CIBLE DE SECURITE CSPN

CIBLE DE SECURITE – CONTROLE DES ACCES

MICRO-SESAME V2018.1

Ce document est la propriété de TIL TECHNOLOGIES.

Cible de sécurité CSPN : Contrôle des accès physiques

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 ML-P2 (Gestion Anti-arrachement Lecteur Clavier)	TIL
09/07/2018	3.4	Mise à jour des versions firmwares ML-P2 & TILLYS NG (Protection des firmwares en AES CBC, réduction délais du certificat)	TIL

Références documentaires

Source	Référence	Version	Titre
ANSSI	[STSC]	1.0	Sécurité des technologies sans-contact pour le contrôle des accès physiques du 19/11/2012
ANSSI	[NOTE-21]	560/ANSSI/SDE/PSS/CCN	Méthodologie pour l'évaluation d'une gamme de produit
STID	[PRTC]	1.3	Protocole de communication SSCP V2
TIL	[SPEC_CRYPTO]	3.2	Spécifications cryptographiques MICRO-SESAME V2018.1
TIL	[GUIDE]	1.1	Guide d'administration Micro-Sésame
TIL	[SPEC_MLV3]	1.2	Protocole MLV3

Liste de diffusion

NOM	Prénom	Société	Contact
-	-	ANSSI	-
MESONA	Jean-Marc	TIL	jm.mesona@til-technologies.fr
BREMOND	Lionel	TIL	l.bremond@til-technologies.fr
REYRE	Olivier	TIL	o.reyre@til-technologies.fr
VIAZZI	Mathieu	TIL	m.viazzi@til-technologies.fr

Ce document est la propriété de TIL TECHNOLOGIES.

TABLE DES MATIERES

1. Identification du produit 5
2. Argumentaire du produit 6
2.1. Description générale du produit 6
a. Présentation de la solution d'accès 6
b. Architecture de la solution d'accès 7
c. Description fonctionnelle et utilisation 7
d. Raccordements & Réseaux 8
e. Réseaux dédiés 8
f. Serveur M.S 9
g. Module de base TILLYS-NG 10
h. Module d'extension ML-P2 déporté 12
i. Lecteur de badge transparent 12
j. Badge 12
2.2. Description de l'environnement d'utilisation du produit 13
2.3. Description des fonctions d'accès 13
a. Identification RFID 13
b. Identification avec confirmation par code PIN 13
2.4. Description des hypothèses sur l'environnement du produit 14
a. Hypothèses sur l'environnement physique du produit 14
b. Hypothèses sur les utilisateurs du produit 14
c. Hypothèses sur l'environnement technique du produit 15
2.5. Description des utilisateurs 16
2.6. Description du perimetre d'évaluation 18
3. Description de l'environnement technique 19
3.1. Dispositif d'accès 19
3.2. Dispositif de raccordements et d'alimentation 19
3.3. Poste informatique 19
3.4. Badges 19
4. Données sensibles 20
5. Mesures d'environnement 21
5.1. Environnement 21

Ce document est la propriété de TIL TECHNOLOGIES.

5.2. Organisations 22
5.3. Mesures de sécurité 22
6. Description des menaces 23
6.1. Agents menaçants 23
6.2. Liste des Menaces 23
7. Description des fonctions de sécurité 25
7.1. Liste des fonctions de sécurité 25
7.2. Argumentaire des fonctions de sécurité 28
8. Définitions et abbréviations 29
9. Annexes 30

Ce document est la propriété de TIL TECHNOLOGIES.

1. IDENTIFICATION DU PRODUIT

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

Organisation éditrice	TIL
Lien vers l'organisation	www.til-technologies.fr
Nom commercial du produit	Micro-Sésame
Numéro de la version évaluée	M.S. V2018.1.2.25223 TILLYS-NG V2.0.0.5234 ML-P2 V2.0.0.953
Catégorie de produit	Identification, authentification et contrôle d'accès

Ce document est la propriété de TIL TECHNOLOGIES.

2. ARGUMENTAIRE DU PRODUIT

2.1. DESCRIPTION GENERALE DU PRODUIT

a. Présentation de la solution d'accès

La solution Micro-Sésame correspond à une solution intégrée pour une gestion centralisée de contrôle d'accès physique.

Elle est composée :

- d'une partie appelée « Serveur » intégrant les postes clients, les bases de données et le serveur pour la configuration et l'exploitation de la solution,
- D'une partie appelée « Coffrets » intégrant les équipements de terrain :
  - Alimentation secourue et sa batterie.
  - Module de base TILLYS-NG.
  - Module d'extension ML-P2 pour la gestion de 2 lecteurs de badges. Ces modules peuvent être déportés car connectés au module de base par bus RS485 (Bus MLV3).
- De lecteurs de badges.

Le système est architecturé autour des équipements représentés ci-dessous et 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 (UTL),
- Automatisme d'accès (déverrouillage, séquencement d'opérations de contrôle de l'ouvrant, état de l'accès physique) géré au niveau du coffret.

Ce document est la propriété de TIL TECHNOLOGIES.

b. Architecture de la solution d'accès

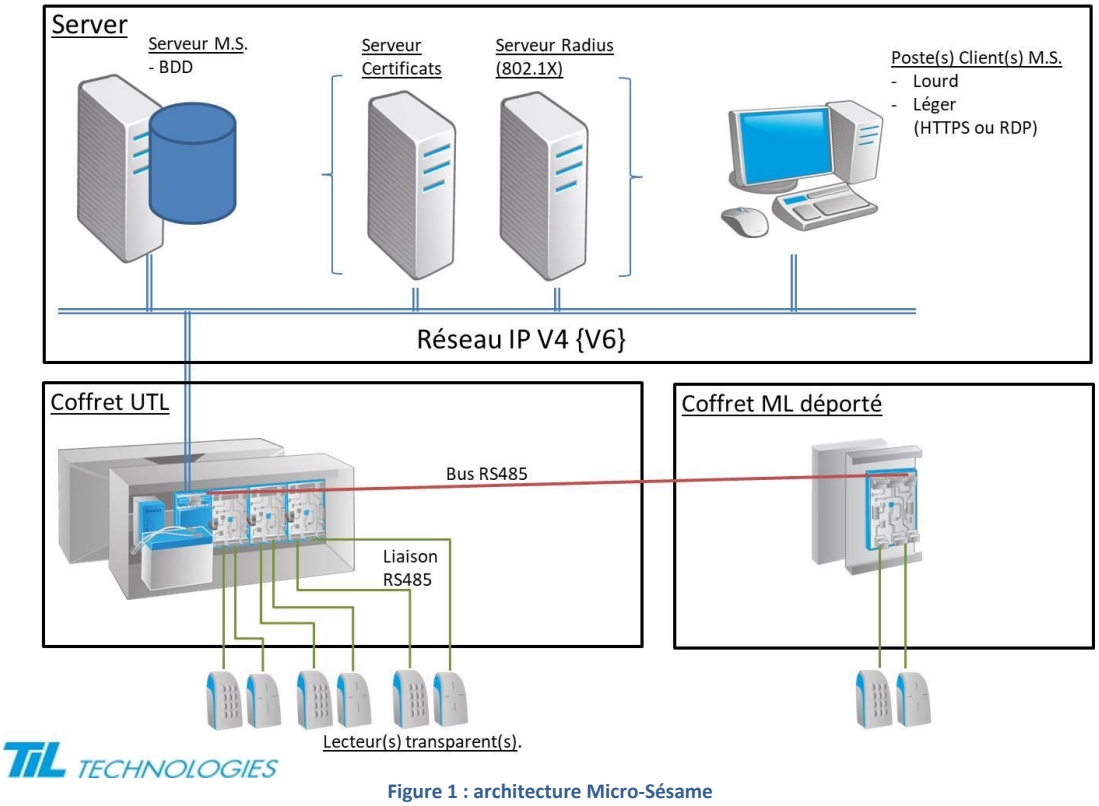


Figure 1 : architecture Micro-Sésame

c. Description fonctionnelle et utilisation

La solution Micro-Sésame permet une gestion centralisée et en temps réel des accès physiques. Les fonctions d'accès sont gérées par une application métier « Serveur ».

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'usagers afin de leur attribuer des droits d'accès.

L'application MS serveur permet :

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

Pour répondre à ces besoins, la solution Micro-Sésame repose :

- sur les équipements suivants côté application métier :
  - un serveur et base de données centrale,
  - des postes clients pour l'exploitation.
- sur les équipements de terrain suivants :
  - des coffrets UTL (enveloppe métallique) avec le module de base TILLYS-NG et un système d'alimentation en énergie (alimentation secourue),
  - des modules d'extension ML-P2 qui peuvent être soient dans le coffret (jusqu'à 4 modules d'extension), soit déportés (jusqu'à 4 déportables),

Ce document est la propriété de TIL TECHNOLOGIES.

- des lecteurs de badges (TIL EVOLUTION),
- des badges d'accès (Mifare Desfire EV1).

d. Raccordements & Réseaux

Le serveur MS, la base de données et les postes clients pour l'exploitation sont raccordés au réseau du client. Ce réseau est généralement un réseau Ethernet sous TCP/IP (IP V4/V6) qui est établi, maintenu et entièrement administré par le client final.

Le réseau LAN du client assure les échanges entre le Serveur et les coffrets (UTL).

Le réseau du client et la communication entre poste client / serveur M.S pour l'exploitation sont **hors périmètre** de l'évaluation CSPN.

e. Réseaux dédiés

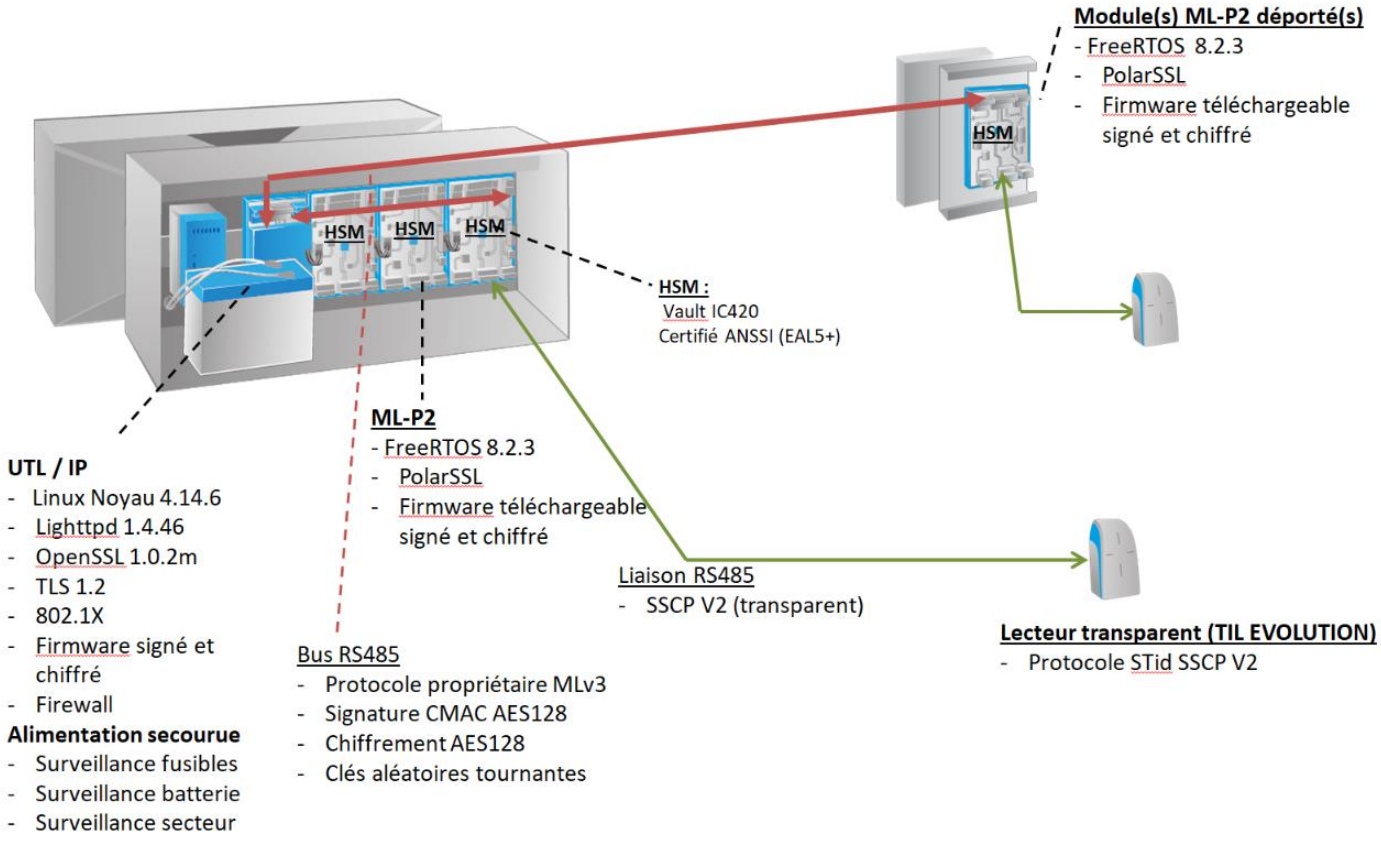


Figure 2 : architecture coffret et module déporté (contrôleur d'accès)

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

Il y a 2 types de réseaux dédiés :

- Les interfaces bus RS485 entre module de base TILLYS-NG et les modules d'extension ML-P2 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.

Ce document est la propriété de TIL TECHNOLOGIES.

- Les interfaces RS485 entre coffret (UTL) et les lecteurs d'accès : ces interfaces correspondent à des liaisons filaires donnant généralement sur des zones protégées ou publiques.

L'interface RS485 entre coffret (UTL) et les lecteurs d'accès fait partie du périmètre d'évaluation.

L'interface BUS RS485 entre coffret (UTL) et les modules ML-P2 déportés fait partie du périmètre d'évaluation.

f. Serveur M.S

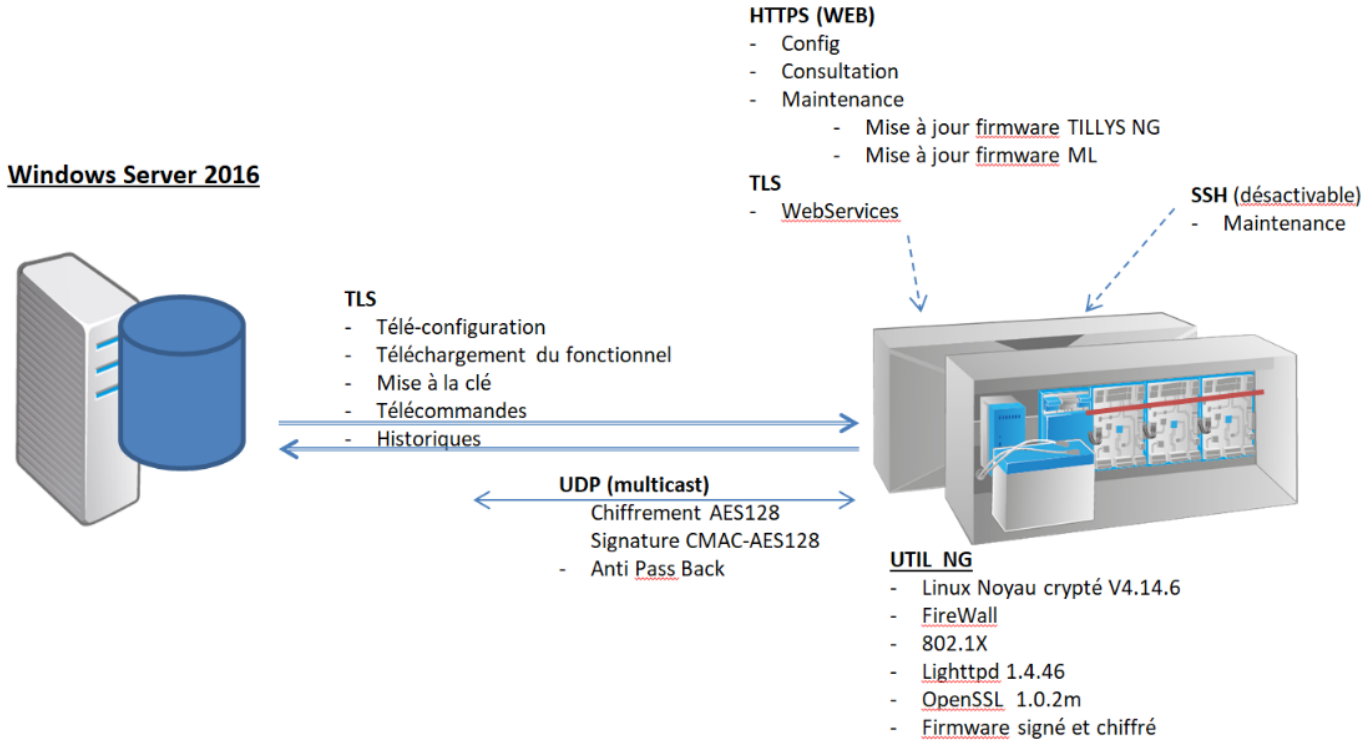


Figure 3 : Communication entre le serveur M.S et le coffret

Le serveur M.S permet la gestion centralisée des accès. Il s'agit d'un poste Windows Serveur avec une base de données Microsoft SQL. Il permet :

- La configuration : permet de définir l'architecture avec les différents équipements déployés sur site (module de base TILLYS-NG, modules d'extension dans le coffret, modules d'extension déportés, lecteurs de badges et badges) au travers d'échanges centralisés,
- L'exploitation pour la gestion des accès, des alarmes, des événements au travers d'échanges en temps réel et centralisés.

La communication entre le « coffret UTL » et le serveur M.S fait partie du périmètre de l'évaluation.

Ce document est la propriété de TIL TECHNOLOGIES.

g. Module de base TILLYS-NG

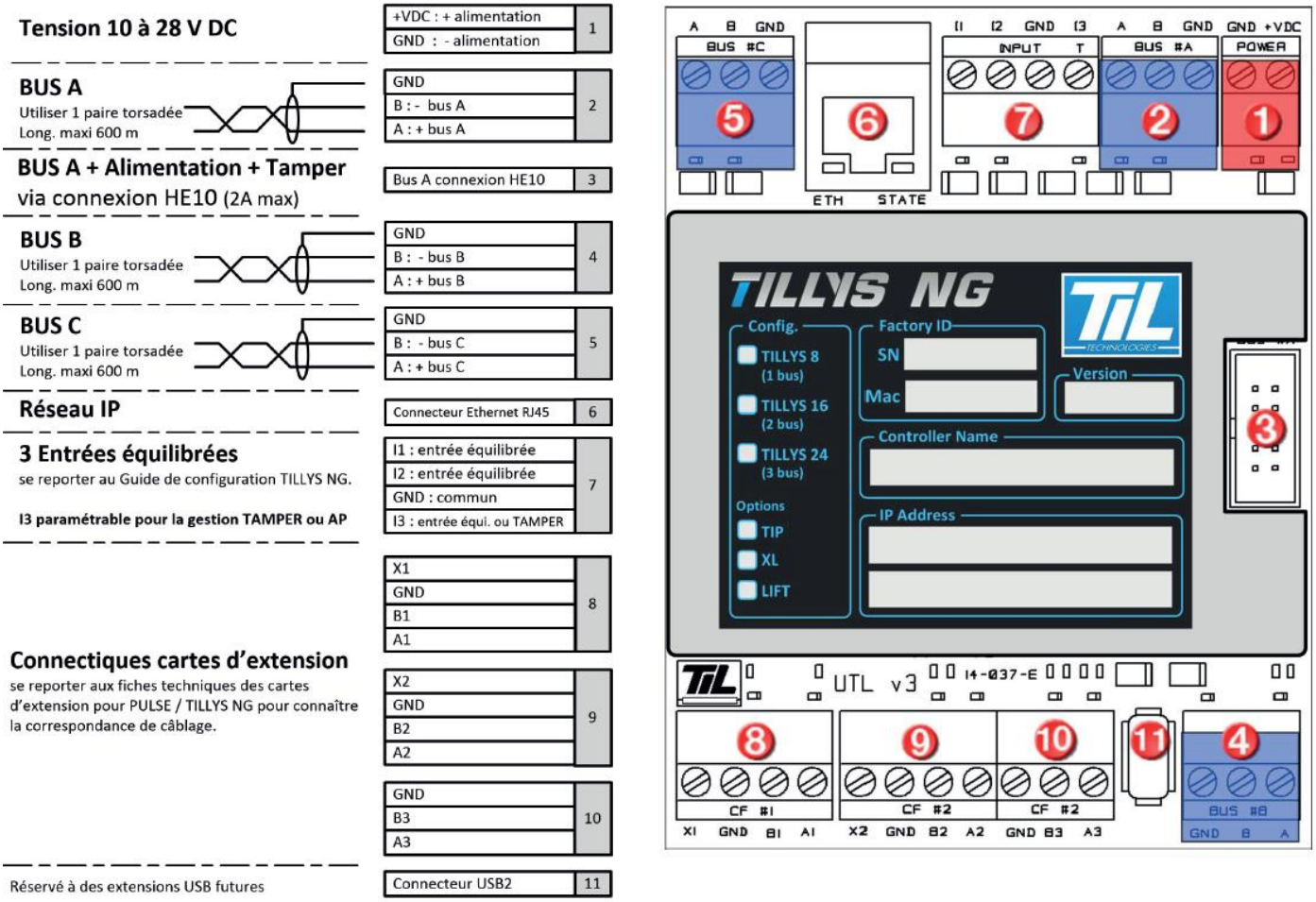


Figure 4 : Description matérielle module de base TILLYS-NG

Caractéristiques module de base TILLYS-NG	
Communication réseau IP	Carte réseau Ethernet 10/100 Mb base T auto-adaptatif (IP fixe ou DHCP), 802.1x, IPV6 ready, cryptage AES 256 bits
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 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 résistance possible
Signalisations	LED sur l'alimentation, le réseau, les bus et chaque entrée
Conformités	CE, RoHS

Ce document est la propriété de TIL TECHNOLOGIES.

Le module TILLYS NG est un automate IP compact qui peut être emboité 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'authentification du badge transmis par le lecteur de badge transparent.

Cet automate unique avec une seule version de firmware permet d'avoir plusieurs configurations possibles :

- TILLYS-NG + Configuration 1 bus,
- TILLYS-NG + Configuration 2 bus,
- TILLYS-NG + Configuration 3 bus.

Pour chacune des configurations, plusieurs options ont possibles :

- Option XL : Augmentation du nombre de personnes (> 10 000),
- Option Intrusion-TIP : Activation de la fonctionnalité de transmission d'alarmes vers télésurveilleur,
- Option LIFT : Activation de la fonctionnalité lecteur de cabine ascenseur.

La configuration du module de base TILLYS-NG : « TILLYS-NG + configuration 1 bus » fait partie du périmètre de l'évaluation.

Ce document est la propriété de TIL TECHNOLOGIES.

h. Module d'extension ML-P2 déporté

Le module d'extension ML-P2 déporté se connecte sur un des bus secondaires du module de base TILLYS-NG.

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.

Emboité sur rail DIN et équipé de connecteurs rapides pour le montage en coffret, le module d'extension ML-P2 peut également être déporté jusqu'à 600 m du module de base TILLYS-NG et intégré dans un boîtier équipé d'un contact d'autoprotection à l'ouverture.

Il est également protégé contre les mauvaises manipulations ou le sabotage.

Le module d'extension ML-P2 déporté est dans le périmètre de l'évaluation.

i. 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 coffret (UTL).

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

- Les lecteurs EVO ST, réf. LEC05XF5200-NB5 qui permettent l'initialisation d'échange de données avec les badges DESFire qui leur sont présentés (RFID),
- Les lecteurs EVO KB, réf. LEC05XF5240-NB5 qui permettent l'initialisation d'échange de données avec les badges DESFire qui leur sont présentés (RFID) et exige un code PIN pour authentifier[1] les porteurs de badge.

Les lecteurs « EVO ST (LEC05XF5200-NB5) et EVO KB (LEC05XF5240-NB5) sont dans le périmètre de l'évaluation.

j. Badge

Le badge (NXP Mifare DESFire) permet d'identifier et d'authentifier le porteur directement à l'UTL (module de base TILLYS-NG). Le badge est sécurisé (Niveau de sureté : 1, 2, 3 voir tableau 2 du document [STSC]) et ne peut donc être cloné. Le badge contient les éléments secrets suivants : clés de chiffrement des échanges.

La communication entre le badge et le lecteur (communication sans contact) est **hors périmètre** de l'évaluation.

[1] Authentification double (badge + code PIN).

Ce document est la propriété de TIL TECHNOLOGIES.

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

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

- Les badges DESFire autorisent le chiffrement des échanges avec AES128. TIL 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 2 du document [STSC]),
- Données névralgiques et clés : téléchargées dans le module de base TILLYS-NG depuis le serveur M.S : le mode transparent correspond au schéma de l'architecture « 1 » hautement recommandée par l'ANSSI (chapitre 4.3.1 du document [STSC]). Cette architecture regroupe le canal sans fil (Interface RF avec le badge) et la liaison filaire avec l'UTL (coffret).

2.3. 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 TIL. 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).

Ce document est la propriété de TIL TECHNOLOGIES.

2.4. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT DU PRODUIT

a. Hypothèses sur l'environnement physique du produit

H.SERVEUR_MS

Il est supposé que le serveur est installé dans un local sécurisé dont l'accès est strictement limité aux personnels habilités (dont les opérateurs).

H.POSTE_OPERATEUR

Les équipements d'administration doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs et aux opérateurs.

H.COFFRET

Le coffret ainsi que le système d'alimentation secouru sont installés dans un local sécurisé dont l'accès est limité.

H.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 ML-P2 déportés est supposé direct. Le câblage de l'ensemble des équipements constituant les environnements de porte est direct : point à point.

H.POSTE_KSM_NG

Un poste KSM NG 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.

b. Hypothèses sur les utilisateurs du produit

H.OPERATEURS

Les opérateurs en charge de la configuration, de la maintenance des postes et des serveurs M.S sont supposés être compétents, formés et de confiance.

H.EXPLOITANTS

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).

Ce document est la propriété de TIL TECHNOLOGIES.

H.AGENTS_TECHNIQUES

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.

H.PORTEURS_BADGES

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).
- Ils sont supposés ne pas confier leur badge, ni communiquer leur code PIN personnel.

c. Hypothèses sur l'environnement technique du produit

H.RESEAU_CLIENTS

Le réseau 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 deux réseaux. Les échanges de données entre les deux réseaux passent systématiquement par le serveur ou via des équipements de type pare-feu à la charge du client. Le réseau LAN du client est placé en zone protégée.

H.PROTECTION_TRANSMISSION_IDENTIFIANT

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.

H.RESEAU_LAN

Le réseau LAN du client est placé en zone protégée et technique.

H.POSTE_SECURE

Les postes d'exploitation sont placés en zone sécurisée.

H.CERTIFICATS_TLS : Le certificat TLS utilisé par le composant TILLYS-NG est à la charge du client final. Ce certificat utilise des algorithmes conformes au RGS et l'administrateur respecte les recommandations du guide d'administration [GUIDE].

H.CLES_KSM

Le générateur d'aléa utilisé pour obtenir les clés nécessaires au fonctionnement de la TOE est conforme au RGS.

Ce document est la propriété de TIL TECHNOLOGIES.

H.CLES_FIXES

Les clés fixes utilisées par la TOE ont été générées par un générateur d'aléa conforme au RGS. La description de ces clés est fournie dans le document [SPEC_CRYPTO].

H.CLES_BADGES

Les clés des badges sont soient tirées, soient saisies depuis l'utilitaire KSM NG. On suppose que le générateur d'aléa utilisé pour obtenir ces clés est conforme au RGS.

H.PIN

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 supposée être conforme au RGS.

H.Protection en transmission de l'identifiant d'accès (ID)

L'ID (identifiant personnel) d'un usager est encodé dans une application de son badge d'accès (application d'accès dans un badge DESFire EV1).

Cet ID est protégé en lecture par un chiffrement en AES 128 bits avec clé AES 128b (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 EV1 (APDU et cryptographie DESFire EV1).

2.5. DESCRIPTION DES UTILISATEURS

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.

Opérateurs : L'opérateur a pour fonction de configurer et d'effectuer la maintenance des postes clients et des serveurs MS.

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 au contrôleur est tracée dans l'historique des événements.

Ce document est la propriété de TIL TECHNOLOGIES.

Porteurs de badges : Les porteurs de badges correspondent aux utilisateurs finaux (Employés, visiteurs, prestataires, stagiaires…). Ils disposent de badges sans contact (RFID) personnel.

Ce document est la propriété de TIL TECHNOLOGIES.

2.6. DESCRIPTION DU PERIMETRE D'EVALUATION

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

- Le coffret (UTL) : TILLYS-NG + option 1 bus accueillant jusqu'à 8 lecteurs de badges transparents (avec le même protocole de communication SSCP, voir document [PRTC]) ;
- Le module ML-P2 déporté ;
- Les lecteurs transparents « EVO ST (LEC05XF5200-NB5) et EVO KB (LEC05XF5240-NB5).

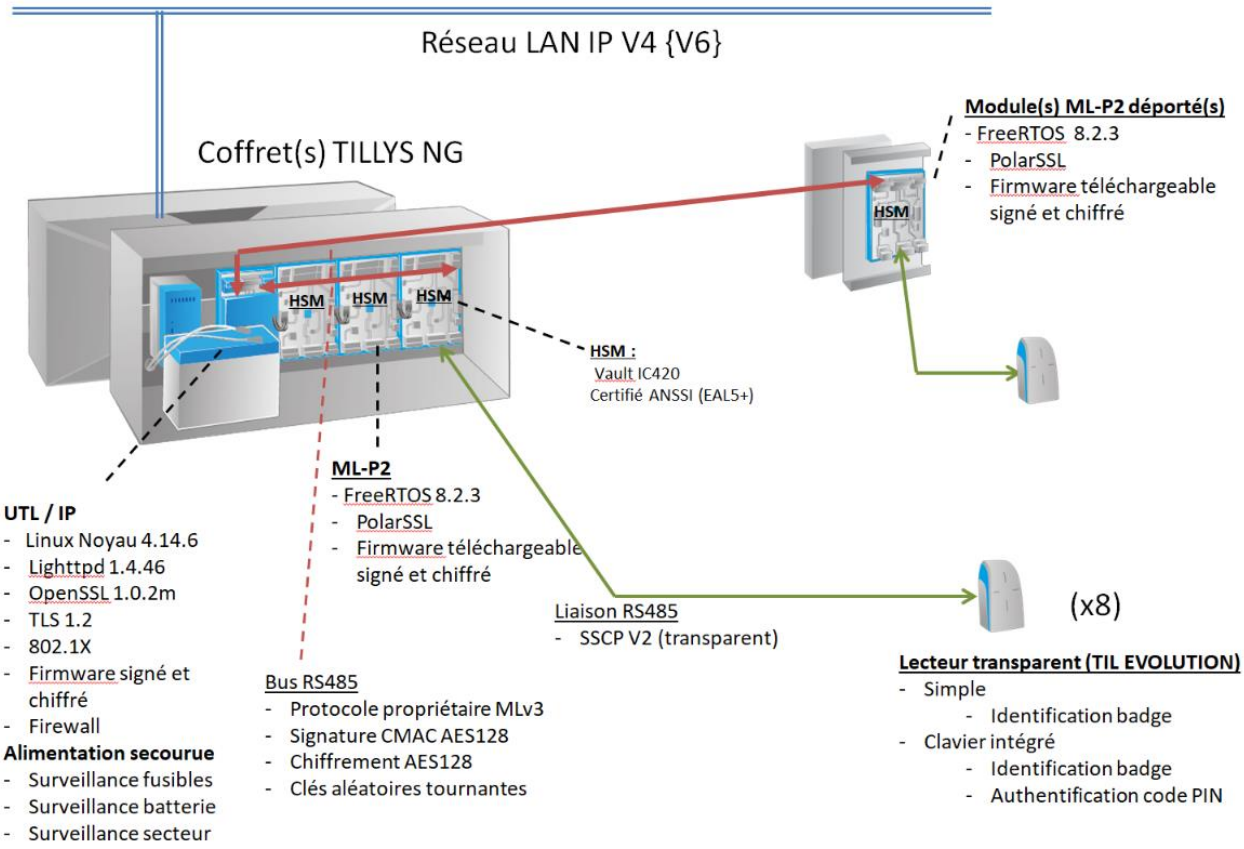


Figure 5 : Périmètre d'évaluation

Les échanges Coffret / Lecteur et module déporté ML-P2 / Lecteur utilisent les commandes du protocole SSCP V2 (voir document [PRTC]).

La note 21 de l'ANSSI [NOTE-21] permet de couvrir les 2 configurations « avec et sans module déporté ML-P2 ».

Ce document est la propriété de TIL TECHNOLOGIES.

3. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE

3.1. DISPOSITIF D'ACCES

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

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

3.2. 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 ML-P2 : liaisons filaires en zones protégées, liaisons dédiées RS485,
- Entre module déporté ML-P2 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.

3.3. POSTE INFORMATIQUE

Les logiciels suivants doivent être installés sur les serveurs MS et les postes clients (Configuration & Exploitation) :

- Microsoft Windows Server 2016,
- Microsoft Windows 10 (64 bits).

3.4. 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 MS.

Dans tous les cas, les badges correspondront aux niveaux II et III du tableau 2 des niveaux de sûreté décrits dans le document [STSC].

Ce document est la propriété de TIL TECHNOLOGIES.

4. DONNEES SENSIBLES

Le tableau ci-dessous référence les biens sensibles de la TOE et leurs besoins de sécurité :

	Confidentialité	Authenticité	Intégrité
Firmware		X	X
Clés des badges	X		
Matériel cryptographique	X		
ID	X		
Code PIN	X		
Droits/autorisation utilisateurs	X		X

Firmware : Afin d'assurer un fonctionnement correct, le firmware des modules doit être protégé à la fois en intégrité et en authenticité.

Les données névralgiques confidentielles regroupent plusieurs types d'informations :

- Clés badges : Les clés des badges permettent de sécuriser les communications entre les badges et le MLP2.
- Matériel cryptographique : la TOE gère et utilise plusieurs clés symétriques et une bi-clé RSA. La description de ces clés est donnée dans la section 3.1 du document [SPEC_CRYPTO].
- 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 opérateur et mémorisés dans la base de données du serveur. Ils sont téléchargés dans le module TILLYS NG via le protocole sécurisé TLS et sont mémorisés dans la base de données interne au module TILLYS NG.

Ce document est la propriété de TIL TECHNOLOGIES.

5. MESURES D'ENVIRONNEMENT

5.1. ENVIRONNEMENT

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

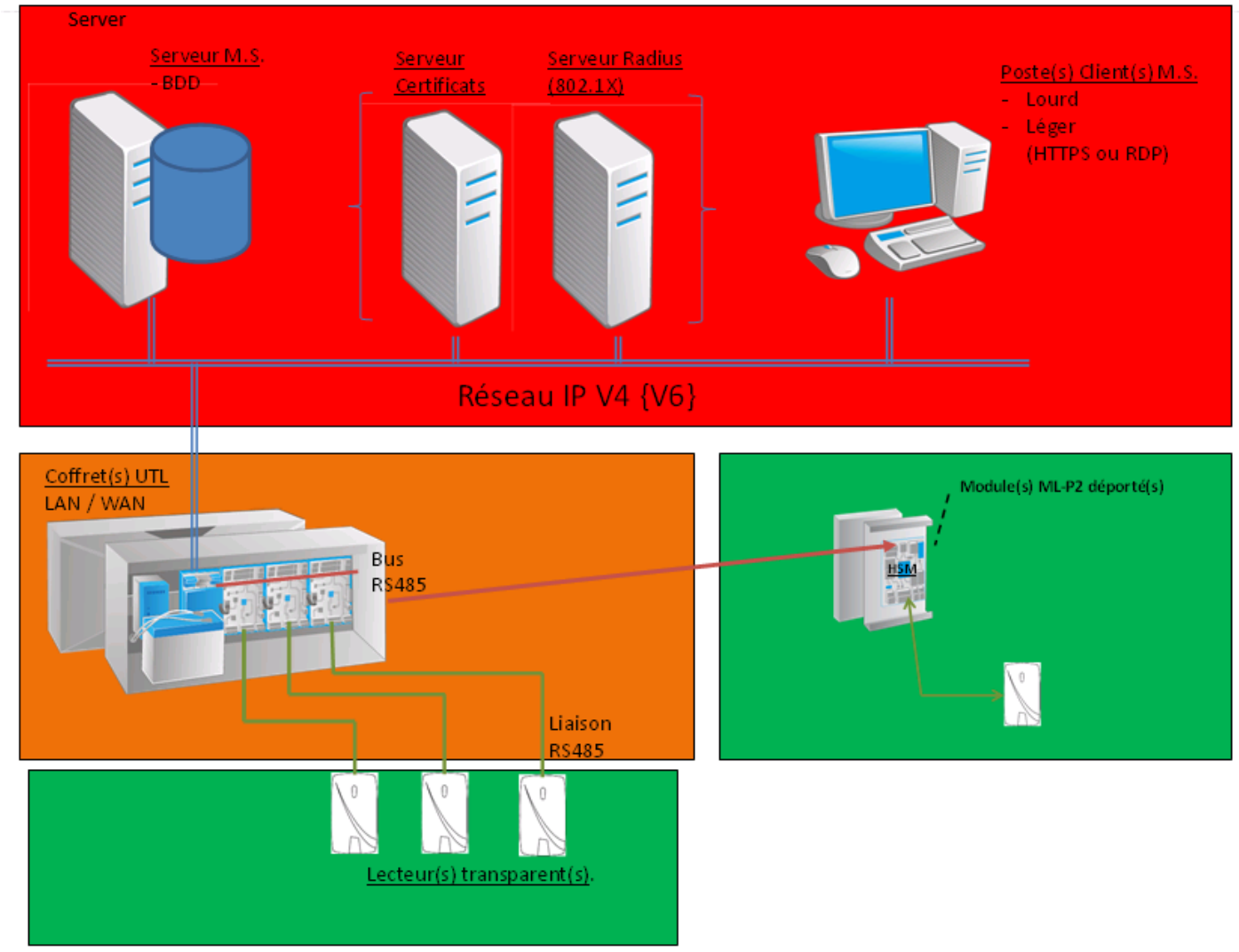


Figure 6 : Architecture type

Zone verte : accessible à tout le monde.

Zone orange : accessible aux employés autorisés et aux visiteurs accompagnés.

Zone rouge : accessible aux seuls employés autorisés et aux visiteurs accompagnés au moyen d'un badge et d'un code.

Ce document est la propriété de TIL TECHNOLOGIES.

5.2. ORGANISATIONS

La solution Micro-Sésame 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).

5.3. MESURES DE SECURITE

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-NG 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-NG 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, autoprotections, 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).

Ce document est la propriété de TIL TECHNOLOGIES.

6. DESCRIPTION DES MENACES

6.1. AGENTS MENAÇANTS

Pour cette évaluation les attaquants suivants sont considérés :

- Attaquant sur le réseau TCP/IP établi entre le serveur MS et le coffret (UTL),
- Attaquant sur le réseau BUS RS485 avec le protocole propriétaire entre le coffret (UTL) et le module déporté ML-P2,
- Attaquant sur le réseau dédié RS485 entre le coffret (UTL) et les lecteurs de badges,
- Attaquant sur le réseau dédié RS485 entre le module déporté ML-P2 et les lecteurs de badges.

Différentes attaques physiques sont considérées :

- Attaque sur le coffret (UTL)
- Attaque sur le module déporté ML-P2
- Attaque sur les lecteurs transparents

6.2. 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 :

Ecoute du canal Serveur M.S – Coffret(s) (UTL) :

Les attaquants disposent de moyens d'écoute 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.

Ecoute des canaux réseaux dédiés RS485

Les attaquants malveillants disposent de moyens d'écoute 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 :

Ce document est la propriété de TIL TECHNOLOGIES.

- 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 les plages horaires (Elargir des périodes d'accès) ;
- Ecoute d'une transaction contenant l'affectation des droits (Modifier/étendre des droits) ;
- Ecoute d'une transaction contenant des commandes (Ouverture d'un accès) ;
- Ecoute des transactions avec le coffret (Emulation d'un ou plusieurs coffrets).

Attaque sur le coffret (UTL)

Tentative de déchiffrement et lecture du code exécutable.

Substitution d'un coffret.

Attaque sur le module déporté ML-P2

Tentative de déchiffrement et lecture du code exécutable.

Substitution d'un module déporté ML-P2.

Attaque sur le lecteur ou lecteur – clavier transparent

Tentative de remplacement du lecteur transparent.

Emulation / Substitution.

Corruption du firmware

L'attaquant parvient à injecter et faire exécuter un firmware corrompu sur la ToE. 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 la ToE 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.

Ce document est la propriété de TIL TECHNOLOGIES.

7. DESCRIPTION DES FONCTIONS DE SECURITE

7.1. LISTE DES FONCTIONS DE SECURITE

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

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 ML-P2 (déporté ou non) grâce au protocole constructeur du lecteur SSCP v2.

Protection des données échangées entre le serveur MS et les coffrets (UTL)

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 TLS Serveur -> Coffret occasionnel :

- Configuration des TILLYS-NG
- Téléchargement des porteurs de badges, de leurs identifiants et de leurs accès

Canal TLS Serveur -> Coffret maintenu :

- Historique des passages de badges
- Alarmes et Evénements GTB
- Télécommandes

Les commandes et les transactions échangées entre le Serveur et les coffrets (UTL) sont protégées en confidentialité.

2. ***Les échanges UDP multicast*.**

Il s'agit de trames de diffusion uniquement mises en œuvre par les mécanismes de gestion de l'anti-passback. Les commandes échangées entre les TILLYS-NG et le serveur MS sont protégées en confidentialité et intégrité. L'anti-passback est un mécanisme qui restreint les autorisations d'accès en fonction de la position de l'usager dans les zones gérées en APB.

Protection des données échangées entre les coffrets (UTL) et le module déporté ML-P2

Ce document est la propriété de TIL TECHNOLOGIES.

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 ML-P2 et le coffret (UTL) sont protégées en confidentialité.

Les tentatives de rejeu sont limitées par la mise en œuvre d'un protocole propriétaire [SPEC_MLV3] et chiffré.

Sécurisation des coffrets (UTL)

Le coffret (UTL) est placé en zone protégée. La détection de défaut génère systématiquement des alarmes techniques vers le serveur MS. 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-NG est doté d'un firewall activable et configurable en vue de filtrer les tentatives d'accès au coffret.

Sécurisation des modules déportés ML-P2

La détection de défaut génère systématiquement des alarmes techniques vers le serveur MS. Cette détection concerne trois types de défaut :

- Arrachement,
- Ouverture ML-P2,
- Défaut communication du bus RS485,

Sécurisation du lecteur -clavier

A l'installation, une clé d'authentification est négociée entre le coffret (UTL) / module déporté ML-P2 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 ML-P2 est bloquée avec cet équipement et une alarme est remontée vers le serveur.

Pour débloquer la communication du coffret (UTL) / module déporté ML-P2 avec un lecteur-Clavier ou lecteur, une intervention d'une personne habilitée doit être réalisée au niveau du coffret (UTL).

Ce document est la propriété de TIL TECHNOLOGIES.

Signature du firmware

À chaque installation d'un nouveau firmware, l'intégrité et l'authenticité de celui-ci sont vérifiées par l'équipement (TILLYS-NG ou MLP2) avant sa prise en compte effective.

Ce document est la propriété de TIL TECHNOLOGIES.

7.2. ARGUMENTAIRE DES FONCTIONS DE SECURITE

	Ecoute du canal Serveur M.S – Coffret(s) (UTL)	Ecoute des canaux réseaux dédiés RS485	Attaque sur le coffret (UTL)	Attaque sur le module déporté ML-P2	Attaque sur le lecteur ou lecteur – clavier transparent	Corruption du firmware
Protection en transmission du code PIN		X				
Protection des données échangées entre le serveur M.S et les coffrets (UTL)	X					
Protection des données échangées entre les coffrets (UTL) et le module déporté ML-P2		X		X		
Sécurisation des coffrets (UTL)	X	X	X			
Sécurisation des modules déportés ML-P2				X		
Sécurisation du lecteur -clavier					X	
Signature du firmware						X

Tableau de couverture des menaces par les fonctions de sécurité.

Ce document est la propriété de TIL TECHNOLOGIES.

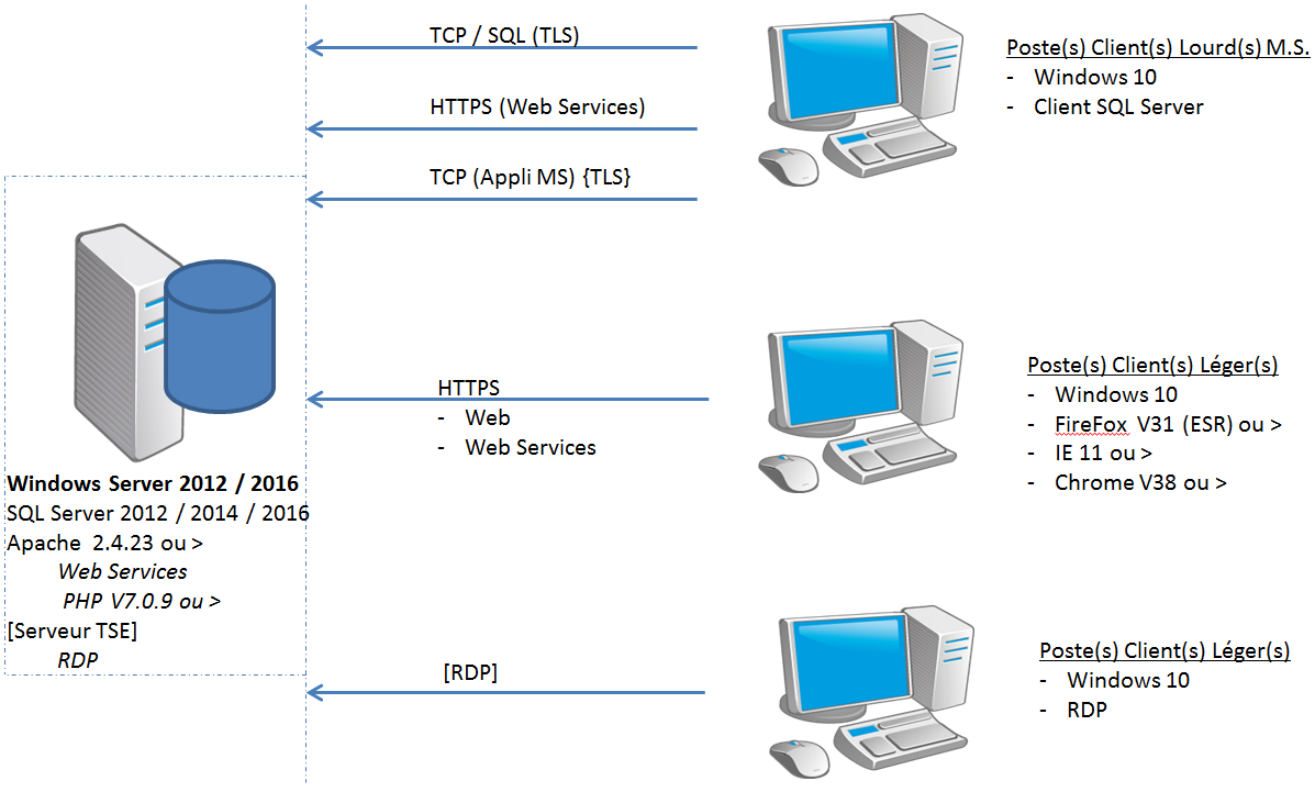
8. DEFINITIONS ET ABBREVIATIONS

RFID	Identification par Radio Fréquence ou aussi appelé sans contact.
RF	Radio Fréquence
ID	Numéro Identifiant
RSS	Responsable de la Sécurité du Site
RSSI	Responsable de la Sécurité du Système d'Information
PIN	Code à saisir au clavier dans le cas d'accès à contrôle renforcé : (Badge Autorisé + Code)
LAN	Réseau local
DESFire	Technologie de badge RFID d'origine NXP
AID DESFire	Application ID Identifiant sur 3 octets des applications contenues dans un badge Desfire
KSM-NG	Utilitaire TIL de gestion et distribution des clés de chiffrement entrant dans la sécurité d'un système Micro-Sésame. L'utilisation de KSM-NG permet de garantir la confidentialité des clés
UTL	Unité de Traitement Local La TILLYS NG est l'UTL de TIL Technologies
APB	Anti-passback (ou Anti-retour) Mécanisme qui restreint les autorisations d'accès en fonction de la position de l'usager dans les zones gérées en APB
TILLYS-NG	UTL de TIL Technologies
Serveur MS	Serveur Micro-Sésame
Périmètre de clé	Information définie sur Micro-Sésame et reprise dans KSM NG. Elle permet à la solution M.S. 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
RS485	Interface de communication série basée sur une paire torsadée + écran. Permet des échanges point à point ou en bus
ML-P2	Module d'extension pour la gestion de 2 portes. Le ML-P2 est piloté par une TILLYS-NG
Bus MLV3	Bus RS485 reliant une TILLYS-NG à ses modules d'extension
GTB	Gestion Technique du Bâtiment
Rail DIN	Mode de fixation standardisé des modules TILLYS-NG et Modules d'extension ML-xx dans les coffrets. Ce mode est très répandu dans les tableaux électriques BT
TOE	Target Of Evaluation (Cible d'évaluation)

Ce document est la propriété de TIL TECHNOLOGIES.

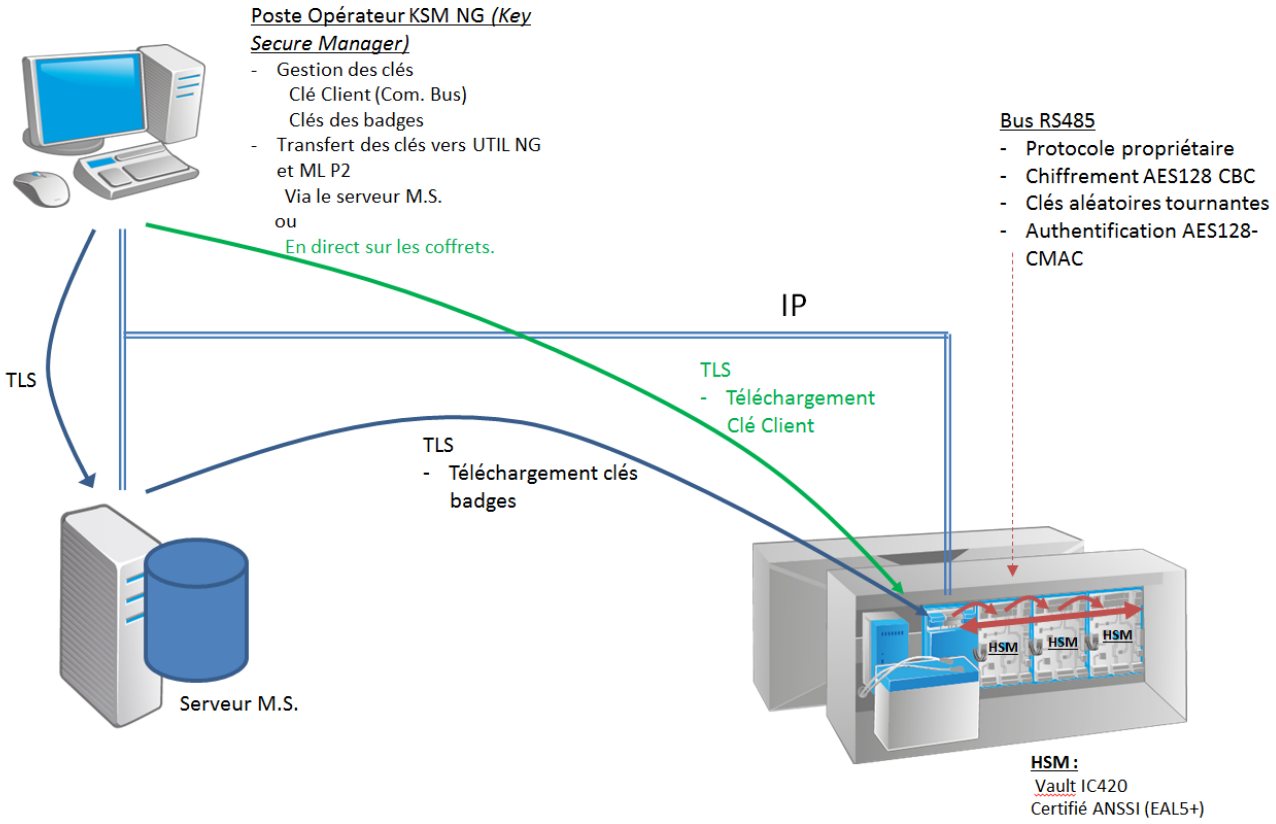
9. ANNEXES

Flux IP Serveur / Poste opérateur



Ce document est la propriété de TIL TECHNOLOGIES.

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 UTIL NG / MLP2.

Cette opération est faite localement sur un réseau spécifique (isolé). Un poste KSM NG 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 KBages[] sont connues, leur transfert dans les HSM est également possible depuis KSM NG 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 NG, 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-NG 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 peut être tiré à titre provisoire sur les équipements. Tout certificat auto-signé devra impérativement être remplacé par un certificat valide fourni par le Client.

Ce document est la propriété de TIL TECHNOLOGIES.