité (C = Confidentialité, I = Intégrité, D = Disponibilité).

Biens essentiels	Descriptions / Commentaires	C	I	D
Règles de contrôle d'accès (sous-ensemble dérivé de la BD globale)	Qui (Liste d'identifiants), Quoi (Liste(s) de "points d'accès"), Quand (plages horaires). Généré à l'extérieur de l'équipement.		x	
Règles de configuration de l'UTL	Définition physique des composantes matérielles constituant une porte, qui est l'entité logique à laquelle s'appliquent les règles d'accès		x	
Propriétés TI de l'UTL	IP, paramètres TLS, etc.		x	
Certificat d'authenticité de l'UTL (format X.509) qui contient la clé privée	Certificat auto-signé chargé en phase de production; possibilité pour le client final de le remplacer. Utilisé pour sécuriser le canal TLS et authentifier l'équipement après l'enrôlement.	x	x	
Identifiants des titulaires de cartes	Identifiant unique généré à l'extérieur de l'équipement.		x	
Codes PIN des titulaires de cartes	Généré à l'extérieur de l'équipement.	x	x	
Éléments d'authentification sur le système d'exploitation local de l'UTL	Login et Mot de Passe (MdP) du Windows local	x	x	
Login et MdP du compte Admin de l'UTL	Login et MdP permettant l'enrôlement de l'UTL.	x	x	
Certificats pour le fonctionnement Peer2Peer (connexion entre UTLs)	Jusqu'à 64 Peers => Chaque UTL peut stocker la partie publique des certificats de jusqu'à 63 UTLs homologues.		x	
Informations Peer2Peer	Dernier état connu des zones (entrées/sorties) et des secteurs (anti-retour).		x	

Biens essentiels	Descriptions / Commentaires	C	I	D
Clés de sécurisation du canal de communication des lecteurs RS-485	Contrairement à l'identifiant transmis en mode transparent, la transmission sécuritaire du code PIN provenant du clavier du lecteur requiert que le canal RS-485 soit sécurisé.	x	x	
Évènements du système recensés dans les journaux (log).	Accès autorisé, accès illicite, porte forcée, incohérence de comportement (ex: gâche actionnée mais pas d'ouverture de porte, …)		x	
Horodatage	Nécessite une installation adéquate. Recommandation d'utilisation d'un serveur NTP (Network Time Protocol).		x	
Clé publique de GENETEC pour mise à jour de l'UTL	Vérification des paquets de mise à jour		x	
Clé d'accès aux cartes SAM	Au démarrage de l'UTL, les cartes SAM sont verrouillées et doivent être déverrouillés afin d'être utilisables.	x	x	
Firmware de la cible d'évaluation	Solution *Softwire*		x	

On notera qu'aucun bien essentiel ne requiert le service de disponibilité.

4.1.2 Biens support

Le tableau suivant localise les biens supports dans lequel sont stockés ou manipulés les biens essentiels.

Biens essentiels	Biens support
Règles de contrôle d'accès (sous-ensemble dérivé de la BD globale)	BLOB dans Flash Nand (CMS) + partiellement en RAM (pagination)
Règles de configuration de l'UTL	BLOB dans Flash Nand (CMS)
Propriétés TI de l'UTL	BLOB dans Flash Nand (CMS)
Certificat d'authenticité de l'UTL (format X.509) qui contient la clé privée	Dans la partie statique de l'OS se trouvant dans la Flash + en RAM (magasin de certificat Windows)
Identifiants des titulaires de cartes	Carte *MIFARE DESFire* (hors périmètre de la ToE) + BLOB dans Flash Nand (CMS) + partiellement en RAM (pagination)
Codes PIN des titulaires de cartes	BLOB dans Flash Nand (CMS) + partiellement en RAM (pagination)

Biens essentiels	Biens support
Éléments d'authentification sur le système d'exploitation local de l'UTL	Dans la partie statique de l'OS se trouvant dans la Flash + en RAM
Login et MdP du compte Admin de l'UTL	Seulement salt+hash est gardé en flash.
Certificats pour le fonctionnement Peer2Peer (connexion entre UTLs)	Certificats sauvegardés en flash (partie publique seulement). Clés publiques non encryptées.
Informations Peer2Peer	BLOB dans Flash Nand (CMS)
Clés de sécurisation du canal de communication des lecteurs RS-485	BLOB dans Flash Nand (CMS)
Évènements du système recensés dans les journaux (log).	Si offline, stockage temporaire (flash) avant d'être repoussé dans la DB de l'Access Manager (hors périmètre).
Horodatage	Heure Windows; RTC en cas de coupure d'alimentation.
Clé publique de GENETEC pour mise à jour de l'UTL	Codée dans l'application. Sauvegardée en flash. Clé publique non encryptée.
Clé d'accès aux cartes SAM	BLOB dans Flash Nand (CMS)
Firmware de la cible d'évaluation	BLOB dans Flash Nand (CMS)

4.2 Hypothèses

4.2.1 Hypothèses sur la cible d'évaluation

H1 – Installation physique

- L'appareil *Synergis Cloud Link* et les accessoires connexes sont installés à l'intérieur d'armoires métalliques verrouillables, en conformité au guide d'installation [GEN_HW_INS], par des personnes formées et certifiées par Genetec.

H2 – Fonctionnement de l'OS Windows

- Le logiciel *Firmware* s'exécute sur un OS Windows 7 Embedded. Les mécanismes de cet OS garantissent :
  - La protection des données sensibles; en particulier, le système NTFS met en place des mesures assurant l'intégrité de ces fichiers et le service *Certificate Store* assure la gestion des certificats. De plus, toutes les données sensibles en confidentialités sont stockées chiffrées (BLOB) lorsqu'elles sont stockées en mémoire persistante,
  - La sécurité de l'accès aux données sensibles lorsqu'elles sont chargées en mémoire volatile par un processus,
  - L'atomicité sur système de fichier en se basant sur le système de fichiers NTFS de Windows,

- Le fonctionnement correct du firewall Windows,
- L'intégrité du *Firmware*.

H3 – Configuration Windows

- La pré-configuration de Windows opérée lors de la phase d'installation du produit n'est pas modifiée de manière incohérente par l'administrateur final.

H4 – Protocole de communication

- Le protocole *Transport Layer Security* (TLS) assure une authentification mutuelle des entités communicantes, prévenant ainsi toute connexion d'un serveur ou d'un UTL malveillant qui serait alors en mesure de lancer des attaques.
- Le protocole Transport Layer Security (TLS) assure l'intégrité et la confidentialité des communications (et l'intégrité des données) entre deux applications qui communiquent sur un réseau : c'est à dire entre *Softwire* sur l'UTL et le serveur. Lorsque le serveur et l'UTL communiquent, TLS vérifie qu'aucun tiers n'intercepte les messages prévenant des attaques de l'homme du milieu.

4.2.2 Hypothèses sur l'environnement

H5 – Formation des personnels

- L'équipement est installé et opéré par des personnels formés et responsables.

H6 – Locaux

- Les locaux qui hébergent la cible d'évaluation sont sous accès contrôlé et strictement limités aux personnels habilités.
- Un attaquant n'a pas d'accès physique au produit.

H7 – Réseaux

- Le réseau IP de communication avec l'UTL, les serveurs et autres équipements forment un réseau fermé non connecté au réseau internet.
- Les serveurs sont installés dans un local informatique sécurisé dont l'accès est strictement limité aux personnels habilités.
- La base de données globale de droits d'accès est réputée de confiance et l'extraction des droits pour un UTL est une opération sûre.
- Le serveur assurant le rôle d'Access Manager est capable d'assurer l'intégrité et la confidentialité des échanges TLS avec l'UTL.
- Les communications TLS appliquent les mesures et recommandations décrites dans le document [ANSSI_TLS].

H8 – Badge

- Le badge assure la confidentialité de ses éléments secrets.
- Les éléments secrets qui garantissent l'authenticité des badges ne doivent pas être exportés hors du périmètre de contrôle du client final.

4.3 Menaces

4.3.1 Agents menaçants

Les agents menaçants considérés sont des évènements de l'environnement ou des attaquants essayant d'utiliser des services illégitimement ou essayant de récupérer les informations des personnes utilisant ces services.

Agents menaçants	Description
Agent externe malveillant	Un agent externe n'a pas d'accès autorisé à l'intérieur du site; il pourrait avoir accès aux installations extérieures selon l'organisation du site. Ce type d'attaquant pourrait ainsi mener des attaques via un lecteur de badge ou une interface de porte, ou utiliser un badge volé.
Visiteur malveillant	Les visiteurs ont un accès aux installations et une proximité avec les employés et leur lieu de travail. Ils pourraient bénéficier de l'inattention de leurs accompagnants pour dérober le badge d'autres employés. Par le biais de plusieurs visites ou par ingénierie sociale lors de ces visites, il pourrait de plus connaitre les installations et de la routine du site (ex. horaires d'entrées/sorties, périodes de congés des employés). Ce type d'attaquant pourrait ainsi mener des attaques via un lecteur de badge ou une interface de porte, ou utiliser un badge volé.
Employé malveillant	Les employés ont un accès aux lecteurs de cartes et connaissent les installations et la routine du site (ex. horaires d'entrées/sorties, périodes de congés des employés). Ils pourraient aussi avoir facilement accès aux badges d'autres employés laissés sans surveillance. Ce type d'attaquant pourrait ainsi mener des attaques via un lecteur de badge ou une interface de porte, ou utiliser un badge volé.
Intégrateur malveillant	L'intégrateur a un accès physique autorisé à l'UTL; de plus, il a un accès autorisé à l'interface de configuration de l'UTL. Ce type d'attaquant pourrait ainsi directement modifier la configuration du produit afin de dégrader la sécurité du système ou encore mener des attaques via les interfaces matérielles de la cible d'évaluation.
Installateur malveillant	L'installateur a un accès physique autorisé à l'UTL (par délégation). Ce type d'attaquant pourrait ainsi mener différents types d'attaques via les interfaces matérielles de la cible d'évaluation.

Agents menaçants	Description
Chargé de maintenance	Le chargé de maintenance a des accès à l'UTL, aux lecteurs de badges et interface de portes, et est en possession d'un badge avec un profile dédié à la maintenance. Ce type d'attaquant pourrait ainsi mener le même type d'attaques qu'un employé (via lecteur de badge et interface de porte) ou que l'installateur (via les interfaces matérielles de la cible d'évaluation).
Opérateur malveillant	L'opérateur a un accès autorisé à l'interface utilisateur de l'UTL par laquelle il pourrait tenter de mener des attaques soit par exploitation de vulnérabilités d'implémentation logicielle soit en remplissant la base de fausses informations par exemple.
Administrateur malveillant	L'administrateur a un accès autorisé à l'interface de configuration de l'UTL; la modification de la configuration pourrait avoir un impact direct important sur la sécurité du système.
Panne électrique	Une panne électrique peut provoquer la mise hors tension de l'UTL qui n'est alors plus en mesure de réaliser ses fonctions de vérification des droits d'accès et d'envoi d'information à l'interface de porte. Ce type d'évènement pourrait provoquer un dysfonctionnement du blocage des portes ne correspondant pas aux règles d'accès gérées par l'UTL.

4.3.2 Évènements redoutés

La cible d'évaluation a pour fonctionnalité principale le contrôle des droits d'accès des titulaires de cartes aux portes qu'elle gère. Les deux risques finaux pour cette fonctionnalité sont :

- l'introduction non autorisée dans les locaux à protéger ;
- la non-détection d'une introduction non autorisée.

Les évènements redoutés sont les évènements pouvant mener à la survenue de tels risques et dont l'on souhaite donc empêcher la survenue. Ils dépendent des sources de menaces (agents d'attaques) et impactent des biens essentiels.

Le tableau ci-dessous liste l'ensemble des évènements redoutés identifiés pour la cible d'évaluation :

- Clonage d'un badge;
- Spoofing de badge;
- Clone de l'UTL;
- Spoofing de l'UTL (au moment de l'enrôlement, pour faire un MITM entre l'Access Manager et l'UTL légitime);
- Exécution du *Firmware* sur une plateforme matérielle non intègre;

- Perturbation du fonctionnement des composants logiciels (*Firmware* et système sous-jacent) :
    - Acceptation d'un badge non authentique sur le réseau;
    - Acceptation d'un badge authentique mais non déclaré;
    - Acceptation d'un badge authentique mais non autorisé;
    - Modifications des accès privilégié (e.g. contournement de l'antiretour);
    - Modification des éléments de configuration de l'UTL;
    - Altération d'un évènement système (log);
- Mise à jour illicite de la plateforme logicielle
- Rétrogradation des fonctions de sécurité de l'UTL (downgrading);
- Perte de disponibilité de l'UTL / compromission de la disponibilité du réseau hôte;
- Incohérence entre les bases de données locales et principales;
- Incohérence des informations P2P.

4.3.3 Scénarios de menace

Exclusion d'agents menaçants

Les hypothèses de la cible d'évaluation permettent d'exclure les agents menaçants suivants :

Agents menaçants non retenus	Justifications
Installateur	H6 : possède un accès physique à l'UTL
Intégrateur	H6 : possède un accès physique à l'UTL
Chargé de maintenance	H6 : possède un accès physique à l'UTL
Administrateurs	H5 : l'administrateur est formé et responsable
Opérateur	H5 : l'administrateur est formé et responsable
Panne électrique	H1 : l'UTL possède une batterie de secours car elle est installée en conformité au guide d'installation.

Exclusion de scénarios de menace

Les hypothèses de la cible d'évaluation permettent d'exclure les scénarios de menaces suivants :

Scénarios de menaces non retenus	Justifications
Clone de l'UTL	H6 – Pas d'accès physique à la zone sécurisée qui contient l'UTL.
Spoofing de l'UTL (à l'enrôlement)	H5 – Installation et maintenance par du personnel de confiance.
Exécution du *Firmware* sur une plateforme matérielle non intègre	H5 – Accès et manipulations par du personnel de confiance. H6 – Pas d'accès physique au local sécurisé dans lequel se trouve l'UTL légitime.

Scénarios de menaces non retenus	Justifications
Mise à jour illicite de la plateforme	H5 – Accès et manipulations par du personnel de confiance. H6 – Pas d'accès physique à la zone sécurisée qui contient l'UTL.
Exécution du *Firmware* sur une plateforme matérielle non intègre	H5 – Accès et manipulations par du personnel de confiance. H6 – Pas d'accès physique au local sécurisé dans lequel se trouve l'UTL légitime
Rétrogradation des fonctions de sécurité de l'UTL (downgrading)	H5 – Accès et manipulations par du personnel de confiance. H6 – Pas d'accès physique à la zone sécurisée qui contient l'UTL.

Scénarios de menaces retenus

Suite à l'analyse de risques globale réalisée précédemment et l'intégration des hypothèses permettant l'exclusion de scenario de menaces, le statut est le suivant :

- Agents menaçant : les agents menaçants sont limités aux « agent externe », « visiteur malveillant » et « employé malveillant ».
- Surface d'attaque (interfaces accessibles aux agents menaçants retenus) :
  - UTL : composants logiciels exposés via les interfaces Ethernet et le port RS-485 (via le lien avec le lecteur);
  - Lecteur : composants logiciels exposés via le capteur sans contact, clavier (si présent), boitier protégeant les composants matériels internes (e.g. mémoire).
- Moyens d'attaques :
  - injections logicielles visant à exploiter de potentielles vulnérabilités des composants logiciels du produit (e.g. failles web, base de données, etc.)
  - écoute passive ou active des communications Serveur AM – UTL;
  - écoute passive ou active des communications UTL – UTL;
  - écoute passive ou active des communications lecteurs – UTL;
  - manipulation physique des lecteurs de badge (remplacement, accès aux mémoires, etc.).

Les différents agents menaçants sont différenciés par la facilité d'accès physique au réseau (en terme de point d'entrée physique et de temps) et aux informations techniques sur l'UTL (pour ciblage des potentielles vulnérabilités logicielles); les attaques elles-mêmes seront ensuite les mêmes.

Le tableau ci-dessous présente la synthèse des menaces, couvrant l'ensemble des évènements redoutés restants, et exprimées en termes de moyens d'attaques par un agent menaçant et de biens impactés :

ID	Attaques	Biens impactés
M1	Attaques par injections sur les interfaces exposées visant l'exploitation de vulnérabilités menant au détournement des fonctionnalités du *Firmware*. *Événements redoutés couverts* : • *Acceptation d'un badge non authentifié (traitement du retour du module SAM).* • *Acceptation d'un badge authentique non déclaré.* • *Acceptation d'un badge authentique déclaré non autorisé.* • *Incohérence des bases de données locales et principales.* • *Modifications des accès privilégié (e.g. contournement de l'antiretour);* • *Incohérence des informations P2P.*	*Firmware*.
M2	Attaques par injections sur les interfaces exposées visant l'exploitation de vulnérabilités logicielles menant à la modification/divulgation des biens stockés en mémoire. *Événements redoutés couverts* : • *Acceptation d'un badge authentique non déclaré.* • *Acceptation d'un badge authentique déclaré non autorisé.* • *Usurpation/clonage d'un badge.* • *Modification des éléments de configuration de l'UTL.* • *Modification des éléments de configuration de la plateforme sous-jacente et ayant un impact sur la sécurité du Firmware.* • *Altération d'un évènement système (log).* • *Incohérence des informations P2P.*	Biens stockés en mémoire (Flash ou RAM) : règles de contrôle d'accès, règles de configurations, propriétés TI, certificat UTL (TLS), identifiants, PIN code, authentifiants OS local, authentifiants P2P, logs, certificat du *Firmware* (pour mise à jour), *Firmware*, Informations P2P.
M3	Attaques protocolaires visant les communications TLS Serveur AM – UTL. *Événements redoutés couverts* : • *Acceptation d'un badge authentique non déclaré.* • *Acceptation d'un badge authentique déclaré non autorisé.* • *Usurpation/clonage d'un badge.* • *Altération d'un évènement système (log).*	Biens contenus dans les échanges : règles de contrôle d'accès, règles de configurations, identifiants, PIN code, logs.

ID	Attaques	Biens impactés
M4	Attaques protocolaires visant les communications TLS UTL - UTL. *<u>Événements redoutés couverts</u> :* • *Incohérence des informations P2P.*	Biens contenus dans les échanges : informations P2P
M5	Attaques logicielles sur les interfaces exposées visant à provoquer un déni de service afin d'empêcher la mise à jour de la base de données ou impacter le réseau hôte. *<u>Événements redoutés couverts</u> :* • *Perte de disponibilité de l'équipement / compromission de la disponibilité du réseau hôte.*	Biens contenus dans la base de données: règles de contrôle d'accès, règles de configurations, identifiants, PIN code, logs.
M6	Piégeage du lecteur (ex. remplacement) visant à faire sortir les données sensibles ou lancer des attaques contre l'UTL. *<u>Événements redoutés couverts</u> :* • *Usurpation/clonage d'un badge;* • *Mêmes évènements que pour les attaques visant le fonctionnement du Firmware*.	Code PIN des titulaires de cartes *Firmware*
M7	Manipulations physiques du lecteur pour accéder à ses composants internes (avec ou sans arrachement) visant à accéder aux données sensibles ou lancer des attaques contre l'UTL. *<u>Événements redoutés couverts</u> :* • *Usurpation/clonage d'un badge;* • *Mêmes évènements que pour les attaques visant le fonctionnement du Firmware.*	Code PIN des titulaires de cartes, clés de sécurisation RS-485 *Firmware*
M8	Écoute/observations de l'entrée d'un PIN sur le clavier du lecteur visant à en découvrir sa value. *<u>Événements redoutés couverts</u> :* • *Usurpation/clonage d'un badge*	Code PIN des titulaires de cartes
M9	Attaques de l'interface sans contact du lecteur visant à obtenir illégalement un accès. *<u>Événements redoutés couverts</u> :* • *Usurpation/clonage d'un badge* (ex. via attaque par relais)	Identifiant des titulaires de cartes

4.4 Politiques organisationnelles de sécurité

OSP_1 : RGS

La mise en conformité de la cible de sécurité doit suivre les modalités de mise en œuvre de la procédure de validation des certificats électroniques [ANSSI_RGS].

5 Fonctions de sécurité du produit

5.1 SF_1 Protections des communications IP

La protection des communications IP s'appuie sur le protocole Transport Layer Security (TLS) qui permet de garantir une communication sécurisée par une identification mutuelle, l'intégrité et la confidentialité des communications entre deux entités sur un réseau (voir hypothèse H4).

Gestion des clés

Lors de l'enrôlement de l'UTL dans *Security Center*, ce dernier envoie son certificat au serveur hébergeant le rôle Gestionnaire d'Accès. La clé publique contenue dans le certificat est alors sauvegardée dans la base de données du serveur principal (rôle Répertoire). C'est cette clé qui permet au serveur d'établir la liaison TLS; le canal sera chiffré au moyen d'une clé de session dérivée de la clé publique de chaque UTL. Le Gestionnaire d'Accès valide la clé publique pour chaque connexion établie avec une UTL connue (modèle de sécurité TOFU).

Enfin l'authentification du serveur auprès de l'UTL s'effectue par un mot de passe configurable par le client. Genetec recommande d'attribuer un mot de passe unique à chaque UTL. L'UTL génère un *token* utilisé comme identifiant de communication.

Plus de détails sont donnés dans le document [GEN_CRYPTO].

Configuration

La version TLS v1.2 reconnue la plus sécurisée est utilisée pour les communications UTL-serveur et UTL-UTL. Les configurations relatives du serveur et des clients respectent les mesures et recommandations décrites dans le document [ANSSI_TLS]. En particulier, toute demande de connexion selon une version antérieure à 1.1 sera rejetée.

De plus, un mécanisme anti force brute et prévenant les risques d'indisponibilités de l'UTL est mis en place sur l'authentification du canal TLS : deux minutes de délai sont ajoutées après trois tentatives infructueuses.

5.2 SF_2 Contrôle des données entrantes

Interfaces Ethernet

La pré-configuration du firewall Windows par Genetec (voir SF_5) lors de la fabrication usine (voir chapitre 3.2.1 du cycle de vie du produit) filtre les requêtes entrantes pour n'autoriser le trafic que sur les ports attendus et par les entités autorisées limitant ainsi l'accès à des services potentiellement sensibles aux attaquants potentiels.

Plus précisément, les données entrantes acceptées sont les requêtes REST accessibles uniquement après établissement d'un canal TLS.

Interfaces RS-485

Les interfaces RS-485 sont utilisées pour connecter l'UTL aux lecteurs de badges ainsi qu'aux portes.

Pour les lecteurs de badges, le canal peut être configuré de deux manières :

- Mode transparent pur pour déploiement utilisant des lecteurs de badges simples (sans claviers).
- Mode *chiffré+signé* pour déploiement avec lecteurs à clavier.

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.

En ce qui concerne les interfaces avec les portes, une installation adéquate ne permet aucun accès physique à ces liens.

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).

5.3 SF_3 Protections du *Firmware*

La protection du Firmware s'appuie sur une hypothèse d'intégrité (voir hypothèse H2), sur le contrôle des données entrantes (voir SF_2) et sur des mesures environnementales (voir chapitre 4.2.2).

L'UTL offre la possibilité de mettre à jour *Softwire* : les nouveaux paquets constituant la mise à jour logicielle sont protégés en intégrité et l'authenticité est vérifiée (voir détails dans [GEN_CRYPTO]).

La mise à jour, par un mécanisme d'*anti-rollback*, ne permet pas de charger une version précédente du logiciel qui serait moins sécurisée: suite à la réception du package de *Firmware upgrade* et à la vérification de sa signature, la version du package est comparée à la version actuelle. Le processus de mise à jour n'est lancé que si la version reçue est supérieure à la version courante.

5.4 SF_4 Protections des données (UTL)

En complément du système de fichiers NTFS gérés par l'OS (voir hypothèse H2), l'UTL dispose d'une protection matérielle contre la perte d'intégrité accidentelle de données lors de coupures de courant : des condensateurs dédiés garantissent que toute commande d'écriture vers la mémoire flash se terminera avant la mise hors tension.

5.5 SF_5 Durcissement du système d'exploitation

Certaines configurations du système d'exploitation sont réalisées lors de la phase de production de l'UTL (voir chapitre 3.2.1) par Genetec (voir hypothèses H1 et H3).

En particulier :

- L'*autorun* USB est désactivé;
- Le *boot* à partir d'une clé USB n'est pas autorisé;
- Le firewall Windows est préconfiguré pour laisser passer le trafic uniquement sur les ports attendus.

De plus, des *Security Rollups* sont publiés régulièrement par Genetec; l'installation sur une base régulière de ceux-ci est recommandée (voir chapitre 8.3.2 du document [GEN_SC_HG]).

5.6 SF_6 Utilisation de la technologie *MIFARE DESFire*

L'utilisation du protocole *MIFARE DESFire* permet l'identification sécurisée des porteurs de badges et l'authentification sécurisée du badge lui-même (voir détails dans [GEN_CRYPTO]).

De plus, l'utilisation de la fonctionnalité *proximity check* du protocole *MIFARE DESFire* permet de se prémunir des attaques par relai permettant à un attaquant d'utiliser les éléments d'identification et d'authentification d'un titulaire autorisé se trouvant à une grande distance du lecteur.

5.7 SF_7 Protections du lecteur et des communications avec l'UTL

Configuration du lien lecteur - UTL

Un lecteur proposant un clavier pour authentification de l'utilisateur par code PIN doit protéger ses communications avec l'UTL. Dans ce but, deux protocoles sont supportés : OSDP et SSCP (voir détails dans [GEN_CRYPTO]).

Dans les deux cas, l'authenticité, l'intégrité et la confidentialité des communications sont assurées et basées des algorithmes cryptographiques robustes. L'échange de clés maîtres, uniques à chaque lecteur, et à partir desquels des clés de sessions seront dérivées et réalisée de manière sécurisée lors de la phase de mise en service.

Protections relatives au clavier

Une configuration adéquate du canal RS-485 permet de prévenir l'écoute et/ou l'observation des codes entrés sur le clavier des lecteurs.

Stockage des biens

Genetec recommande de configurer les lecteurs de sorte à ce que les clés ne soient pas stockées en mémoire persistante (voir [GEN_ANSSI_CSPN]).

Les lecteurs *STid* en particuliers sont de plus munis d'un accéléromètre pouvant servir à effacer les clés lors de l'arrachement.

6 Couverture de la problématique de sécurité

6.1 Menaces vs Fonctions de sécurité

Menaces	Fonctions de sécurité	SF_1	SF_2	SF_3	SF_4	SF_5	SF_6	SF_7
		TLS	Contrôle données entrantes	Prot. *Firmware*	Prot. Données (UTL)	Durcisse-ment OS	*MIFARE DESFire*	Prot. lecteur
M1	Injections impactant l'exécution du *Firmware*		X	X		X		
M2	Injections impactant le stockage des biens		X		X	X		
M3	Attaques protocolaires TLS (serveur – UTL)	X			X	X		
M4	Attaques protocolaires TLS (UTL – UTL)	X			X	X		
M5	Injections impactant la disponibilité du produit/système	X				X		
M6	Piégeage du lecteur							X
M7	Manipulations physiques sur le lecteur							X
M8	Écoute/observations du clavier du lecteur						X	
M9	Attaques via l'interface sans contact du lecteur						X	

7 Annexes

7.1 Positionnement de l'UTL *Synergis Cloud Link* dans le référentiel ANSSI

L'UTL *Synergis Cloud Link* est conforme au plus haut niveau de sûreté (niveau IV) spécifié dans le ***guide de sécurité des technologies sans-contact pour le contrôle des accès physiques*** [ANSSI_CTRL_ACC].

Niveau de sûreté	Résistance aux attaques logiques	Méthode	Technologie	Caractéristiques
I	-	Identification du badge, ou information mémorisée, ou élément biométrique.	Transpondeurs 125kHz et assimilés, cartes ISO14443 ou ISO15693 sans usage de la cryptographie ou à cryptographie défaillante ou propriétaire.	Facilement clonable
II	L1	Authentification du badge.	Carte ISO 14443, authentification à cryptographie symétrique.	Authentification reposant sur une clef commune; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
III	L2	Authentification du badge, clefs dérivées recommandées.	Carte ISO 14443, authentification à cryptographie symétrique	Authentification reposant sur une clef dérivée d'une clef maîtresse; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
IV	L3	Authentification du badge et du porteur par un second facteur (information mémorisée ou élément biométrique). Clefs dérivées.	Carte ISO 14443, authentification à cryptographie symétrique. Saisie d'un code mémorisé ou d'un élément biométrique.	Authentification reposant sur une clef dérivée d'une clef maitresse; Algorithmes et protocoles d'authentification connus et réputés (3DES, AES).

L'atteinte de ces niveaux de sûreté et de résistance aux attaques logiques est rendue possible grâce à la mise en œuvre des technologies suivantes tel que précédemment décrit :

- Utilisation de badges *MIFARE DESFire*
- Lecteurs de badges RS-485 opérant en mode transparent (Architecture n°1, hautement recommandée)
- Utilisation de cartes *MIFARE SAM AV2* pour stocker les secrets requis par l'UTL
- Chiffrement AES-128 pour les badges *MIFARE DESFire*
- Canaux de communication IP sécurisés avec TLS 1.2; authentification et chiffrement conformes aux recommandations du document [ANSSI_TLS]. Le tableau suivant offre un récapitulatif des recommandations :

Recommandation du guide TLS de l'ANSSI	Conformité Synergis Cloud Link	Description
R1	Oui	Tous les clients et serveurs de la solution Genetec Synergis sont compatibles avec TLS 1.2.
R2	Oui	Les composantes dont dépendent le déploiement TLS peuvent facilement être mises à jour.
R3	Oui	TLS 1.2 est privilégié et TLS 1.1 est accepté. TLS 1.0 et SSLv3 ne sont pas acceptés.
R4	Oui	SSLv2 n'est pas prise en charge.
R5	Oui	Le serveur est authentifié par le client au moyen d'un certificat X.509
R6	Oui	L'emploi d'une suite cryptographique reposant sur un échange de clés Diffie–Hellman éphémère (ECDHE) est privilégié.
R7	Oui	Les échanges de clés par ECDHE sont privilégiés.
R8	Oui	Le chiffrement des messages échangés sur le canal TLS est fait par AES; AES-256 est privilégié.
R9	Oui	Le HMAC protégeant l'intégrité des messages échangés sur le canal TLS est construit avec SHA. Les représentants de la famille SHA-2 (SHA-384 et SHA-256) sont privilégiés.
R10	Oui	Le chiffrement intègre par GCM est disponible avec l'utilisation de certificats avec clés ECDSA.
R11	Oui	Le Synergis Cloud Link supporte plusieurs des suites cryptographiques recommandées par l'ANSSI. La liste exhaustive est disponible dans le document dédié aux mécanismes cryptographiques [GEN_CRYPTO].
R12	Oui	L'ordre de préférence des suites cryptographiques est contrôlée par le Synergis Cloud Link, qui agit comme serveur TLS.
R13	Oui*	L'implémentation TLS est basée sur Microsoft Secure Channel, qui offre le support des extensions supported_groups, signature_algorithms, extended_master_secret et renegotiation_info. L'extension sct est sans objet étant donné que les certificats EV ne sont pas supportés par l'UTL. Enfin, l'usage d'un certificat ECDSA priorise l'emploi du mode de chiffrement GCM; le serveur ne doit pas retourner l'extension encrypt_then_mac dans ce contexte (RFC7366).
R14	S.O.	Ces extensions ne sont typiquement pas utiles dans le contexte d'utilisation du Synergis Cloud Link.
R15	Oui	Aucune de ces extensions n'est utilisée par le Synergis Cloud Link.
R16	Oui	Le générateur d'aléas offert par Microsoft Secure Channel est réputé fiable.
R17	Oui	Le générateur d'aléas offert par Microsoft Secure Channel n'inclut pas de préfixe prédictible.
R18	Oui	La compression TLS n'est pas supportée.
R19	Oui	Les reprises de session TLS sont supportées.
R20	Oui	Les renégociations TLS sont sécurisées au moyen de l'extension renegotiation_info.
R21	Oui	La fonction de hachage utilisée pour la signature du certificat X.509 est SHA-384.
R22	Oui	L'interface de configuration de l'UTL permet de spécifier une période de validité inférieure à 3 ans lors de la génération des certificats X.509.
R23	Oui	Les clés de type RSA et ECDSA sont supportées. Afin d'assurer la protection de l'information au-delà de 2030, leur longueur est de : 3072 bits pour RSA 384 bits pour ECDSA
R24	Oui	L'extension Key Usage est présente, est marquée comme critique.

		L'extension contient la valeur DigitalSignature pour tous les types de clés. Pour une clé RSA, l'extension contient également la valeur keyEncipherment.
R25	Oui	L'extension Extended Key Usage est présente et marquée comme non-critique dans le certificat X.509 présenté par l'UTL; elle contient les valeurs id-kp-serverAuth et id-kp-clientAuth car le même certificat est utilisé pour authentifier comme serveur que comme client (mode peer-to-peer).
R26	Oui	L'interface de configuration de l'UTL permet de spécifier le contenu du champ SubjectAlternativeName contenu dans le certificat X.509 de l'UTL.
R27	Oui	L'UTL Synergis Cloud Link n'offre qu'une seule terminaison TLS à tous ses clients.
R28	Oui	Le certificat X.509 présenté par l'UTL contiendra l'extension AKI dans la mesure où l'autorité de certification l'a incluse.
R29	Oui	Le certificat X.509 présenté par l'UTL contiendra l'extension CRLDP dans la mesure où l'autorité de certification l'a incluse.
R30	Oui	L'emploi d'un certificat X.509 dûment signé par une autorité de certification inclura la chaîne complète et ordonnée, depuis le certificat terminal jusqu'au certificat intermédiaire signé par la racine de confiance. Le certificat de la racine de confiance n'est pas transmis sauf si le certificat terminal est auto-signé.
R31	Oui*	Le certificat X.509 présenté par l'UTL contiendra les informations de révocation telles que fournies par l'autorité de certification ayant signé le certificat. Lorsque l'UTL agit comme client d'une autre UTL (mode peer-to-peer), les mécanismes de révocation sont la responsabilité du gestionnaire d'accès auquel le groupe d'UTLs se rapporte (hors-périmètre).
R32	S.O.	La redondance des moyens de révocation n'est pas la responsabilité de l'UTL.
R33	S.O.	Le comportement en l'absence d'informations de révocation est la responsabilité du client. Lorsque l'UTL agit comme client d'une autre UTL (mode peer-to-peer), la vérification des informations de révocation sont la responsabilité du gestionnaire d'accès auquel le groupe d'UTLs se rapporte (hors-périmètre).
R34	S.O.	Ceci est la responsabilité de l'autorité de certification ayant signé le certificat.
R35	S.O.	Ceci est la responsabilité du client TLS. Lorsque l'UTL agit comme client d'une autre UTL (mode peer-to-peer), la vérification des informations de révocation sont la responsabilité du gestionnaire d'accès auquel le groupe d'UTLs se rapporte (hors-périmètre).

7.2 Utilisation de la technologie *MIFARE*

La solution *Genetec Synergis* utilise la technologie *MIFARE* de NXP afin que les clés de chiffrement protégeant les identifiants ne soient pas exposées en zone non-sécurisée.

D'une part, les badges d'accès (qui sont hors périmètre de la présente évaluation) utilisent la technologie *MIFARE® DESFire* pour stocker l'identifiant de manière sécurisée. Ces badges sont destinés à être lus par des lecteurs RS-485 raccordés directement à l'UTL *Synergis Cloud Link* et faisant partie de la liste fournie à la section 2.2.3 du présent document.

L'authentification des badges et le décryptage des identifiants extraits des badges se fait au niveau de l'UTL, et non au niveau des lecteurs. On parle donc de lecteurs transparents répondant à l'architecture n°1 préconisée dans [ANSSI_CTRL_ACC] et désignée comme « hautement recommandée ».

Pour un maximum de sûreté, les clés cryptographiques ne sont pas chargées directement sur l'UTL, mais plutôt dans des cartes *MIFARE SAM AV2*. Ceci comporte trois avantages considérables sur le plan de la sécurité :

a) Il est pratiquement impossible de voler les clés de chiffrement, même en ayant un accès physique complet à l'UTL.
b) Les clés de chiffrement sont distribuées de manière sécuritaire aux UTL, les cartes SAM jouant le rôle de transport physique entre la station de production et le lieu d'installation final.
c) Les clés de chiffrement ne sont pas exposées dans le cas de recyclage de l'UTL ou en cas d'un échange sous garantie.

L'emploi combiné des technologies MIFARE DESFire et MIFARE SAM AV2 implique que certaines manipulations soient conduites préalablement à la mise en service du système. Ces étapes sont :

1) Production des cartes SAM destinées aux UTL

   Cette opération est réalisée par un responsable sûreté habileté qui agit aussi à titre de gardien des secrets. Elle a lieu au niveau d'un poste de production dédié et est totalement indépendante de la configuration et du déploiement du système de contrôle d'accès. La note d'application [GEN_SYAN_MIFARE] couvre en détail les étapes de la production des cartes SAM afin de garantir leur compatibilité avec la solution *Genetec Synergis*.

2) Production des SKB destinés aux stations d'encodage de badges *DESFire*

   Les encodeurs de table USB *STid ARC-G* requièrent que les secrets soient chargés au moyen d'un *Secure Key Bundle* (SKB). Il est possible de créer un SKB à partir d'un badge *DESFire* vierge et de l'application *SeCard* de *STid*. Cette opération est également réalisée par un responsable sûreté habileté qui agit aussi à titre de gardien des secrets.

3) Encodage des badges *DESFire*

Cette opération est réalisée au niveau d'un poste d'encodage; il peut exister de multiples stations d'encodage pour un même système *Genetec Synergis*. Les stations d'encodage doivent être sous le contrôle de responsables sûreté habiletés, mais ces responsables n'ont pas à être gardien des secrets. Leur rôle est limité à traiter les demandes de création de badges; les encodeurs mis à leur disposition contiennent déjà les secrets nécessaires au formatage des badges *DESFire* et à l'encodage des identifiants.