Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2020/21

Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité

Version 2.1.1

Paris, le 9 juin 2020

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification
ANSSI-CSPN-2020/21
Nom du produit
Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité
Référence/version du produit
Version 2.1.1
Catégorie de produit
Identification, authentification et contrôle d'accès
Critères d'évaluation et version
CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire
ARD SAS **Micropolis – Bâtiment Clématis** **CS 26003** **05000 GAP CEDEX**
Développeur
ARD SAS **Micropolis – Bâtiment Clématis** **CS 26003** **05000 GAP CEDEX**
Centre d'évaluation
Oppida **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**
Fonctions de sécurité évaluées **Protection en transmission de l'identifiant individuel du porteur** **Protection des données échangées entre l'UTL OTES3 et le lecteur de badge** **Protection des données échangées entre le serveur de gestion et l'UTL OTES3** **Sécurisation du lecteur de badge C2 et du lecteur de badge C2-Clavier**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage **Non**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est «l'Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité, version 2.1.1 » développé par ARD SAS.

La solution ARD Access permet de gérer de façon centralisée et en temps réel le contrôle des accès des personnes (appelés porteurs) à un site, un bâtiment ou un local.
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 Unités de Traitement Logique (UTL) OTES3 et des lecteurs C2 (avec ou sans clavier 12 touches).

Dans le cas de cette évaluation, le produit évalué est composé par l'UTL OTES3 et les lecteurs C2 (avec ou sans clavier).

La figure ci-dessous explicite l'architecture du produit évalué.

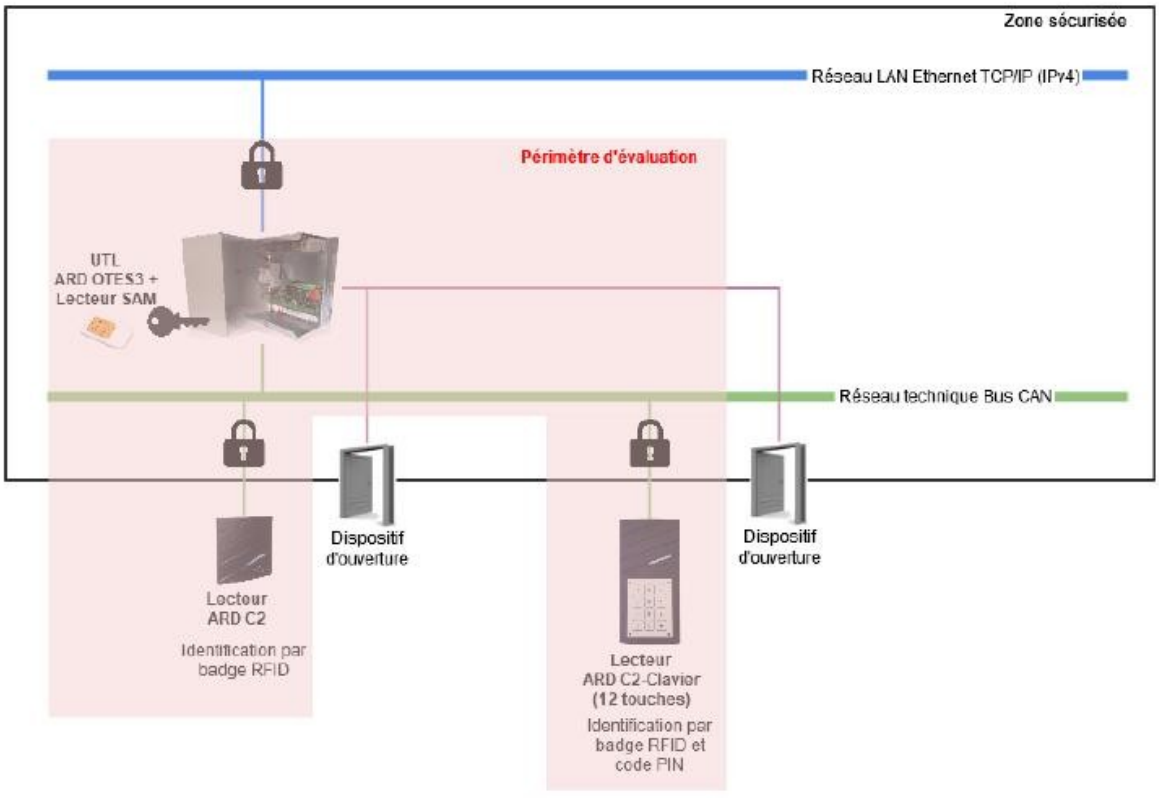

Figure 1 - Architecture Produit.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐	1 – détection d'intrusions
☐	2 – anti-virus, protection contre les codes malicieux
☐	3 – pare-feu
☐	4 – effacement de données
☐	5 – administration et supervision de la sécurité
☒	**6 – identification, authentification et contrôle d'accès**
☐	7 – communication sécurisée
☐	8 – messagerie sécurisée
☐	9 – stockage sécurisé
☐	10 – environnement d'exécution sécurisé
☐	11 – terminal de réception numérique (*Set top box*, STB)
☐	12 – matériel et logiciel embarqué
☐	13 – automate programmable industriel
☐	99 – autre

1.2.2. Identification du produit

Nom du produit	Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité
Numéro de la version évaluée	2.1.1
Référence de l'UTL (ARD OTES3)	E04130
Référence du pack de sécurisation cryptographique pour OTES2/OTES3	E04121
Référence du lecteur de badge ARD C2	E30253
Référence du lecteur de badge ARD C2-Clavier	E30307

La version certifiée du produit peut être identifiée de la manière suivante :

- l'identification de la version du logiciel évalué est possible au travers de l'interface d'administration de ARD Access ;
- l'identification de l'UTL se fait par lecture de l'étiquette présente sur la carte OTES3.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- protection en transmission de l'identifiant individuel du porteur ;
- protection des données échangées entre l'UTL OTES3 et le lecteur de badge ;
- protection des données échangées entre le serveur de gestion et l'UTL OTES3 ;
- sécurisation du lecteur de badge C2 et du lecteur de badge C2-Clavier.

1.2.4. Configuration évaluée

La configuration évaluée correspond à la version détaillée à la section 1.2.2.
La plateforme de test est constituée des éléments suivants :

- 1 unité de traitement logique ARD OTES3 + carte SAM ;
- 2 lecteurs de cartes (avec clavier et sans clavier) montés sur une plaque de démonstration avec les mécanismes de simulation d'un accès physique ;
- 1 serveur hébergeant la machine virtuelle de gestion des accès contrôlés (ARD Virtual Box).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2..

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité.

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

L'environnement d'évaluation a été fourni par ARD SAS sous forme de maquette préinstallée et prête à l'emploi. L'évaluateur ne peut donc pas se prononcer sur cet aspect de l'évaluation.

2.3.1.3. Durée de l'installation

Sans objet.

2.3.1.4. Notes et remarques diverses

Néant.

2.3.2. Analyse de la documentation

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation. Il estime que tous les documents sont clairs et qu'ils permettent d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3. Revue du code source (facultative)

L'évaluateur a revu le code source de l'intégralité du produit.
Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée. Cependant le produit utilise des librairies tierces comportant des vulnérabilités, mais celles-ci ne sont pas exploitables dans le contexte du produit et pour le niveau d'attaquant visé.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Avis d'expert sur la facilité d'emploi

Le produit est facile à utiliser, et ne nécessite pas de formation particulière pour son utilisation.

2.3.8.3. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci a identifié des non-conformités au RGS (voir RGS) mais celles-ci n'engendrent pas de vulnérabilités exploitables pour le niveau d'attaquant visé.

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé, il en ressort que le produit utilise soit un composant externe, qui n'a pas fait l'objet d'une analyse au titre de cette évaluation, soit des librairies logicielles *Open Source* qui n'introduisent pas des vulnérabilités.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité, version 2.1.1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.
L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS].

Aucune recommandation particulière n'est formulée par l'évaluateur.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité ;* Version : 2.1.1 ; Date : *16 avril 2020.*
[RTE]	*Rapport Technique d'Evaluation CSPN – DRA ARD Access* Référence : OPPIDA/CESTI/DRA/RTE/1.3 ; Version : 1.3 ; Date : *10 mars 2020.*
[GUIDES]	*Guide utilisateur ARD ACCES Calendriers ;* Version : 1.6.2. *Guide utilisateur ARD ACCES Badge + code PIN ;* Version : 1.5.1. *Guide de prise en main rapide ;* Version : 1.10.0.

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.0 du 6 septembre 2018. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/2.0 du 6 septembre 2018. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.