elsylog
Parc d'activités des Berges de Seine 3
10-12 rue Marcel Paul - 96870 Bezons
Fax : +33 (0)1.39.61.57.59 - accueil@elsylog.com
+33 (0)1.39.61.05.80 www.elsylog.com

Cible de sécurité gamme COSMOS

Cosmos / Syrius / Orion

PROJET CORNAC

30/01/2021

Date	Ver.	Motif	Rédacteur
01/08/2018	V1.0	Version initiale	OPPIDA
25/10/2018	V1.1	Correction des versions des logiciels	OPPIDA
04/07/2019	V1.2	Mise à jour des versions logiciels Ajout d'une hypothèse manquante sur la protection en intégrité,confidentialité et authenticité de la clé diversifiée stockée dans le badge desfire. Ajout d'une hypothèse manquante sur les exploitants. Retrait, du dialogue badge desfire / lecteur, du périmètre de certification Ajout d'une protection en intégrité sur la fonction F.PROTEC_COM_RS485 Ajout de traçabilité entre menaces,biens et fonctions de sécurité. Ajout d'une hypothèse H_INJECTION_CLE_SSCPV2 et de la fonction F_PROTECT_FIRMWARE. Modification de F_PROTECT_CODE_PIN, F_PROTECT_UTL et M.PHYS_UTL	ELSYLOG
28/01/2020	V1.3	Modification de la version (devient 1660f) du firmware utl dans le tableau "Configuration évaluée". Nouveau firmware pour parer au problème de l'attaque relai.	ELSYLOG

22/01/2021	V1.4	Mise jour du document avec la solution full web COSMOS des UTL(s) Orion et Syrius (version IP et RS-485). Nom de projet CORNAC Ajout des menaces M.PHYS_UTL_BPS et M.PHYS_UTL_EFF, M.INTERCEPT_GAC_AUTHEN, M.INTERCEPT_GAC_ROLE M.ACCES_GAC_BD Ajout des hypotèses : H_POSTES_CLIENTS, H_CERTIFICATS, H_SYSYMES_EXPLOITATION, H_RADIUS Ajout des biens sensibles B.K_SESSION_ENC_COM_UTL_SERVER, B.K_SESSION_DEC_COM_UTL_SERVER, B.K_SESSION_CMAC_COM_UTL_SERVER, B.K_CHIFFRE_BD, B.K_FIRMWARE Ajout des protections F_PROTECT_AUTHENCOM_UTL_COMET F_PROTECT_BPS, F_PROTECT_EFF_ACCES, F_PROTECT_GAC_AUTHENT,F_PROTECT_GAC_BD, F_PROTECT_PROFILS_GAC, F_PROTECT_COM_CLIENT	ELSYLOG
31/05/2021	V1.5	Mise à jour avec les dernières versions des logiciels et matériels. Sélection sur la partie graphique du lien UTL/tête de lecture comme faisant partie du périmètre d'évaluation. Ajout versions des SAM AV2/AV3 et Desfire EV3.	

22/07/2021	V1.6	Mise à jour du tableau des biens sensibles pour B.PINCODE. Ajout de la description de B.K_CODE_PIN. Ajout de B.K_SESSION_SYNC_COM_UTL_SERVER Mise à jour de B.ROLE et B.BD dans le tableau des biens sensibles	
02/12/2021	V1.7	Mise à jour de la version Syrius/Orion en conformité avec la version affichée lors de l'évaluation. Ajout des références cartes SAM AV2/AV3 dans la liste des éléments de la TOE. Ajout d'un complément de description sur l'hypothèse H.LAN_SUP_SECU Ajout d'un item sur le support et mise à jour. Ajout des menaces paragraphe 4.4.1 postes client / UTL IP - Comet/UTL IP et Serveur web UTL. Ajout de l'hypothèse H.Configuration, de la menace M_SERVEUR_WEB_LANTRONIX et de la sécurité F_PROTECT_LANTRONIX et mise à jour du tableau. Complément sur H.SYSTEMES_EXPLOITATION Ajout de l'hypothèse H_NXP Ajout du serveur Cosmos dans le périmètre graphique. Ajout d'une hypothèse sur les fonctions cryptographiques de windows H.CRYPTO_WINDOWS	

Liste de diffusion

Nom	Prénom	Société	Contact
-	-	ANSSI	-
MARY	Olivier	OPPIDA	olivier.mary@oppida.fr
ZAHM	Vincent	ELSYLOG	vincent.zahm@elsylog.com
LAVENU	Bertrand	ELSYLOG	bertrand.lavenu@elsylog.com
PELLERIN	Philippe	ELSYLOG	philippe.pellerin@elsylog.com

Table des matières

1 IDENTIFICATION DU PRODUIT

Ce document constitue la cible de sécurité pour une évaluation CSPN du système de contrôle d'accès COSMOS développé par la société ELSYLOG.

Editeur	ELSYLOG
Site de l'éditeur	https://www.elsylog.com
Nom commercial du produit	COSMOS
Version évaluée	4.6.0.96
Catégorie de produit	Identification, authentification pour le contrôle d'accès physique

2 ARGUMENTAIRE DU PRODUIT

2.1 DESCRIPTION GÉNÉRALE DE LA GAMME COSMOS

La gamme Cosmos est une solution intégrée pour une gestion centralisée de contrôle d'accès physique.
Elle se compose :

- d'un GAC Cosmos assurant la gestion des UTL(S) et la saisie des différents paramètres nécessaires au fonctionnement sécurisé du système.
- d'UTL(S) Syrius assurant la sécurisation de 2 portes séparées ou 1 porte en entrée / sortie.
- d'UTL(S) Orion assurant la sécurisation de 4 portes séparées.

Il est à noter que le firmware des 2 types de matériel est identique mise à part la gestion logique et physique des accès supplémentaires. Les fonctions cryptographiques sont sous forme de librairie ou hardware et communes aux deux équipements.

Le produit est architecturé autour d'équipements décrits ci-dessous son but est de filtrer les flux des personnes, autorisées ou non à pénétrer sur un site, un bâtiment ou des locaux.
Les fonctionnalités suivantes sont nécessaires au bon fonctionnement du système :

- Identification par badge RFID (sans contact) et authentification PIN code.
- Les droits d'accès sont gérés au niveau des unités de traitement (UTL).
- Les actions d'accès (déverrouillage, séquencements d'opérations de contrôle de l'ouvrant, état de l'accès physique) sont gérées aux droits des l'UTL(S).
- La tête de lecture déportée est seule accessible vis à vis de l'extérieur.

Le système de contrôle d'accès COSMOS est composé de :

- Badges Mifare Desfire EV1/EV2, norme ISO 14443. Le mode transparent ainsi qu'une détection automatique de la technologie EV2, permet d'utiliser le « Secure messaging » et la vérification de la proximité entre le badge et la tête de lecture.

- Lecteurs de Proximité MIFARE DESFIRE (Modèle SYL123-S-ARCDES), compatibles avec tous les identifiants Mifare sécurisés Classic - Mifare Plus - Desfire EV1/EV2 ISO 14443 A et B ISO 18092 - Portée de lecture 5 cm environ.

  Dans le cadre de l'évaluation la cible sera constituée de lecteurs de badges DESFIRE (SY-DES4ko) et badges MIFARE DESFIRE EV1/EV2.

- Raccordés sur des unités de traitement SYRIUS 2P2L-EXT : gestion de 2 ou 4 accès
  Ces UTL acceptent en standard, le raccordement sur un réseau TCP/IP ou RS-485

- Raccordés sur des unités de traitement ORION 4P-8L-EXT : gestion de 8 têtes de lecture en entrées/sorties
  Ces UTL acceptent en standard, le raccordement sur un réseau TCP/IP ou RS-485

Comet :
PC industriel équipé d'une à huit voies 485.
Il converti les trames IP en 485, assure le polling des UTL et la mise à jour des anti-pass-back

- Les unités de traitement embarquent une carte SAM AV2/AV3 NXP permettant la gestion et la sécurisation des clés utilisées dans le cadre des communications chiffrées avec le badge, ainsi que celles nécessaires à la communication chiffrée avec le serveur.

- Les informations enregistrées par les unités de traitement sont centralisées par notre logiciel COSMOS full web.
  Configuré en multiposte il permet l'accès à plusieurs opérateurs en simultané.

- Un certain nombre de modules peuvent être ajoutés dans le logiciel COSMOS afin de gérer des éléments particuliers (Ascenseurs, Personnalisation de badges, …)

- Le système est administré via des postes clients légers équipés d'un lecteur encodeur / enrôleur (Modèle OMNIKEY 5422 compatible PCSC) permettant aux opérateurs, outre d'encoder les badges, d'accéder, sur simple lecture de leur badge, au logiciel de façon rapide, d'effectuer les fonctions d'activation et de rendu de badge, d'identifier un badge du site trouvé (numéro de série des badges non sérigraphié).

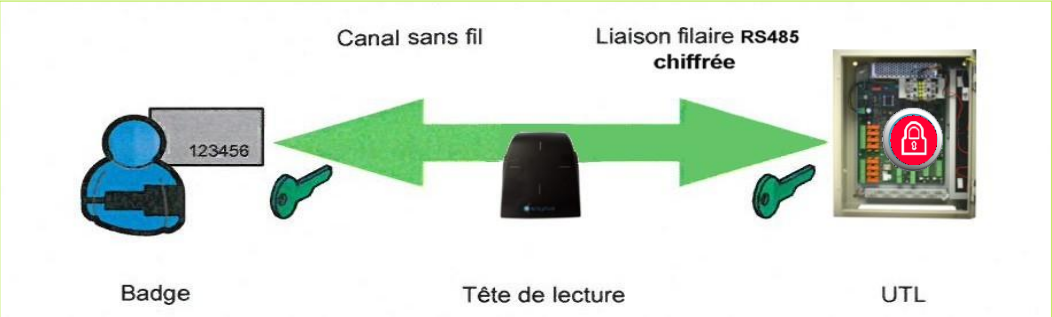
Le lecteur encodeur/enrôleur utilise une carte SAM assurant la sécurité des clés d'accès aux badges DESFIRE.

- La solution est couverte un support hot line de premier niveau. Les formations, mises à jour logiciels et support de haute disponibilité sont disponibles par options dans nos contrats de maintenance. Une prise en main à distance est envisageable aux conditions du clients final.

2.2 DESCRIPTION FONCTIONNELLE DU PRODUIT

2.2.1 Le mode transparent.

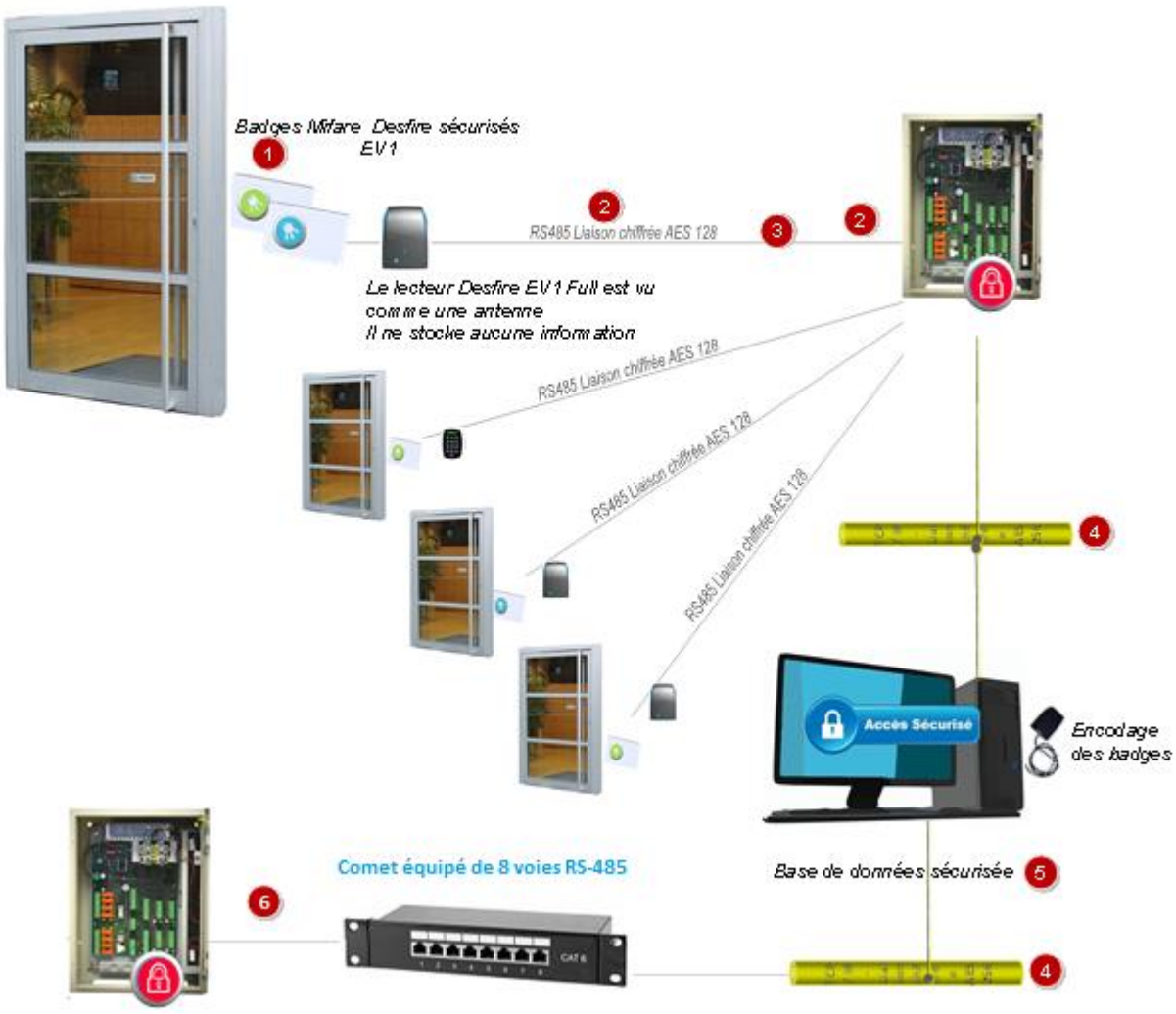
Le système de contrôle d'accès COSMOS repose sur l'utilisation du mode transparent des lecteurs de badges. Ce mode de fonctionnement est préconisé par l'ANSSI.



Dans ce mode de fonctionnement, les clés de chiffrement de la communication entre le badge et l'UTL ne sont pas stockées dans la tête de lecture mais dans l'UTL. En l'occurrence dans la carte SAM pour le sujet qui nous concerne.

2.2.2 Architecture générale

Le schéma ci-dessous présente l'architecture générale du système COSMOS



1. **Badge Mifare Desfire EV1/EV2, norme ISO 14443,**

2. **Maillon Lecteur / UTL :**

   Le lecteur transparent garantit que les clefs d'accès aux données des badges ne se trouvent pas dans le lecteur lui-même, mais stockées dans la carte SAM de l'UTL (Unité de Traitement Locale) placée en zone sécurisée à l'intérieur du bâtiment. Le risque de se voir dérober un lecteur contrôlant un accès périmétrique du site contenant des informations sensibles n'existe plus.

3 **Maillon communication entre le lecteur et l'UTL :**

La liaison entre le lecteur et l'UTL est assurée via une interface RS-485. Sur cette liaison est mis en œuvre un chiffrement des données en AES128 (voir protocole SSCPV2 Stid). Le mode transparent étant utilisé un double chiffrement est donc effectué. La détection automatique du type **EV2** active le **« Secure messaging »** et ajoute une sécurité d'authentification au protocole.

4 **Maillon Réseau IP :**

Liaison chiffrée impérative aujourd'hui, le réseau IP étant devenu un standard de communication dont les multiples moyens d'écoute représentent une vulnérabilité certaine : afin de résoudre cette faille de sécurité potentielle, ELSYLOG chiffre toutes les données entre les UTL et le serveur (chiffrement AES 256 + CMAC 256 encapsulé dans un chiffrement TLS 1.2, support 802.1X et X509 pour l'authentification, gestion de certificat) intégrant un mécanisme d'anti-rejeu.

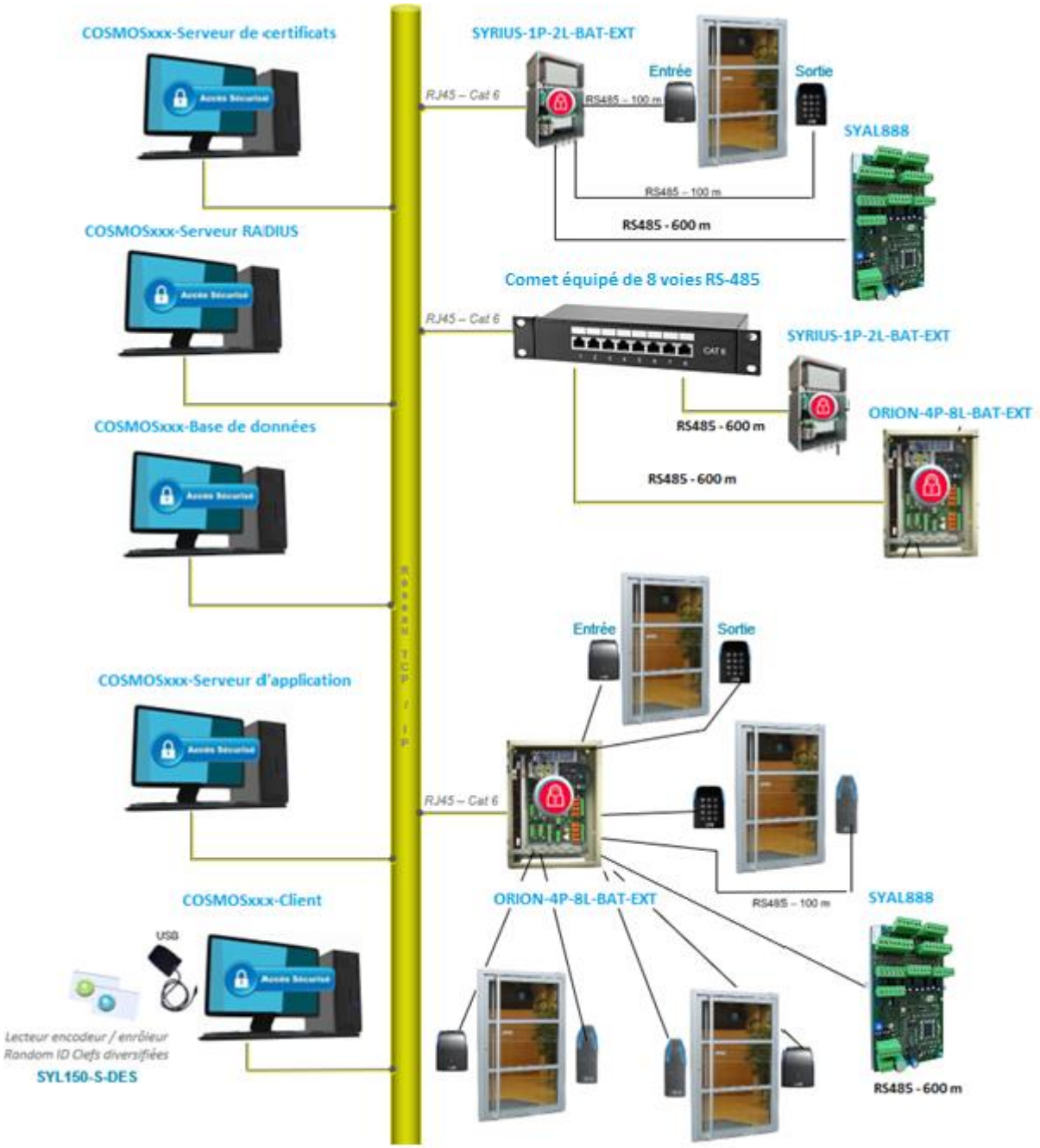
5 **Maillon Serveur :**

Nous préconisons l'installation du logiciel sur une machine virtuelle et assurons une exploitation avec une base de données sécurisée SQL SERVER. Dans le cas où la base de données est désolidarisée du serveur d'application, le flux SQL TLS assure la confidentialité des échanges.

6 **Maillon bus de terrain RS-485 (4 fils) :**

Liaison chiffrée impérative aujourd'hui, le réseau RS-485 entre UTL et serveur est protégé (chiffrement AES 256 + CMAC AES 256) intégrant un mécanisme d'anti-rejeu.

Le schéma ci-après présente l'implantation logique d'une installation typique de COSMOS



SYL123-S-ARC1-DESF SYL123-S-ARCDESF SYL123-S-ARCDESF-C

2.2.3 Tête de lecture 13,56 MHz Stid – RS485 - Architect

- Tête de lecture, déportée de l'électronique de gestion de l'accès (UTL) évolutive (option faces multifonctions interchangeables)
  Réf. Modèle standard : SYL123-S-ARCDESF
  Réf. Modèle de faible encombrement pour montants de porte : SYL123-S-ARC1-DESF.
- Lecture de tous les identifiants normés 13,56 MHz Mifare Classic, Mifare Plus et Desfire EV1/EV2, pouvant assurer le basculement progressif d'une technologie à l'autre.
- Lecteur de Très Haut Niveau de Sécurité (AES 128 protocole SSCPV2)
- Fonctionnement mode transparent.
- Numéro de badge encodé avec des clefs de sécurité privées et transmis par l'UTL sur une liaison sécurisée RS-485 (confidentialité des données transmises par chiffrement et authentification).
- Portée de l'ordre de 5 cm selon le type d'identifiant et d'environnement
- Fonctions Badgez, Accès autorisé, Accès refusé, position de la porte (ouverte / fermée) et mode de gestion de l'accès (libre, interdit) matérialisées par 1 buzzer et 1 leds à 3 couleurs.
- Solution d'autoprotection et d'anti-arrachement intégrée
- Modèle robuste et protégé des intempéries pour intégration dans tous types d'environnement.
- Boîtier compact : capot démontable et interchangeable (option faces multifonctions interchangeables) – IP 65 hors connectique – IK 10.
- Excellente résistance à la poussière, à l'humidité et au vandalisme grâce à sa coque en polycarbonate renforcée et sa carte électronique tropicalisée.
- Raccordement aisé par bornier à vis débrochable.
- Arrachement détecté par un accéléromètre configurable par badge (sortie contact sec).

2.2.4 Tête de lecture 13,56 MHz Stid – RS485 – Architect avec clavier

- Têtes de lecture déportées de l'électronique de gestion de l'accès (UTL) avec clavier : Boîtier compact et résistant (antenne et contrôleur / décodeur totalement encapsulés dans de la résine)
  Réf SYL123-S-ARCDESF-C
- Fonctionnement possible sur plages horaires en Badge + Code secret pour augmenter le niveau de sécurité dans l'identification du badge.
  - « Badge seul » pour tous.
  - « Code seul » pour tous.
  - « Badge ou code seul » selon.
  - « Badge et code seul » selon.
- Proximité 13,56 MHz Mifare sécurisé Classic - Mifare Plus - Desfire EV1/EV2 ISO 14443 A et B ISO 18092 (NFC) pour projets multi-applicatifs.
- Portée 4 à 6 cm selon l'identifiant et l'environnement.
- Lecteur de Très Haut Niveau de Sécurité (AES 128 protocole SSCPV2)
- Fonctionnement mode transparent.
- Numéro de badge encodé avec des clefs de sécurité privées et transmis par l'UTL sur une liaison sécurisée RS485 (confidentialité des données transmises par chiffrement et authentification).
- Fonctions Badgez, Accès autorisé, Accès refusé, position de la porte (ouverte / fermée) et mode de gestion de l'accès (libre, interdit) matérialisées par 1 buzzer et 3 Leds.
- Grande robustesse en environnements intérieurs ou extérieurs et haut niveau de résistance au vandalisme (boîtier compact, clavier étanche, coque autoextinguible, antenne et contrôleur / décodeur encapsulés dans de la résine).
- Raccordement aisé par bornier à vis.

- Arrachement détecté par un accéléromètre configurable par badge (sortie contact sec)

2.2.5 Unité de traitement 1 à 8 lecteurs – RS485 ou IP

Réf. **SYRIUS 2P2L-EXT-BAT / ORION-4P8L-EXT-BAT**

Gestion locale par lecteur adaptée à chaque configuration d'accès :

- ❖ 1 lecteur : 40 000 badges autorisés et 1 024 événements
- ❖ 2 lecteurs : 20 000 badges autorisés et 1 024 événements
- ❖ 3 à 4 lecteurs ; 10 000 badges autorisés et 1 024 événements

Photo non contractuelle

- Temps de traitement d'un badge : < 1 seconde.
- Alim. 220 V à découpage + bat. 12V 12Ah (3 A dispo sous 12 V).
- Prise de décision locale, sans dégradation du niveau de sécurité en cas de rupture de dialogue avec le système de gestion.
- Génération de l'événement correspondant et diffusion au système de gestion en temps réel.
- Raccordement au système de gestion via IP ou RS-485.
- Gestion classique ou évoluée des accès (sas, ascenseur, parking …)
- Armoire métallique fermée à clef - IP 55-9.
- Plaque support presse étoupes prédécoupées pour sorties de câbles (12 presse étoupes ø 9, 11, 13 mm).
- Raccordements par borniers à vis embrochables.
- Circuit horloge calendaire sauvegardé.
- Contact d'autoprotection du coffret.
- B.P.S et surveillance de l'accès protégés par des entrées équilibrées.

Ces UTL(S) peuvent gérer en standard jusqu'à 8 têtes de lecture en mode 4 portes entrée/sortie. Dans cette configuration, elles permettent de mémoriser localement jusqu'à 10 000 badges autorisés et 1 024 événements par tête raccordée.
Le même modèle permet un raccordement au système de gestion via bus terrain RS-485 ou via réseau TCP / IP

2.2.6 Comet équipé de 8 voies RS485

- Permet la conversion IP / RS485 sur 8 voies séparées 16 UTL par canal
- Assure la collecte des évènements et les transmet vers le serveur
- Assure la mise à jour des anti-pass back
- Assure les automatismes en cas de coupure du serveur.

2.2.7 Contrôle d'accès COSMOS

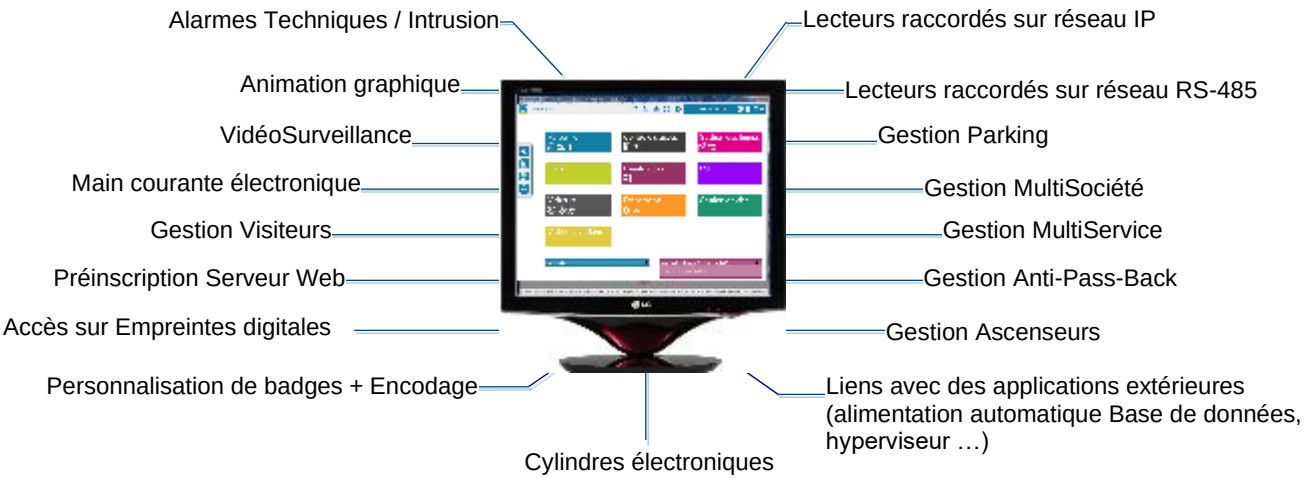
- Solution haut de gamme de Contrôle d'accès multi-poste
- Ergonomie intuitive accompagnée d'une aide en ligne (touche F1)
- Environnement Microsoft Windows 64 bits

  Principe réseau : support Ethernet avec protocole TCP/IP (architecture full web).

- Conception modulaire :

  ❖ Licences pour 8, 16, 32, 64, 128, 512, 896 ou 2 048 lecteurs gérés

  ❖ Nombreuses fonctionnalités :



2.2.8 Caractéristiques des serveurs et des postes d'exploitation

Gestion OFF Line
Avec mise à jour des droits d'accès via Notebook et / ou Borne de mise à jour
Aperio - Dorma

Gestion ON Line
Avec mise à jour des droits d'accès directe depuis COSMOS
Aperio - UZ

	< 16 lecteurs – 300 badges	< 128 lecteurs – 1 000 badges		> 128 lecteurs – 1 000 badges	
	Monoposte	**Serveur**	**Client**	**Serveur**	**Client**
Processeur	**Intel I3** ou équivalent et >	**Intel I5** ou équivalent et >	**Intel I3** ou équivalent et >	**Intel I7** ou équivalent et >	**Intel I3** ou équivalent et >
Mémoire RAM	**4 Go pour les postes clients et 16 Go pour le serveur**				
Disque dur	**250 Go pour postes clients et 500 Go SSD pour Serveur**				
Ecran	**Pour COSMOS seul : 17 pouces et >** **Pour COSMOS (intrusion, synoptiques) : 21 pouces et Résolution selon les plans**				
Périphériques	**USB, COM1, COM2** – Fonction des équipements retenus pour le poste : **concentrateur (RS232C**), **lecteur enrôleur (USB ou RS232C)**, imprimante Rapports etc… ***Prévoir une unité de sauvegarde (données, historique) : Disque dur externe, graveur, clef USB …***				

	Poste Serveur 64 bits	Poste Client 64 bits
Environnement Windows	**Windows Serveur 2012** **Windows Serveur 2016** **Windows Serveur 2019**	**Windows 10**

3 CONTEXTE D'EVALUATION

3.1 PÉRIMÈTRE D'ÉVALUATION

La ToE est composée des éléments physiques suivants :

- Badges Mifare Desfire EV1/EV2, norme ISO 14443.
- Lecteurs de Proximité MIFARE DESFIRE (Ref Esylog : SYL123-S-ARCDESF – Ref Stid : ARC A), (Ref Elsylog : SYL123-S-ARCDESF-C -Ref Stid : ARC B) raccordées sur des unités de traitement SYRIUS/ORION via une liaison RS485.
- UTL SYRIUS (SYRIUS-2P2L-IP-EXT v1661z) et ORION (ORION-4P8L-EXT v1661z) raccordées au serveur COSMOS via un bus de terrain RS-485 ou un réseau IP. Les UTL(S) disposent d'un module de sécurité SAM AV2/AV3 de la société NXP. Ce module hérite d'une certification Critères Communs EAL5+.

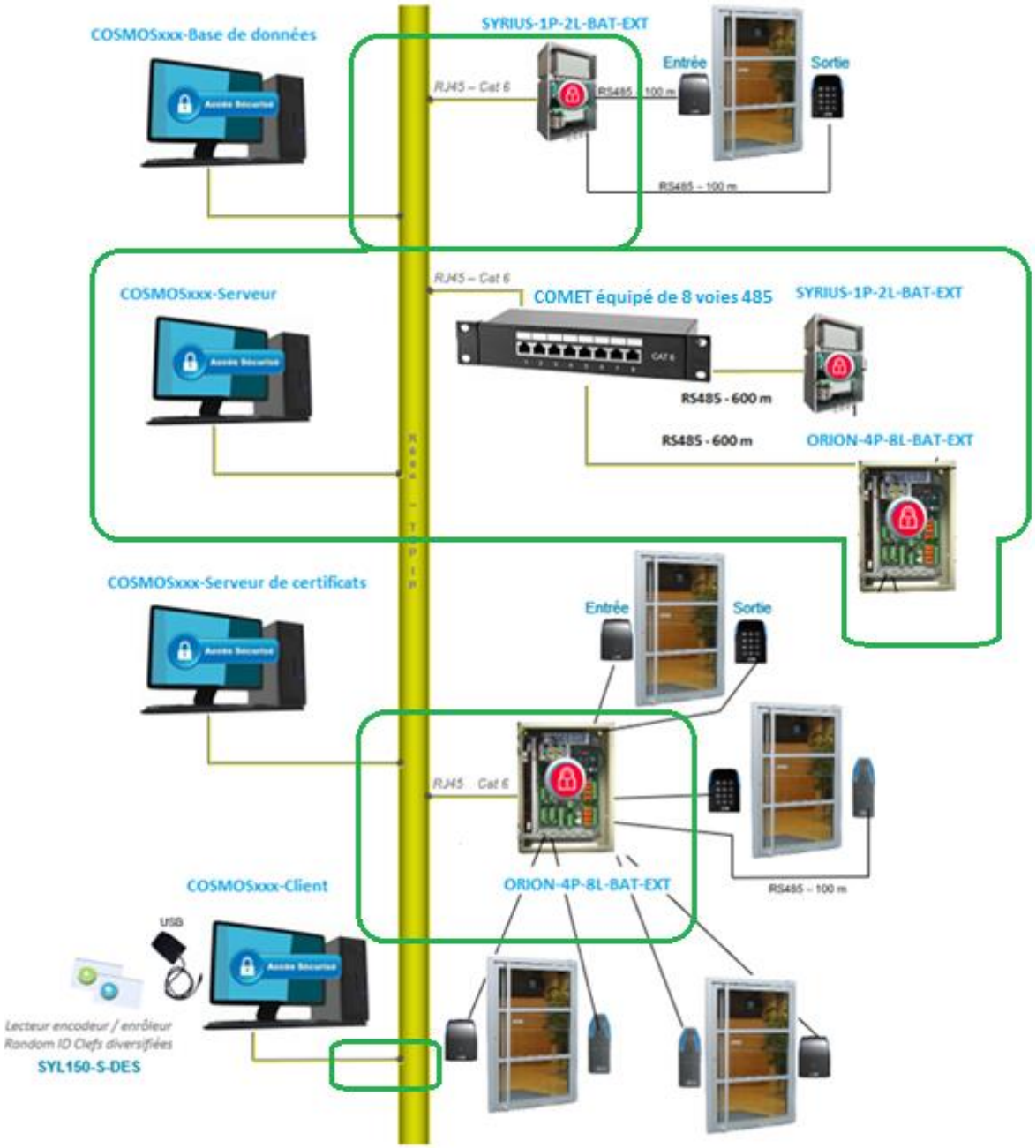
La carte SAM et le badge DESFIRE ne font pas partie du périmètre d'évaluation.

L'interface de communication entre le badge et la tête de lecture ne fait pas partie du périmètre d'évaluation.

Les interfaces de la ToE suivantes font partie du périmètre de l'évaluation :

- Interface de communication entre les lecteurs de proximité et l'UTL (RS485).
- Interface de communication entre l'UTL et Comet (réseau IP).
- Interface de communication entre Comet et le serveur COSMOS (réseau IP).
- Interface de communication entre Comet et les UTL(s) (bus de terrain 485).
- Le GAC Cosmos.

Le périmètre d'évaluation est représenté en vert sur le schéma ci-dessous :



 SYL123-S-ARC1-DESF

 SYL123-S-ARCDESF

 SYL123-S-ARCDESF-C

Composant 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**		X	
	Applicatifs: **Authentication GAC** **Rôles utilisateurs** **Logs**	X X X		
	Fonctions cryptographiques	X		
	Bases de données et annuaire: **Authentification BD** **Transport des données entre serveur et BD**	X X		
	Serveur RADIUS		X	
	Certificats		X	
	Système d'exploitation	**NON CONCERNE OS INEXISTANT**		
	Applicatifs	X		

UTL	**Fonctions cryptographiques**	**X**		
	Certificats		**X**	
LECTEURS	**Lecteurs simples**	**X**		
	Lecteurs-clavier	**X**		
BADGES			**X**	

3.2 DÉTAIL SUR LA SÉCURITÉ DES ECHANGES

3.2.1 Cosmos Serveur / Cosmos base de données

- TLS 1.2
- Renouvellement des clés de session
- Support x509

3.2.2 Cosmos serveur / Cosmos client

- HTTPS
- TLS 1.2
- Renouvellement des clés de session

3.2.3 Cosmos Serveur, UTL IP et Comet sont tous:

- Authentifiés par un serveur RADIUS

3.2.4 Cosmos Serveur / Comet

- TLS 1.2
- Support x509
- Renouvellement des clés de session

3.2.5 Comet / UTL interface IP

Protocole propriétaire Els V6 sécurisé (double chiffrement) par

- Encapsulation TLS 1.2 de
  - Chiffrement AES 256
  - Signature CMAC AES 256
- Support de 802.1X et X509
- Renouvellement des clés de session
- Protection contre le rejeu de trames

3.2.6 Comet / UTL interface 485

Protocole propriétaire Els V6 sécurisé par

- Chifffement AES 256
- Signature CMAC 256
- Renouvellement des clés de session
- Protection contre le rejeu de trames

3.2.7 UTL / têtes de lecture (mode transparent norme iso 14443 – A)

- Chiffrement AES 128
- Signature CMAC 128
- Renouvellement des clés de session à chaque authentification.
- Protocole STID SSCPV2
- Pour les versions EV2 (détection automatique). Le protocole “Secure messaging”, offrant une sécurité d’authentification, est encapsulé dans le protocole STID SSCPV2

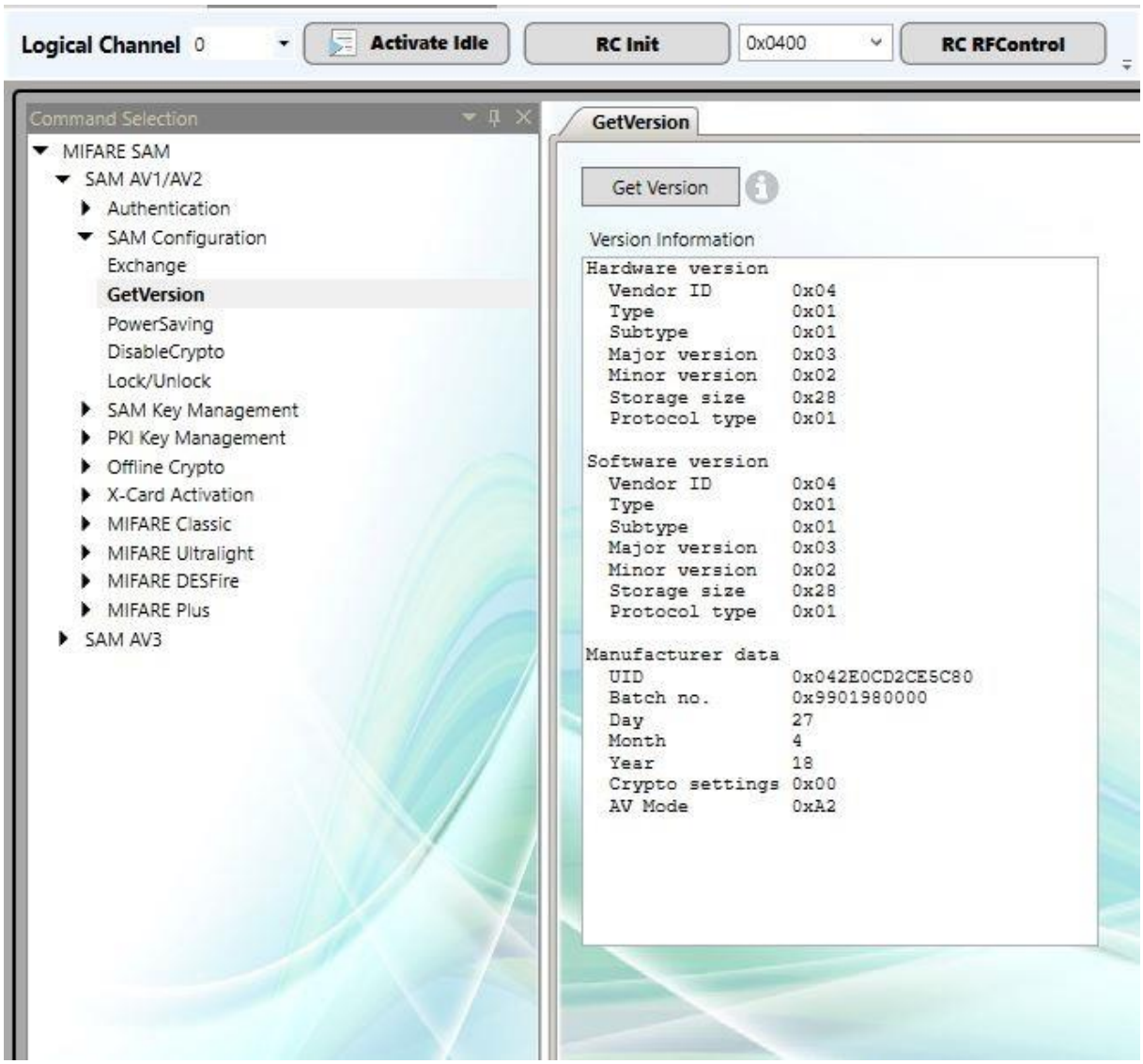
3.3 CONFIGURATION ÉVALUÉE

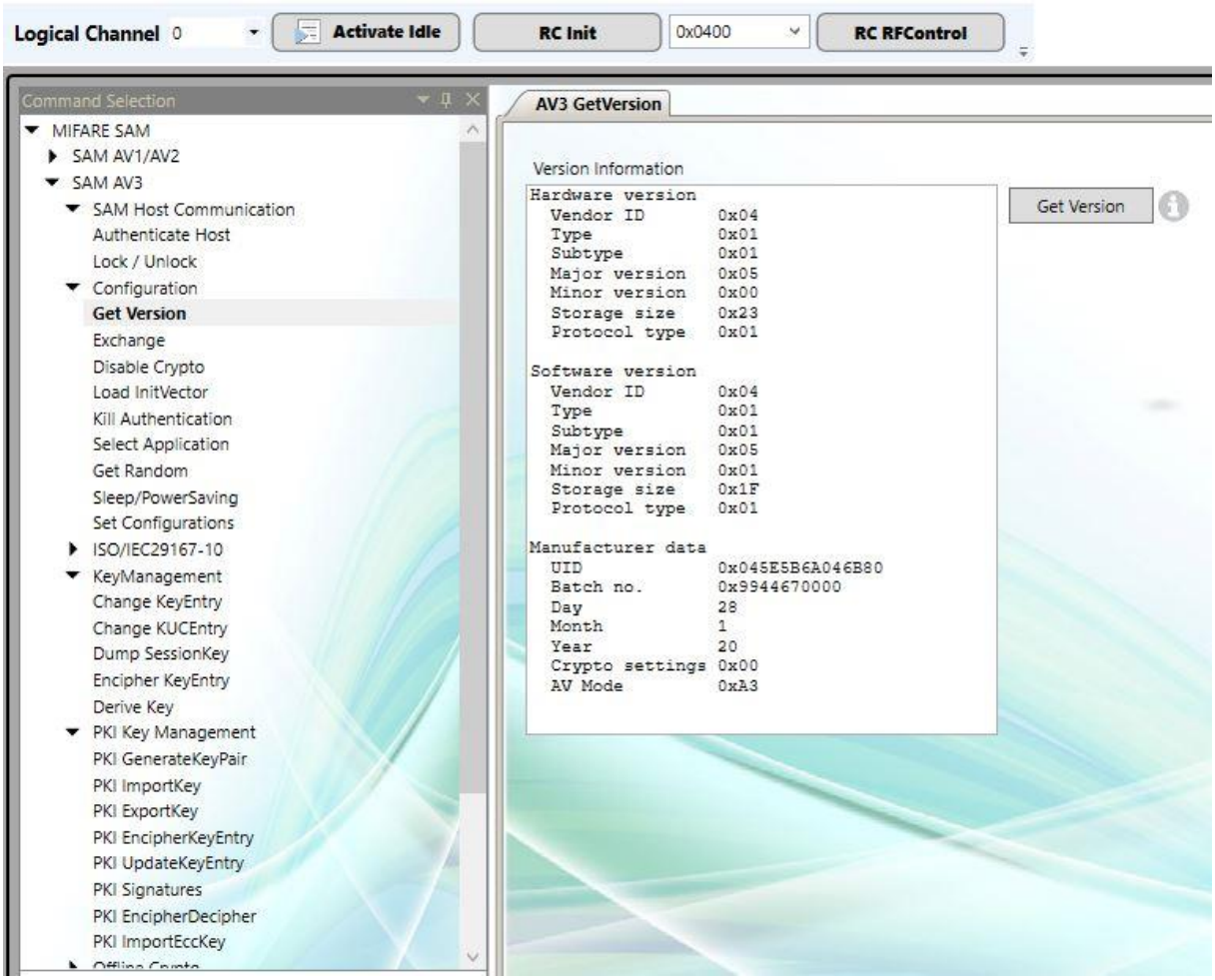
La configuration évaluée est détaillée au sein des tableaux ci-dessous :

Solution	COSMOS
Version	4.6.0.96
Editeur	Elsylog
Site Web	https://www.elsylog.com
Type de produit	Contrôle d’accès et gestion des temps

Nomenclature des composants retenus pour l’évaluation :

Description	Nom	Fabricant	Modèle / Version
Lecteur de proximité	Lecteur simple	STID	ARC A
	Lecteur avec clavier	STID	ARC B
Unité de traitement	SYRIUS 2 Portes	ELSYLOG	Firmware: SYRIUS-2P2L-EXT version 1661z PCB: 181101 ind. D
	ORION 4 Portes	ELSYLOG	Firmware: ORION-4P8L-EXT version 1661z PCB: 180102 Ind. D
Concentrateur	COMET	ELSYLOG	Comet version 4.1.0.86
Badges		NXP	Mifare Desfire EV1/EV2/EV3
SAM		NXP	SAM AV2 P5DF081 SAM AV3 MF4SAM30


Logical Channel 0
Activate Idle
RC Init
0x0400
RC RFControl
Command Selection
MIFARE SAM
SAM AV1/AV2
Authentication
SAM Configuration
Exchange
GetVersion
PowerSaving
DisableCrypto
Lock/Unlock
SAM Key Management
PKI Key Management
Offline Crypto
X-Card Activation
MIFARE Classic
MIFARE Ultralight
MIFARE DESFire
MIFARE Plus
SAM AV3
GetVersion
Get Version
Version Information
Hardware version
Vendor ID 0x04
Type 0x01
Subtype 0x01
Major version 0x03
Minor version 0x02
Storage size 0x28
Protocol type 0x01
Software version
Vendor ID 0x04
Type 0x01
Subtype 0x01
Major version 0x03
Minor version 0x02
Storage size 0x28
Protocol type 0x01
Manufacturer data
UID 0x042E0CD2CE5C80
Batch no. 0x9901980000
Day 27
Month 4
Year 18
Crypto settings 0x00
AV Mode 0xA2


Logical Channel 0
Activate Idle
RC Init
0x0400
RC RFControl
Command Selection
MIFARE SAM
SAM AV1/AV2
SAM AV3
SAM Host Communication
Authenticate Host
Lock / Unlock
Configuration
Get Version
Exchange
Disable Crypto
Load InitVector
Kill Authentication
Select Application
Get Random
Sleep/PowerSaving
Set Configurations
ISO/IEC29167-10
KeyManagement
Change KeyEntry
Change KUCEntry
Dump SessionKey
Encipher KeyEntry
Derive Key
PKI Key Management
PKI GenerateKeyPair
PKI ImportKey
PKI ExportKey
PKI EncipherKeyEntry
PKI UpdateKeyEntry
PKI Signatures
PKI EncipherDecipher
PKI ImportEccKey
AV3 GetVersion
Version Information
Hardware version
Vendor ID 0x04
Type 0x01
Subtype 0x01
Major version 0x05
Minor version 0x00
Storage size 0x23
Protocol type 0x01
Software version
Vendor ID 0x04
Type 0x01
Subtype 0x01
Major version 0x05
Minor version 0x01
Storage size 0x1F
Protocol type 0x01
Manufacturer data
UID 0x045E5B6A046B80
Batch no. 0x9944670000
Day 28
Month 1
Year 20
Crypto settings 0x00
AV Mode 0xA3
Get Version

4 DEFINITION DU PROBLEME DE SECURITE

4.1 UTILISATEURS DU PRODUIT

Usager porteur de badge

Il s'agit de l'utilisateur final du système de contrôle d'accès. L'usager porteur de badge interagit avec la tête de lecture et se voit octroyer des droits d'accès en fonction de son profil. L'interaction avec le lecteur de badge peut se faire de deux manières : présentation simple du badge ou présentation du badge avec saisie d'un code PIN.

Exploitant

L'exploitant configure et exploite le système de contrôle d'accès à partir d'une station d'exploitation. Il configure notamment les droits d'accès des usagers. Les exploitants n'ont pas d'accès aux UTL.

Installateur/Mainteneur

Il s'agit des personnels qui mettent en œuvre le système à son installation et qui en assurent la maintenance. Ce sont ces personnels qui ont accès aux UTL.

Officier de sécurité

Ces personnels ont le plus haut niveau de droits d'accès au système. Ils possèdent les privilèges maximums sur le serveur et ils paramètrent également les données de sécurité du système (clés de gestion du badge, profils des exploitants, injections de clés dans les cartes SAM sans en avoir forcément connaissance).

4.2 HYPOTHÈSES SUR L'ENVIRONNEMENT D'UTILISATION DU PRODUIT

4.2.1 Hypothèses sur l'environnement physique

H.UT_SECU

Les UTL et leur alimentation secourue sont installées dans un local sécurisé à accès contrôlé. Seuls les personnels autorisés ont accès aux UTL (installateur/mainteneur & officiers de sécurité).

H.LECTEUR_SECU

Les lecteurs sont reliés aux UTL via une interface RS-485 qui est considérée comme directe, traversante et non accessible facilement (câbles non exposés).

H.LAN_SUP_SECU

Les machines et le serveur Cosmos sont installés dans un local sécurisé à accès contrôlé. Seuls les exploitants, les officiers de sécurité et les installateurs/mainteneurs sont autorisés à accéder à ce local. Le réseau Lan est sécurisé et se trouve en zone protégée. L'ouverture/fermeture des ports/protocoles réseaux permettant la configuration et mise à jour du système sont supposés administrés selon des règles sécuritaires (ex : verrouillage du protocole telnet)

H.UTL_BUS_COMET_SECU

Comet est installé dans un local sécurisé à accès contrôlé. Seuls les exploitants, les officiers de sécurité et les installateurs/mainteneurs sont autorisés à accéder à ce local. Les UTL(S) y sont raccordées via une interface RS-485 qui est considérée comme directe, traversante et non accessible facilement (câbles non exposés).

H.CERTIFICATS

Le certificat est fourni par le client final. Il est supposé conforme aux règles RGS en vigueur. Sa mise en place est faite par un agent de confiance et suit la procédure d'installation.

H.STATION_PERSO_SECU

La machine servant à la personnalisation des badges et à l'initialisation des UTL (mise à la clé) est située dans un local à accès contrôlé uniquement accessible aux officiers de sécurité et aux exploitants. Toutefois on peut imaginer d'avoir la base de données sur un pc portable et effectuer la mise en service sur l'UTL in situ. La base de données dans ce cas sera restreinte aux informations d'installations seules et administrée par un officier de sécurité.

H.POSTES_CLIENTS

Les postes d'exploitation sont utilisés et demeurent dans des zones sécurisées.

4.2.2 Hypothèses sur les intervenants

H.OFF_CONFIANCE

Les officiers de sécurité sont formés à l'utilisation du système et sont considérés de confiance.

H.INST_CONFIANCE

Les installateurs et les mainteneurs sont formés à l'utilisation du système et sont considérés de confiance.

H.PORTEUR_SENSIBILISATION

Les porteurs de badges (les usagers) sont sensibilisés à l'utilisation de leur badge et des accès qu'il leur permet. En particulier, ils sont sensibilisés au fait de ne pas prêter, échanger leur badge ainsi que de ne pas divulguer leur code PIN lorsque l'installation en prévoit un en plus du badge individuel. Les porteurs sont censés prévenir les exploitants en cas de perte ou vol de leur badge.

H.EXPLOITANT_CONFIANCE

Les exploitants sont chargés de l'attribution ou de la définition des droits d'accès sur l'ensemble des portes et obstacles physiques contrôlés, ils sont supposés être compétents, formés et de confiance. Les exploitants ne se connectent jamais physiquement sur les coffrets (UTL).

4.2.3 Hypothèse sur l'environnement technique

H.INJECTION_CLE_SAM

L'injection des clés mères (B.K_MERE_COM_BADGE_UTL, B.K_BI-CLE_UTL_COM_UTL_SERVEUR et B.K AUTH SAM) nécessaires à la sécurité des communications entre lecteur/UTL et UTL/Serveur est faite dans un module de sécurité SAM AV2/AV3 de la société NXP, module intégré dans l'UTL. Ce module de sécurité hérite d'une certification Critères Communs EAL5+. La cérémonie d'injection de clés est réalisée par l'officier de sécurité ou pour plus de confiance par deux officiers de sécurité. La cérémonie de clés est assurée dans un local sécurisé. La clé B.K AUTH SAM est transférée chiffrée en AES 256 directement sur l'UTL via une liaison série. La carte SAM protège en intégrité et confidentialité les éléments stockés par elle.

H.INJECTION_DONNES DESFIRE EV1/EV2

Le badge DESFIRE EV1/EV2 protège en intégrité et confidentialité les éléments stockés par lui.

H.INJECTION_CLE SSCPV2

Le changement de la clé par défaut du protocole SSCPV2 dans les lecteurs est protégé en intégrité, confidentialité, authenticité par un badge SKB unique par site.

H.CODE_PIN

Attribué par l'exploitant du site il est supposé être généré conformément aux règles RGS puis transmis au porteur de badge de façon sécuritaire et individuelle.

H.ID

L'identifiant attribué à chacun des utilisateurs est protégé par la technologie DESFIRE. A savoir par clés diversifiées ou non permettant sa lecture et le chiffrement en AES 128 de son transport sur la liaison RS-485.

H.RADIUS

Le serveur Radius est supposé fiable il s'agit au final d'un élément fournit par le client répondant aux contraintes du S.I interne.

H.SYSTEMES_EXPLOITATION

Les systèmes d'exploitation des serveurs et postes client sont supposés fiables il s'agit au final d'OS fournit par le client répondants aux contraintes du S.I interne. Ils disposent des derniers des patchs de sécurité. La mise à jour du logiciel Cosmos est prise en compte au travers d'un contrat de maintenance assurant la compatibilité avec la mise à jour des O.S

H.CONFIGURATION

La configuration est faite en respectant les préconisations du document « Configuration CSPN_Cosmos »

H.NXP

Les éléments relatif à NXP (badges desfire Ev1,Ev2,Ev3 et Sam AV2 ,AV3) sont supposés conformes fonctionnellement aux documents et références fournies par le constructeur.

H.CRYPTO_WINDOWS

Les fonctions cryptographiques inhérentes au système d'exploitation windows, utilisées par la TOE sont considérées fiables, robustes et de confiance. Celles-ci sont identifiées et décrites dans le document relatif à la cryptographie.

4.3 BIENS SENSIBLES

B.K_MERE_COM_BADGE_UTL

Il s'agit de la clé AES mère qui permet de générer des clés diversifiées utilisées dans les communications UTL / Badge. Cette clé est injectée dans la carte SAM par l'officier

de sécurité à l'aide du logiciel de gestion des cartes SAM fourni par Elsylog ou celui en place dans l'entreprise.

B.K_DIVERSIFIEE_COM_BADGE_UTL

Il s'agit d'une clé qui permet d'authentifier un badge et de chiffrer les nombres aléatoires composants les clés de sessions, nécessaires à la communication entre l'UTL et le badge. Cette clé propre au badge est initialisée à l'enrôlement d'un badge. Elle est stockée dans le badge uniquement. Il s'agit d'une clé dérivée de B.K_MERE_COM_BADGE_UTL

B.K_SESSION_COM_BADGE_UTL

Il s'agit des clés de session utilisées pour protéger les communications en mode transparent entre badge/UTL. Ces clés sont chiffrées à partir de la clé diversifiée B.K_DIVERSIFIEE_COM_BADGE_UTL correspondant à un badge donné. Elles sont générées aléatoirement par la carte SAM et l'UTL.

B.FICH_ID

Il s'agit du fichier contenant l'identifiant du badge.

B.SESSION_AUTHENT_GAC

Il s'agit du couple login et mot de passe associé à un utilisateur lors de sa connexion au GAC. Bien sensible lors le transport vers le serveur.

B.BD

Il s'agit du couple login et mot de passe de l'accès à la base de données.

B.LOGS

Il s'agit des logs générés par le GAC et ceux remontés par les UTL(S). Ils sont stockés dans la même base de données mais dans des tables SQL différentes.

B.K_CHIFFRE_BD

Il s'agit de la clé de chiffrement utilisée pour chiffrer les paramètres sensibles en base de données.

B.ROLE

Il s'agit des profils d'accès aux différentes fonctionnalités du GAC. Les profils sont un regroupement de droits d'accès aux menus du logiciel mais aussi des attributs qui sont : attribution, lecture seul, lecture / écriture de données. Ils permettent une classification facilement identifiable des administrateurs, mainteneurs, exploitants etc…
Les droits configurables concernent :

- Les profils d'accès au GAC
  - Création
  - Modification
  - Visualisation
  - Attribution

- La gestion des UTL(S)
  - Création
  - Modification
  - Visualisation

- La gestion des droits d'accès aux zones géographiques
  - Création
  - Modification
  - Attribution
  - Visualisation

- La gestion des collaborateurs
  - Création
  - Modification
  - Visualisation

- L'édition de rapports
  - Utilisateurs
  - Droits d'acces
  - Logs UTL(S)
  - Logs GAC
  - Etc …..

- L'encodage et personnalisation des badges
  - Création / modification de gabarits d'impression
  - Encodage

- Le paramétrage
  - Des sauvegardes
  - Des éléments de sécurité des badges
  - Etc …

B.PINCODE

Il s'agit du code d'accès à 4 chiffres de l'usager lorsqu'il le rentre sur le lecteur-clavier. Ce code est associé à l'identifiant pour valider une authentification de l'usager.

B.FIRMWARE

Il s'agit du firmware de l'UTL.

B.DROITS_PORTEURS

Il s'agit des droits d'accès d'un usager sur les dispositifs de contrôle d'accès de l'installation. Ces droits sont transmis et stockés dans l'UTL.

B.K_DEVERROUILLAGE_SAM_UTL_SESSION

Il s'agit de la clé utilisée pour chiffrer le secret qu'envoie l'UTL au serveur COSMOS à l'initialisation. Si le secret est correct, le serveur accepte d'envoyer la clé B.K_AUTH_SAM (de déverrouillage la carte SAM de l'UTL) chiffrée par cette clé de session.

B.K_AUTH_SAM

Il s'agit d'une clé AES128 d'authentification de la carte SAM. Cette clé permet de déverrouiller la carte SAM. Elle est saisie lorsqu'on initialise l'UTL et également stockée de manière sécurisée dans la base de données du serveur COSMOS. Elle est envoyée à l'UTL soit au moyen d'une liaison série à l'initialisation dans une salle sécurisée, soit par un officier de sécurité muni d'un PC portable en configuration monoposte avec une base de données à jour. Cette phase ne sera jamais accessible par réseau IP. Cette clé est utilisée pour autoriser la génération des clés publiques et privées de l'UTL.

B.K_BI-CLE_UTL COM_UTL_SERVER

Bi-clé générée après authentification dans la carte SAM. La partie publique est transférée chiffrée en AES-256 à la base de données.

B.K_BI-CLE_SERVER_COM_UTL_SERVER

Bi-clé du serveur pour les communications entre serveur et UTL. Une commande à partir du logiciel Cosmos (sur le serveur uniquement) permettra le calcul d'une nouvelle bi-clé. Une commande permettra sa diffusion vers les UTL.

B.K_SESSION_ENC_COM_UTL_SERVER (chiffrement)
B.K_SESSION_DEC_COM_UTL_SERVER (déchiffrement)

Clés de session AES256 calculées pour les communications entre UTL et serveur. Une commande à partir du logiciel Cosmos pourra à tout moment démarrer une demande de renouvellement de clés. Sur acquittement de l'UTL, le chiffrement prendra cette nouvelle clé comme référence.

B.K_SESSION_CMAC_COM_UTL_SERVER

Clé d'authentification calculée pour les communications entre UTL et serveur. Son renouvellement est similaire à K_SESSION_ENC_COM_UTL_SERVER et K_SESSION_DEC_COM_UTL_SERVER.

B.K_SESSION_SYNC_COM_UTL_SERVER

Clé d'authentification calculée pour les communications entre UTL et serveur. Elle sert à la synchronisation du compteur utilisé dans le calcul du CMAC contenu dans les échanges entre UTL et serveur. Son renouvellement est similaire à K_SESSION_ENC_COM_UTL_SERVER et K_SESSION_DEC_COM_UTL_SERVER.

B.K_CODE_PIN

Il s'agit de la clé de chiffrement du protocole SSCPV2 qui assure la protection du code pin

B.K_FIRMWARE

Clé de chiffrement calculée pour le chiffrement du firmware.

Le tableau ci-dessous présente les besoins de sécurité de chaque bien sensible

Bien sensible	Confidentialité	Disponibilité	Intégrité	Authenticité
B.K_MERE_COM_BADGE_UTL	X		X	X
B.K_DIVERSIFIEE_COM_ BADGE _UTL	X		X	X
B.K_SESSION_COM_BADGE_UTL	X		X	X
B.FICH_ID	X			
B.PINCODE	X		X	X

B.FIRMWARE	X		X	X
B.DROITS_PORTEURS			X	
B.K_AUTH_SAM	X		X	X
B.K_DEVERROUILLAGE_SAM_UTL_SESSION	X		X	X
B.K_BI-CLE_UTL COM_UTL_SERVER	X		X	X
B.K_BI-CLE_SERVER_COM_UTL_SERVER	X		X	X
B.K_SESSION_ENC_COM_UTL_SERVER	X		X	X
B.K_SESSION_DEC_COM_UTL_SERVER	X		X	X
B.K_SESSION_CMAC_COM_UTL_SERVER	X		X	X
B.K_SESSION_SYNC_COM_UTL_SERVER	X		X	X
B.SESSION_AUTHENT_GAC	X		X	X
B.BD	X		X	X
B.LOGS	X		X	X
B.K_CHIFFRE_BD	X		X	X
B.ROLE	CA		CA	CA
B.K_CODE_PIN	X		X	X
B.K_FIRMWARE	X		X	X

4.4 MENACES

4.4.1 Profil des attaquants

Les attaquants potentiels peuvent mener des attaques logiques ou physiques sur les constituants de la ToE. Les attaquants ont un accès physique aux UTL rendu difficile de par le fait que les équipements sont en zone à accès contrôlé. Les attaquants peuvent être des usagers porteurs de badge ou des individus malveillants ne possédant pas de badge.

Pour les attaques logiques, on distingue les points d'accès suivants :

- Le réseau entre le Serveur et l'UTL
- La liaison entre le serveur et Comet
- La liaison RS-485 entre une UTL et un lecteur de badges
- La liaison RS-485 entre Comet et une UTL
- La liaison IP entre Comet et une UTL
- La liaison IP entre un poste client et une UTL
- La liaison entre les UTL et lecteur de badges
- Paramétrage de la configuration IP au travers du server WEB Lantronix

Les attaques physiques sont considérées sur les équipements suivants :

- Le lecteur de badges
- Les UTL(S) Syrius et Orion
- Le bouton poussoir de sortie
- La détection d'ouverture de porte

Concernant les attaques logiques du GAC Cosmos, on distingue les points d'accès suivants :

- L'Authentification d'accès au logiciel

- Les profils d'accès liés aux différents rôles métier.

- La base de données
- Le poste client

4.4.2 Liste des menaces

M.FIRMWARE_CORRUPT

Un attaquant tente de corrompre le firmware d'un UTL en utilisant soit une mise à jour malveillante fournie à l'insu d'un utilisateur autorisé soit en tentant de l'injecter lui-même.

M.INTERCEP_UTL_SERVEUR

Un attaquant tente d'intercepter les communications entre une UTL et le serveur afin de pouvoir compromettre, modifier, rejouer des communications. L'impact de cette menace peut être l'interception de biens sensibles (ex : code PIN) ou l'octroi de droits d'accès par modification/rejeu de commandes.

M.INTERCEP_LECT_UTL

Un attaquant tente d'intercepter les communications entre un lecteur et une UTL afin de pouvoir compromettre, modifier, rejouer des communications. L'impact de cette menace peut être l'interception de biens sensibles (ex : code PIN) ou l'octroi de droits d'accès par modification/rejeu de commandes.

M.INTERCEP_COMET_UTL

Un attaquant tente d'intercepter les communications entre un Comet et une UTL afin de pouvoir compromettre, modifier, rejouer des communications. L'impact de cette menace peut être l'interception de biens sensibles (ex : code PIN) ou l'octroi de droits d'accès par modification/rejeu de commandes.

M.PHYS_LECTEUR

Cette menace couvre les attaques physiques pouvant être menées par un attaquant dans le but de modifier le comportement des lecteurs de badges. L'attaquant peut tenter d'ouvrir ou de substituer le lecteur.

M.PHYS_UTL_INTRUSION

Cette menace couvre les attaques physiques pouvant être menées par un attaquant dans le but de modifier le comportement des UTL. L'attaquant peut tenter d'ouvrir ou de substituer l'UTL.
Il peut tenter d'isoler une UTL pour empêcher la remontée d'évènements.

M.PHYS_UTL_BPS

Cette menace couvre les attaques physiques pouvant être menées par un attaquant dans le but d'ouvrir ou d'empêcher l'accès en court-circuitant ou coupant le câble de l'entrée bouton poussoir de sortie.

M.PHYS_UTL_EFF_ACCES

Cette menace couvre les attaques physiques pouvant être menées par un attaquant dans le but d'empêcher la détection d'effraction de l'accès en coupant le câble de l'entrée de surveillance de l'accès.

M.INTERCEPT_GAC_AUTHEN

Un attaquant tente d'intercepter, le couple login / password d'un utilisateur et de se faire passer pour qui il n'est pas.

M.OUTREPASS_GAC_ROLE

Un attaquant tente d'outrepasser ses droits pour augmenter son périmètre de fonctionnalités.

M.LOGS

Un attaquant tente de modifier, de supprimer ou d'injecter des logs applicatifs ou remontés des UTL(S)

M.ACCES_GAC_BD

Un attaquant tente de se connecter à la base de données pour falsifier ou supprimer des évènements des données contenues par elle.

M.SERVEUR_WEB_LANTRONIX

Un attaquant tente de modifier les paramètres de configuration pour isoler sa communication.

5 FONCTIONS DE SECURITE

F_PROTECT_DIAL_LECT

La protection des communications entre le lecteur et l'UTL est assurée selon la norme ISO 14443-A-B . La norme met en œuvre un protocole de sécurité qui s'appuie sur :

- Une phase d'authentification mutuelle utilisant les clés diversifiées (B.K_DIVERSIFIEE_COM_BADGE_UTL)
- La génération d'une clé de session AES 128 bits qui protège alors les communications (B.K_SESSION_COM_BADGE_UTL).

La protection des communications en dehors de l'authentification mutuelle et du chiffrement, inclus également une protection contre le rejeu et assure la gestion de l'intégrité des données dans les phases de lecture/écriture , essentiel dans un mécanisme de contrôle d'accès physique. Le détail des mécanismes cryptographiques mis en œuvre est fourni dans le document de spécifications cryptographiques [CRYPTO].
Pour rappel la clé mère B.K_MERE_COM_BADGE_UTL permettant de générer les clés diversifiées B.K_DIVERSIFIEE_COM_BADGE_UTL est protégée par un module SAM AV2/AV3 de la société NXP. Ce module de sécurité hérite d'une certification critères commun EAL5+. La clé est injectée dans la carte SAM par l'officier de sécurité à l'aide
du logiciel de gestion des cartes SAM fourni par Elsylog ou celui en place dans l'entreprise.

F_PROTECT_AUTHENCOM_UTL_SERVEUR
F_PROTECT_AUTHENCOM_UTL_COMET

La protection des communications entre l'UTL , COMET et le serveur COSMOS est assurée par un protocole établissant un canal sécurisé entre l'UTL / serveur COSMOS (interface IP) d'une part et entre UTL / COMET (interface RS-485) d'autre part.

Ce protocole se base sur les bi-clés des deux équipements (B.K_BI-CLE_UTL_COM_UTL_SERVER et B.K_BI-CLE_SERVEUR_COM_UTL_SERVER) Il permet la réalisation d'une authentification mutuelle et le chiffrement d'aléas, générés de part et d'autres, servant à la création deux clés de session B.K_SESSION_ENC_COM_UTL_SERVER et B.K_SESSION_DEC_COM_UTL_SERVER et K_SESSION_CMAC_COM_UTL_SERVER. La construction de celles-ci (voir document de cryptographie) démarrera le chiffrement des échanges sécurisés.
A noter ces BI-CLE sont communes quelque soit l'interface utilisée.

Pour rappel le bi-clé B.K_BI-CLE_UTL_COM_UTL_SERVER est protégé par un module SAM AV2/AV3 de la société NXP. Ce module de sécurité hérite d'une certification Critères Communs EAL5+. La clé est injectée dans le SAM à l'initialisation de l'UTL.

Le protocole assure l'authentification mutuelle, l'échange de clés de session ainsi que l'intégrité des communications. Concernant la protection contre le rejeu un mécanisme propriétaire est mis en œuvre associant un champ aléatoire aux commandes passées. Le générateur d'aléa est identifié dans le document de spécifications cryptographiques de COSMOS [CRYPTO] .

F_PROTECT_AUTHENCOM_COMET_SERVEUR

La protection des communications entre COMET et le serveur est assurée par un protocole établissant un canal sécurisé TLS 1.2 avec support X509 et authentification sur serveur Radius.

F_PROTECT_CODE PIN

Lorsque le code PIN est saisi par le porteur de badge sur le lecteur, le code PIN est envoyé chiffré à l'UTL via le protocole SSCPv2. La comparaison du code saisi sur le lecteur est faite dans l'UTL et ne remonte pas vers le serveur. Sauf dans un cas, si le porteur du badge fait son changement de code PIN à partir du lecteur de badge muni d'un clavier. Dans ce cas il est envoyé au serveur via le canal sécurisé de la fonction F_PROTECT_AUTHEN_COM_UTL_SERVEUR,

F_PROTECT_AUTHEN_COM_COMET_SERVEUR, F_PROTECT_COM_CLIENT et F_PROTECT_AUTHEN_COM_COMET_UTL Le code pin est stocké chiffré dans l'UTL et la base de données Cosmos.

F_PROTECT_UTL

L'UTL dispose d'une fonction de détection d'ouverture sous la forme d'un contact sec qui remonte une alarme vers le serveur COSMOS en cas de détection d'effraction ou d'arrachement. Ne recevant plus de trame en vie, la perte de dialogue est quant à lui signalé par le logiciel d'exploitation.Le passage sur alimentation secourue (batterie) est remonté vers le serveur ainsi que « Batterie basse » lorsque celle-ci arrive au seuil critique. En cas de coupure complète les informations sont sauvegardées plusieurs jours, permettant ainsi un redémarrage et la reprise immédiate de la sécurisation de l'accès.

F_PROTECT_LECTEUR

Les lecteurs de badges disposent d'un mécanisme de détection d'ouverture et d'un mécanisme de détection d'arrachement. En cas de détection, une alarme est remontée au niveau du serveur COSMOS.

F_PROTECT_FIRMWARE

Les fichiers de mise à jour firmware sont protégés en confidentialité par du chiffrement AES 256 , en intégrité par une empreinte numérique et en authenticité par une signature numérique. Le fichier de mise à jour contient une clé maitre. Reçue par l'UTL elles sera ensuite dérivée pour obtenir la clé de déchiffrement. L'authenticité réside sur la connaissance de l'algorithme de dérivation et la signature numérique. La reprogrammation ne sera possible qu'une fois les vérifications effectuées et correctes

F_PROTECT_BPS

L'UTL dispose d'une entrée équilibrée permettant la détection de court-circuit ou coupure de boucle de la fonction bouton poussoir de sortie. Les évènements associés sont transmis vers le logiciel d'exploitation.

F_PROTECT_EFF_ACCES

L'UTL dispose d'une entrée équilibrée permettant la détection de court-circuit ou coupure de boucle de la surveillance de l'acccès.Les évènements associés sont transmis vers le logiciel d'exploitation

F_PROTECT_GAC_AUTHENT

L'authentification (login / mot de passe) utilisateurs est envoyée chiffrée au serveur.
Le mot de passe de l'authentification est stockés en tant qu'empreinte numérique.

F_PROTECT_PROFILS_GAC

L'exploitant attribut des rôles aux divers intervenants habilités à utiliser le GAC. Ces rôles forment différents profils d'accès aux fonctions proposées et limitent ainsi l'activité des intervenants à celle qui leur sont octroyée.

F_PROTECT_COM_CLIENT

Le poste client dialogue au protocole HTTPS. Les informations échangées sont protégées par le protocole TLS 1.2.

F_PROTECT_GAC_BD

L'accès à la base de données est protégé par un compte avec attribut login / password. Ces données sont chiffrées et stockées sur le serveur uniquement. Les postes clients et comet n'ont pas accès directement à la base de données.

F_PROTECT_LANTRONIX

Seul le protocole HTTPS sera utilisé pour le paramétrage. Fermeture du port du serveur Web une fois l'utl installée.

Le tableau ci-dessous présente la couverture des menaces par les fonctions de sécurité

	M.SERVEUR_WEB_LANTRONIX	M.INTERCEPT_COMET_UTL	M.FIRMWARE_CORRUPT	M.INTERCEP_UTL_SERVEUR	M.INTERCEP_LECT_UTL	M.PHYS_LECTEUR	M.PHYS_UTL_INTRUSION	M.PHYS_UTL_BPS	M.PHYS_UTL_EFF_ACCES	M.INTERCEPT_COMET_SERVEUR	M.INTERCEPT_GAC_AUTHEN	M.ACCES_GAC_BD	M.OUTREPASS_GAC_ROLE	M._LOGS
F_PROTECT_DIAL_LECT					X									
F_PROTECT_AUTHENCOM_UTL_SERVEUR **F_PROTECT_AUTHENCOM_COMET_SERVEUR** **F_PROTECT_AUTHENCOM_UTL_COMET** **F_PROTECT_COM_CLIENT**		X	X	X						X	X		X	X
F_PROTECT_CODE PIN		X		X	X					X				
F_PROTECT_UTL							X							
F_PROTECT_LECTEUR						X								
F_PROTECT_FIRMWARE			X											
F_PROTECT_BPS								X						
F_PROTECT_EFF_ACCES									X					
F_PROTECT_GAC_AUTHENT											X		X	
F_PROTECT_GAC_BD											X	X	X	X
F_PROTECT_PROFILS_GAC													X	
F_PROTECT_LANTRONIX	X													

6 LEXIQUE

APB	Anti-pass back
UTL	Unité de traitement logique
DESFIRE	Technologie badge de proximité sécurisée NXP
TCP/IP	Protocole de dialogue réseau
RS485	Bus de terrain
LAN	Réseau ethernet local
SAM	Secure access module
ToE	Cible d'évaluation
PIN	Personal identification Number
FIRMWARE	Logiciel embarqué dans les UTL
GAC	Gestionnaire des accès contrôlés