

MICROSESAME



CIBLE DE SECURITE CSPN CONTROLE DES ACCES PHYSIQUES

MICROSESAME & TILLYS CUBE HIGH SECURE

Historique des versions

Date	Version	Motif	Rédacteur
23/01/2017	1.0	Version initiale	TIL
23/06/2017	2.0	Modifications périmètre, hypothèses et fonctions de sécurité	TIL
12/10/2017	3.0	Ajout de la vérification d'intégrité sur firmware	TIL
15/12/2017	3.1	Mise à jour des versions suite au pré-test OPPIDA	TIL
01/03/2018	3.2	Mise à jour des versions des logiciels TIL (page 5)	TIL
27/06/2018	3.3	Mise à jour de la version du firmware MLP2 (Gestion Anti-arrachement Lecteur Clavier)	TIL
09/07/2018	3.4	Mise à jour des versions firmwares MLP2 & TILLYS-NG (Protection des firmwares en AES CBC, réduction délais du certificat)	TIL
22/11/2018	3.5	Qualification : Ajustement schéma environnement d'installation des équipements. Suppression d'erreurs documentaires concernant les tailles de clés AES.	TIL
07/12/2020	4.0	Mise à jour selon [NOTE 07] et évolution du produit	CESTI THALES - TIL
16/03/2021	4.1	Corrections suite aux pré-tests	TIL
07/06/2021	4.2	Mise à jour des versions	TIL
08/11/2021	4.3	Mise à jour de la version du firmware TILLYS CUBE	TIL
08/03/2022	4.4	Mise à jour de la version de MICROSESAME	TIL
01/08/2022	4.5	Mise à jour de la référence au guide ANSSI-PA-72 version 2.0	TIL
31/01/2023	4.6	Mise à jour des versions de tous les produits et des références documentaires	TIL
05/09/2023	4.7	Modifications mineures suite aux commentaires du CESTI THALES	TIL
05/05/2025	4.8	Mise en jour en suivant les directives de la [NOTE 9] Mise à jour des éléments pour une nouvelle CSPN	HIRSCH
27/08/2025	4.9	Mise de jour des composants tiers	HIRSCH
29/09/2025	4.10	Modifications suite aux remarques de l'ANSSI	HIRSCH
22/05/2026	4.11	Modifications pour la publication	HIRSCH

Références documentaires

Source	Référence	Version	Titre
ANSSI	[ANSSI-PA-72]	2.2	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection
ANSSI	[NOTE 9]	1.0	Contenu et structure de la cible de sécurité CSPN
ANSSI	[NOTE 7]	2.1	Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN
ANSSI	[TLS]	1.2	Recommandations de sécurité relatives à TLS, N°SDE-NT-35/ANSSI/SDE/NP
ANSSI	[ANSSI-PG-083]	2.04	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
STID	[PRTC]	1.15.2	Protocole de communication SSCP V2
HIRSCH	[SPEC_CRYPT0]		Spécifications cryptographiques MICROSESAME TILLYS CUBE
HIRSCH	[GUIDE]		Guide Administration et Sécurité MICROSESAME
HIRSCH	[SPEC_MLV3]	1.3	Protocole MLV3
HIRSCH	[GUIDE_APPLET]		Guide de paramétrage applet pour ML 5.x et UTL 6.x

Liste de diffusion

NOM	Prénom	Société	Contact
-	-	ANSSI/CCN	certification@ssi.gouv.fr
BREMOND	Lionel	HIRSCH	l.bremond@hirschsecure.fr
REYRE	Olivier	HIRSCH	o.reyre@hirschsecure.fr
VIAZZI	Mathieu	HIRSCH	m.viazzi@hirschsecure.fr

TABLE DES MATIERES

1. Produit à évaluer.....	5
1.1. Identification du produit	5
a. Procédures d'identification	5
Identification de la version du logiciel de gestion	5
Identification de la version des TILLYS CUBE	5
Identification de la version des modules déportés MLP2	5
1.2. Description détaillée et usage attendu du produit	6
a. Présentation de la solution d'accès.....	6
b. Description fonctionnelle et utilisation	6
c. Raccordements & Réseaux	6
d. Réseaux de terrain dédiés	8
e. Module de base TILLYS-CUBE	9
f. Module d'extension MLP2 déporté.....	10
g. Lecteur de badge transparent	10
h. Badge	10
1.3. Description de l'environnement d'utilisation du produit.....	11
1.4. Description des fonctions d'accès	11
a. Identification RFID	11
b. Identification avec confirmation par code PIN	11
1.5. Environnement technique	11
1.6. Description du perimetre d'évaluation	12
2. Problème de sécurité	14
2.1. Biens sensibles.....	14
2.2. Utilisateurs.....	15
2.3. Mesures environnementales.....	16
a. Environnement	16
b. Organisation	16
c. Mesures de sécurité	17
d. Hypothèses sur les mesures environnementales.....	17
2.4. Menaces	21
a. Agents menaçants	21
b. Liste des Menaces.....	22
3. Fonctions évaluées – Fonctions de sécurité	25
4. Surface d'attaque : synthèse des interfaces vers les fonctions du produit	28
5. Annexes.....	31
5.1. Définitions et abréviations	31
5.2. Mises à la clé des HSM	32

1. PRODUIT A EVALUER

1.1. IDENTIFICATION DU PRODUIT

Cette cible de sécurité a été élaborée en vue d'une évaluation pour une Certification de Sécurité de Premier Niveau (CSPN).

Organisation éditrice	HIRSCH
Lien vers l'organisation	www.hirschsecure.fr
Nom commercial du produit	MICROSESAME et TILLYS - CUBE HIGH SECURE
Numéro de la version évaluée	MICROSESAME V2025.2.1 TILLYS-CUBE V8.0.1 MLP2 V8.0.1
Catégorie de produit	Identification, authentification et contrôle d'accès

a. Procédures d'identification

IDENTIFICATION DE LA VERSION DU LOGICIEL DE GESTION

L'identification des versions des programmes MICROSESAME CUBE peut se faire des manières suivantes :

1. Lancement du menu principal de MICROSESAME CUBE
 - Renseignement des login – mot de passe d'un opérateur.
 - Vérification de la version dans le « A Propos » ou « ? ».
 - Programmes, lister les programmes
 - Fichier : se_menu.exe

IDENTIFICATION DE LA VERSION DES TILLYS CUBE

La méthode d'identification de la version d'une TILLYS CUBE est la suivante :

- Connexion sur la TILLYS CUBE avec un navigateur web (https).
 - Renseignement des login – mot de passe d'un utilisateur.
 - Page d'accueil, section « Version et numéro de série ».

IDENTIFICATION DE LA VERSION DES MODULES DEPORTES MLP2

La méthode d'identification de la version d'un MLP2 est la suivante :

- Connexion sur la TILLYS CUBE avec un navigateur web (https)
 - Renseignement des login – mot de passe d'un utilisateur.
 - Menu « Matériel ».
 - Menu « Diagnostic du bus ».

Le tableau indique la version des modules connectés sur les bus 485.

1.2. DESCRIPTION DETAILLEE ET USAGE ATTENDU DU PRODUIT

a. Présentation de la solution d'accès

La solution MICROSESAME CUBE correspond à une solution de gestion centralisée de contrôle d'accès physique. Elle est composée :

- d'une partie appelée « GAC » intégrant :
 - Un serveur de base de données
 - Un serveur hébergeant les applications de paramétrage et d'exploitation du contrôle d'accès
 - Un serveur de certificat (non fourni)
 - Un serveur RADIUS (non fourni)
 - Les postes clients d'exploitation de la solution de contrôle d'accès
- d'une partie appelée « Coffrets » intégrant les équipements de terrain :
 - Alimentation secourue avec une batterie,
 - Module de base TILLYS CUBE,
 - Module d'extension MLP2 pour la gestion de 2 lecteurs de badges. Ces modules peuvent être déportés via des bus RS485 (Bus MLV3).
- de lecteurs de badges avec et sans clavier.
- de badges MIFARE DESFire EV3.

Le système a pour objectif de filtrer les flux des personnes autorisées ou non à pénétrer sur un site, un bâtiment ou des locaux.

Pour assurer les contrôles sur les accès, le système d'accès remplit les fonctions suivantes :

- Identification par badge RFID (sans contact) et authentification PIN code,
- Traitement des droits d'accès gérés au niveau du coffret d'accès (TILLYS CUBE),
- Automatisme d'accès (déverrouillage, séquençement d'opérations de contrôle de l'ouvrant, état de l'accès physique) géré au niveau du coffret.

b. Description fonctionnelle et utilisation

La solution MICROSESAME permet une gestion centralisée et en temps réel des accès physiques.

Les fonctions d'accès sont gérées par une application métier.

Cette application est utilisée, chez le client final, par des responsables de sécurité qui gèrent toutes les fonctions d'accès à des zones sécurisées ou protégées via des moyens d'identification d'utilisateurs afin de leur attribuer des droits d'accès.

L'application MICROSESAME serveur permet :

- de référencer de façon unique les utilisateurs dans la base de données,
- de donner des droits d'accès au personnel de l'entreprise/société et aux visiteurs,
- de référencer les éléments de sécurité SI (droits d'administration, droits d'accès au SI,...).

c. Raccordements & Réseaux

Le serveur MICROSESAME, la base de données et les postes clients pour l'exploitation sont raccordés aux réseaux du client. Ces réseaux sont généralement des réseaux Ethernet sous TCP/IP (IP V4/V6) qui sont établis, maintenus et entièrement administrés par le client final.

Ces réseaux assurent les échanges :

- entre le Serveur MICROSESAME et les TILLYS CUBE (réseau de gestion)
- entre le Serveur MICROSESAME et les services d'entreprise du client final (réseau d'entreprise)



Les échanges TCP entre le serveur MICROSESAME et la TILLYS CUBE sont inclus dans le périmètre de l'évaluation



Les échanges TCP entre le serveur MICROSESAME et les poste clients sont inclus dans le périmètre de l'évaluation

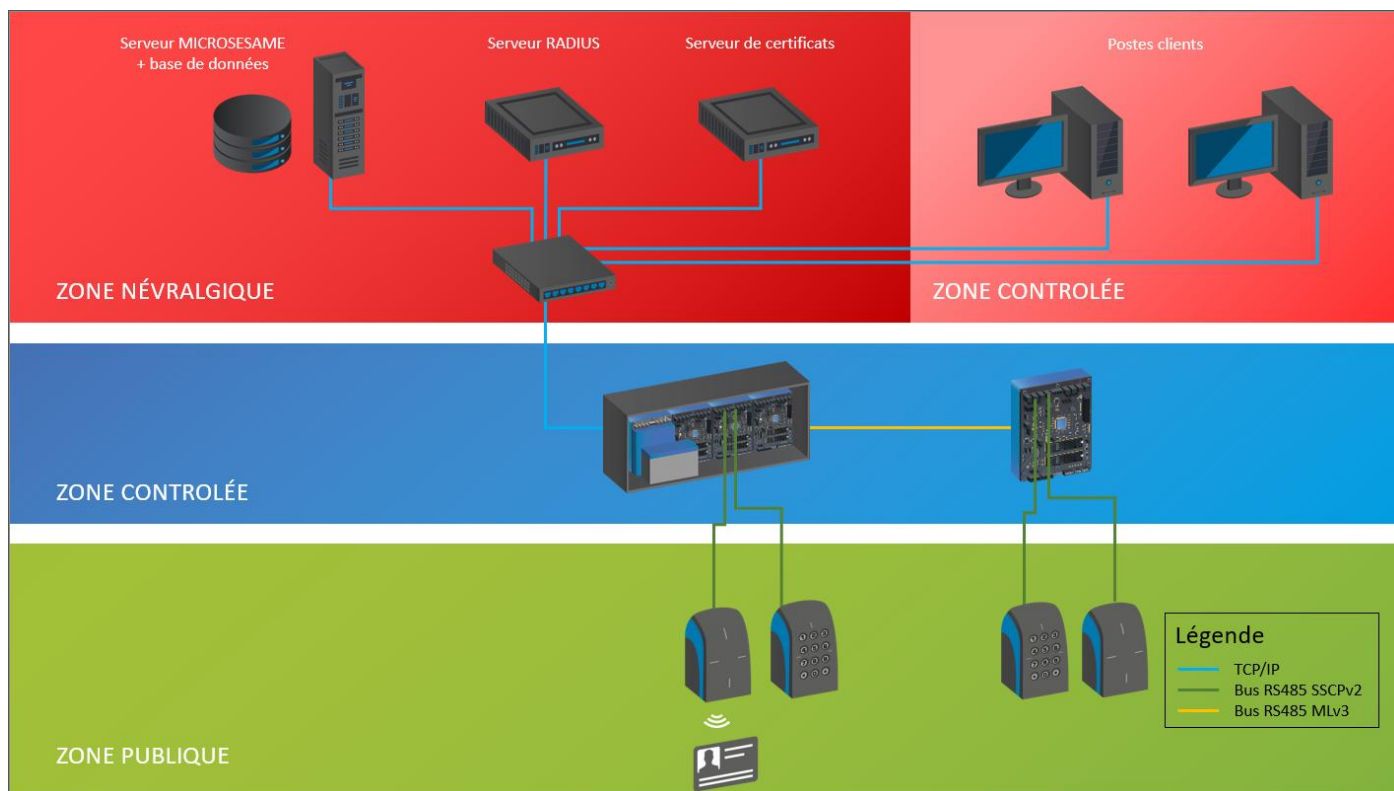


Figure 1 : architecture MICROSESAME



Les serveurs radius et de certificats ne sont pas inclus dans le périmètre de l'évaluation

d. Réseaux de terrain dédiés

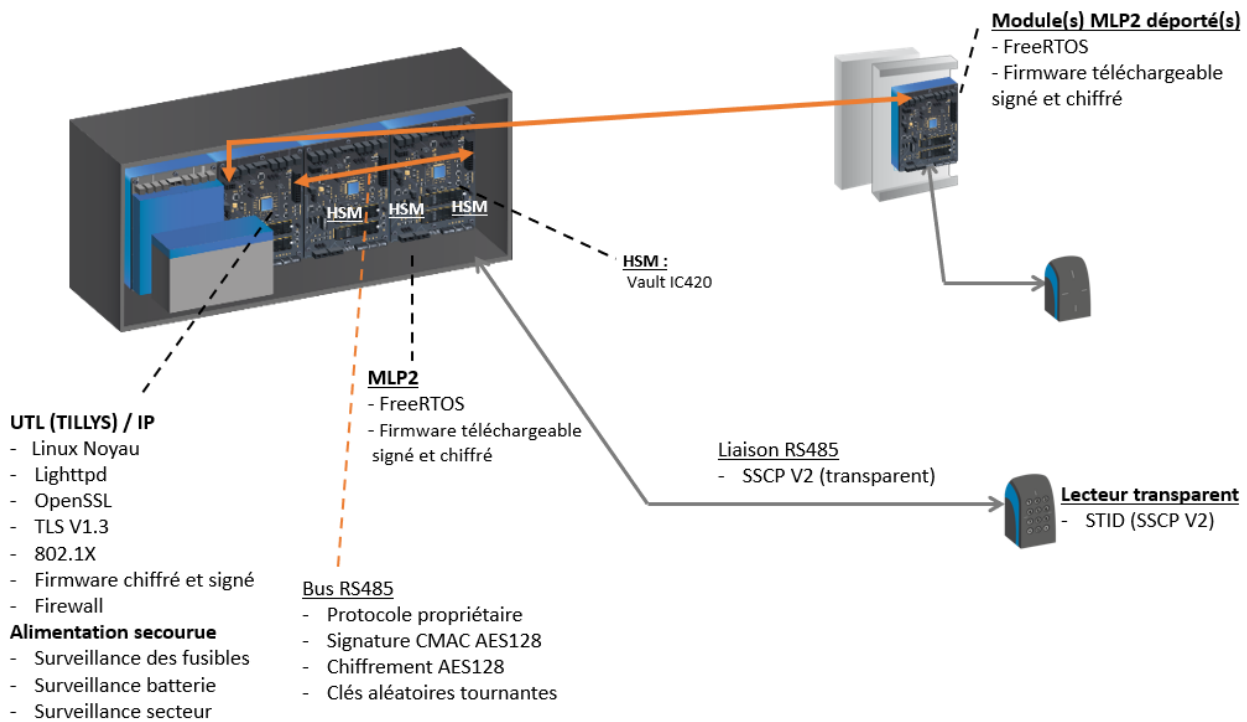


Figure 2 : architecture coffret et module déporté (contrôleur d'accès)

Les réseaux de terrain dédiés correspondent à des liaisons filaires utilisées exclusivement pour les installations de contrôles d'accès physiques.

Il y a 2 types de réseaux de terrain dédiés :

- Les interfaces bus RS485 entre module de base TILLYS CUBE et les modules d'extension MLP2 déportés : ces bus correspondent à des liaisons filaires situées en zones protégées et assurent des communications sécurisées avec un protocole propriétaire « Bus MLV3 » développé par TIL.
- Les interfaces RS485 entre MLP2 (intégrés ou déportés) et les lecteurs d'accès : ces interfaces correspondent à des liaisons filaires donnant généralement sur des zones protégées ou publiques.



Les 2 types de réseaux terrains sont inclus dans le périmètre de l'évaluation

e. Module de base TILLYS-CUBE

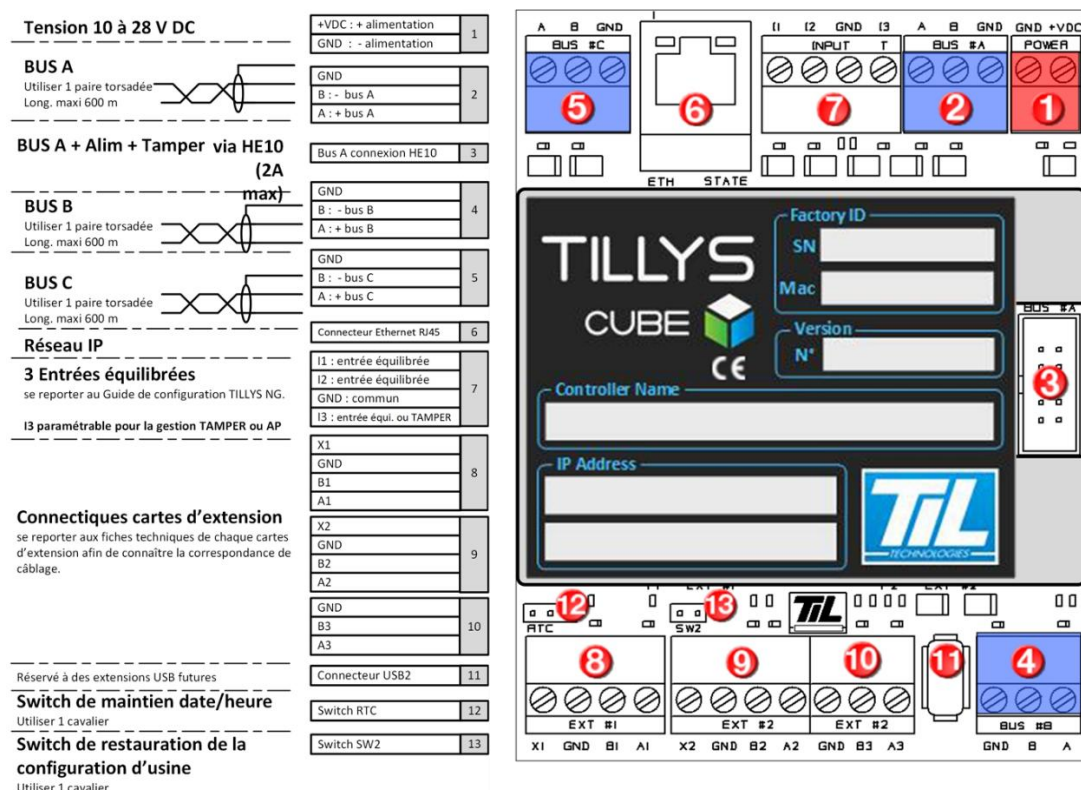


Figure 4 : Description matérielle module de base TILLYS-CUBE

Caractéristiques module de base TILLYS-CUBE	
Communication réseau IP	Carte réseau Ethernet 10/100 Mb base T auto-adaptatif (IP fixe ou DHCP), 802.1x, IPV6 ready, TLS 1.3, AES128
Communication bus RS485	57600 bauds, raccordement des modules d'extension localement ou déportés jusqu'à 600 m Chiffrement AES 128 bits CBC; Code authentification AES128 - CMAC Clés authentification et chiffrement aléatoires renouvelées périodiquement
Nombre max de lecteurs	8 par bus, jusqu'à 3 bus
Horloge / calendrier	Secourue par pile lithium débrochable / 128 programmes horaires
Connectiques	1 connecteur RJ45 1 connecteur USB (non utilisé) Borniers débrochables à vis et de couleur pour alimentation (rouge), bus RS485 MLV3 (bleu) et entrées (noir) 1 connecteur nappe HE10 avec report du bus A et de l'alimentation (2 A maxi)
Entrées	3 entrées paramétrables : TOR, comptage, équilibrée 4 états ou 5 états, dont 1 entrée prédisposée pour l'autoprotection Les entrées équilibrées proposent plusieurs jeux de résistances possibles
Signalisations	LED sur l'alimentation, le réseau, les bus et chaque entrée
Conformités	CE, RoHS

Le module TILLYS CUBE est un automate IP compact qui peut être fixé sur rail DIN dans le coffret UTL, pour la gestion du contrôle d'accès, de l'intrusion et de la gestion technique du bâtiment. Il effectue l'identification du badge transmis par le lecteur de badge en mode transparent.



Le module TILLYS CUBE est inclus dans le périmètre de l'évaluation

f. Module d'extension MLP2 déporté

Le module d'extension MLP2 déporté se connecte sur un des bus secondaires du module de base TILLYS CUBE.

Il permet de gérer 2 lecteurs quelle que soit la configuration des accès :

- 2 lecteurs en entrée,
- 2 lecteurs en sortie,
- 1 lecteur en entrée + 1 lecteur en sortie.

Emboîté sur rail DIN et équipé de connecteurs rapides pour le montage en coffret, le module d'extension MLP2 peut également être déporté jusqu'à 600 m du module de base TILLYS CUBE et intégré dans un boîtier équipé d'un contact d'autoprotection à l'ouverture.

Le MLP2 dispose d'un HSM (VaultIC420) afin de stocker les clés de sécurité des badges. Ce HSM, développé par Wisekey, est basé sur le microcontrôleur AT90SO128 et sa Toolbox cryptographique qui sont certifiés EAL5+.

Le MLP2 est également protégé contre les mauvaises manipulations ou le sabotage.



Le MLP2 est inclus dans le périmètre de l'évaluation

g. Lecteur de badge transparent

Les lecteurs de badges sont les lecteurs avec le protocole de communication SSCP V2 (voir document [PRTC]).

Le qualificatif « *transparent* » signifie que le lecteur ne dispose d'aucune clé privée dans sa mémoire locale, les clés privées sont sécurisées dans un HSM implanté dans le MLP2.

Il y a 2 types de lecteurs employés dans la solution :

Type	Constructeur	Référence HIRSCH	Référence constructeur	Version firmware
Lecteur	STID	LEC05XF5200-NB5	ARC-W33-A/Ph5-7ADy	Z23 (23.0.0)
Lecteur - clavier	STID	LEC05XF5240-NB5	ARC-W33-B/Ph5-7ADy	Z23 (23.0.0)

y : couleur coque (1 : noir - 2 : blanc)



Les lecteurs sont inclus dans le périmètre de l'évaluation

h. Badge

Le badge (NXP MIFARE DESFire) permet d'identifier le porteur directement à l'UTL (module de base TILLYS CUBE). Le badge est sécurisé (Niveaux de sureté II et III, voir tableau D.1 du document [ANSSI-PA-72]) et ne peut donc être cloné. Le badge contient les éléments secrets suivants : clés de chiffrement des échanges.

Les clés des badges sont diversifiées pour assurer des clés uniques par badge.



Les badges ne sont pas inclus dans le périmètre de l'évaluation

1.3. DESCRIPTION DE L'ENVIRONNEMENT D'UTILISATION DU PRODUIT

Pour répondre aux besoins actuels du marché du contrôle d'accès physiques et sécurisés par badges RFID basés sur la technologie MIFARE DESFire avec mécanismes de chiffrement, HIRSCH prend en considération les bases suivantes :

- Les badges DESFire autorisent le chiffrement des échanges en AES128. HIRSCH préconise l'utilisation du chiffrement AES128
- Mode de lecture : transparent
- Présence de clés de sécurité dans le lecteur : aucune clé dans le lecteur,
- Utilisation des clés cryptographiques des badges dans le coffret (ces clés correspondent à celles du tableau D.1 du document [ANSSI-PA-72]),
- Données névralgiques et clés : téléchargées dans le module de base TILLYS-CUBE depuis le serveur MS : le mode transparent correspond au schéma de la configuration type n°1 recommandée par l'ANSSI (chapitre 6.5.1 du document [ANSSI-PA-72]). Cette architecture regroupe le canal sans fil (Interface RF avec le badge) et la liaison filaire avec l'UTL (coffret).

1.4. DESCRIPTION DES FONCTIONS D'ACCES

a. Identification RFID

Les badges d'accès ont plusieurs origines possibles :

- Fournisseur spécialisé et retenu pour des marchés gouvernementaux (par exemple : un ministère, un opérateur de téléphonie),
- Achat par le client final,
- Fournisseur HIRSCH. Dans ce cas, la sécurité du support est assurée un marquage au verso. Ce marquage permet d'assurer la traçabilité des lots de badges livrés au client,
- Le coffret est compatible avec les badges multi-applicatifs.

b. Identification avec confirmation par code PIN

Cette fonction est paramétrable depuis l'application Serveur et conditionne la fonction de contrôle d'accès au niveau du coffret (UTL).

1.5. ENVIRONNEMENT TECHNIQUE

Dispositif d'accès

Les équipements minimums requis pour utiliser le produit sont les suivants :

- Lecteur de badge,
- Mécanisme de verrouillage,
- Sortie libre par bouton poussoir,
- Alimentation secourue.

Dispositif de raccordements et d'alimentation

Les raccordements des équipements mentionnés au chapitre 3.1 :

- Entre lecteurs transparents et coffret (UTL) : liaisons filaires en zones protégées, liaisons dédiées RS485,
- Entre lecteurs transparents et module déporté MLP2 : liaisons filaires en zones protégées, liaisons dédiées RS485,
- Entre module déporté MLP2 et coffret (UTL) : liaisons bus RS485 avec le protocole propriétaire détaillé dans [SPEC_MLV3],
- Entre coffret (UTL) et réseau du client Ethernet sous TCP/IP : liaisons filaires, point d'accès LAN,
- Les alimentations secourues.

Poste informatique

Les logiciels suivants doivent être installés sur le serveur MICROSESAME et les postes clients (Configuration & Exploitation) .

- Microsoft Windows Server 2022,
- Microsoft Windows 11 (64 bits).

Badges

Les badges d'accès sécurisés basés sur la technologie MIFARE DESFire sont des:

- badges livrés pré-encodés selon les différents niveaux de sécurité,
- badges encodés à partir de l'application d'accès Serveur MICROSESAME.

Dans tous les cas, les badges correspondront aux niveaux II et III du tableau D.1 des niveaux de sûreté décrits dans le document [ANSSI-PA-72].

1.6. DESCRIPTION DU PERIMETRE D'ÉVALUATION

La cible de sécurité prévoit l'évaluation de la sécurité des fonctions de contrôle d'accès gérées par les éléments suivants :

Composant du système		Inclus dans la cible de l'évaluation	Non évalué (environnement)	
			Supposé de confiance	Attaquant potentiel
GAC	Système d'exploitation		Windows Server 2025	
	Applicatifs	MICROSESAME 2025.2.1		
	Fonctions cryptographiques	TLS 1.3 Open SSL 3.4.0		
	Bases de données et annuaires		SQL Server 2022	
UTL	Système d'exploitation	TILLYS CUBE Linux 6.12.41 MLP2 FreeRTOS 11.1.0		
	Applicatifs	TILLYS CUBE 8.0.1 MLP2 8.0.1		
	Fonctions cryptographiques	TLS 1.3 Open SSL 3.4.2		
	HSM		VaultIC420	
Lecteurs	Lecteurs simples	STID ARC-W33-A/Ph5-7ADy Z23		
	Lecteurs-clavier	STID ARC-W33-B/Ph5-7ADy Z23		
Badges			MIFARE DESFire EV3	

La figure suivante illustre également une configuration type déployée sur les réseaux fournis par le client final :

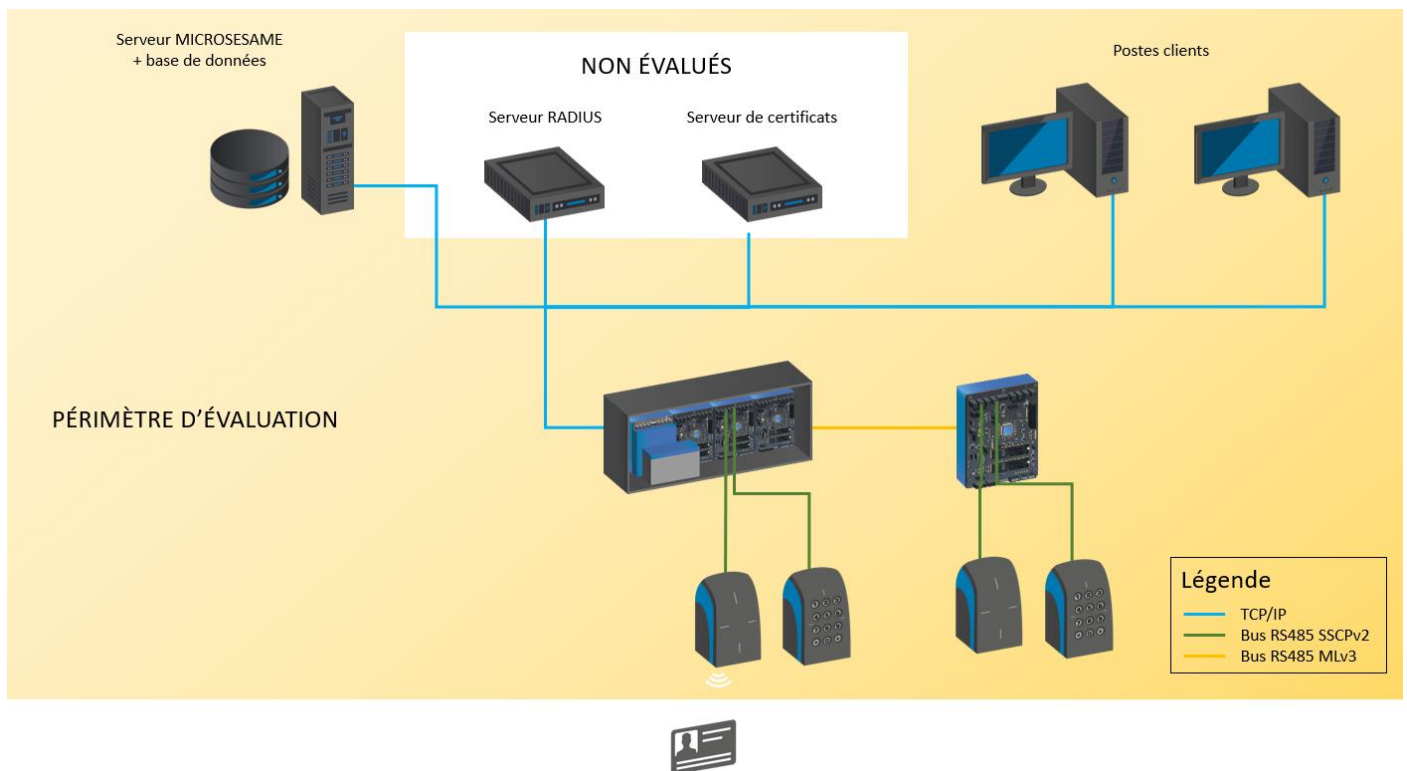


Figure 5 : Périmètre d'évaluation

Le badge est hors périmètre, mais peut être considéré comme une source de menace. Ce qui est dans un badge légitime, en revanche, est considéré de confiance (clés / fichiers sont protégés).

2. PROBLEME DE SECURITE

2.1. BIENS SENSIBLES

Le tableau ci-dessous référence les biens sensibles du produit évalué et leurs besoins de sécurité :

		Confidentialité	Authenticité	Intégrité
ID	Biens métier			
B.1	Clés des badges et de proximity check	X		
B.2	ID	X		
B.3	Code PIN	X		
B.4	Droits/autorisation utilisateurs			X
Biens techniques				
B.5	Authentification et contrôle d'accès de la gestion		X	X
B.6	Firmware		X	X
B.7	Matériel cryptographique	X	X	X

Les biens sensibles métier sont les biens présentant des besoins de sécurité vis-à-vis de fonctions métier du produit :

- Clés badges : Les clés des badges permettent de sécuriser les communications entre les badges et le MLP2.
- Identifiant d'accès ID Accès, Sécurisé dans AID DESFire (Application Contrôle d'accès) et dans un fichier Desfire avec accès chiffré par clé AES 128 diversifiée.
- Codes PIN : Le code PIN va permettre à un porteur de badge de s'authentifier (en plus de la possession de son badge).
- Droits et autorisations utilisateurs : Les droits d'accès des personnes (gérés par le coffret UTL).

Pour chaque utilisateur, ces droits définissent :

- La période de validité du badge,
- La liste des accès autorisés avec leur plage horaire d'accès,
- L'application ou non des conditions d'APB.

Ces droits sont gérés par les exploitants/opérateurs et mémorisés dans la base de données du serveur. Ils sont téléchargés dans le module TILLYS CUBE via le protocole sécurisé TLS et sont mémorisés dans la base de données interne au module TILLYS CUBE.

Les biens techniques sont les biens relatifs à la gestion technique du produit :

- Authentification et contrôle d'accès de la gestion: cette fonction permet de garantir que toutes les modifications de paramétrage sont réalisées par des personnes dûment autorisées. Différents modes de fonctionnement sont possibles :
 - Gestion interne au produit : le produit gère de manière interne les utilisateurs de sa gestion et leurs mots de passe de connexion ainsi que les rôles correspondants.
 - Gestion par annuaire : le produit est configuré pour associer des groupes d'annuaire à des rôles de la gestion. Un utilisateur de la gestion authentifié dans l'annuaire se voit automatiquement attribuer les autorisations relatives au groupe auquel il appartient.
- Firmware : afin d'assurer un fonctionnement correct, le firmware des modules doit être protégé à la fois en intégrité et en authenticité.
- Matériel cryptographique : le produit gère et utilise plusieurs clés symétriques et asymétriques. La description de ces clés est donnée dans le document [SPEC_CRYPTO].
- Les journaux d'événements.

2.2. UTILISATEURS

ID	Nom	Description	Degré de confiance
A.1	Exploitants	L'exploitant a pour fonction de configurer et adapter au quotidien les différentes fonctions du système qui concourent à attribuer des autorisations d'accès sur l'ensemble des portes et obstacles physiques contrôlés. Toute connexion des exploitants au système de gestion est tracée dans l'historique des événements.	Attaquant potentiel
A.2	Agents techniques	Les agents techniques interviennent dans le cadre des opérations de mise en service (déploiement) et de maintenance ainsi que les mises à jour firmware. Aucun exploitant ni opérateur n'est amené à se connecter directement et indirectement sur les coffrets ; c'est une prérogative des agents techniques. Toute connexion aux TILLYS CUBE est tracée dans l'historique des événements.	De confiance
A.3	Porteurs de badges	Les porteurs de badges correspondent aux utilisateurs finaux (employés, visiteurs, prestataires, stagiaires...). Ils disposent de badges sans contact (RFID) personnel.	Attaquant potentiel
A.4	Administrateur informatique	Les personnes en charge de la maintenance des équipements informatiques (maintien en sécurité de serveurs) et du réseau	De confiance
A.5	Opérateur logistique	Opérateur qui transporte, réceptionne les matériels, les met en stock et les expédie	Attaquant potentiel

2.3. MESURES ENVIRONNEMENTALES

a. Environnement

La solution MICROSESAME s'intègre dans l'environnement du client final. Pour répondre aux exigences de sécurité, les équipements doivent être installés en respectant les règles suivantes :

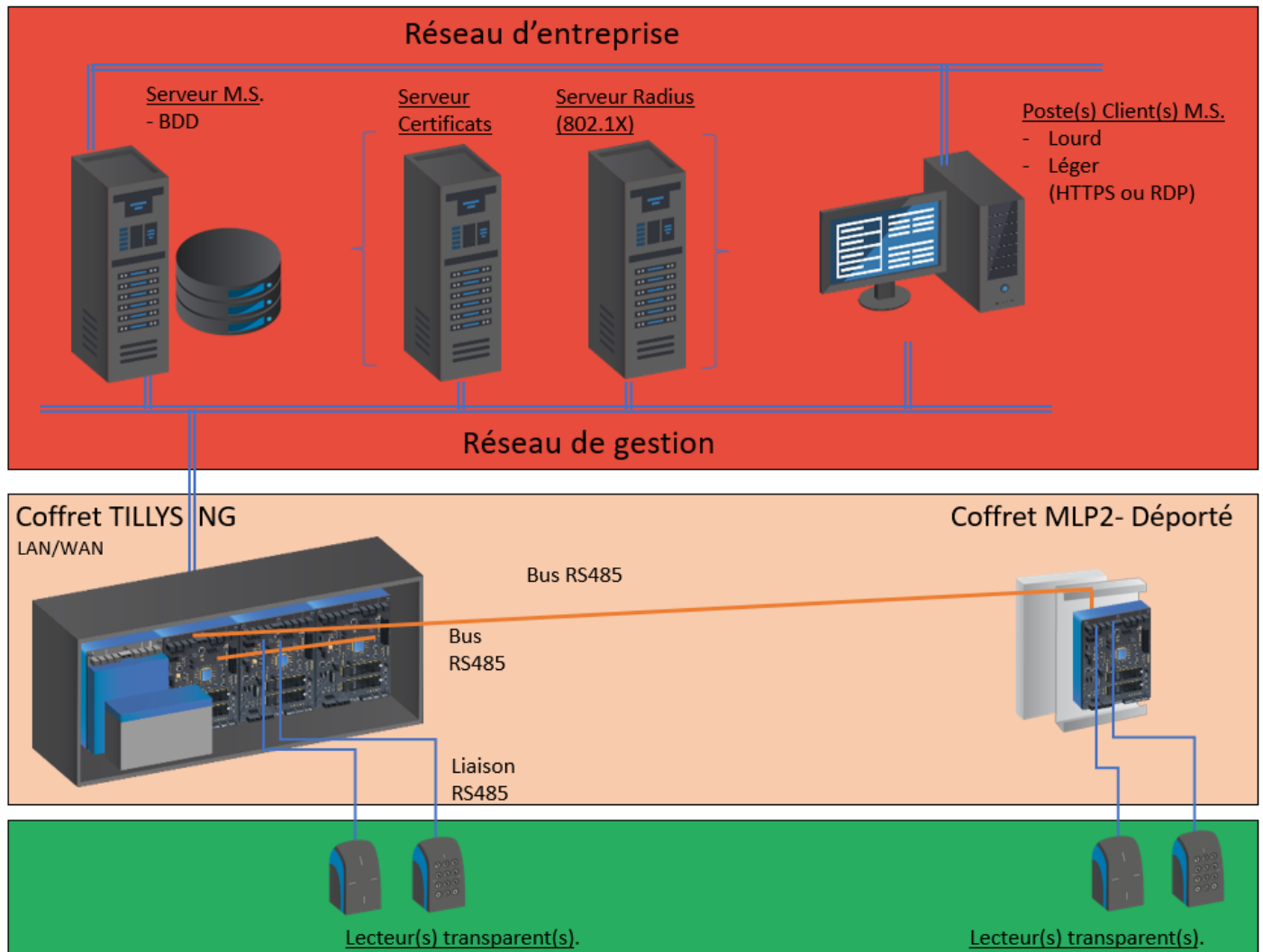


Figure 6 : Architecture type

Zone verte : accessible à tout le monde

Zone orange : accessible aux employés autorisés et aux visiteurs accompagnés

Zone rouge : accessible via badge et un code aux seuls employés autorisés et aux visiteurs accompagnés

b. Organisation

La solution MICROSESAME est une solution centralisée qui nécessite un minimum d'organisation :

- RSS : Responsable sûreté du site avec des droits d'administration (Gestionnaire des clés de sécurité des badges),
- RSSI : topologie du réseau, plan d'adressage, mise à jour des logiciels, gestion des mots de passe, délivrance des Certificats.
- Agents Techniques : Mises en service, déploiement et maintenance des équipements.
- Opérateur(s) exploitant(s) (surveillance des écrans sur les postes, prise en compte des alarmes, gestion/signalement des incidents).

c. Mesures de sécurité

Ces mesures sont :

- La mise à la clé ou « cérémonie des clés » fait partie des mesures sécuritaires :
 - Cette mise à la clé nécessite l'utilisation de l'utilitaire KSM de gestion et diffusion des clés d'installation.
 - L'installation initiale s'opère en deux temps :
 - Installation de la clé Client KAES128CLI qui permet la mise en place de la clé diversifiée KAES128CLI-D dans le HSM des MLP2 via réseau local isolé,
 - Chargement des clés des badges KBadges[] dans le HSM via l'opération de wrapping (par KSM) et unwrapping dans HSM.
 - Cette mise à la clé badge peut-être générale, limitée à un ensemble de modules TILLYS CUBE d'un territoire ou limitée aux modules spécifiés.
- Les consignes font parties des mesures sécuritaires :
 - Cas de perte ou de vol d'un badge,
 - Cas d'un oubli d'un badge ou d'un code PIN,
 - Cas des interventions sur les équipements de la cible de sécurité,
 - Cas des alarmes techniques (coupure d'alimentation, autoprotectons, défaut de communications).
- Les mises à jour régulières font partie des mesures sécuritaires :
 - Suppression d'un usager et de ses droits,
 - Suppression d'un badge,
 - Ajout d'un usager avec son badge,
 - Vérifications régulières de l'unicité des couples (ID, PIN).
- Les éléments fournis par le client final font l'objet d'une sécurisation en cohérence avec le besoin de sécurité :
 - Réseau d'entreprise
 - Réseau de gestion
 - Locaux techniques
 - Système d'exploitation du serveur MS
 - Services annexes (bases de données, annuaires, ...)

d. Hypothèses sur les mesures environnementales

Référence de l'hypothèse	Type de mesure	Description de la mesure	Acteurs en charge de la mesure
H.1	Environnement physique	Localisation du serveur MICROSESAME Il est supposé que le serveur soit installé dans un local sécurisé dont l'accès est strictement limité aux personnels habilités.	RSSI
H.2	Environnement physique	Localisation des postes d'administration Les équipements d'administration doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs	RSSI
H.3	Environnement physique	Localisation des coffrets Les coffrets TILLYS CUBE et modules MLP2 déportés ainsi que le système d'alimentation secouru sont installés dans un local sécurisé dont l'accès est limité.	RSS

H.4	Environnement physique	Installation des lecteurs transparents Pour un accès à partir d'une zone publique, aucun câble, ni aucun équipement ne sont posés/installés à l'exception du lecteur de badge. Le câble de raccordement des lecteurs de badge doit être traversant. Il ne doit pas courir le long de la porte en zone non protégée, même au travers d'une goulotte ou d'un tube de protection. Le Bus RS485 assurant la liaison entre les lecteurs, les coffrets et modules d'extension MLP2 déportés est supposé direct. Le câblage de l'ensemble des équipements constituant les environnements de porte est direct : point à point.	RSS
H.5	Environnement physique	Localisation du poste disposant de KSM Un poste KSM est relié directement sur le coffret (UTL) pour la première mise à la clé. Cette opération est faite localement sur un réseau isolé. Ce poste se situe dans un local sécurisé et n'est utilisé que par le RSS et les agents techniques.	RSSI
H.6	Organisationnelle	Maintenance des postes, du serveur MICROSESAME et des réseaux	Administrateur informatique
H.7	Organisationnelle	Les exploitants en charge de l'attribution des autorisations d'accès sur l'ensemble des portes et obstacles physiques contrôlés sont supposés être compétents, formés et de confiance. Les exploitants ne se connectent jamais physiquement sur les coffrets (UTL).	RSS
H.8	Organisationnelle	Les agents techniques en charge des opérations de mise en service (déploiement) et de maintenance (techniciens) sur les coffrets (UTL) sont supposés être compétents, formés et de confiance.	RSS
H.9	Organisationnelle	Les porteurs de badges appliquent les règles de sécurité suivantes : • Pas de prêt d'un badge. • Passage uniquement. • Ces porteurs sont supposés ne réaliser de demande d'accès que pour leur usage personnel et ne pas permettre l'accès à toute autre personne (tiers et collègues inclus).	RSS

		Ils sont supposés ne pas confier leur badge, ni communiquer leur code PIN personnel.	
H.10	Environnement technique	Les réseaux du client et les réseaux dédiés sont physiquement ou logiquement séparés. Aucune passerelle, informatique ou de transmission de données, ne peut être mise en œuvre entre ces différents réseaux.	RSSI
H.11	Environnement technique	L'ID (identifiant personnel) d'un porteur est encodé dans son badge d'accès (application d'accès dans un badge DESFire). Cet ID est protégé par un chiffrement en AES 128 bits avec une clé commune (niveau II) ou des clés dérivées d'une clé maitresse (niveau III). La communication sans contact (badge/lecteur) est sécurisée par le protocole DESFire. Ensuite, la communication entre le lecteur de badge et le coffret est sécurisée par le protocole SSCP.	RSS
H.12	Environnement physique	Les postes d'exploitation et autres services d'entreprise du réseau d'entreprise du client sont placés en zone sécurisée et sécurisés en cohérence avec les besoins de sécurité du client.	RSSI
H.13	Environnement technique	Le certificat TLS utilisé par le composant TILLYS-CUBE est à la charge du client final. Ce certificat utilise des algorithmes conformes à [ANSSI-PG-083] et l'administrateur respecte les recommandations du guide d'administration [GUIDE]	RSSI
H.14	Environnement technique	Mise à la clé Les conditions de sécurité de mise à la clé garantissent l'absence d'attaquant sur l'ensemble des flux échangés pendant cette phase (réseau isolé ou vérification préalable du réseau). Le générateur d'aléa utilisé pour obtenir les clés nécessaires au fonctionnement du produit est supposé conforme à [ANSSI-PG-083].	RSSI
H.15	Environnement technique	Clés fixes Les clés fixes utilisées par le produit ont été générées par un générateur d'aléa conforme à [ANSSI-PG-083].	Développeur de la solution

		La description de ces clés est fournie dans le document [SPEC_CRYPTO].	
H.16	Environnement technique	Les clés des badges sont soit tirées, soit saisies depuis l'utilitaire KSM, qui est supposé conforme à [ANSSI-PG-083].	RSS
H.17	Environnement technique	Le code PIN est attribué par l'exploitant du contrôle d'accès pour chaque porteur de badge concerné et est donc sous le contrôle du client final. Il est communiqué au porteur par un échange direct et confidentiel au choix de l'exploitant (de vive voix ou par une communication écrite et confidentielle). La génération de ce code PIN est conforme à [ANSSI-PG-083].	RSS
H.18	Environnement technique	L'ID (identifiant personnel) d'un usager est encodé dans une application de son badge d'accès (application d'accès dans un badge DESFire EV3). Cet ID est protégé en lecture par un chiffrement en AES 128 bits avec clé simple (niveau II) ou clé diversifiée (niveau III). La confidentialité, lors de la transmission dans l'interface air (badge/lecteur) et jusqu'au coffret, est assurée par les mécanismes d'échanges Mifare® DESFire EV3 (APDU et cryptographie DESFire EV3).	RSS
H.19	Environnement technique	Mise au rebut La mise au rebut des matériels respectera la procédure de désensibilisation décrite dans le guide GR-10012-fr-Guide_de_re_ference_TILLYS_CUBE_7_0.pdf – chapitre 37.	RSS

2.4. MENACES

Ce chapitre détaille les scénarios de menace pouvant entraîner les risques définis par la [NOTE 07] :

- R1. entrée non autorisée dans les locaux ;
- R2. dissimulation (non-détection par le système) d'une entrée dans les locaux.

a. Agents menaçants

Pour cette évaluation les attaquants suivants sont considérés :

- Attaquant sur le réseau d'entreprise,
- Attaquant sur le réseau de gestion (entre le serveur MS et les UTL),
- Attaquant sur le réseau BUS RS485 avec le protocole propriétaire entre le coffret (UTL) et le module déporté MLP2,
- Attaquant sur le réseau dédié RS485 entre les UTL et les lecteurs de badges,
- Attaquant sur le réseau dédié RS485 entre les modules déportés MLP2 et les lecteurs de badges.

Différentes attaques physiques sont considérées :

- Attaques sur l'application de gestion
- Attaque sur le coffret (UTL)
- Attaque sur le module déporté MLP2
- Attaque sur les lecteurs transparents

b. Liste des Menaces

Les menaces dont les points d'entrée sont les serveurs, les postes clients et les badges ne sont pas prises en compte. En tenant compte des hypothèses sur l'environnement, les menaces retenues sont les suivantes :

ID	Description	Interface d'attaque	Acteur de la menace	Bien impacté
M.1	Ecoute/intrusion sur le canal Serveur MICROSESAME – Poste client Attaques avec des moyens d'écoute et d'intrusion dans le but d'identifier des données d'authentification ou d'usurper l'identité d'un exploitant.	Réseau IP	Acteurs ayant accès à un poste d'exploitation ou à un port du réseau dédié au contrôle d'accès physique	B.2 ID B.3 Code PIN B.4 Droits/autorisation utilisateurs B.5 Authentification et contrôle d'accès de la gestion
M.2	Ecoute/intrusion sur le canal Serveur MICROSESAME – TILLYS CUBE : Les attaquants disposent de moyens d'écoute et d'intrusion dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes. Les écoutes de transaction échangées sur le LAN permettraient aux attaquants par exemple de : • Intercepter le format des identifiants DESFire pour reproduire un badge ou en créer un autre ; • Interception du code PIN associé à un badge ; • Rejouer une transaction modifiée pour réaliser des modifications de droits d'un badge existant afin de lui mettre des autorisations étendues ; • Rejouer une transaction pour modifier la plage horaire ; • Rejouer une transaction modifiée pour transférer les droits d'accès d'une personne sur le badge d'une autre personne ; • Rejouer une commande d'ouverture de porte.	Réseau IP	Acteurs ayant accès à un port du réseau dédié au contrôle d'accès physique	B.2 ID B.3 Code PIN B.4 Droits/autorisation utilisateurs B.5 Authentification et contrôle d'accès de la gestion B.7 Matériel cryptographique

M.3	Ecoute/intrusion sur les réseaux dédiés RS485 Les attaquants malveillants disposent de moyens d'écoute et d'intrusion dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes. Ces écoutes de transaction permettraient par exemple aux attaquants de : • Ecoute d'une transaction contenant l'ID (Copie du badge) ; • Ecoute d'une transaction contenant le Code PIN (Usurpation d'identité) ; • Ecoute d'une transaction contenant des commandes (Ouverture d'un accès) ; • Ecoute des transactions avec le coffret (Emulation d'un ou plusieurs coffrets). • Rejouer une commande d'ouverture de porte.	Bus de terrain RS 485	Acteurs ayant accès aux locaux sécurisés où sont installés les coffrets	B.1 Clés des badges et de proximity check B.2 ID B.3 Code PIN B.6 Firmware
M.4	Attaque sur le TILLYS CUBE Extraction d'informations sensibles. Substitution d'un TILLYS CUBE. Déni de service : empêcher quelqu'un de sortir. Détectabilité des accès : entrer / sortir sans être détecté.	Interface physique	Acteurs ayant accès aux locaux sécurisés où sont installés les coffrets	B.1 Clés des badges et de proximity check B.2 ID B.3 Code PIN B.4 Droits/autorisation utilisateurs B.6 Firmware B.7 Matériel cryptographique
M.5	Attaque sur le module déporté MLP2 Extraction d'informations sensibles. Substitution d'un module déporté MLP2.	Interface physique	Acteurs ayant accès aux locaux sécurisés où sont installés les coffrets	B.1 Clés des badges et de proximity check B.2 ID B.3 Code PIN B.6 Firmware B.7 Matériel cryptographique

M.6	Attaque sur le lecteur ou lecteur – clavier transparent Tentative de remplacement du lecteur transparent. Emulation / Substitution. Attaque par relai (établissement d'un relai de communication à distance à l'insu du porteur de badge).	Interface physique	Tous les acteurs – Zone publique	B.2 ID B.3 Code PIN B.6 Firmware B.7 Matériel cryptographique
M.7	Corruption du firmware L'attaquant parvient à injecter et faire exécuter un firmware corrompu sur le produit. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée. L'attaquant peut également réussir à substituer une mise à jour corrompue à une mise à jour légitime. Un utilisateur pourra alors tenter d'installer cette mise à jour dans le produit par des moyens légitimes. Enfin, l'attaquant peut également tenter d'installer une version légitime du firmware sans en avoir le droit. Les mises à jour par les opérateurs légitimes (agents techniques) ne sont pas considérées comme des attaquants car ce sont eux qui s'assurent de la provenance du firmware avant l'installation.	Interface physique	Acteurs ayant accès aux matériels avant leur installation	B.6 Firmware B.7 Matériel cryptographique

3. FONCTIONS EVALUEES – FONCTIONS DE SECURITE

En tenant compte des hypothèses sur l'environnement, les fonctions de sécurité retenues sont les suivantes :

ID	Description	Argumentaire de couverture des menaces
FS.1	Authentification et contrôle d'accès des exploitants et opérateurs	L'authentification des exploitants et agents techniques peut être réalisée selon l'un des deux modes suivants : • Authentification intégrée par login / mot de passe. Dans ce mode : ○ les secrets d'authentification et leur sécurisation sont gérés par l'application de gestion elle-même ; ○ l'application de gestion ne tient pas compte de l'identité de l'utilisateur qui est gérée par le système d'exploitation ; ○ l'attribution d'un rôle et des privilèges associée se fait unitairement dans l'application ; • Authentification déléguée et gestion des droits par groupe. Dans ce mode : ○ les secrets d'authentification et leur sécurisation sont gérés par l'environnement de l'application ; ○ l'application est configurée pour attribuer des rôles et privilèges associés en fonction de l'appartenance de l'utilisateur à des groupes spécifiques.
FS.2	Etablissement d'un canal protégé serveur MS – Postes Client (s'appuie sur le système d'exploitation du serveur)	L'application offre un service d'exploitation distante via le réseau d'entreprise. L'accès à ce service peut se réaliser depuis un navigateur sur une interface Web ou depuis un client lourd utilisant des Webservices. La sécurité des webservices est dans le périmètre d'évaluation. La sécurité du client lourd est hors du périmètre d'évaluation.
FS.3	Protection en transmission du code PIN	Les codes PIN sont protégés en confidentialité et en authenticité lors de leur transmission entre le lecteur et le module MLP2 (déporté ou non) grâce au protocole constructeur du lecteur SSCP v2.
FS.4	Protection des données échangées entre le serveur MS et les UTL TILLYS-CUBE	Les échanges utilisent 2 protocoles distincts : 1. Communications TLS : Un canal de communication garantit la confidentialité et l'intégrité avec établissement préalable d'une session avec authentification mutuelle. • Canal permanent TLS Serveur → UTL : ○ Historique des passages de badges ○ Alarmes et Evénements GTB ○ Télécommandes • Canal ponctuel TLS Serveur → UTL : ○ Configuration des TILLYS-CUBE ○ Téléchargement des porteurs de badges, de leurs identifiants et de leurs accès

		Les commandes et les transactions échangées entre le Serveur et les coffrets (UTL) sont protégées en confidentialité et en intégrité. 2. Les échanges UDP multicast. Il s'agit de trames de diffusion uniquement mises en œuvre par les mécanismes de gestion de l'anti-retour. Ces échanges : • permettent à un TILLYS CUBE d'informer les autres TILLYS CUBE de l'entrée ou de la sortie d'un utilisateur dans une zone de sécurité, • sont protégés en confidentialité et intégrité par un chiffrement et un motif d'intégrité, Les clés de mise en œuvre de ces mécanismes sont diffusées et mises à jour via les flux TLS entre le serveur MS et les UTL.
FS.5	Protection des données échangées entre les TILLYS CUBE et les modules déportés MLP2	Cette protection passe par l'établissement d'un canal de communication chiffré, les deux parties ayant ouvert une session avec une authentification mutuelle au préalable. Les commandes et les transactions échangées entre le module déporté MLP2 et l'UTL TILLYS-CUBE sont protégées en confidentialité et en intégrité. Les tentatives de rejeu sont limitées par la mise en œuvre d'un protocole propriétaire [SPEC_MLV3] chiffré.
FS.6	Sécurisation des UTL TILLYS-CUBE	La TILLYS-CUBE est placée en zone protégée. La détection de défaut génère systématiquement des alarmes techniques vers le serveur MICROSESAME. Cette détection concerne quatre types de défaut : • Arrachement, • Ouverture coffret, • Défaut communication TLS / UDP / bus RS485, • Défauts générés par l'alimentation : ○ Perte Secteur, ○ Défaut fusible 12V, ○ Défaut batterie. Chaque TILLYS-CUBE est doté d'un firewall n'autorisant que les flux réseau prévus par les services mis en œuvre.
FS.7	Sécurisation des modules déportés MLP2	La détection de défaut génère systématiquement des alarmes techniques vers le serveur MS. Cette détection concerne trois types de défaut : • Arrachement, • Ouverture MLP2, • Défaut communication du bus RS485,
FS.8	Sécurisation du lecteur -clavier	A l'installation, une clé d'authentification est négociée entre l'UTL TILLYS-CUBE ou le module déporté MLP2 et chaque lecteur-Clavier : il y a appairage [SPEC_CRYPTO].

		En cas de substitution d'un lecteur-Clavier ou lecteur, la communication du coffret (UTL) / module déporté MLP2 est bloquée avec cet équipement et une alarme est remontée vers le serveur. Pour débloquer la communication du coffret (UTL) / module déporté MLP2 avec un lecteur-Clavier ou lecteur, une intervention d'une personne habilitée doit être réalisée au niveau de l'UTL.
FS.9	Signature du firmware	À chaque installation d'un nouveau firmware, l'intégrité et l'authenticité de celui-ci sont vérifiées par l'équipement (TILLYS-CUBE ou MLP2) avant sa prise en compte effective.

4. SURFACE D'ATTAQUE : SYNTHESE DES INTERFACES VERS LES FONCTIONS DU PRODUIT

Fonctions de sécurité Menaces		Authentification et contrôle d' accès des exploitants et opérateurs	Etablissement d' un canal protégé serveur MS – Postes Client	Protection en transmission du code PIN	Protection des données échangées entre le serveur MS et les TILLYS CUBE	Protection des données échangées entre les TILLYS CUBE et les modules déportés MLP2	Sécurisation des UTL TILLYS CUBE	Sécurisation des modules déportés MLP2	Sécurisation du lecteur -clavier	Signature du firmware
		FS.1	FS.2	FS.3	FS.4	FS.5	FS.6	FS.7	FS.8	FS.9
Canal Serveur MICROSESAME – Poste client	M.1	X	X							
Canal Serveur MICROSESAME – TILLYS-CUBE	M.2				X		X			
Canaux réseaux dédiés RS485	M.3			X		X	X			
Attaque sur le TILLYS CUBE	M.4				X	X	X			
Attaque sur le module déporté MLP2	M.5					X		X		
Attaque sur le lecteur	M.6								X	
Corruption du firmware	M.7									X

Couverture des menaces par les fonctions de sécurité

Menaces Biens sensibles		Clés des badges et de proximity check	ID	Code PIN	Droits/autorisation utilisateurs	Authentification et contrôle d' accès de la gestion	Firmware	Matériel cryptographique
		B.1	B.2	B.3	B.4	B.5	B.6	B.7
Canal Serveur MICROSESAME – Poste client	M.1		X	X	X	X		
Canal Serveur MICROSESAME – TILLYS-CUBE	M.2		X	X	X	X		X
Canaux réseaux dédiés RS485	M.3	X	X	X			X	
Attaque sur le TILLYS CUBE	M.4	X	X	X	X		X	X
Attaque sur le module déporté MLP2	M.5	X	X	X			X	X
Attaque sur le lecteur	M.6		X	X			X	X
Corruption du firmware	M.7						X	X

Couverture des menaces par rapport aux biens sensibles

Type de surface d'attaque	Interfaces (accessibles ou non accessibles)	Fonction concernée (évaluée ou non évaluée)	Acteurs ayant accès aux interfaces
Interfaces physiques	Ports ethernet des réseaux	Echanges entre serveur et client, serveur et TILLYS CUBE FS.2 FS.4	Utilisateurs ayant accès au port RJ45 - A.1 A.2 A.4
	Accès aux coffrets	Gestion de l'anti arrachement et de l'ouverture des coffrets FS.6 FS.7	Utilisateurs ayant accès aux locaux sécurisés – A.2 A.4
	Liaison RS 485 entre la TILLYS CUBE et le MLP2	Canal RS485 chiffré avec authentification mutuelle FS.5	Utilisateurs ayant accès aux locaux sécurisés – A.2 A.4
	Liaison RS 485 entre le MLP2 et les lecteurs	Canal RS485 chiffré FS.8	Tous les utilisateurs (zone publique)
	Accès physique aux lecteurs	Canal RS485 chiffré et gestion de l'anti arrachement FS.8	Tous les utilisateurs (zone publique)
	Accès physique aux matériels avant installation	Accès au matériel pour une usurpation de firmware FS.9	Utilisateurs ayant accès aux matériels avant l'installation A.2 A.5
	Interface de debug sur le MLP2 SWD	Interface désactivée F.7	Utilisateurs ayant accès aux locaux sécurisés – A.2 A.4
	Interface de debug sur la TILLYS CUBE JTAG	Interface désactivée F.6	Utilisateurs ayant accès aux locaux sécurisés – A.2 A.4
Interfaces logiques	Accès aux Interfaces Homme Machine de MICROSESAME	Modification des droits d'accès, télécommandes des ouvertures FS.1	Utilisateurs utilisant le logiciel MICROSESAME A.1 A.2 A.4
	Interface vers l'OS des postes d'exploitation	Fonction non évaluée – OS des postes et du serveur ne sont pas dans le périmètre d'évaluation	Utilisateurs exploitants du logiciel -A.1 A.2 A.4
	Interface vers le réseau HTTPS (port par défaut 443 sur MICROSESAME et TILLYS CUBE) : Application Web et API REST	Gestion de l'authentification et des privilèges de l'utilisateur FS.1	Tous les utilisateurs ayant accès au réseau dédié à la sécurité physique - A.1 A.2 A.4

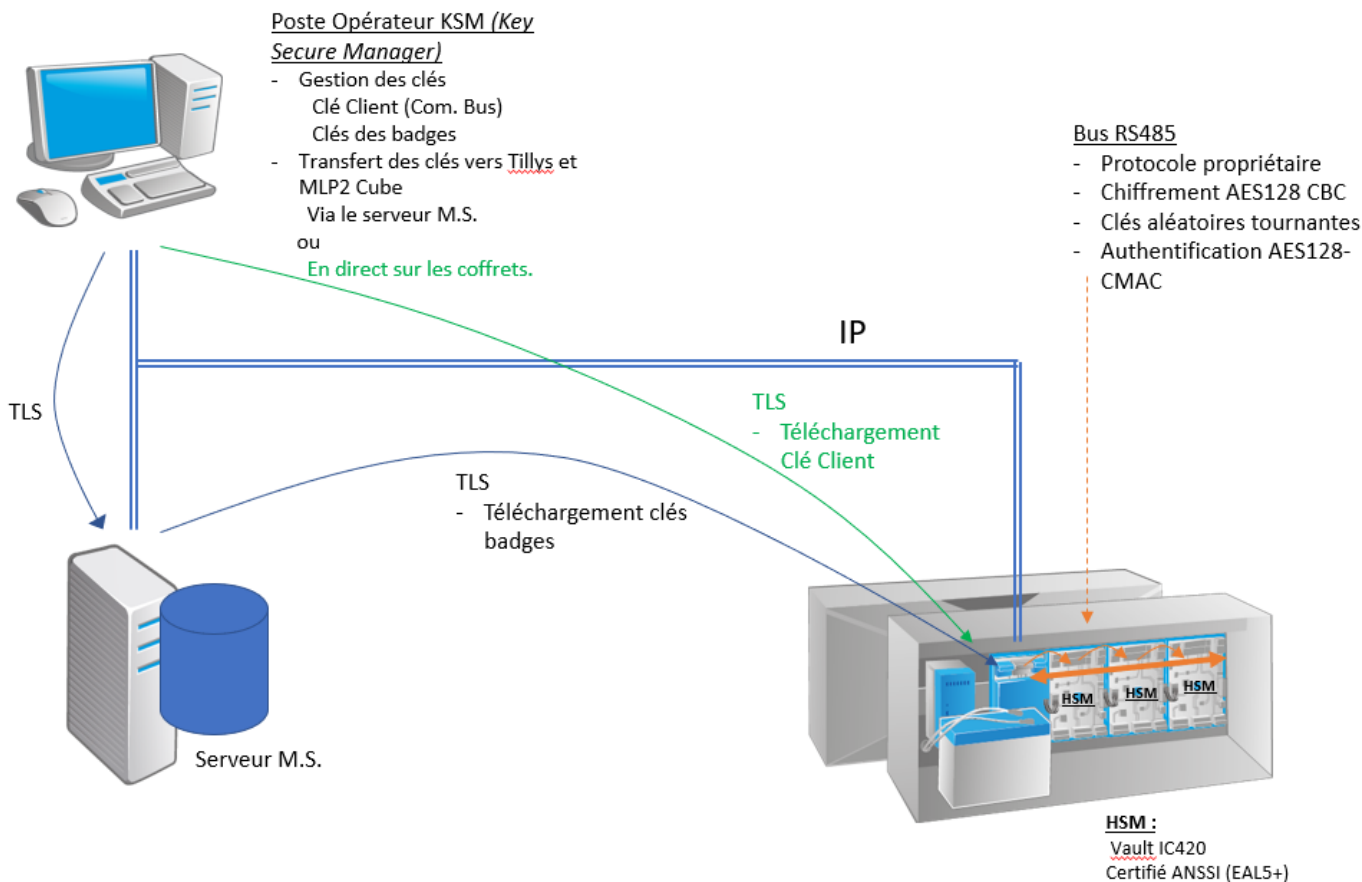
5. ANNEXES

5.1. DEFINITIONS ET ABBREVIATIONS

AID DESFire	Application ID Identifiant sur 3 octets des applications contenues dans un badge Desfire
APB	Anti-retour (ou Anti- passback) Mécanisme qui restreint les autorisations d'accès en fonction de la position de l'utilisateur dans les zones gérées en APB
Bus MLV3	Bus RS485 reliant une TILLYS-CUBE à ses modules d'extension
DESFire	Technologie de badge RFID d'origine NXP
GAC	Gestion des accès contrôlés
GTB	Gestion Technique du Bâtiment
HSM	Hardware Security Module, correspond à la notion de SAM dans la [NOTE 7]
ID	Numéro Identifiant
KSM	Utilitaire HIRSCH de gestion et distribution des clés de chiffrement entrant dans la sécurité d'un système MICROSESAME. L'utilisation de KSM permet de garantir la confidentialité des clés
LAN	Réseau local
MLP2	Module d'extension pour la gestion de 2 portes. Le MLP2 est piloté par une TILLYS-CUBE
Périmètre de clé	Information définie sur MICROSESAME et reprise dans KSM. Elle permet à la solution MS de limiter les conséquences d'une éventuelle corruption de clés en créant des périmètres de clés. Cela concerne des installations centralisées avec des implantations locales ayant chacune un périmètre de clé des badges qui leur est propre
PIN	Code à saisir au clavier dans le cas d'accès à contrôle renforcé (badge autorisé + code)
Rail DIN	Mode de fixation standardisé des modules TILLYS-CUBE et modules d'extension ML-xx dans les coffrets. Ce mode est très répandu dans les tableaux électriques BT
RF	Radio Fréquence
RFID	Identification par Radio Fréquence ou aussi appelé sans contact.
RS485	Interface de communication série basée sur une paire torsadée + écran. Permet des échanges point à point ou en bus
RSS	Responsable de la Sécurité du Site
RSSI	Responsable de la Sécurité du Système d'Information
Serveur MS	Serveur MICROSESAME, correspond à la notion de GAC dans la [NOTE 7]
TILLYS-CUBE	UTL de HIRSCH
UTL	Unité de Traitement Local La TILLYS CUBE et le module MLP2 sont les UTL de HIRSCH

5.2. MISES A LA CLE DES HSM

Flux des mises à la clé des HSM

**Principe de mise à la clé :**

1. La mise à la clé est faite en 2 temps :

a. Mise à la clé client des TILLYS CUBE / MLP2.

Cette opération est faite localement sur un réseau spécifique (isolé). Un poste KSM est alors relié directement sur un coffret pour la mise à la clé client.

b. Transfert des clés des badges dans les HSM. Si les clés KBadges[] sont connues, leur transfert dans les HSM est également possible depuis KSM sur le même réseau local isolé que ci-dessus. Sinon, ce transfert des clés des KBadges[] peut être différé, et réalisé en toute sécurité depuis KSM, via le serveur et le réseau du site, après la mise en place des coffrets.

Le serveur reste le point d'entrée privilégié de KSM pour cette opération:

- Il détient la liste des UTL connectées et de leur territoire d'appartenance.
- Il est en capacité de communiquer avec toutes les UTL.

2. Installation des certificats (TLS) sur le serveur et les UTL :

Un certificat auto-signé est généré à titre provisoire sur les équipements. Ces certificats doivent impérativement être remplacés par des certificats valides et propres à chaque déploiement.