ARD Sureté et Monétique

Micropolis, Bâtiment Clématis
CS26003
05005 GAP CEDEX
Tél. : 33 (0) 492 525 800
Fax : 33 (0) 492 525 801
E-mail : contact@ard.fr

Cible de sécurité CSPN

Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité

Identification, authentification et contrôle d'accès

Historique des révisions

Révision	Date	Nom du rédacteur	Commentaire
0.0	Mars 2018	Bertrand Gasnier	Création de la version préliminaire de base pour la démarche CSPN.
1.0	19/04/2018	Bertrand Gasnier	Finalisation du document en vue de l'évaluation CSPN.
1.1	26/04/2018	Bertrand Gasnier	Corrections sur la protection des échanges de données entre l'UTL et les lecteurs de badge.
1.2	03/05/2018	Bertrand Gasnier	Modification des versions de logiciels.
2.0	04/09/2019	Bertrand Gasnier	Corrections suite aux remarques de l'ANSSI.
2.1	30/10/2019	Bertrand Gasnier	Modification de l'identification du produit et des utilisateurs suite aux remarques de l'ANSSI. Mise à jour de la liste des documents de référence.
2.1.1	16/04/2020	Bertrand Gasnier	Correction d'une référence produit suite aux remarques de l'ANSSI.

Liste des documents de référence

Source	Référence	Version	Commentaire
ANSSI	ANSSI-CSPN-CER-P-01/2.0	2.0	Procédure – Certification de sécurité de premier niveau des produits des technologies de l'information
ANSSI		1.0	Guide – Sécurité des technologies sans-contact pour le contrôle des accès physiques
ANSSI	Annexe B1	2.03	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
ARD	ANSSI-CSPN-ARD-Spécifications Cryptographiques	2.1	Spécifications Cryptographiques Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité Identification, authentification et contrôle d'accès

Table des matières

1. INTRODUCTION 6

1.1. Identification de la cible de sécurité 6

1.2. Identification du produit 6

1.3. Références et désignations 6

2. ARGUMENTAIRE DU PRODUIT 7

2.1. Description générale du produit 7
2.1.1. Architecture globale de la solution 7
2.1.2. Schéma 8
2.1.3. Description fonctionnelle et utilisation 8
2.1.4. Raccordements et réseaux 9
2.1.5. Réseau dédié (ou réseau technique) 9
2.1.6. Serveur de Gestion des Accès Contrôlés (AVB) 9
2.1.7. Poste d'exploitation 10
2.1.8. Unité de Traitement Logique OTES3 10
2.1.9. Lecteur de badges C2 10
2.1.10. Lecteur de badges C2-Clavier 11

2.2. Description de l'environnement d'utilisation du produit 12

2.3. Description d'une procédure d'accès 13
2.3.1. Identification RFID sans code PIN 13
2.3.2. Identification RFID avec confirmation par code PIN 13

2.4. Hypothèse sur l'environnement physique du produit 13
2.4.1. Installation du serveur 13
2.4.2. Installation du poste de gestion 13
2.4.3. Installation de l'UTL 14
2.4.4. Installation des lecteurs de badge 14

2.5. Hypothèses sur les utilisateurs du produit 14

2.6. Hypothèses sur les porteurs de badges 14

2.7. Hypothèses sur l'environnement technique du produit 14
2.7.1. Serveur de Gestion des Accès 15
2.7.2. Réseaux 15
2.7.3. Poste de gestion 15

2.8. Description des utilisateurs 15
2.8.1. Administrateur 15
2.8.2. Exploitant 15
2.8.3. Agent technique 16
2.8.4. Porteur 16

2.9. Description du périmètre de l'évaluation 16

3. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT 18

3.1. Dispositif d'accès 18

3.2. Dispositif de raccordements et d'alimentation 18

3.3. Postes informatiques 18

3.4. Badges 18

3.5. Carte SAM 18

4. DONNEES SENSIBLES 19

4.1. Description 19

4.2. Données sensibles dans l'UTL OTES3 19

4.3. Données sensibles dans le lecteur C2 19

4.4. Données sensibles dans le lecteur C2-Clavier 20

5. DESCRIPTION DES MENACES 21

5.1. Intrusion sur le réseau LAN 21

5.2. Intrusion sur le réseau technique CAN 21

5.3. Attaque physique sur le lecteur C2 ou le lecteur C2-Clavier 22

6. DESCRIPTION DES FONCTIONS DE SECURITE 23

6.1. Fonctions de sécurité 23

6.2. Correspondance entre les menaces et les protections mises en œuvre 24

7. ANNEXES 25

7.1. Annexe 1 – Tableau 1 ANSSI - Les quatre niveaux de sûreté 25

7.2. Annexe 2 – Tableau 2 ANSSI - Correspondance entre le niveau de sûreté et la résistance aux attaques logiques.....26

1. INTRODUCTION

1.1. IDENTIFICATION DE LA CIBLE DE SECURITE

Ce document constitue la cible de sécurité pour une évaluation CSPN dans la catégorie « Identification, authentification et contrôle d'accès » n°6.

1.2. IDENTIFICATION DU PRODUIT

Nom commercial du produit	**Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité** Version 2.1.1
Constructeur	**ARD S.A.S.** Micropolis – Bâtiment Clématis CS 26003 05000 GAP CEDEX http ://www.ard.fr
Catégorie du produit	Identification, authentification et contrôle d'accès

1.3. REFERENCES ET DESIGNATIONS

Désignation	Référence	Description
ARD OTES3	E04130	Unité de Traitement Logique (UTL)
Pack de sécurisation cryptographique pour OTES2/OTES3	E04121	Double support SAM pour OTES2/OTES3
ARD C2	F30253	Lecteur de badges RFID
ARD C2-Clavier	F30307	Lecteur de badges RFID avec clavier 12 touches

2. ARGUMENTAIRE DU PRODUIT

2.1. DESCRIPTION GENERALE DU PRODUIT

2.1.1. Architecture globale de la solution

ARD Access est une solution intégrée de gestion centralisée de contrôle d'accès physique à des sites administratifs, industriels et tertiaires.
Elle est composée :

- D'une partie serveur appelée AVB (ARD Virtual Box) intégrant l'application full web de gestion des accès contrôlés et sa base de données ;
- D'une partie terrain comprenant des UTLs OTES3 et des lecteurs C2 (avec ou sans clavier 12 touches).

La solution, architecturée autour des équipements présentés dans le schéma ci-dessous a pour objectif de filtrer les flux d'individus souhaitant pénétrer à l'intérieur d'un site, d'un bâtiment ou d'un local.
Pour assurer cette fonction, elle s'appuie sur :

- Une identification par badge RFID (sans contact) au travers des lecteurs C2 avec ou sans authentification par code PIN;
- Un traitement des droits d'accès au niveau des UTLs OTES3 ;
- Des automatismes d'accès (verrouillage, déverrouillage ou séquencement d'actions sur l'ouvrant) depuis les UTLs OTES3 ;
- Une remontée des événements au gestionnaire depuis les UTLs OTES3 vers le serveur de gestion AVB.

> ☞ *ARD Access entre dans le cadre des dispositifs de sécurité utilisant les technologies sans-contact pour le contrôle des accès physiques tels que définis par l'ANSSI dans son guide intitulé « SECURITE DES TECHNOLOGIES SANS-CONTACT POUR LE CONTROLE DES ACCES PHYSIQUES ».*

2.1.2. Schéma

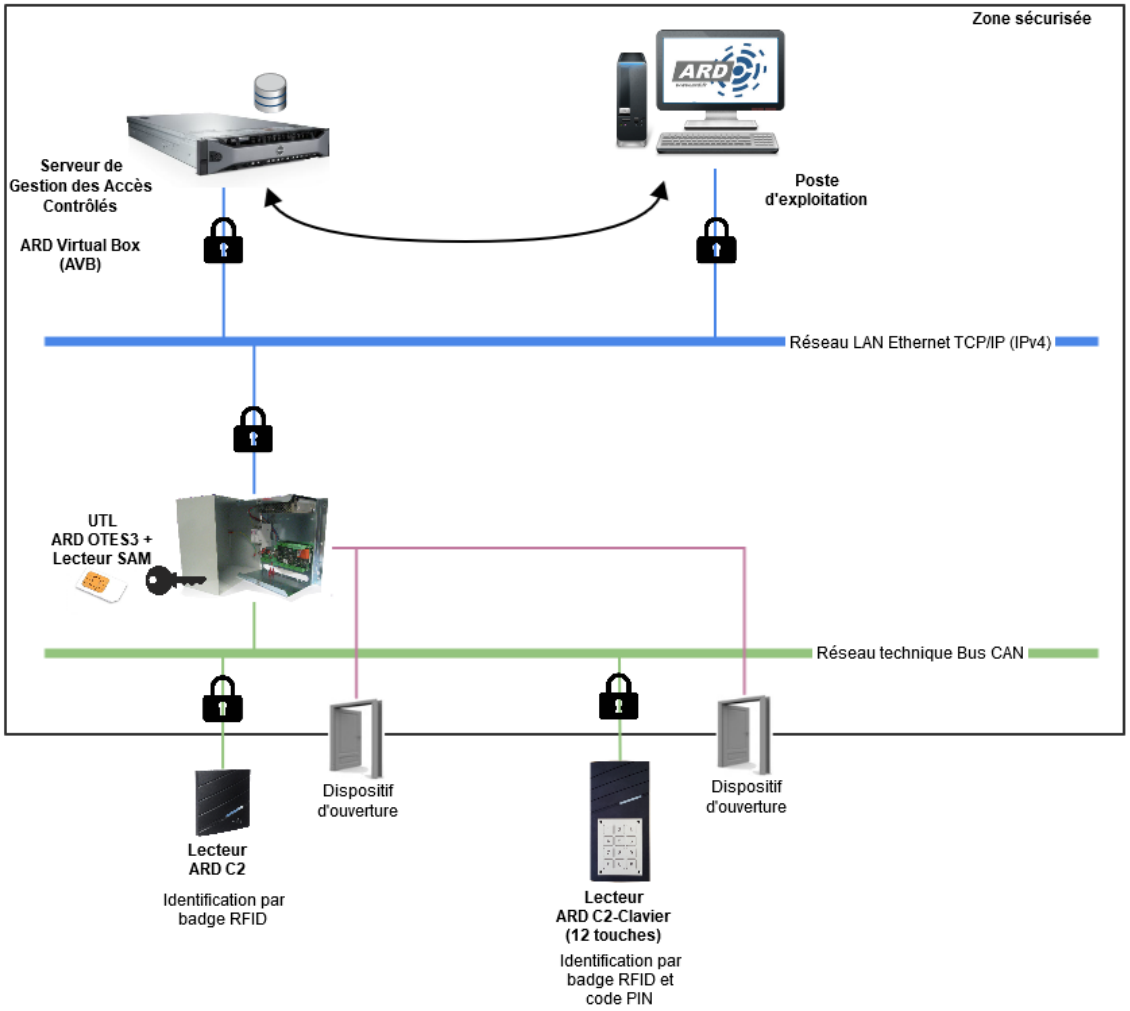


Figure 1 - Schéma global ARD Access

2.1.3. Description fonctionnelle et utilisation

La solution ARD Access permet de gérer de façon centralisée et en temps réel le contrôle des accès à un site, un bâtiment ou un local des personnes (appelés porteurs).

Ces fonctions sont gérées par une application développée par ARD (appelée AVB) fonctionnant sur le serveur de gestion central. Celle-ci s'appuyant sur les technologies « full web » permet à un Gestionnaire ou un Responsable de la sécurité (utilisateur) de gérer toutes les fonctions depuis un simple navigateur web (poste de gestion).

Chaque utilisateur du poste de gestion dispose de son propre identifiant et mot de passe de façon à gérer les droits d'accès aux fonctionnalités de l'application et de tracer les actions effectués par chaque utilisateur.

Les porteurs disposent d'un badge sans contact en technologie RFID et éventuellement un code PIN d'authentification. Leurs droits d'accès sont préalablement définis par l'exploitant

dans l'AVB et chargés dans les UTLs. Le paramétrage de ces droits est entièrement sous la responsabilité du Responsable de la sécurité.

Pour accéder à une zone, le porteur doit présenter son badge dans le champ magnétique du lecteur et éventuellement saisir son code PIN d'authentification. Le système ARD Access accorde alors ou non l'accès à la zone selon les critères définis.

Les lecteurs de badges sont installés en dehors de la zone à sécuriser. Ils ne disposent pas des clés de lecture du badge. Celles-ci sont stockées dans un module SAM (Security Application Module) intégré au boîtier de l'UTL.

Les UTLs sont installées à l'intérieur de la zone à sécuriser. Elles décident des autorisations d'accès ou non à une zone, pilotent les automatismes d'actions sur les ouvrants et remontent les événements à l'application serveur AVB pour journalisation.

2.1.4. Raccordements et réseaux

Le serveur de Gestion et les UTLs sont raccordés au réseau de l'exploitant de la solution de contrôle d'accès. Ce réseau est un réseau LAN Ethernet TCP/IP (IPv4) intégré dans un VLAN dédié au contrôle d'accès, établi, maintenu et entièrement administré par lui.

Ce réseau constitue le réseau principal assurant les connexions entre le(s) poste(s) de gestion, l'application AVB et les UTLs de terrain. Les communications entre ces différents éléments sont chiffrées.

2.1.5. Réseau dédié (ou réseau technique)

Les UTLs sont connectées aux lecteurs de badge via un réseau dédié (appelé aussi réseau technique) utilisé exclusivement pour les installations de contrôle d'accès physiques. Ce réseau s'appuie sur un bus CAN filaire. Ce bus assure la communication entre une UTL et ses lecteurs de badges.

2.1.6. Serveur de Gestion des Accès Contrôlés (AVB)

Le serveur de gestion héberge l'application AVB développée par ARD. Celle-ci a pour but de gérer de manière centralisée toutes les fonctions d'accès.

Le serveur est constitué d'un poste informatique sous environnement Linux doté d'une base de données MySQL. Ce serveur est hébergé sous la forme d'une Machine Virtuelle dans l'infrastructure informatique de l'exploitant de la solution de contrôle d'accès.

Reposant sur les technologies « full web », l'application présente une interface de configuration et d'exploitation accessible depuis un navigateur Internet sur un poste de gestion.

Le serveur de gestion gère les échanges avec les UTLs de terrain et centralise l'historique des événements, les paramètres de configuration, les droits d'accès, les badges, les populations de porteurs de badges, les alarmes anti-intrusion… dans sa base de données. La communication avec les UTLs est sécurisée via un chiffrement en AES128 et une authentification MAC décrits dans le document « Spécifications cryptographiques ».

2.1.7. Poste d'exploitation

Le poste d'exploitation est constitué d'un simple ordinateur connecté au réseau Ethernet de l'exploitant de la solution de contrôle d'accès et disposant d'un navigateur Internet. Chaque utilisateur du poste de gestion dispose de son propre identifiant et mot de passe pour s'authentifier sur l'interface fournie par l'application de gestion des accès.

2.1.8. Unité de Traitement Logique OTES3

L'UTL ARD OTES3 a pour fonction de contrôler la validité des demandes de passage vers les zones sécurisées des personnes munies d'un badge sans contact. Elle s'appuie sur sa base de données locale contenant les droits sur les accès qu'elle gère. Elle dispose d'une capacité de conservation de l'ensemble de ses données en cas de rupture de communication avec le serveur de gestion des accès. Pendant le temps de cette rupture, l'exploitation continue en mode dégradé sur les points suivants :

- Pas de possibilité de modifier les droits d'accès dans l'UTL ;
- Pas de visualisation des événements depuis le poste de gestion.

L'UTL continue néanmoins à mémoriser l'ensemble des événements, qu'elle remonte automatiquement au serveur de gestion lors du rétablissement de la communication.

Son rôle est également de piloter les automatismes d'actions sur les ouvrants qu'elle gère.

Elle est intégrée dans un coffret auto-protégé contre son ouverture et son arrachement grâce à des capteurs remontant des alertes au serveur de gestion en cas de détection d'anomalie. Les communications avec le serveur de Gestion AVB et les lecteurs de badges sont sécurisées via un chiffrement en AES128 et une authentification MAC décrits dans le document « Spécifications cryptographiques ».

Caractéristiques techniques :

Composant	Description
Désignation	ARD OTES3 + support SAM
Référence produit	E04130 + E04121
Version du logiciel	Version 3.0.1.0
Emplacement	Zone sécurisée
Processeur	ARM 32 bits STM32
AP	Détection d'ouverture coffret et d'arrachement
Module de sécurité	Support SAM

2.1.9. Lecteur de badges C2

Le lecteur de badges ARD C2 a pour fonction l'identification RFID des badges en mode « transparent » (ou passif). Il ne dispose d'aucune clé de lecture des badges. Celles-ci sont

sécurisées dans une carte SAM (Secure Access Module) insérée dans l'un des supports SAM de l'UTL OTES3 (implantée dans la zone sécurisée).

L'identification se fait alors au travers d'un jeu d'échanges de messages chiffrés et de challenges avec le SAM.

Le lecteur est, en outre, auto-protégé contre son arrachement grâce à un capteur remontant une alerte au serveur de gestion en cas de détection d'anomalie.

La communication avec les UTLs est sécurisée via un chiffrement en AES128 et une authentification MAC décrits dans le document « Spécifications cryptographiques ».

Caractéristiques techniques :

Composant	Description
Désignation	ARD C2
Référence produit	F30253
Version du logiciel	Version 3.0.1.0
Emplacement	Zone publique ou zone protégée
OS embarqué	FreeRTOS
Processeur	ARM 32 bits STM32
AP	Détection d'arrachement

2.1.10. Lecteur de badges C2-Clavier

Le lecteur de badges ARD C2-Clavier, équipé d'un clavier 12 touches, a pour fonction l'identification RFID des badges en mode « transparent » (ou passif) complété par une authentification par code PIN. Il ne dispose d'aucune clé de lecture des badges. Celles-ci sont sécurisées dans une carte SAM (Secure Access Module) insérée dans l'un des supports SAM de l'UTL OTES3 (implantée dans la zone sécurisée).

L'identification se fait alors au travers d'un jeu d'échanges de messages chiffrés et de challenges avec le SAM.

Le code PIN est, d'autre part, protégé en confidentialité, authenticité et intégrité grâce au chiffrement des données échangées sur le réseau technique.

Le lecteur est, en outre, auto-protégé contre son arrachement grâce à un capteur remontant une alerte au serveur de gestion en cas de détection d'anomalie.

La communication avec les UTLs est sécurisée via un chiffrement en AES128 et une authentification MAC décrits dans le document « Spécifications cryptographiques ».

Caractéristiques techniques :

Composant	Description
Désignation	ARD C2-Clavier

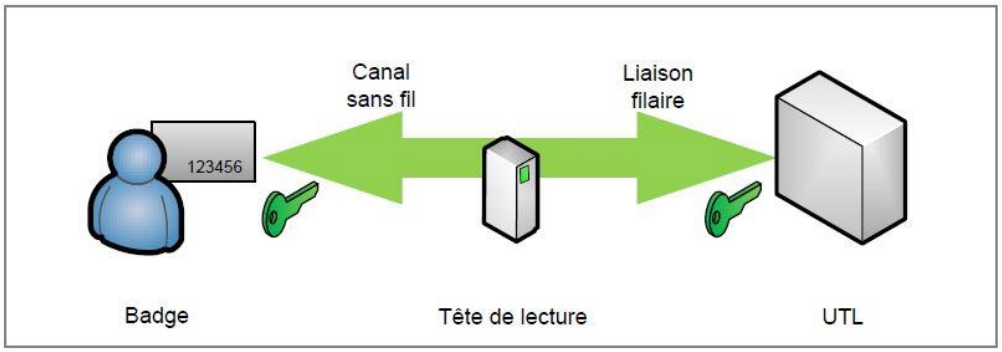
Référence produit	F30307
Version du logiciel	Version 3.0.1.0
Emplacement	Zone publique ou zone protégée
OS embarqué	FreeRTOS
Processeur	ARM 32 bits STM32
AP	Détection d'arrachement

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

Le système de contrôle des accès physiques ARD Access a pour objectif de filtrer les flux d'individus souhaitant pénétrer à l'intérieur d'un site, d'un bâtiment ou d'un local.

Pour répondre au besoin croissant d'une sécurisation optimum des échanges de données par badges RFID dans ce système, ARD a fait évoluer sa solution en prenant en compte :

- Le chiffrement de la communication entre le badge et le lecteur de badge de technologie NXP DESFire EV1 ou EV2 ;
- La mise en place d'un lecteur de badges en mode « transparent » (aucune clé de lecture de badge stockées dans le lecteur), installée généralement dans la zone publique ;
- La mise en place d'un SAM contenant les clés de lecture des badges, installé dans la zone sécurisée.



Cette solution suit les recommandations de l'ANSSI décrites dans son guide « Sécurité des technologies sans-contact pour le contrôle des accès physiques » en mettant notamment en œuvre l'architecture n°1, hautement recommandée par l'ANSSI.

Elle permet la sécurisation des clés de lecture des badges dans la zone sécurisée et leur gestion facilitée pour l'exploitant de la solution de contrôle d'accès par l'utilisation de cartes SAM insérée dans l'un des supports SAM de l'UTL OTES3 (implantée dans la zone sécurisée).

2.3. DESCRIPTION D'UNE PROCEDURE D'ACCES

2.3.1. Identification RFID sans code PIN

Les badges utilisés sont de technologie NXP DESFire EV1 ou EV2. Ils sont soit préprogrammés par ARD, soit programmés par l'exploitant de la solution de contrôle d'accès au moyen d'une application fournie par ARD. L'application permet de charger sur le badge une « application » dédiée au contrôle d'accès comportant un trousseau de clés AES128.

Lorsqu'un badge DESFire est présenté par son porteur dans le champs du lecteur, l'application DESFire transmet en clair l'UID du badge au lecteur qui le transmet à son tour à l'UTL.

Une authentification en 3 étapes commence ensuite entre le SAM et le badge au moyen de défis. Elle permet d'assurer au SAM et au badge DESFire la connaissance mutuelle d'un secret sans que celui-ci ne transite. Elle permet aussi d'établir une clé AES128 de session pour les échanges chiffrés suivants.

A l'issue de l'authentification, l'UTL demande au badge la lecture de l'identifiant de contrôle d'accès du porteur.

L'identifiant chiffré est alors transmis du badge au SAM qui le déchiffre avant de le transmettre à l'UTL pour décision d'ouverture de l'accès ou non.

2.3.2. Identification RFID avec confirmation par code PIN

Cette fonction permet, en plus de l'identification RFID décrite ci-dessus, de confirmer la demande d'accès par la saisie d'un code PIN. Celui-ci est protégé en confidentialité grâce au chiffrement des données échangées sur le réseau technique.
Le niveau de protection de ces échanges est décrit dans le document « Spécifications cryptographiques ».

Des éléments complémentaires sur l'utilisation de la solution de contrôle d'accès ARD sont décrits dans son manuel d'utilisation.

2.4. HYPOTHESE SUR L'ENVIRONNEMENT PHYSIQUE DU PRODUIT

2.4.1. Installation du serveur

Il est supposé que le serveur de gestion des accès (hébergeant l'application AVB et sa base de données) est installé dans un local informatique sécurisé dont l'accès est strictement limité aux personnels habilités.

2.4.2. Installation du poste de gestion

Un poste de gestion est un équipement administratif. Il est supposé qu'il est installé, comme tout poste administratif pouvant contenir des données sensibles, dans un local sécurisé dont l'accès est contrôlé et restreint aux personnels habilités.

2.4.3. Installation de l'UTL

Il est supposé que l'UTL accompagnée du SAM sont installés dans un local technique sécurisé dont l'accès est strictement limité.

2.4.4. Installation des lecteurs de badge

Il est supposé que le lecteur est installé de façon à garantir une gestion périmétrique du site, d'une zone ou d'un local.

Aucun câble, ni aucun équipement ne sont posés ou installés en zone non protégée, à l'exception du lecteur de badges. Le câble de raccordement du lecteur de badges 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 câble (bus CAN) assurant la liaison entre le lecteur et l'UTL est supposé direct.

Le câblage de l'ensemble des équipements constituant les environnements de porte est direct, point à point.

2.5. HYPOTHESES SUR LES UTILISATEURS DU PRODUIT

Les personnels exploitants de la solution (Gestionnaire ou Responsable de la sécurité) sont supposés appartenir à l'organisation interne de gestion de la sureté, ou être mandataires de ce service sous son contrôle et autorité.

Ils sont supposés avoir suivi une formation spécifique à leurs attributions et aux tâches qui leurs sont confiées.

Ils disposent tous d'un compte individuel leur permettant de se connecter à l'interface de gestion AVB à l'aide d'un couple Identifiant/Mot de passe. La gestion des comptes exploitants devra s'appuyer sur les « Recommandations de sécurité relatives aux mots de passe » rédigées par l'ANSSI.

2.6. HYPOTHESES SUR LES PORTEURS DE BADGES

Les porteurs de badge sont les usagers du contrôle d'accès. Ils disposent de badges sans contact de technologie NXP DESFire EV1 ou EV2 (RFID).

Ces porteurs sont supposés ne réaliser de demande d'accès que pour leur usage personnel et ne permettre l'accès à aucune autre personne (tiers et collègues inclus). Ils sont supposés ne pas confier ou prêter leur badge ni communiquer leur code PIN.

2.7. HYPOTHESES SUR L'ENVIRONNEMENT TECHNIQUE DU PRODUIT

2.7.1. Serveur de Gestion des Accès

L'application de Gestion AVB fonctionne dans un environnement Linux régulièrement protégé des virus et ne permet pas l'exécution de code malveillant.

Les mises à jour de sécurité et outils disponibles sont installés.

Le niveau de protection des échanges entre le serveur et l'UTL est décrit dans le document « Spécifications cryptographiques ».

Il existe un compte Administrateur, doté de tous les privilèges de configuration et d'exploitation.

Il existe un compte Exploitant, doté de privilèges restreints et réservé à l'utilisation courante du système.

2.7.2. Réseaux

Le réseau de l'exploitant de la solution de contrôle d'accès et le réseau dédié (réseau technique) sont physiquement et logiquement séparés. Les échanges entre les deux réseaux passent systématiquement par l'UTL OTES3.

Le réseau LAN est placé en zone sécurisée. Il est supposé séparé logiquement des autres réseaux LAN de l'exploitant.

2.7.3. Poste de gestion

Le poste de gestion est supposé placé dans en zone sécurisée. L'accès au système d'exploitation du poste est supposé fait via une session individuelle avec politique de mot de passe gérée par l'exploitant de la solution de contrôle d'accès. L'accès à l'interface de gestion se fait depuis un navigateur Internet et une authentification par un couple Identifiant/Mot de passe individuel.

2.8. DESCRIPTION DES UTILISATEURS

2.8.1. Administrateur

L'administrateur est un personnel appartenant au service informatique de l'exploitant ou mandaté par ce service. Il a pour fonction d'assurer le bon fonctionnement du serveur de gestion des accès.

2.8.2. Exploitant

Les exploitants sont les personnels (Gestionnaire ou Responsable de la sécurité) appartenant à l'organisation interne de gestion de la sureté, ou mandataires de ce service sous son contrôle et son autorité.

Ils ont pour fonction de configurer et adapter au quotidien les différentes fonctions du système de contrôle d'accès qui concourent à attribuer des autorisations d'accès sur l'ensemble des portes et obstacles physiques contrôlés. Ils sont considérés être compétents, formés et de confiance.

Toute connexion des exploitants au système de gestion des accès est tracée dans l'historique des événements.

2.8.3. Agent technique

Les agents techniques sont des personnes intervenant dans le cadre des opérations de mise en service (déploiements) et de maintenance (techniciens) sous le contrôle d'ARD ou d'un de ses partenaires. Ils sont considérés être compétents, formés et de confiance.

Aucun exploitant n'est amené à se connecter directement et indirectement sur les UTLs ; c'est une prérogative des agents techniques.

2.8.4. Porteur

Les porteurs de badge sont les utilisateurs finaux de la solution. Ils disposent de badges individuels sans contact de technologie NXP DESFire EV1 ou EV2 (RFID) et éventuellement de code PIN pour accéder aux zones protégées ou aux zones sécurisées.

2.9. DESCRIPTION DU PERIMETRE DE L'EVALUATION

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

- UTL ARD OTES3
- Lecteur de badges ARD C2
- Lecteur de badges ARD C2-Clavier

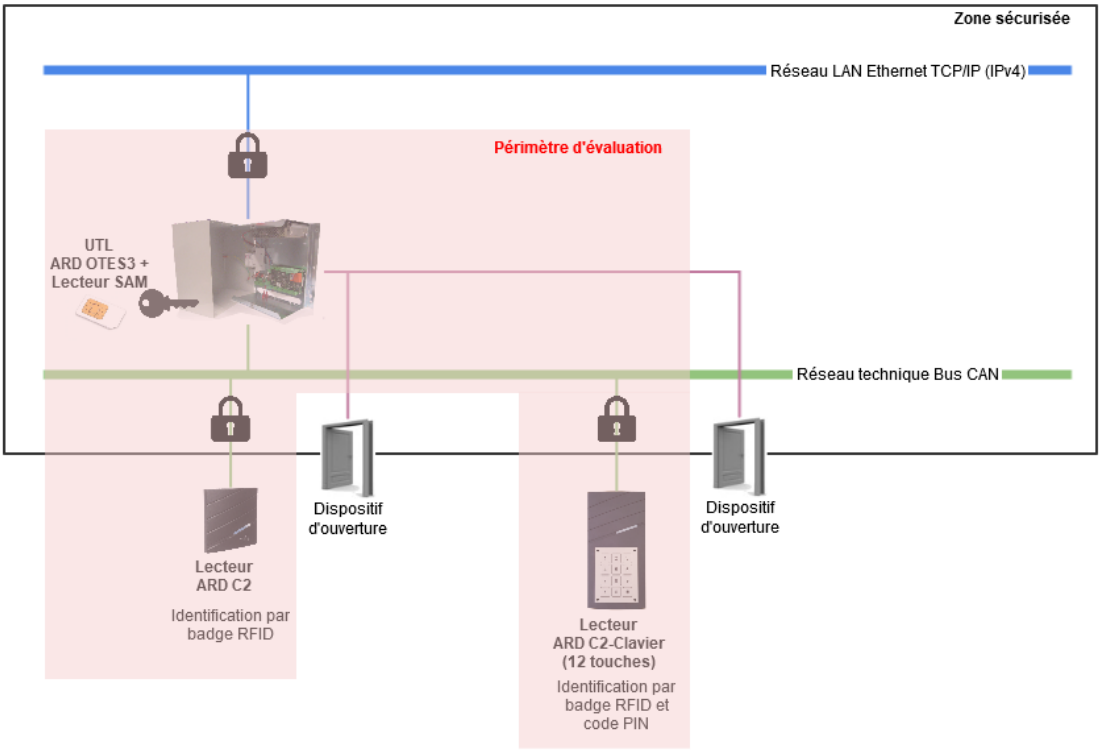


Figure 2 - Périmètre de l'évaluation

3. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

Les éléments suivants sont nécessaires à l'évaluation.

3.1. DISPOSITIF D'ACCES

Gestion d'environnement d'accès disposant des équipements minimums :

- Détecteur d'ouverture de porte (état de la porte)/ contact de verrouillage.
- Sortie libre par bouton poussoir (commande de sortie).
- Organe de serrurerie condamnant l'accès (commande par contact sec et alimentation secourue).

3.2. DISPOSITIF DE RACCORDEMENTS ET D'ALIMENTATION

Les raccordements des équipements figurent dans le schéma de la cible de sécurité (voir paragraphe 2.9).

S'y ajoutent :

- Les raccordements des équipements mentionnés dans le paragraphe 3.1 ci-dessus.
- Les alimentations secourues.

3.3. POSTES INFORMATIQUES

- Serveur de gestion des accès ARD Access (Configuration et Exploitation) hébergeant l'application AVB et sa base de données.
- Poste de gestion Windows 10 (64 bits) avec derniers correctifs et navigateur Internet (Chrome ou Firefox).

3.4. BADGES

- Badges d'accès sécurisés basés sur la technologie NXP Mifare® DESFire EV1 ou EV2 livrés pré-encodés.

3.5. CARTE SAM

- Cartes SAM livrées préprogrammées avec les clés de lecture des badges.

4. DONNEES SENSIBLES

4.1. DESCRIPTION

Les données névralgiques confidentielles regroupent plusieurs types d'informations :

- Clés de lecture de badge et de chiffrement/déchiffrement de données.
- Identifiants individuels des porteurs de badge.
- Codes PIN associés aux badges.
- Droits d'accès des porteurs de badge (plages horaires d'accès).

4.2. DONNEES SENSIBLES DANS L'UTL OTES3

Les données sensibles protégées par l'UTL OTES3 accompagnée du SAM sont :

Donnée	Description
Clé DESFire	Clé de lecture du badge DESFire
Clés de chiffrement/déchiffrement	Clés de chiffrement/déchiffrement des messages échangés entre l'UTL et le serveur, et entre l'UTL et les lecteurs de badge
Code PIN	Code PIN associé au badge du porteur
Identifiant	L'identifiant d'accès du porteur du badge
Droits d'accès	Droits d'accès du porteur du badge

Le mécanisme de protection de ces données est décrit dans le document « Spécifications cryptographiques ».

4.3. DONNEES SENSIBLES DANS LE LECTEUR C2

Le lecteur C2 fonctionnant en mode « transparent » lors de l'identification RFID des badges, il ne contient aucune donnée sensible affectant la protection en confidentialité de la clé DESFire ou de l'identifiant d'accès du porteur du badge.

Les données sensibles protégées par le lecteur C2 sont :

Donnée	Description
Clés de chiffrement/déchiffrement	Clés de chiffrement/déchiffrement des messages échangés entre l'UTL et le lecteur de badge

Le mécanisme de protection de ces données est décrit dans le document « Spécifications cryptographiques ».

4.4. DONNEES SENSIBLES DANS LE LECTEUR C2-CLAVIER

Le lecteur C2-Clavier fonctionnant en mode « transparent » lors de l'identification RFID des badges, il ne contient aucune donnée sensible affectant la protection en confidentialité de la clé DESFire ou de l'identifiant d'accès du porteur du badge.

Les données sensibles protégées par le lecteur C2-Clavier sont :

Donnée	Description
Clés de chiffrement/déchiffrement	Clés de chiffrement/déchiffrement des messages échangés entre l'UTL et le lecteur de badge
Code PIN	Code PIN associé au badge du porteur

Le mécanisme de protection de ces données est décrit dans le document « Spécifications cryptographiques ».

5. DESCRIPTION DES MENACES

Pour l'évaluation, les attaquants suivants sont considérés :

- Attaquant sur le réseau LAN Ethernet TCP/IP de l'exploitant de la solution de contrôle d'accès ;
- Attaquant sur le réseau CAN technique dédié au contrôle d'accès.
- Attaquant sur le lecteur de badge C2 ou le lecteur de badge C2-Clavier

Ne sont pas pris en compte les menaces dont les points d'entrée sont les postes informatiques serveurs et postes d'exploitation, ni les badges.

En tenant compte des hypothèses d'environnement, sont considérées les menaces suivantes :

5.1. INTRUSION SUR LE RESEAU LAN

Un attaquant est connecté sur le réseau Ethernet TCP/IP de l'exploitant de la solution de contrôle d'accès et déploie des moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes.

Ecoute transactions	Menaces
Ecoute d'une transaction contenant l'identifiant individuel du porteur	Copie du badge
Ecoute d'une transaction contenant le Code PIN du porteur	Usurpation d'identité (Authentification PIN par le malveillant)
Ecoute d'une transaction contenant les plages horaires	Elargissement des périodes d'accès
Ecoute d'une transaction contenant l'affectation des droits	Modification/affectation des droits d'accès d'un badge existant
Ecoute d'une transaction contenant des commandes	Ouverture d'un accès pour permettre son franchissement

5.2. INTRUSION SUR LE RESEAU TECHNIQUE CAN

Un attaquant, situé en zone non protégée, est connecté sur le bus CAN entre le lecteur de badge et l'UTL OTES3 et déploie des moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes..

Ecoute transactions	Menaces
Ecoute d'une transaction contenant l'identifiant individuel du porteur	Copie du badge
Ecoute d'une transaction contenant le Code PIN du porteur	Usurpation d'identité (Authentification PIN par le malveillant)

5.3. ATTAQUE PHYSIQUE SUR LE LECTEUR C2 OU LE LECTEUR C2-CLAVIER

Un attaquant tente d'arracher le lecteur de badge ou le lecteur de badge + clavier dans le but de le substituer ou de l'émuler.

6. DESCRIPTION DES FONCTIONS DE SECURITE

6.1. FONCTIONS DE SECURITE

La fonctionnalité principale d'ARD Access est de fournir à l'exploitant de la solution de contrôle d'accès la capacité de mettre en œuvre une solution d'accès sécurisée dans sa propre infrastructure réseau. Cette mise en œuvre passe par :

- La définition des sites, des zones et leur niveau de sécurité, des point d'accès (locaux ou portes) ;
- La définition d'une architecture adaptée au contrôle des flux (transfert d'informations) ;
- L'adoption d'une politique de sécurité cohérente et non ambiguë par rapport aux moyens organisationnels ;
- L'application d'une politique d'identification (identifiant unique et code PIN pour chaque usager) ;
- L'exploitation des audits analyse/consultation des historiques ;
- La mise en place d'une politique de sécurité pour les clés (génération, protection, programmation des SAM, installation sur les UTLs).

Les protections :

1. Protection en transmission de l'identifiant individuel du porteur
   Les identifiants personnels des porteurs de badge, encodés dans les badges DESFire EV1 ou EV2, utilisés dans la solution, sont protégés en confidentialité lors de leur transmission par un chiffrement en AES128.

2. Protection des données échangées entre l'UTL OTES3 et le lecteur de badge
   Les commandes et les transactions échangées entre l'UTL OTES3 et les lecteurs de badge sont protégées en confidentialité, authenticité et intégrité grâce à un chiffrement en AES128 et une authentification MAC.
   Dans le cas de l'utilisation du lecteur de badge C2-Clavier, les codes PIN sont ainsi également protégés en confidentialité, authenticité et intégrité.

3. Protection des données échangées entre le serveur de gestion et l'UTL OTES3
   Les commandes et les transactions échangées entre le serveur de gestion et l'UTL OTES3 sont protégées en confidentialité, authenticité et intégrité grâce à un chiffrement en AES128 et une authentification MAC.

4. Sécurisation du lecteur de badge C2 et du lecteur de badge C2-Clavier
   Les deux lecteurs sont équipés d'une protection à l'arrachement via un capteur accéléromètre/gyroscope qui déclenche une alarme vers l'UTL OTES3 puis vers le poste de gestion. Le lecteur ne disposant d'aucune clé de lecture des badges, l'attaquant ne disposera pas d'éléments lui permettant d'émuler un lecteur de badge dans le but de déchiffrer les données échangées avec le badge.
   En cas de substitution d'un lecteur, la communication avec l'UTL ne sera pas possible (pas de clé Client d'initialisation présente dans le lecteur).

6.2. CORRESPONDANCE ENTRE LES MENACES ET LES PROTECTIONS MISES EN ŒUVRE

Le tableau ci-dessous montre la correspondance entre les menaces décrites dans le paragraphe 5 et les protections mises en œuvre dans la solution.

Menaces	Protections			
	1	2	3	4
INTRUSION SUR LE RESEAU LAN				
Copie du badge			[redacted]	
Usurpation d'identité (Authentification PIN par le malveillant)				
Elargissement des périodes d'accès				
Modification/affectation des droits d'accès d'un badge existant				
Ouverture d'un accès pour permettre son franchissement				
INTRUSION SUR LE RESEAU TECHNIQUE CAN				
Copie du badge	[redacted]			
Usurpation d'identité (Authentification PIN par le malveillant)				
ATTAQUE PHYSIQUE SUR LE LECTEUR ARD C2 OU LE LECTEUR ARD C2-CLAVIER				
Substitution du lecteur				[redacted]

7. ANNEXES

7.1. ANNEXE 1 – TABLEAU 1 ANSSI - LES QUATRE NIVEAUX DE SURETE

Menaces potentielles			Niveaux de sûreté
Qui ?	**Quels moyens ?**	**Quelles connaissances ?**	
Franchissement « naturel » d'un point d'accès			
Pénétrations involontaires ou de curieux	Pas de matériel ou matériel basique (marteau léger, téléphone portable…)	Pas de connaissance	I
Franchissement par attaque mécanique et/ou logique « simple »			
Pénétrations préméditées de personnes faiblement équipées	Matériel et méthode obtenus dans le commerce ou sur Internet.	Connaissance basique du système acquise au travers de documents publicitaires ou technico-commerciaux émis par le fabricant ou les distributeurs.	II
Franchissement par attaque mécanique et/ou logique « évoluée »			
Pénétrations préméditées de personnes initiées et équipées.	Matériel ou maquette électronique spécifique facilement réalisable.	Connaissances recueillies à partir de l'examen d'un dispositif.	III
Franchissement par attaque mécanique et/ou logique « sophistiquée »			
Pénétrations préméditées de personnes initiées, fortement équipées et renseignées.	Matériel comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place.	Connaissances sur la conception et l'exploitation du système. Ceci implique d'avoir accès à des informations confidentielles du fabricant.	IV

7.2. ANNEXE 2 – TABLEAU 2 ANSSI - CORRESPONDANCE ENTRE LE NIVEAU DE SURETE ET LA RESISTANCE AUX ATTAQUES LOGIQUES

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