Cible de sécurité CSPN

Lecteurs LXS-W33-E/Ph5-7AD

Version 1.0

Suivi des modifications

Edition	Date	Auteur	Modifications
0.1	22/08/2011	Eric MUGNIER	Version initiale
0.2	16/09/2011	Eric MUGNIER	Précisions sur le périmètre de la cible
0.9	27/03/2012	Eric MUGNIER	Modification suite revue LETI-CESTI
1.0	11/07/2012	Eric MUGNIER	Modifications suite aux remarques de l'ANSSI

Table des matières

1 INTRODUCTION 3

2 IDENTIFICATION DU PRODUIT 3

3 ARGUMENTAIRE DU PRODUIT 3

3.1 DESCRIPTION GENERALE DU PRODUIT 3
3.2 ARCHITECTURE DU PRODUIT 3
3.3 DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT 4
3.4 HYPOTHESES ET REGLES DE SECURITE 5
3.4.1 Hypothèses sur l'environnement 5
3.4.2 Règles de sécurité 5
3.5 DESCRIPTION DES DEPENDANCES 5
3.5.1 Préconisation pour les outils tiers 5
3.5.2 Préconisation sur les éléments cryptographiques 5
3.6 DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES 5
3.7 DEFINITION DU PERIMETRE DE L'EVALUATION 6

4 ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT DU PRODUIT 7

4.1 ENVIRONNEMENT 7
4.2 UTILISATION CLASSIQUE 7

5 BIENS SENSIBLES DEVANT ETRE PROTEGES PAR LE PRODUIT 8

6 DESCRIPTION DES MENACES 9

6.1 MENACES PHYSIQUES 9
6.2 MENACES LOGICIELLES 9

7 DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT 9

7.1 GENERALITES 9
7.2 MAINTENANCE 10
7.3 ARRACHEMENT 10
7.4 AUTHENTIFICATION DES PARTIES 10
7.5 CHIFFREMENT ET AUTHENTIFICATION DE LA COMMUNICATION ENTRE LES PARTIES 11

8 DESCRIPTIONS DES MECANISMES CRYPTOGRAPHIQUES 11

9 ANNEXES 12

9.1 GLOSSAIRE 12
9.2 REFERENCES 12
9.3 CONTACTS 13

Table des figures

ARCHITECTURE FONCTIONNELLE DU LECTEUR - FIGURE 1 4
ARCHITECTURE INTERNE DU LECTEUR ET PERIMETRE DE SECURITE - FIGURE 2 6
ENVIRONNEMENT ET FONCTIONNEMENT - FIGURE 3 7

1 Introduction

Ce document décrit la cible de sécurité relative au produit LXS-W33-E/Ph5-7AD en vue de l'obtention d'une certification de sécurité de premier niveau des technologies de l'information (CSPN).

2 Identification du produit

Société éditrice	STid
Lien vers la société	www.stid.com
Nom commercial du produit	Lecteurs LXS W33–E/Ph5-7AD
Numéro de la version évaluée	1.0
Catégorie de produit	Identification, Authentification et Contrôle d'accès ; Communication sécurisée.

3 Argumentaire du produit

3.1 Description générale du produit

Constructeur d'équipements et développeur de solutions standards ou spécifiques, STid répond aux problématiques d'**identification de personnes** (contrôle d'accès, gestion horaire, etc.), de **véhicules** (contrôle d'accès automatique de véhicules, gestion de flottes, tracking, etc.) et d'**objets** (traçabilité d'objets critiques, logistique, etc.).

STid développe et commercialise une gamme complète de solutions et produits dédiés à l'identification des personnes. Elaborées sur les technologies RFID opérant à toutes les fréquences (125 kHz, 13.56 MHz et UHF), compatibles avec l'ensemble des technologies de puces (NXP Mifare® et DESFire, ST, EM, Inside, Legic, etc.) et standards internationaux (ISO 14443 A-B, ISO 15693, ISO 18000, etc.) les solutions STid intègrent les dernières fonctionnalités et niveaux de sécurité.

Les lecteurs STid de nouvelle génération basés sur les technologies Mifare Plus / DESFire EV1 permettent d'exploiter les dernières technologies de puces sans contact Mifare avec de nouveaux dispositifs de sécurisation des données. Ils utilisent tous les algorithmes de sécurité disponibles dans ces puces, anciens et nouveaux : Crypto1, DES, TDES, AES, etc. Un dispositif de chargement des clés de sécurisation par badge permet à l'utilisateur de personnaliser les lecteurs encodeurs en toute confidentialité et indépendance.
Ces lecteurs assurent la confidentialité des données entre le lecteur et le contrôleur/PC sur lequel ils sont raccordés, grâce au protocole de communication sécurisé SSCP. Le protocole permet le chiffrement des données (AES) et l'authentification mutuelle lecteur-contrôleur (HMAC-SHA) avant toute communication.

Le produit LXS-W33-E/Ph5-7AD dont il est question dans ce document est un lecteur RFId de technologie 13,56MHz, conforme aux normes RFId ISO 14443-A et 14443-B, il implémente en particulier toutes les fonctionnalités de la famille Mifare® de NXP. Mais, il peut être en outre utilisé avec toutes les puces conformes à ces normes.

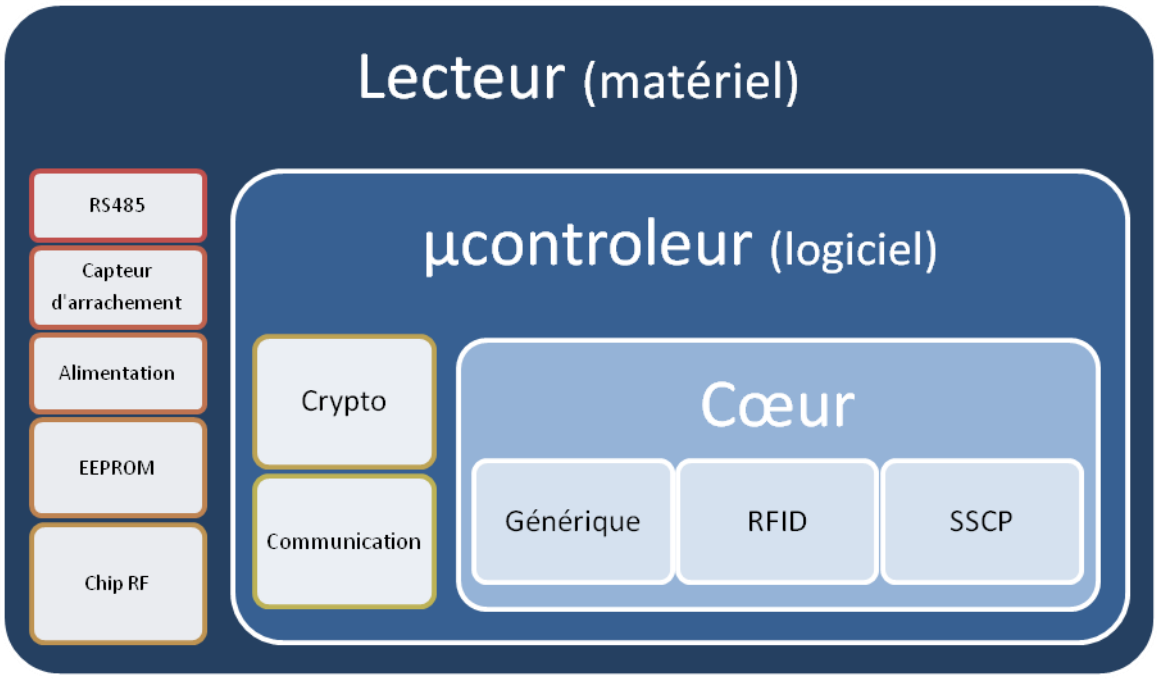
3.2 Architecture du produit

Nous allons décrire ici les différents modules fonctionnels constituant l'architecture du lecteur, ainsi que les liens et les protocoles de communication utilisés entre ces modules.

En utilisant le paradigme des poupées russes, l'architecture du produit se décompose en trois parties :

- Le lecteur au sens matériel
- qui intègre le microcontrôleur au sens logiciel
- qui intègre la partie cœur logiciel du lecteur

Le schéma suivant illustre les imbrications des ces trois parties.



Architecture fonctionnelle du lecteur - Figure 1

Description physique et fonctionnelle des trois parties :

1. Le lecteur est physiquement composé d'une partie *analogique* l'antenne RFId qui est hors domaine de la cible, et d'une carte *numérique* qui comprend : le microcontrôleur, un module d'alimentation, un module de communication (RS485), un capteur d'arrachement, une EEPROM où seront stockés les paramètres de fonctionnement du lecteur (entre autre les clés), et une puce RF qui réalisera le dialogue avec la carte RFId.
2. Le microcontrôleur embarque du code logiciel qui est divisé en plusieurs modules fonctionnels. La partie cryptographique, qui met en œuvre les méthodes décrites dans ce document, la gestion de la communication (empaquetage, gestion des trames ...) et un cœur logiciel.
3. Le cœur logiciel du microcontrôleur gère quant à lui toute la partie RFID, la mise en forme des données au format SSCP et toute la gestion générique et classique d'un code embarqué.

3.3 Description de la manière d'utiliser le produit

Une fois le produit connecté (et habituellement fixé à un montant de porte), il est démarré au lancement du système de contrôle d'accès et reste actif en permanence.
Il est piloté par le contrôleur, qui met en œuvre le protocole de communication sécurisé (SSCP v2) pour gérer le contrôle d'accès.
Le produit ne comporte en son sein aucun mécanisme physique de contrôle d'accès. Il n'y a par exemple ni relais d'ouverture/fermeture de gâche, ni capteur de comptage/détection de passage. Il est vu par le système comme une « tête RF » qui permet le lire/écrite des informations depuis/vers une carte RFId.

3.4 Hypothèses et règles de sécurité

3.4.1 Hypothèses sur l'environnement

Aucune hypothèse n'est faite sur l'environnement physique du produit, il est considéré en milieu hostile, un attaquant peut avoir un accès physique au produit.
L'attaquant n'a pas accès à l'UTL (le contrôleur), qui est en milieu sécurisé.
Le lien de communication entre le lecteur et le contrôleur est supposé permettre l'échange de données sans problème de perturbation électrique (signal parasite, bruit, diaphonie ...).
Le lecteur doit être physiquement fixé au mur et ne faire apparaître aucun élément d'interconnexion (réseau de données ou réseau électrique).
Le code embarqué du lecteur peut être mise à jour. Le protocole de mise à jour du micro-logiciel embarqué étant confidentiel et spécifique au fournisseur du microcontrôleur, nous faisons l'hypothèse qu'il est réalisé en milieu sécurisé par du personnel habilité.

3.4.2 Règles de sécurité

- A la première utilisation (sortie usine) le lecteur a les clés par défaut, l'utilisateur doit les modifier au plus tôt pour sécuriser ses échanges.
- Le lecteur est résiné et doit rester physiquement fixé, connecté et alimenté par le système de contrôle d'accès.
- De même l'utilisateur doit configurer le capteur d'arrachement pour être informer d'un vandalisme éventuel, et permettre par exemple au lecteur d'effacer les clés.
- La mise à jour du code embarqué du lecteur doit être effectuée par du personnel habilité et avec les outils mis à disposition par le fournisseur du microcontrôleur.
- Les utilisateurs du lecteur (et par extension du contrôle d'accès) ne doivent pas prêter leurs badges RFId.

3.5 Description des dépendances

Qualité du câblage du lien de communication RS485 entre le lecteur et le contrôleur.
Logiciel embarqué dans les contrôleurs

3.5.1 Préconisation pour les outils tiers

Bonne pratique du développement logiciel spécifique à la sécurité.
A titre d'exemple nous donnons comme référence le livre blanc de Microsoft sur le « Cycle de développement d'une sécurité informatique fiable » [9].

3.5.2 Préconisation sur les éléments cryptographiques

Utilisation d'un crypto-processeur ou de logiciels standards et éprouvés.

3.6 Description des utilisateurs typiques concernés

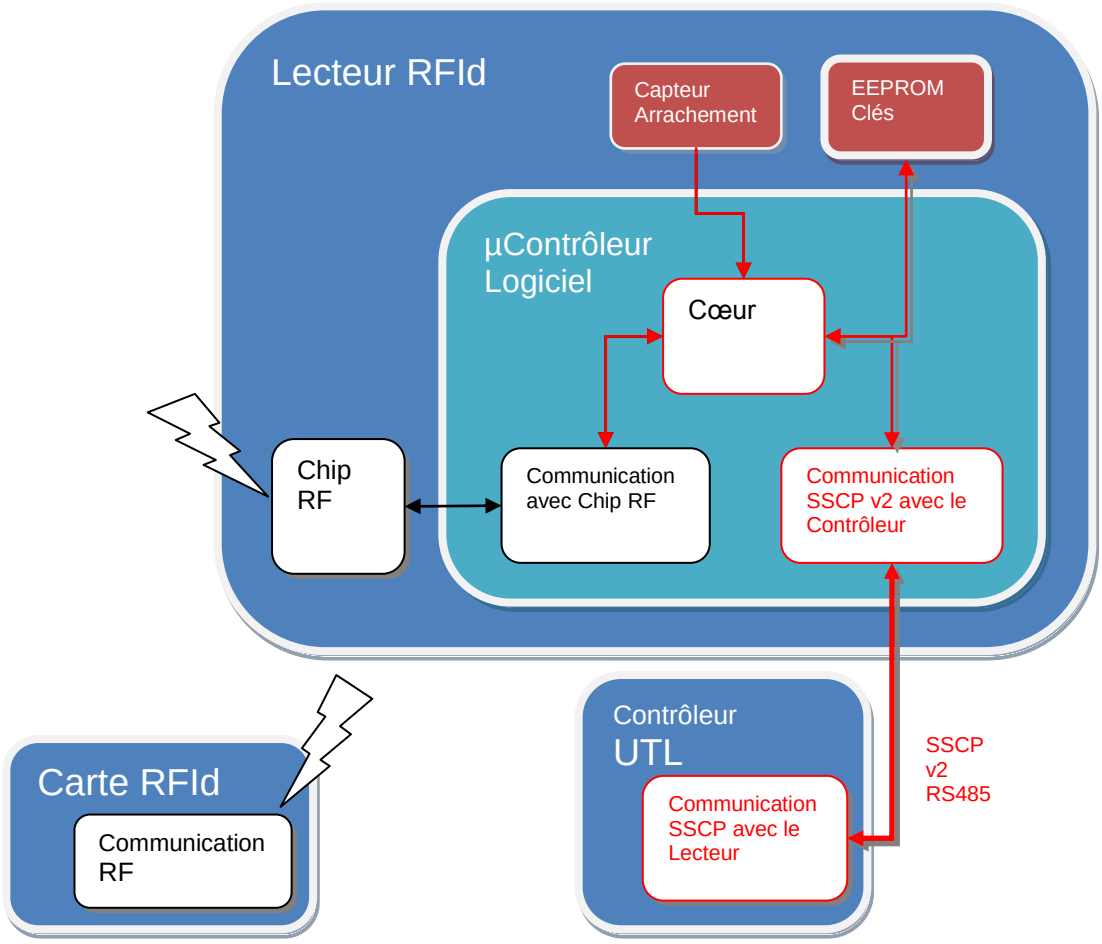
Il y a deux types d'utilisateurs typiques :

- Les intégrateurs, et développeurs des UTL (logiciel embarqué dans les contrôleurs). Les lecteurs sont dans ce cas connectés à des UTL de systèmes de contrôle d'accès.
- Ou directement les utilisateurs finaux qui pilotent sans intermédiaire les lecteurs a des fins d'encodage ou de lecture de cartes RFId. Les lecteurs sont dans ce cas connectés à des PC.

Les attaquants peuvent faire parti de ces deux types, en effet, ils peuvent, soit attaquer directement le lecteur comme les utilisateurs finaux (via le lien entre PC et lecteur), soit comme les intégrateurs en passant via l'UTL pour accéder au lecteur.

3.7 Définition du périmètre de l'évaluation

Le schéma fonctionnel suivant délimite physiquement le périmètre :



Architecture interne du lecteur et périmètre de sécurité - Figure 2

Les éléments appartenant au périmètre (en rouge) sont :

- le lien SSCP RS485 entre le Contrôleur.UTL et le lecteur RFId, c'est ce lien qui met en jeu les mécanismes d'authentification et de sécurisation.
- la communication entre le cœur logiciel du µcontrôleur et l'EEPROM où sont stockées les clés utilisées par la phase d'authentification.
- la gestion du capteur d'arrachement et du chip RFId.

Ainsi, l'évaluation portera sur l'ensemble du produit à l'exception des fonctions RF (la sécurité RF étant liée à la puce RFId utilisée) et de mise à jour du firmware.

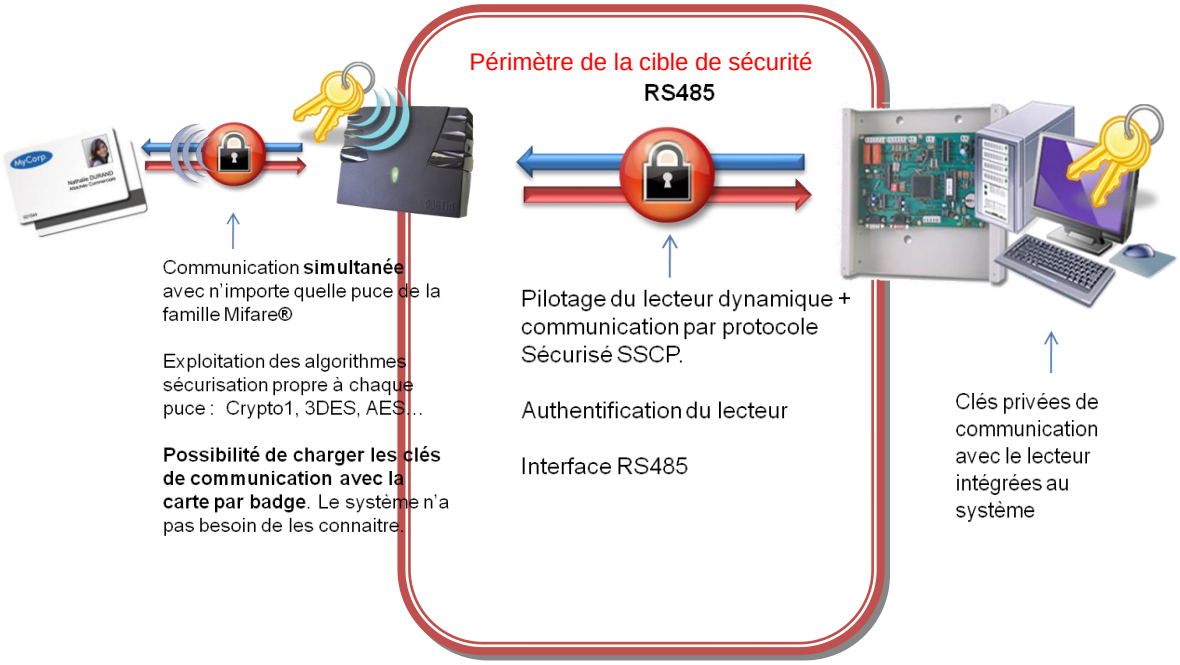
4 Environnement technique de fonctionnement du produit

4.1 Environnement

Les lecteurs LXS sont composés d'un logiciel embarqué et d'un matériel électronique résiné, ils sont connectés à un contrôleur.
Ils nécessitent une alimentation 12V (5-24V) et une connexion physique (RS485). Ils sont « esclaves » *i.e.* ils ne font rien tous seuls, ils attendent d'être pilotés par un contrôleur (UTL).
Ils sont fournis avec :

- Soit le protocole de communication sécurisé SSCP v2, et c'est l'intégrateur qui suit cette spécification pour son développent
- Ou soit un kit de développement qui intègre une librairie qui implémente le protocole de communication SSCP v2. Dans ce cas l'intégrateur n'a pas à redévelopper SSCP v2, mais uniquement à interfacer sont produit (le contrôleur, ou PC hôte) avec cette librairie.

Le contrôleur/PC pilote le lecteur RFID via le protocole sécurisé SSCP v2, effectuant ainsi toutes les commandes RFId utiles au contrôle d'accès.



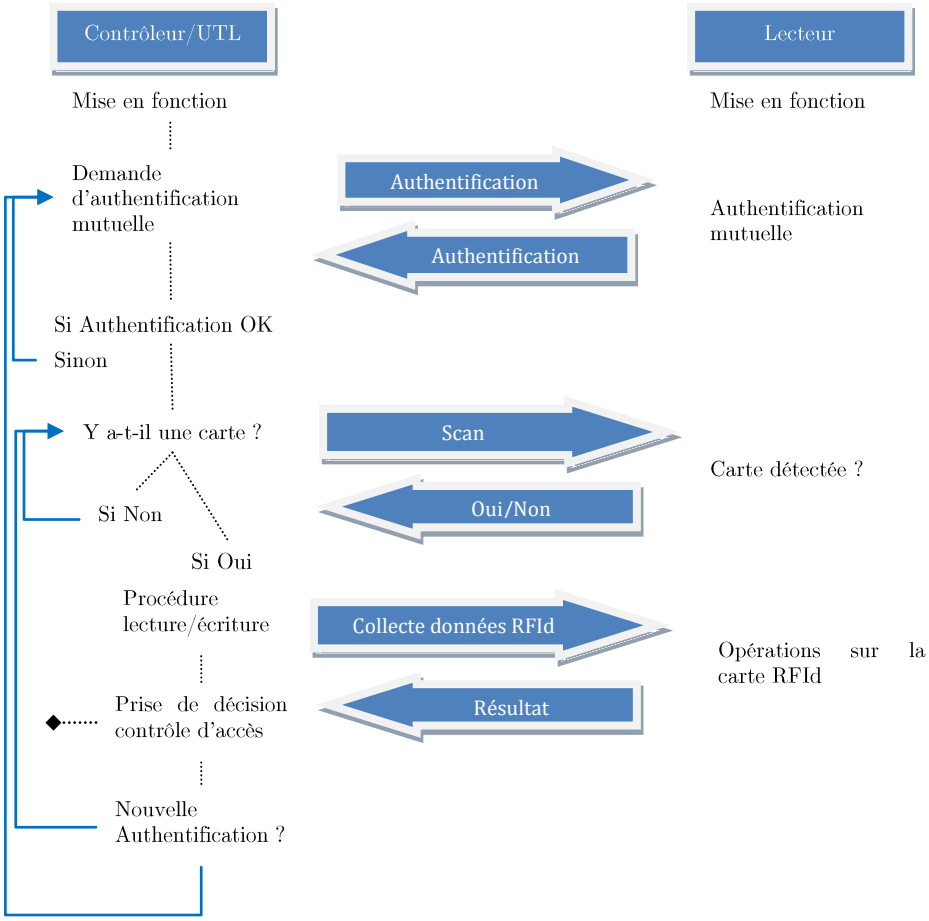
Environnement et fonctionnement - Figure 3

4.2 Utilisation classique

Le lecteur est mis en fonction.
Le contrôleur et le lecteur s'authentifient mutuellement avec la clé courante. Avant cette étape aucun dialogue n'est possible.
Le contrôleur dialogue alors avec le lecteur de manière sécurisée.
Il interroge continuellement le lecteur selon une procédure qui lui est propre.
L'utilisateur présente son badge au lecteur.
Le contrôleur reçoit une réponse de présence de carte et déroule sa procédure de lecture/écriture d'informations dans le badge RFId. Typiquement il collecte un identifiant qui lui permet de déterminer l'action à réaliser sur le contrôle d'accès (accès autorisé, ouverture porte, « blacklist » de l'identifiant...).

Le contrôleur retourne alors dans sa phase d'interrogation continuelle du lecteur, et ainsi de suite...
Régulièrement (voir [10]) le contrôleur est contraint de provoquer une nouvelle phase d'authentification. Chose qu'il peut aussi faire de son propre chef.

Voici ces étapes résumées dans le schéma suivant :



5 Biens sensibles devant être protégés par le produit

Les biens sensibles à protéger sont :

- Les clés de sécurité utilisées par les badges de contrôle d'accès, ainsi que toutes les informations RFId, c'est-à-dire les paramètres qui constituent une configuration utilisateur (par exemple l'application à lire dans le badge RFId, le type de protocole, le type de donné à lire, le type de conversion à effectuer...) qui transitent sur le média de communication

  Ces biens sont à protéger en Confidentialité, toute lecture de ces paramètres doit être impossible, et en intégrité l'altération d'une trame de communication doit être détectée et refusée par le lecteur.

- La clé privée utilisateur utilisée par le protocole SSCP v2.

  Cette clé doit être protégée en confidentialité et en intégrité. Il doit être impossible de la retrouver à partir des trames échangées, il doit être impossible de la modifier sans s'être authentifié au préalable, et l'altération de cette clé doit être détectée et impliquer l'arrêt des communications.

En résumé, les biens sensibles à protéger sont les clés RFId, la clé SSCP v2 contenue dans l'EEPROM et les communications SSCP v2 entre le lecteur et le contrôleur/PC.
En ce sens le code du microcontrôleur qui gère le stockage des clés et la communication SSCP v2 et un bien sensible à protéger en Confidentialité (ne pas retrouver les clés RFId et SSCP v 2) et en Intégrité (une clé altérée ne doit pas permettre l'authentification, et donc l'utilisation du lecteur).

6 Description des menaces

L'acteur des menaces ou « attaquant » peut être n'importe quelle personne qui a physiquement accès au lecteur. Il peut s'agir soit d'un utilisateur du contrôle d'accès (donc du lecteur) sans aucune connaissance du système, ou soit d'un opérateur malveillant qui a connaissance incomplète du système (il ne connaît pas la clé de communication SSCP v2), ou soit d'un administrateur qui a la connaissance totale du système (y compris la clé de communication du protocole SSCP v2).

6.1 Menaces physiques

Arrachement (classiquement le lecteur est fixé sur l'encadrement d'une porte) ou destruction du lecteur, récupération des informations qu'il contient.

6.2 Menaces logicielles

La principale attaque logicielle est l'attaque de liaison de communication entre le lecteur et le contrôleur.
Nécessite une attaque physique au préalable pour accéder à la liaison.

Les attaques logicielles ont pour objectifs :

- Récupérer les clés de communications et/ou des clés RFId en écoutant les échanges ;
- Réémettre des échanges valides pour leurrer et être authentifier par le système de contrôle d'accès ;
- Reconstruire ou altérer des requêtes valides grâces aux clés retrouvées ;
- Usurper l'identité (d'un « vrai » lecteur authentifié) grâce aux clés de communications déduites d'échanges enregistrés.

7 Description des fonctions de sécurité du produit

7.1 Généralités

Les mécanismes suivants sont mis en œuvre par le produit et sont précisés dans les prochains paragraphes.

- Mécanismes d'authentification des parties (lecteurs/contrôleurs) (SSCP v2),
  - Identifier le lecteur
  - Identifier le contrôleur
  - Générer des clés de session pour les communications qui suivront

- Mécanismes de sécurisation de la communication entre les parties (SSCP v2)
  - La communication n'est possible que suite à une authentification réussie
  - La communication est chiffrée
  - La communication est signée
  - Le mécanisme vérifie l'intégrité (la non-altération) des données transmises
  - Le mécanisme protège contre le rejeu de données

- Gestions des clés cryptographiques
    - La clé privée est sauvegardée de manière sécurisée (Chiffrée et Opacifiée)
    - Ces clés peuvent être effacées automatiquement à l'arrachement du lecteur et/ou remisent à leurs valeurs initiales (paramètres configurables)
    - Communication avec le chip RF (sécurité fonction des puces RF utilisées)

7.2 Maintenance

Dans le cas d'une programmation d'un lecteur que l'on a retiré de sa fixation murale et uniquement si le lecteur a été configurer pour cela, les clés seront remises à leur valeurs par défaut.

Lors d'une mise à jour du code embarqué les clés cryptographiques ne sont pas modifiées/vérifiées.

7.3 Arrachement

Le lecteur possède un capteur d'arrachement connecté au microcontrôleur.

La réaction du lecteur au déclenchement du capteur d'arrachement (changement d'état) est configurable, par une commande du protocole SSCP v2 qui ne peut être passée au lecteur qu'après une authentification :

- Activation/désactivation ;
- Remise des toutes les valeurs (paramétrables) aux leurs valeurs usines (exemple la clé privée utilisateur) ;
- Effacement des clés RFId.

La commande de configuration est décrite dans [1].
Cette fonction de sécurité répond à la menace physique d'arrachement pour n'importe quel attaquant.

7.4 Authentification des parties

Avant toute communication entre le lecteur et le contrôleur (UTL, PC, ...) il DOIT être effectué une authentification mutuelle des deux parties. Dans le cas contraire toutes les communications seront refusées par le lecteur.

L'authentification est réalisée par la méthode AKEP2 tel que définit dans le document « Fournitures cryptographiques ». Elle protège de l'usurpation d'identité.

La génération des clés de session qui suit directement l'authentification est réalisée par la diversification KDF3 telle que défini dans le document « Fournitures cryptographiques » [10]. Elle protège contre la réutilisation des mêmes clés statiques et limite l'attaque de la clé du protocole SSCP v2 à l'attaque des clés de sessions (limitées dans le temps).
L'authentification et la génération des clés est un processus atomique.

Cette fonction de sécurité répond à la menace logicielle d'usurpation d'identité pour tous les attaquants sauf l'administrateur.

7.5 Chiffrement et authentification de la communication entre les parties

Le chiffrement des données contenues dans les trames de communication est réalisé par l'AES 128 bits, l'authentification de l'émetteur par un HMAC-SHA256. Le chiffrement protège contre la menace d'écoute et l'authentification contre la menace d'altération des données et d'usurpation d'identité.

Pour chaque trame émise, le lecteur (réciproquement contrôleur) chiffre les données « RFID » ainsi qu'un compteur anti-rejeu en utilisant une clé de session issue du processus d'authentification, et rajoute une signature (aussi calculée à l'aide d'une clé de session issue du processus d'authentification) à la fin de la trame.
Pour chaque trame reçue, le lecteur (réciproquement par le contrôleur) vérifie la signature, déchiffre les données si la signature est vérifiée, puis vérifie le compteur anti-rejeu, et enfin utilise les données RFID déchiffrées si le compteur est valide. Il répond alors une trame d'acquittement (également sécurisée) qui contient soit une erreur (erreur d'authentification ou erreur RFID) soit la réussite de l'opération.

Cette fonction de sécurité répond aux menaces logicielles de récupération (écoute), reconstruction et réémission (rejeu) d'échanges valides. Et cela pour tous les attaquants y compris l'administrateur, si ce dernier n'a pas enregistré au préalable la phase d'authentification (il connaît la clé de communication SSCP v2 mais pas les clés de session issues de l'authentification).

8 Descriptions des mécanismes cryptographiques

Voir le document « Fournitures cryptographiques » [10].

9 Annexes

9.1 Glossaire

UTL ou **U**nité de **T**raitement **L**ogique c'est le contrôleur qui est en zone sécurisée et qui pilote le lecteur. C'est l'UTL qui gère le contrôle d'accès physique, qui prend la décision d'ouvrir ou pas les portes.

SSCP ou **S**Tid **S**ecure **C**ommunication **P**rotocol c'est le nom commercial du protocole de communication visé comme le cœur de la cible de sécurité. Voir [1]

Opacifiée ou Obfusquée (pour une clé) de l'anglais *obfuscation* qui signifie cacher, noyer des informations dans un flot afin de les rentre incompréhensibles par un humain. N'est pas en soi une méthode cryptographique, mais rajoute une certaine difficulté au *reverse engineering*. Voir [10].

NXP Mifare® est une famille de carte à puce RFId de NXP.

Crypto1 est un mécanisme d'authentification privé utilisé par les cartes d'ancienne génération, les Mifare® Classic. Il a été découvert par *reverse engineering* et est de nos jours facilement contournable. Il ne constitue plus une véritable sécurité.

DES et **TDES** sont des algorithmes de chiffrement symétriques. Voir [4].

AES pour **A**dvanced **E**ncryption **S**tandard (ex. Rijndael) est l'algorithme standard actuel du chiffrement symétrique. Voir [2]

HMAC est un type de code d'authentification de message (de l'anglais *keyed-**H**ash **M**essage **A**uthentication **C**ode)* calculé à l'aide d'une fonction de hachage cryptographique et d'une clé secrète. Voir [5].

SHA est une fonction de hachage cryptographique. Voir [7] et [8].

Une **fonction de hachage** est une fonction particulière qui fournie à partir de données d'entrée une empreinte servant à les identifier.

AKEP2 est un mécanisme d'authentification et de distribution de clés. Voir [3].

KDF3 est un mécanisme de diversification de clés. Voir [6] et [7].

9.2 Références

[1] STid, "Spec_Protocole_7AD_MIFARE_GLOBAL_V0.9.pdf" 9 Juillet 2012.

[2] FIPS PUB 197, "ADVANCED ENCRYPTION STANDARD (AES)", November 26, 2001.

[3] M. BELLARE et ROGAWAY, "Entity Authentication and Key Distribution" publication, August 1993

[4] FIPS PUB 46-3, "Data Encryption Standard" October 25, 1999.

[5] FIPS PUB 198, "The Keyed-Hash Message Authentication Code (HMAC)" Issued March 6, 2002.

[6] ISO-18033-2:2006, "*Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers*", Ed. Victor Shoup, 2006. The final committee draft version *FCD 18033-2*, dated December 2004.

[7] FIPS PUB 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)", NIST Special Publication 800-56A March, 2007.

[8] FIPS PUB 180 et 180-1, "SECURE HASH STANDARD", 1995 April 17

[9] Steve LIPNER et Michael HOWARD, Microsoft, « Cycle de développement d'une sécurité informatique fiable » 23 Août 2055, http://msdn.microsoft.com/fr-fr/library/ms995349.aspx.

[10] STid, «CSPN, Fournitures Cryptographiques, Lecteurs LXS-W33-E-7AD », Mars 2012.

9.3 Contacts

STid

Siège Social
20 Parc d'Activités des Pradeaux
13850 Gréasque, France
Tel. +33 (0)4.42.12.60.60
Fax +33 (0)4.42.12.60.61
info@stid.com - www.stid.com

Agence Paris IDF
28, rue de la redoute
Immeuble le Fahrenheit
92260 Fontenay-aux-Roses, France
Tel. +33 (0)1.43.50.11.43
Fax +33 (0)1.43.50.27.37