PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2023/26

Dorlet Physical Access Control System

Version 1.2

Paris, le 19 Janvier 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2023/26**
Nom du produit **Dorlet Physical Access Control System**
Référence/version du produit **Version 1.2**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **DORLET S.A.U.** C/ Albert Einstein, 34 01510 Miñano, Álava, Espagne
Développeur <cas un développeur> **DORLET France** 2 bis voie La Cardon 91120 Palaiseau, France
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées Protection des communications ACU-DASSnet Protection des communications ACU-Lecteur Protection du code PIN Fonction anti-effraction Fonction anti-retour
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Non

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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.cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Dorlet Physical Access Control System, Version 1.2 » développé par DORLET France.

Ce produit est un système de contrôle d'accès physique centralisé fournissant une solution d'autorisation d'accès sécurisée.

Le produit est composé des éléments suivants :

- **DASSnet** : le centre de gestion des accès contrôlés (GAC) de la solution, composé de postes client et d'un serveur pour contrôler et interroger l'état du système ;
- **ASDx** (ou **ACU**) : l'unité de traitement local (UTL) de la solution, en charge de valider l'accès des utilisateurs en fonction de leurs droits et de fournir des informations sur l'état du système ;
- **Lecteurs de badge** à circuit intégré RFID (modèles : EVOpass20, EVOpass20K avec clavier pour code PIN, EVOpass40 avec module biométrique, EVOpass40K avec module biométrique et clavier pour code PIN).

Les éléments suivants sont également intégrés à la solution et participent à l'authentification des utilisateurs, mais ne sont pas couverts par le présent certificat :

- Les badges (modèle MIFARE DESFire EV2 de la société NXP) présentés par les utilisateurs afin de s'authentifier au système ;
- Les modules de sécurité *MIFARE Secure Access Module* (SAM), modèle AV3, placés au cœur des ACU, dans chaque lecteur et éventuellement au niveau du poste client ;
- Le module biométrique *OEM IDEMIA biometric module*, intégré dans les lecteurs EVOpass40 et EVOpass40K.

Le tableau ci-dessous synthétise le périmètre de l'évaluation :

Composants du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE), supposé de confiance
GAC	Système d'exploitation		Windows 11
	Applicatifs	DASSnet v2.7.200	
	Fonctions cryptographiques	WolfSSL v5.2.0	
	Bases de données et annuaires		SQL Express 2019
UTL	Système d'exploitation	Sans O.S.	
	Applicatifs	ASD/4 v1.58 anssi v1.03	
	Fonctions cryptographiques	WolfSSL v5.2.0	
	SAM		MF4SAM3X84 (SOT658-1)
Lecteurs	Lecteurs simples	EvoPass20 v11.21.00 anssi v1.00 Evopass40 v11.21.00 anssi v1.00	

	Lecteurs-clavier	EvoPass20K v11.21.00 anssi v1.00 Evopass40K v11.21.00 anssi v1.00	
	SAM		MF4SAM3HN (SOT617-3)
Badges			MIFARE DESFire EV2

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*

Produit	
Nom du produit	Dorlet Physical Access Control System
Numéro de la version évaluée	Version 1.2

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

- Pour le GAC (composant logiciel DASSnet client et serveur) :
  - Dans l'application cliente, sous le menu Aide > A propos :

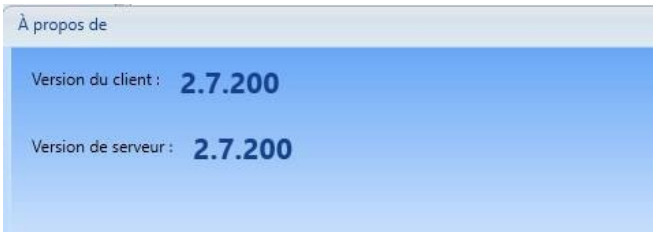

Figure 1 – Identification de la version du GAC.

- Pour l'UTL (module ASD/4) et pour les lecteurs de badge :

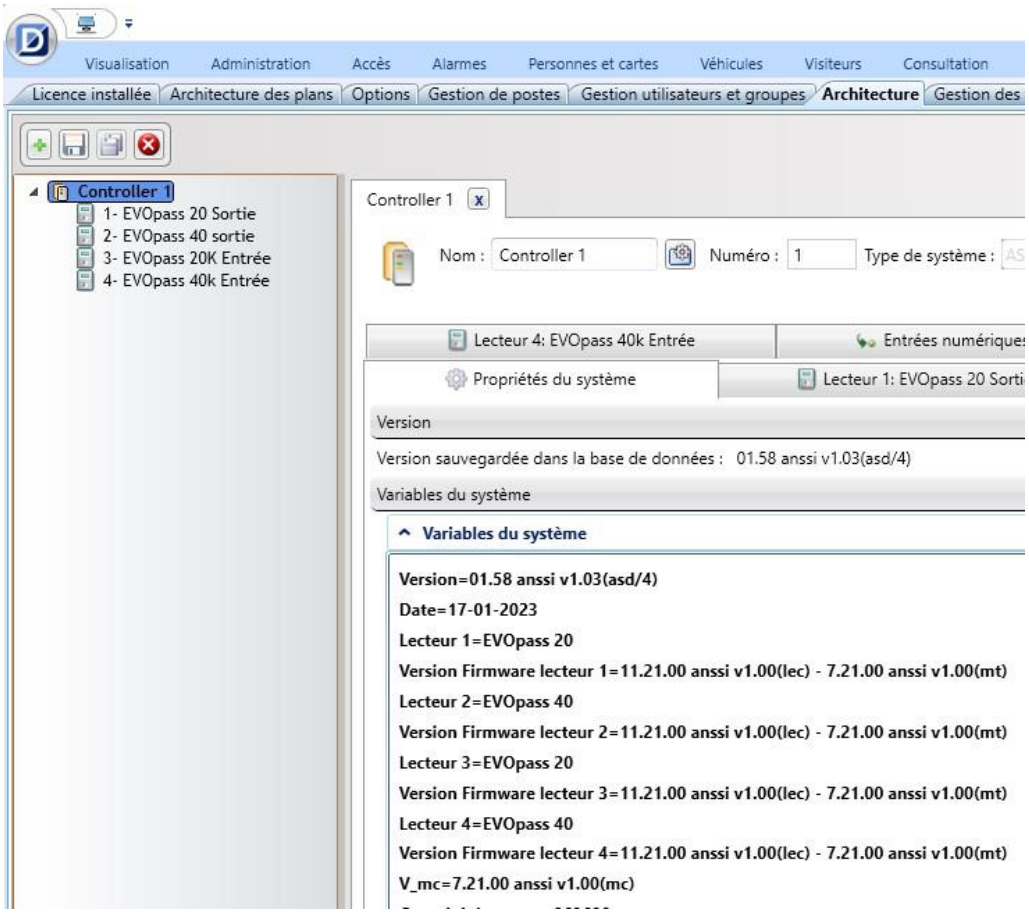

Figure 2 – Identification de la version de l'UTL et des lecteurs.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection des communications ACU-DASSnet ;
- la protection des communications ACU-Lecteur ;
- la protection du code PIN ;
- la fonction anti-effraction ;
- la fonction anti-retour ;

1.2.4 *Configuration évaluée*

La configuration évaluée est décrite au paragraphe 3.5 « Périmètre de l'évaluation » de la cible de sécurité [CDS] et est résumée dans le tableau de synthèse du périmètre d'évaluation précisé au paragraphe 1.1 du présent rapport.

La plateforme de test est constituée des éléments suivants :

- quatre lecteurs de badge ;
- un ACU modèle ASD/4 ;
- une *Master key* ;
- une machine Windows 11 pour l'environnement DASSnet.

La figure ci-dessous explicite la plateforme de test :

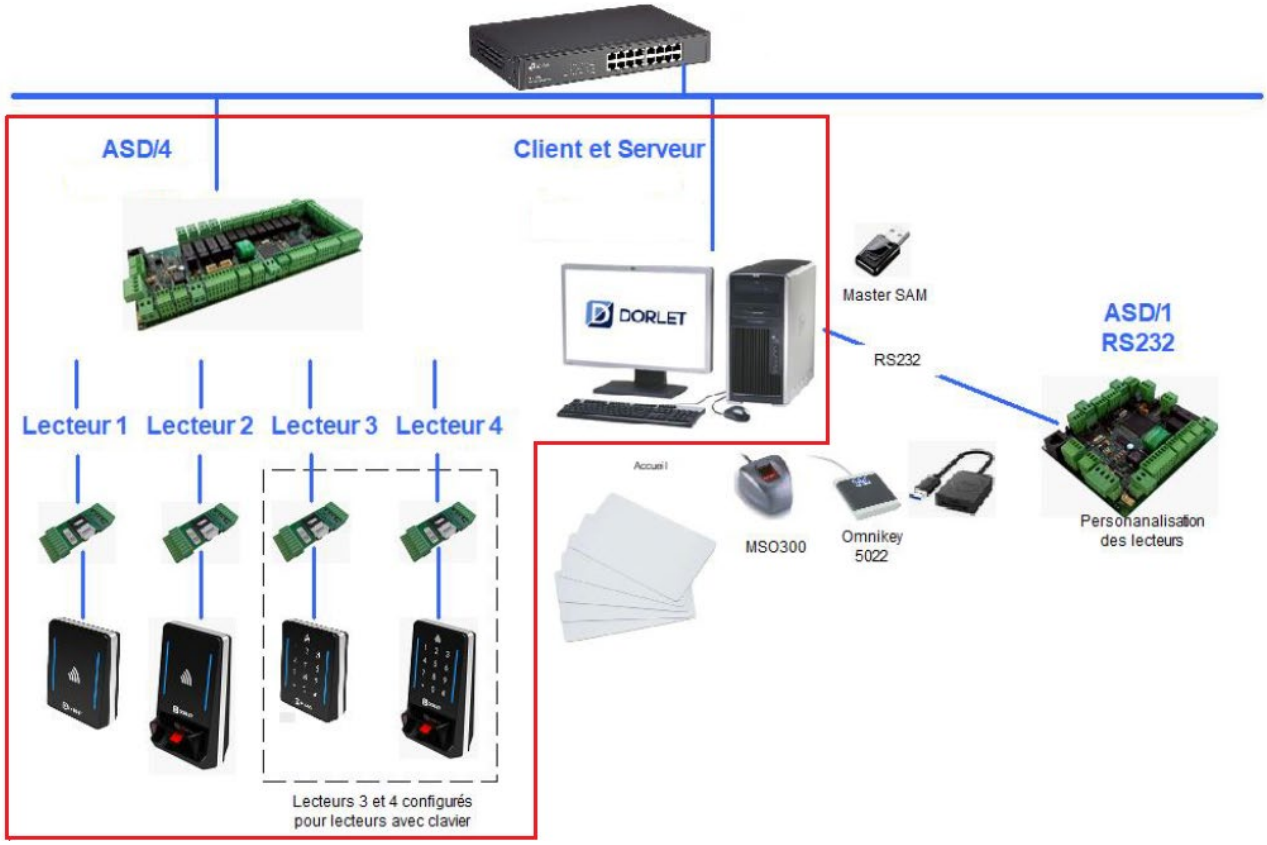

Figure 3 – Plateforme de test (le périmètre d'évaluation est entouré en rouge).

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-07].

2.2 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 [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

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

2.2.1.2 Description de l'installation et des non-conformités éventuelles

L'installation a été réalisée en suivant les procédures et directives décrites dans [GUIDES].

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

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

2.2.5 *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.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS]

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 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.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

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

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 « Dorlet Physical Access Control System, Version 1.2 » 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], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - *Dorlet Physical Access Control System* – Cible de sécurité, version 1.15, 5 décembre 2023.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – Produit *Dorlet Physical Access Control System* - version 1.2 référence CSPN-RTE-DORLET3-1.01, version 1.01, 7 décembre 2023.
[GUIDES]	Guides d'installation et d'utilisation du produit : - Guide d'installation sécurisée DASSnet ANSSI, référence « FR_Guide dinstallation sécurisé DASSnet ANSSI V1.5.pdf », version 1.5 - Manuel ASD/4 ANSSI, contrôle des accès/alarmes – Guide d'installation v1.66 rev0.2, référence « FR Guide ASD4 V1.66 HW V1.6 Rev.02 (ENU.) ANSSI .pdf » - Guide de l'utilisateur du système de sécurité ANSSI, référence « FR_Guide de l'utilisateur du système de sécurité ANSSI v1.2.pdf », version 1.2.

ANNEXE B. Références liées 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, version 4.0, 3 mars 2022. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[NOTE-07]	Note d'application - Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN, référence ANSSI-CSPN-NOTE-07, version 1.0, 7 juillet 2020.