Dorlet Physical Access Control System - Cible de sécurité

V1.15

05/12/2023

Créé par

AMOSSYS

Historique des modifications

Version	Date	Auteur	Commentaires
1.0	24/05/2019	Alberto del Río Aguilar	Première édition.
1.1	28/06/2019	Alberto del Río Aguilar	Corrections des commentaires du 06/07/2019 d'Amossys.
1.2	16/07/2019	Alberto del Río Aguilar	Corrections des commentaires du 04/07/2019 d'Amossys.
1.3	24/07/2019	Alberto del Río Aguilar	Corrections des commentaires du 24/07/2019 d'Amossys.
1.4	01/03/2021	Jesús Pérez	Added EVOpass40 reader with Idemia CBM Version numbers of Evaluation Scope elements updated SF. ACU – DASSnet communication protection
1.5	09/11/2021	Martin Moreau	Corrections following a cryptographic design change
1.6	22/03/2022	Josu Mujika	Added SAM recognizer and card recognizer at the client workstation
1.7	18/05/2022	Julie Lemeteyer	Corrections following discussion with the developer
1.8	24/05/2022	Julie Lemeteyer	Figures review and corrections
1.9	16/06/2022	Francois Fontanet	Traduction au Français et finalisation du document
1.10	24/06/2022	Francois Fontanet	Version finale
1.11	08/08/2022	Francois Fontanet	Revue du protocole d'échange de clés

1.12	14/10/2022	Julie Lemeteyer	Prise en compte des retours ANSSI (anssi-cspn-note-07)
1.13	13/04/2023	Francois Fontanet	Prise en compte des retours du pré-audit Hardware
1.14	28/09/2023	Josu Mujika	mise à jour des versions de la portée de l'évaluation .
1.15	05/12/2023	Julie Lemeteyer	Prise en compte des retours ANSSI et évaluateur

Table des matières

Table des illustrations

1 Introduction

1.1 Document référence

Titre: Dorlet Physical Access Control System - Cible de sécurité

Version: v1.15

Auteur: Dorlet, **AMOSSYS**

Evaluation lab: **AMOSSYS**

Date de publication: 05/12/2023

1.2 Objet du document

Le présent document a été élaboré conformément à **[CSPN-CER-P01]** et **[CSPN-CER-I02]** en tant que cible de sécurité pour une évaluation CSPN pour le Dorlet Physical Access Control System v1.2.

1.3 Références

Reference	Document
[CC-19-207017]	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408) 29/01/2019.
[CSPN-CER-CRYPTO]	Fournitures nécessaires à l'analyse de mécanismes cryptographiques, v1.2.
[CSPN-CER-P-02]	Critères d'évaluation pour la certification de sécurité de premier niveau, v4.0.
[CSPN-CER-P-01]	Certification de premier niveau pour les produits des technologies de l'information, v4.0.
[DORLET-CRYPTO]	Système de contrôle d'accès physique Dorlet - Informations cryptographiques, v1.14
[FIPS-PUB-197]	Publication des normes fédérales de traitement de l'information 197.
[CC-SAM-AV3]	• Plate-forme matérielle certifiée CC EAL6+ du 24/06/2021 (basée sur SmartMX2 P6022y VB de NXP) • Composite certifié avec MIFARE Security Evaluation Scheme (équivalent à EMVCo Évaluation de la sécurité) (Laboratoire d'évaluation : TÜViT, Laboratoire de certification : UL) • Certifié FIPS 140-2 CAVP.

Reference	Document
[MIFARE-SAM]	Module d'accès sécurisé MIFARE SAM AV3 – Fiche produit courte 561930 révision 3.0.
[PIC24FJ12-DOC]	Fiche technique de la famille de microcontrôleurs PIC24FJ256GB406
[STM32L443-DOC]	STM32L443RC fiche technique du microcontrôleur, révision 5.
[TOE-ASD-MAN]	FR Guide ASD4 V1.66 HW V1.6 Rev.02 (ENU.) ANSSI
[TOE-INSTALL]	FR Guide d'installation sécurisée DASSnet ANSSI V1.5
[TOE-MAN]	FR Guide de l'utilisateur du système de sécurité ANSSI, v1.2.
[WOLFSSL-LIB]	Wolfssl-5.2.0
[IDEMIA-CBM]	cbm-series-idemia-brochure-201902
[ANSSI-NOTE07]	Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN, version 1.00
[ANSSI-Guide]	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection, version 2.00

1.4 Abbreviations

Reference	Document
ACU	Access Control Unit
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CC	Common Criteria
CSN	Chip Serial Number
DRNG	Deterministic Random Number Generation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCM	Galois/Counter Mode
ICC	Integrated Circuit Card
SAM	Secure Access Module
SMU	SAM Management Unit
ST	Security Target
TOE	Target Of Evaluation
TRNG	True Random Number Generation
WCF	Windows Communication Foundation

2 Identification du produit

Les données suivantes permettent d'identifier sans équivoque la TOE. Chaque partie particulière qui compose la TOE a également une référence unique, qui peut être trouvée dans la *Figure 9. Éléments de la portée de l'évaluation*.

Catégorie de produit : Identification, authentification et contrôle d'accès.

Nom commercial: Dorlet Physical Access Control System

Version évaluée : 1.2

Développeur : Dorlet

3 Description du produit

Cette section fournit une description détaillée du produit comprenant ses principales caractéristiques, la façon dont il doit être utilisé et une brève description du type d'environnement pour lequel il a été conçu et prévu de fonctionner.

La spécification de l'environnement comprend les menaces auxquelles le produit peut être confronté et comment ses fonctions de sécurité fonctionnent pour les atténuer.

3.1 Description générale du produit

Le système de contrôle d'accès Dorlet v1.2 est un système de contrôle d'accès physique centralisé développé par Dorlet et constitué de différents éléments qui fonctionnent ensemble pour fournir une fonctionnalité d'autorisation d'accès sécurisées. Le produit se compose des éléments suivants :

- **DASSnet.** Logiciel de gestion développé par Dorlet et composé de postes client et d'un serveur pour contrôler et interroger l'état du système. L'installation du logiciel se fait par un fichier exécutable qui permet à l'utilisateur d'installer les différents modules tel que le serveur, et le logiciel client.
- **ASDx**. La fonctionnalité de cet élément est au cœur du système d'authentification car il est en charge du contrôle des informations qu'il reçoit en entrée. Par conséquence, l'ACU validera (ou pas) l'accès des utilisateurs en fonction de leurs droits. Il fournit également différentes informations concernant l'état de l'ensemble du système et l'identité de chaque utilisateur du système. Il existe trois modèles différents d'ACU : ASD/1, ASD/2 et ASD/4, ce dernier étant le seul inclus dans le périmètre de l'évaluation. Ils ont tous des caractéristiques similaires, la seule différence étant leurs capacités matérielles qui n'impacte pas leurs fonctionnalités.
  Un ACU contient :
  - Un **Module de Communications (CM).** Installé avec l'ACU, il dispose d'un SAM qui est en charge de l'authentification des communications DASSnet-ACU.
  - Un **Module Transparent (TM)** par lecteur. Installé avec l'ACU dans les entrées du lecteur, il dispose d'un SAM où les clés Desfire pour lire/écrire la carte Desfire EV2 sont stockées en toute sécurité et réalise la fonction d'authentification des communications entre ACU et Lecteur
- **Reader**. Cet élément du produit est un lecteur de carte à circuit intégré RFID. Il existe quatre variantes de cet élément :

- **EVOpass20/EVOpass20K**, La différence est que EVOpass20K a un clavier pour codes NIP qui n'est pas présent sur les EVOpass20. Ce code NIP est utilisé comme deuxième facteur d'authentification des utilisateurs vis-à-vis du système.
- **EVOpass40/EVOpass40K**, présentent exactement les mêmes caractéristiques et le même niveau de sécurité. Contrairement à la famille EVOpass20, ce lecteur intègre un module biométrique d'Idemia, afin de fournir un accès par carte plus une empreinte digitale, où l'empreinte digitale est stockée sur la carte elle-même et ledit module compare l'empreinte digitale lue avec celle stockée dans la carte, dans le cas du EVOpas40K un code NIP est utilisé en troisième facteur.

Les sections suivantes décrivent les éléments qui sont utilisés dans le système et nécessaires au fonctionnement de la TOE, mais qui sortent du cadre de l'évaluation.

3.1.1 Éléments non-TOE impliqués dans la solution

D'autres éléments sont intégrés à la solution mais sortent du cadre de l'évaluation :

- **MIFARE DESFire EV2 (User card)** : Ce sont les cartes qui sont présentées par les utilisateurs afin de s'authentifier auprès du système. Cet élément ne fait pas partie de la TOE, mais sa description est pertinente du fait de sa communication avec le reste du système. Les ICC MIFARE DESFire EV2 sont développés par NXP et sont certifiés Critères Communs, comme indiqué dans **[CC-19-207017]**.
- **MIFARE Secure Access Module (SAM)**: AV3 MF4SAM3X84 (SOT658-1) and MF4SAM3HN (SOT617-3): Ce module est placé:
  - Au sein du CM de l'ACU et du TM de l'ACU (SOT658-1). Il est utilisé pour stocker la paire de clés asymétrique utilisée pour l'authentification et la génération de clés de session. Ce module joue un rôle principal dans les communications entre les cartes et la TOE car il est capable de lire les données protégées des cartes pour vérifier l'identité de l'utilisateur. En fin de compte, le canal de communication utilisé pour vérifier l'identité d'un utilisateur est établi entre le SAM (TM) et les cartes Desfire d'identification de l'utilisateur.
  - Dans chaque lecteur (SOT617-3) un SAM au format IC est utilisé pour générer des nombres aléatoires. Ils stockent également la paire de clés asymétrique utilisée pour l'authentification et la génération de clés de session.

- Dans le module RC (SOT658-1). Cet élément peut être utilisé au niveau du poste client, il stocke en toute sécurité les clés Desfire nécessaires à la lecture/écriture des cartes par le biais du lecteur de carte.

Les modules d'accès sécurisé MIFARE AV3 sont certifiés Critères communs avec un niveau d'assurance d'évaluation de matériel EAL 6+. Vous trouverez plus d'informations sur ce module dans **[MIFARE-SAM] et [CC-SAM-AV3].**

- **OEM Idemia biometric module** : Ce module fabriqué par Idemia est intégré dans les lecteurs EVOpass40 **[IDEMIA-CBM]**. Lors de la lecture d'une carte, si le fonctionnement est configuré en accès carte plus empreinte digitale, le lecteur lit le modèle d'empreinte digitale de l'utilisateur stocké dans la carte DESFire, puis l'envoie à ce module pour valider sa correspondance avec l'empreinte qui sera présentées par l'utilisateur. Si elles correspondent, les données de la carte sont envoyées à l'ACU pour que celle-ci autorise ou refuse l'accès en fonction des autorisations programmées pour cette carte.

3.1.2 Autres éléments non TOE utilisés pour l'installation de la TOE

Les éléments suivants sont nécessaires pour mettre en place la plateforme mais ils sortent du cadre de l'évaluation :

1. **SMU (SAM Management Unit) :** Cette SMU est utilisée uniquement sur le site dans un local sécurisé pour établir la communication entre le DASSnet et les éléments à personnaliser, c'est-à-dire les lecteurs et les SAM de terrain.
   Pour cela, les lecteurs équipés de la SAM (LT) au format IC doivent être connectés à l'entrée lecteur de l'ACU, elle-même connectée au port série de la SMU. Pour les SAM de terrain, une autre méthode de personnalisation consiste à utiliser un module lecteur de carte à puce connecté par USB.
2. **Enrôleur Omnikey**. Utilisé pour les opérations de configuration de la carte Desfire sur la station de gestion SAM. Peut également être utilisé sur la station client avec le module SAM RC
3. **SAM RC** pour la lecture/écriture des cartes Desfire depuis les postes clients, si utilisé à la place du SMU pour l'enrôlement des badges.
4. **SAM Master module**. Cet élément, Utilisé uniquement dans un local sécurisé, stocke en toute sécurité toutes les clés requises dans le système. Il est également en charge de la certification du reste des éléments de l'installation.
5. **Smart card reader module**. Utilisé uniquement dans un local sécurisé pour la personnalisation des SAM de terrain.

3.2 Description fonctionnelle du produit

Le scénario typique pour l'utilisation de la TOE est un utilisateur qui tente d'être authentifié par le système. L'utilisateur étant en possession d'une carte d'identification valide enregistrée dans le système, la première étape serait que cette carte soit lue par l'un des lecteurs du système.

MIFARE DESFire EV2 ICC est le modèle de carte utilisé dans le système pour authentifier les utilisateurs. Ces cartes sont munies de clés d'utilisation (importées lors de leur phase de personnalisation) et sont présentées aux lecteurs afin de vérifier l'identité de l'utilisateur.

Le processus d'authentification d'un utilisateur consiste en la présentation d'une carte au lecteur, qui envoie une demande d'authentification à l'ACU. Dans le cas des lecteurs EVOpass40, il est possible d'ajouter la condition de vérification de l'empreinte digitale de la personne pour autoriser l'accès. Le modèle de l'empreinte digitale est stocké dans un fichier chiffré sur la carte. Il est nécessaire de s'authentifier avant d'accéder à ce modèle.

L'ACU demande au SAM (TM) une opération d'authentification puis les communications entre l'ICC et le SAM (TM) s'effectuent à l'aide d'un protocole DESFire, de manière transparente pour le lecteur.

Ce processus d'authentification est basé sur la vérification des clés présentes dans une carte d'un utilisateur. Cela n'inclut pas la vérification du code PIN de l'utilisateur dans le cas où le lecteur utilisé dans le système présente un clavier PIN. Le processus de vérification des codes PIN repose sur l'ACU.

En cas de réponse réussie, l'ACU transmet au lecteur une réponse valide afin de confirmer à l'utilisateur que son identité a été vérifiée. Dans le même temps, l'ACU envoie les détails du processus de validation au serveur DASSnet, qui stocke ces informations.

Du point de vue d'un administrateur système, le panneau de contrôle offert par le logiciel de gestion DASSnet permet de gérer les utilisateurs et les cartes, d'interroger le système pour une variété d'informations, etc.

Les ACU ont un mode de défaillance, abondamment décrit dans [TOE-MAN], qui indique au DASSnet de ne pas communiquer avec elles. Lors de la détection d'un problème matériel, une alarme est déclenchée et l'ACU entre en mode de défaillance indiquant au DASSnet de ne pas tenter d'établir des communications. L'ACU reste dans ce mode jusqu'à ce qu'il soit réparé ou remplacé. Ce mode sort du cadre de l'évaluation et n'est pas considéré comme faisant partie du fonctionnement correct et sécurisé de la TOE.

Le schéma de communication entre les différentes parties du système est représenté sur la *figure 1*.

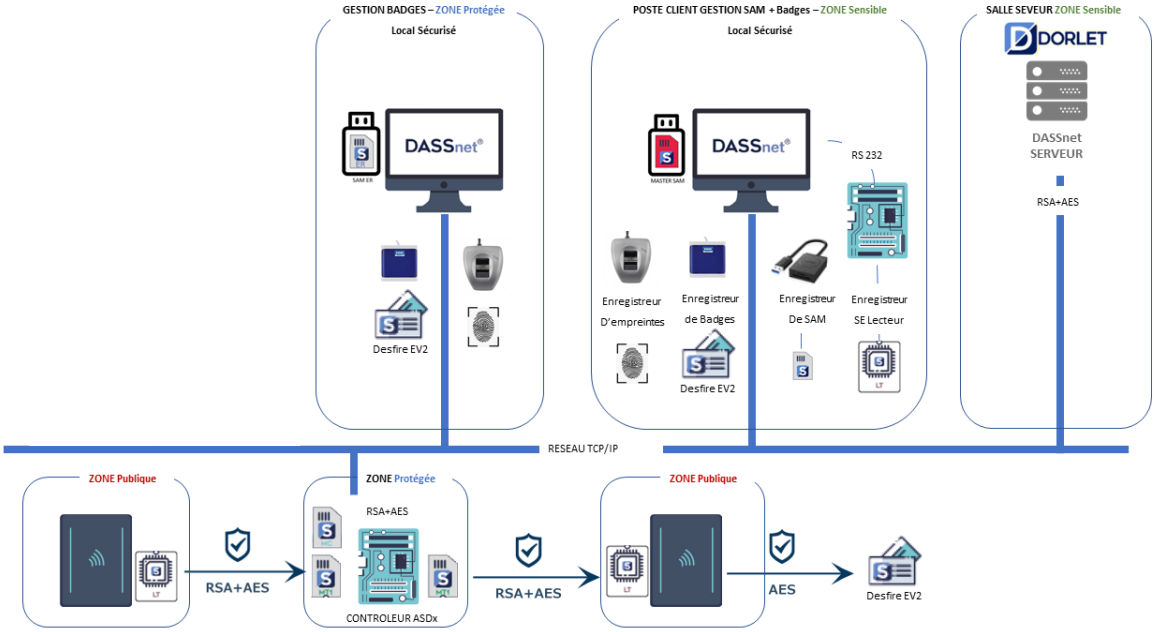

Figure 1. Schéma des éléments de communication du produit

Le schéma de distribution des clés dans les différents éléments du système est représenté sur la *figure 2.*

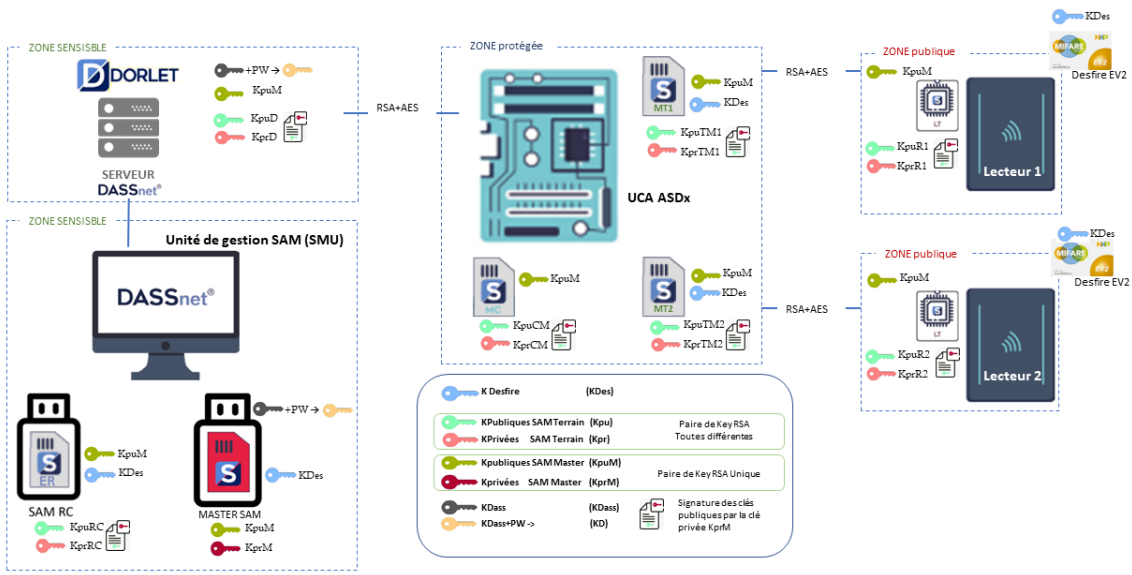

Figure 2. Schéma de distribution des Keys

Les sous-sections suivantes détaillent chaque composant de la TOE.

3.2.1 DASSnet

DASSnet est un logiciel de gestion développé par Dorlet qui permet la gestion des systèmes de sécurité intégrée tel que stipulé dans sa licence :

- Le contrôle d'accès (Visiteur , Alarmes, Synoptique, Personnalisation des badges, Gestion d'accès des entreprises)
- La vidéosurveillance (désactivé pour l'évaluation) ;
- La détection d'intrusion (désactivé pour l'évaluation).

Le logiciel est orienté utilisateur, offrant une interface accessible et comprenant la prise en charge de tous les appareils modernes.
Compte tenu de ses capacités modulaires, DASSnet peut s'adapter à des systèmes de toutes tailles, des petits systèmes de contrôle d'accès aux grands projets nécessitant une gestion partagée. Étant donné que ce logiciel est une technologie multithread, il est capable de fonctionner comme un serveur de communication entre différentes machines (physiques et virtuelles), gérant des installations avec de grandes quantités de composants de sécurité tout en offrant une haute disponibilité du système de gestion.

Ce logiciel est développé de façon à ce que son déploiement s'effectue à deux niveaux : serveur et client. Le côté serveur de l'application utilise une base de données SQL dans laquelle il stocke toutes les informations non critiques, c'est-à-dire toutes les informations relatives à l'utilisateur qui ne sont pas des données d'authentification de carte. D'autre part, du côté du client, il est possible de gérer les comptes d'utilisateurs et de vérifier diverses informations sur l'état du système. Les services de base de données pris en charge sont Microsoft SQL Server, et Microsoft SQL Server express.

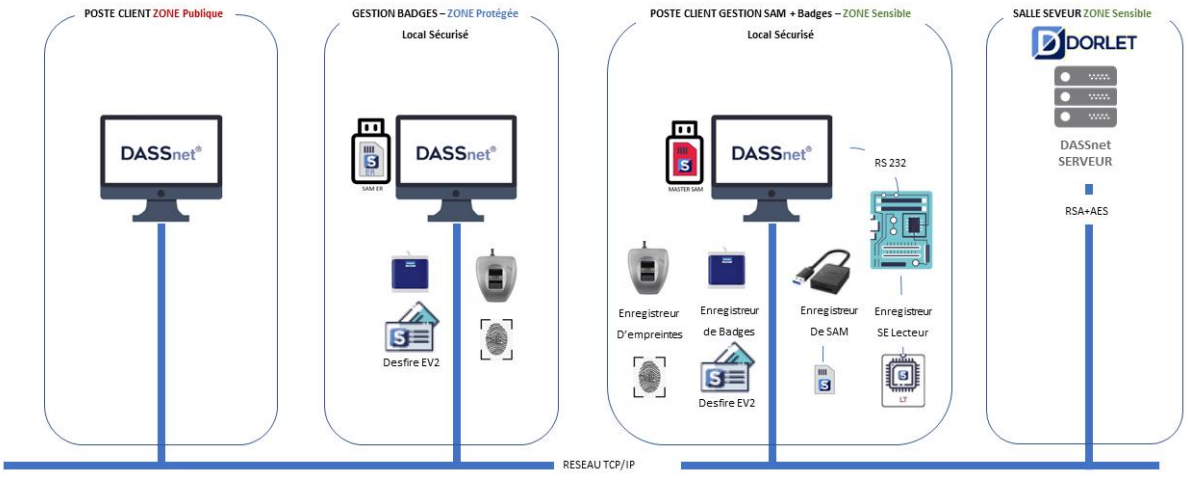

Figure 3. Produit élément DASSnet

À partir de la *Figure 1. Schéma de communication des éléments du produit*, le serveur DASSnet est installé sur une seule machine serveur avec les caractéristiques décrites dans *3.3*

Description des dépendances, et une ou plusieurs machines exécutant le logiciel client et connectées au serveur via un réseau IP. Toutes ces machines sont placées sur site, c'est-à-dire dans l'installation que le système vise à protéger.

Les communications établies entre le serveur DASSnet et ses clients sont toujours initiées par les clients via une authentification auprès du serveur. Ces communications sont basées sur Windows Communication Foundation et utilisent le port TCP 11000 par défaut.

3.2.2 ASDx (ACU)

Dans le contexte de ce document, ASDx fait référence aux modèles ASD/1, ASD/2 et ASD/4 de l'unité de contrôle d'accès ASD de Dorlet. Les unités ASDx sont des contrôleurs haut de gamme pour le contrôle d'accès et l'interaction des entrées d'alarmes.

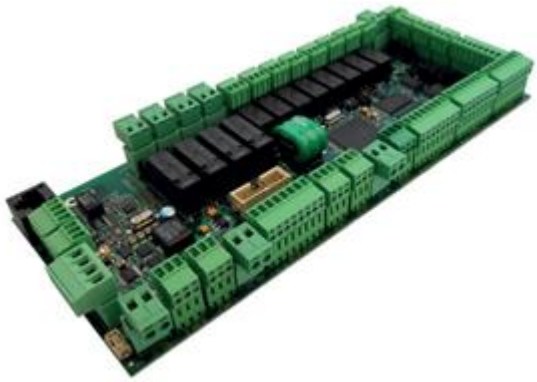

Figure 4. ASD/4

Ces unités ont :

- Une connexion Ethernet directe jusqu'à 100 Mbps, une mémoire vive de 8 Mo et une fonction AES GCM-128 (proposée par WolfSSL Library) pour assurer la sécurité des communications ;
- Un module de communication (CM), en charge de la génération de clé de session entre DASSnet et ACU[1].

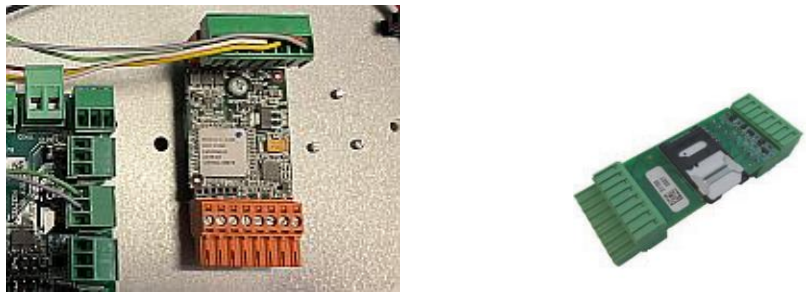

Figure 5. Communication Module (CM)

- Un module transparent (TM) par lecteur, en charge du stockage des clés Desfire et des communications AES128-GCM entre l'ACU et les lecteurs :

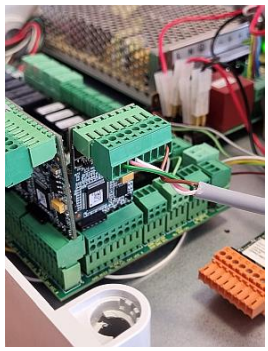

Figure 6. Transparent Module (TM)

Toute la configuration de ces unités de contrôle d'accès est stockée dans une mémoire au sein de la même unité, réalisant ainsi un système remarquablement souple, fonctionnant à la fois dans le cadre d'un système plus large ou de manière autonome.

Les unités ASDx sont chargées de stocker en toute sécurité les informations essentielles au bon fonctionnement du système. Pour cela, un module d'accès sécurisé est associé à chaque composant (CM d'ASDx, TM d'ASD et lecteur) et utilisé pour stocker en toute sécurité toutes les informations critiques (tel que la clé d'authentification) et pour obtenir des nombres aléatoires. Ce module est décrit dans *3.2.5 Module d'accès sécurisé*. Entre autres informations, les unités ASDx stockent des informations concernant l'état du système et des mesures de l'état des unités elles-mêmes. Certaines de ces informations sont transmises au DASSnet via un canal sécurisé pour alimenter sa base de données et tenir l'utilisateur informé de l'état du système et de tous les événements de sécurité en temps réel.

Les unités ASDx sont également préparées à recevoir des informations du serveur DASSnet pour créer, effacer et modifier les informations de l'utilisateur. Par exemple, ce moyen de communication est utilisé lors de l'enregistrement des cartes d'identification dans le système.

Les unités ASDx présentent également un niveau supplémentaire de sécurité physique en étant capables de détecter quand elles sont manipulées ou retirées de leur emplacement d'installation.

Toutes les communications entre les différents composants de l'ACU sont chiffrées.

Le micro BootLoader dispose d'une sécurité d'accès par ID CODE qui interdit tout accès a la lecture et l'écriture sans celui-ci.

3.2.3 EVOpass20

L'EVOpass20 et l'EVOpass20K sont des lecteurs ICC, développés par Dorlet, qui sont utilisés dans le schéma TOE pour fournir une interface d'entrée pour les informations d'authentification de la carte.

La différence entre EVOpass20 et EVOpass20K est la présence d'un clavier dans ce dernier qui peut être utilisé pour des étapes d'authentification supplémentaires.

Figure 7. EVOpass20

Les Lecteurs possèdent une autoprotection par un contact mécanique, doublé d'un détecteur accéléromètre qui détectent si le lecteur est séparé du mur ou s'il est manipulé, générant ainsi une alarme « Lecteur manipulé ».

La déconnexion du lecteur génère également une alarme de « Lecteur déconnecté ».La communication établie entre le lecteur et l'ACU est protégée par AES-128-GCM avec une clé de session obtenue lors de l'authentification entre le lecteur et le module transparent (TM).

Les lecteurs sont également équipés d'un module d'accès sécurisé, avec les caractéristiques décrites dans la section *3.2.5 Module d'accès sécurisé*.

3.2.4 EVOpass40

L'EVOpass40 et l'EVOpass40K sont des lecteurs ICC, développés par Dorlet, qui sont utilisés dans le schéma TOE pour fournir une interface d'entrée pour les informations d'authentification de la carte.

La différence entre EVOpass40 et EVOpass40K est la présence d'un clavier dans ce dernier qui peut être utilisé pour des étapes d'authentification supplémentaires.

De plus, il intègre un module biométrique pour la lecture des empreintes digitales, afin de renforcer la sécurité d'accès, nécessitant une carte valide avec la même empreinte digitale que celle utilisée pour générer le modèle stocké sur la carte. C'est une condition supplémentaire d'accès, puisque seul l'accès avec une empreinte digitale ne sera jamais autorisé.

Figure 8. EVOpass40

Les Lecteurs possèdent une autoprotection par un contact mécanique, doublé d'un détecteur accéléromètre qui détectent si le lecteur est séparé du mur ou s'il est manipulé, générant ainsi une alarme « Lecteur manipulé ».

La déconnexion du lecteur génère également une alarme de « Lecteur déconnecté ».

La communication établie entre le lecteur et l'ACU est protégée par AES-128 avec une clé de session obtenue lors de l'authentification entre le lecteur et le module de communication ACU.

Les lecteurs sont également équipés d'un module d'accès sécurisé, avec les caractéristiques décrites dans la section *3.2.5 Module d'accès sécurisé*.

3.2.5 Module d'accès sécurisé

Les modules d'accès sécurisé MIFARE (SAM) AV3 MF4SAM3 sont des ICC qui sont installés dans l'unité de contrôle d'accès (dans CM et TM) et les lecteurs (LT). Dans le cas du TM de l'ACU, ce module est chargé d'interagir avec les cartes des utilisateurs afin de vérifier l'identité de l'utilisateur. Il stocke de manière sécurisée les clés, qui peuvent être modifiées via les canaux sécurisés.

D'autre part, le SAM du MT est également capable de communiquer directement avec les cartes utilisateurs en utilisant le protocole DESFire chiffrés sans l'intervention des autres parties de la TOE sauf pour la transmission des messages chiffrés. Le SAM du MT est également capable de communiquer dans les deux sens avec l'ACU pour recevoir des demandes d'authentification et renvoyer des informations de validation d'utilisateur.

Les SAM sont également utilisés à la fois par l'ACU et les lecteurs pour générer des nombres aléatoires en utilisant leur algorithme DRNG vérifié et pour stocker la paire de clés asymétrique avec laquelle la clé de session est générée dans le processus d'authentification.

Le MIFARE SAM AV3 est certifié Critères Communs EAL 6+.

Les lecteurs sont également équipés d'un module d'accès sécurisé, avec les caractéristiques suivantes : SAM AV3 certifié EAL +6. Ce module est utilisé pour générer des nombres aléatoires qui sont ensuite utilisés pour établir des canaux de communication sécurisés et pour stocker les clés asymétriques utilisées pour l'authentification. Le module d'accès sécurisé est également utilisé pour la génération de clé de session.

3.3 Description des dépendances

En termes de dépendances, le produit ne nécessite que l'élément suivant :

- **Microsoft SQL Serveur** : une version SQLServer Express 2019 est fournie avec le module d'installation du logiciel DASSnet, une version non « Express » peut être utilisée.

  Quel que soit la version installée, les modalités d'installation indiquées, en termes de sécurité, dans le guide d'installation doivent être respectées.

Pour le reste, le système est entièrement fonctionnel par lui-même et ne nécessite la présence d'aucun autre matériel ou microprogramme dans le système afin de développer correctement ses fonctionnalités.

3.4 Environnement opérationnel technique

Le logiciel de gestion DASSnet peut être installé sur n'importe quel ordinateur personnel exécutant Windows 10 ou version ultérieure et Windows Server 2016 ou version ultérieure. Les autres systèmes d'exploitation ne sont pas recommandés. Cela s'applique à la fois au logiciel serveur et au logiciel client. Pour l'évaluation, Windows 11 sera considéré.

Une base de données SQL doit être installée conformément aux indications décrites dans *3.2.1 DASSnet* et **[TOE-INSTALL]**.

D'autre part, les dispositifs ASDx et EVOpass sont des matériels autonomes qui sont conçus pour fonctionner ensemble lorsqu'ils sont connectés aux autres éléments de la TOE avec la seule exigence d'une alimentation électrique. Les SAM doivent être installés dans l'ASDx et les lecteurs eux sont équipés d'un modèle de type IC.

Des lecteurs avec clavier PIN (EVOpass20K, EVOpass40K) doivent être placés dans les entrées où un utilisateur valide peut être contraint à autoriser l'accès à des acteurs malveillants. C'est-à-dire, dans chaque environnement dans lequel ***T. COERCION*** est possible.

Dans ces conditions, la configuration minimale consisterait en un dispositif EVOpass pour lire les cartes d'utilisateur, une carte d'utilisateur, un ASDx de n'importe quel type de ceux englobés dans le cadre de l'évaluation et d'un PC exécutant la configuration complète du

logiciel de gestion DASSnet. Cette configuration se compose du module serveur susmentionné, d'une base de données SQL et d'au moins un module client DASSnet.

3.5 Périmètre de l'évaluation

Le périmètre de l'évaluation comprend tous les éléments qui participent à l'authentification des utilisateurs grâce à l'utilisation du système de contrôle d'accès physique Dorlet à l'exception de :

- Les puces MIFARE DESFire EV2 utilisées comme cartes d'authentification des utilisateurs ;
- Les différents SAM AV3 (TM, CM) placés dans l'ACU et celui du lecteur (LT) qui sont certifiés EAL 6+ ;
- Le protocole DESFire utilisé pour les communications entre la carte utilisateur et le SAM ;
- L'administration de la solution (administration locale depuis le serveur DASSnet ou administration à distance depuis un client DASSnet).

Ainsi, les éléments qui sont à l'intérieur de la portée de l'évaluation sont répertoriés dans la *figure 9* et constituent la version 1.2 de la solution Dorlet Physical Access Control System.

Reference	Element description	Localisation
ASDx	ASD/4 unit, version 1.58 anssi v1.03	Zone protégée
DASSnet	Dorlet Advanced Security Software for .NET, version 2.7.200	Zone protégée
EVOpass20	EVOpass20 and EVOpass20K readers, version v11.21.00 anssi v1.00	Zone publique
EVOpass40	EVOpass40 and EVOpass40K readers, version v11.21.00 anssi v1.00	Zone publique
Transparent module	v7.21.00 anssi v1.00(mt)	Zone protégée (dans les ASDx)
Communications module	v7.21.00 anssi v1.00(mc)	Zone protégée (dans les ASDx)

Figure 9. Éléments de la portée de l'évaluation

Le tableau suivant reprend la configuration évaluée conformément à [ANSSI-NOTE07] :

Composants du système		Inclus dans la TOE	Non évalué (environnement de la TOE)	
			Supposé de confiance	Est un attaquant potentiel
GAC (Dassnet)	Système d'exploitation		Windows 11	
	Applicatifs	DASSnet 2.7.200		
	Fonctions cryptographiques	WolfSSL 5.2.0		
	Bases de données et annuaires		SQL server express 2019	
UTL	Matériel	ASD/4 unit		
	Système d'exploitation	Sans OS		
	Applicatifs	version ASDx v1.58 anssi v1.03		
	Fonctions cryptographiques	WolfSSL 5.2.0		
	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	

Figure 10. Configuration d'évaluation du produit

La figure suivante illustre la plateforme d'évaluation.

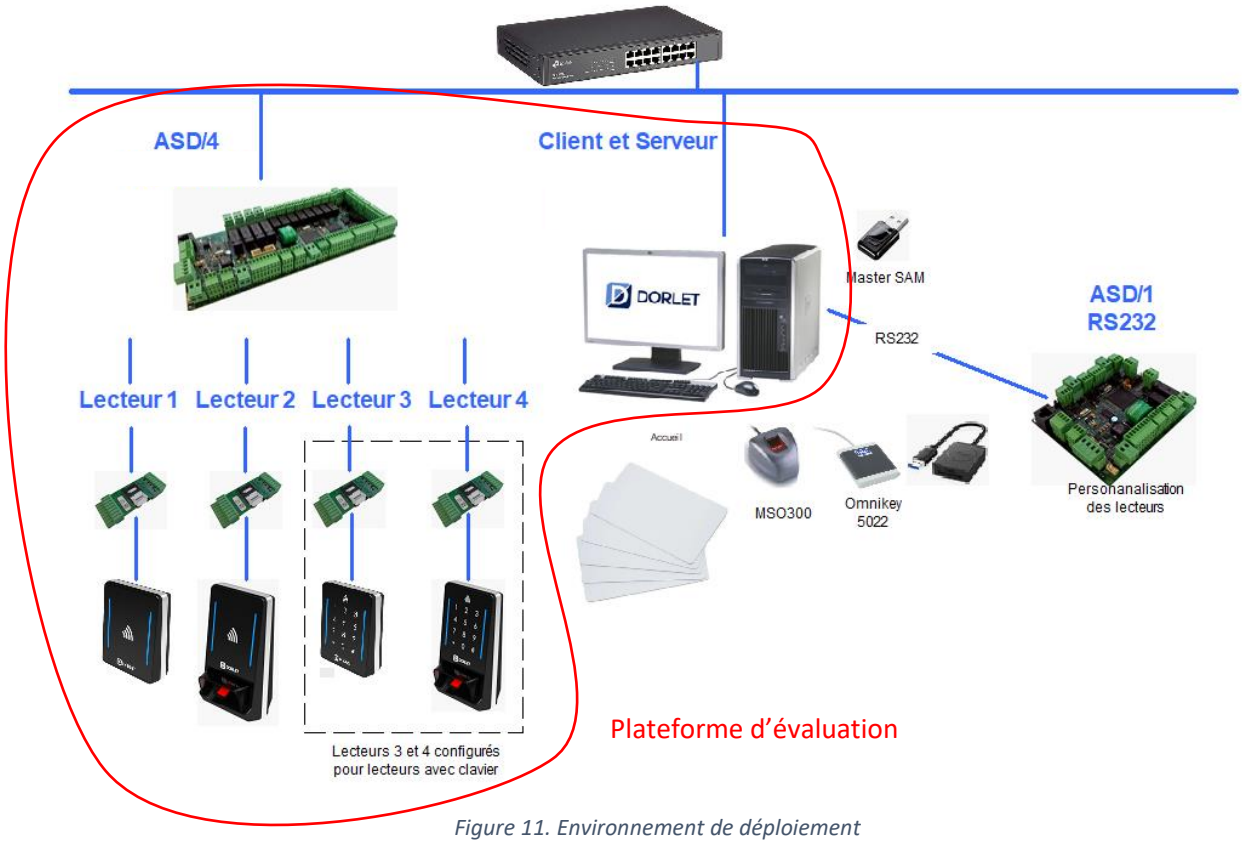

Figure 11. Environnement de déploiement

Les systèmes d'exploitation et autres logiciels nécessaires au fonctionnement de la TOE font partie de l'environnement opérationnel et ne relèvent pas de la portée de la TOE.

L'ajout d'autres éléments à la configuration de base n'entraînerait qu'une configuration plus complexe mais le fonctionnement serait le même.

En matière de documentation, **[TOE-INSTALL]** et **[TOE-MAN]** sont fournis, contenant des informations pour les fonctions de sécurité concernant l'utilisateur, les instructions d'installation et la configuration et l'administration sécurisées du produit.

4 Définition du problème de sécurité

4.1 Utilisateurs

Plusieurs utilisateurs interagissent avec la TOE :

- **Administrateur système** en charge de la personnalisation du système à partir du SAM Management Unite (SMU) et de l'administration de la TOE avec le logiciel de gestion

DASSnet (c'est-à-dire gestion des utilisateurs et des cartes, interrogation du système pour diverses informations, etc.).

- **Utilisateurs finaux** qui utilisent la TOE pour s'authentifier auprès du système.

4.2 Données sensibles

Cette section décrit les données sensibles à protéger par la TOE.

Identifier	Description
A. AUTHENTICATION_FACTOR	Informations utilisées pour authentifier l'utilisateur par la solution (PIN, empreinte digitale et cartes). Besoin de sécurité : confidentialité
A. ACU_DASSNET_COM	Informations sensibles transmises dans les communications ACU-DASSnet et DASSnet-ACU. Ces communications comprennent un large éventail d'informations. De l'ACU, le DASSnet recevra des informations sur l'état de l'unité, les tentatives d'identification qu'il reçoit, etc. Inversement, le DASSnet envoie des informations à l'ACU pour mettre à jour les informations d'identification qu'il stocke, soit lors de la création, de la suppression ou des mises à jour. Besoin de sécurité : confidentialité, intégrité, disponibilité et authenticité
A. ACU_DATA	Toutes les informations stockées dans l'unité de contrôle d'accès (hors SAM), telles que : - Etat de l'ACU - Etat du lecteur - Les cartes - Données de configuration - PIN codes associés aux utilisateurs du système. Besoin de sécurité : confidentialité, intégrité et disponibilité
A. ACU_READER_COM	Cet actif représente le canal de communication établi entre l'unité de contrôle d'accès et le lecteur. Ce canal de communication contient des informations telles que les demandes d'authentification et leurs réponses respectives.

Identifier	Description
	Besoin de sécurité : confidentialité, intégrité, disponibilité et authenticité
A. DASSNET_DATA	Toutes les informations stockées sur le serveur DASSnet. Cela inclut toutes les données de gestion et les clés utilisées pour établir des canaux de communication sécurisés avec l'ACU, comme décrit dans **[DORLET-CRYPTO].** Les clés AES dérivées des processus d'authentification avec l'ACU sont également stockées dans le DASSnet et considérées comme faisant partie de cet actif. Cet actif comprend également les données stockées et partagées avec les clients DASSnet. Besoin de sécurité : confidentialité, intégrité et disponibilité
A. READER_DATA	Comme les lecteurs sont exposés à des utilisateurs malveillants, toutes les informations stockées dans le lecteur sont considérées comme sensibles. Besoin de sécurité : confidentialité, intégrité et disponibilité
A. MANIPULATED_KEYS	Toutes les clés manipulées par la TOE. Besoin de sécurité : confidentialité et intégrité

Figure 12. Table des biens sensibles

Les informations présentées dans la *Figure 13. Correspondance de sécurité des biens sensibles* résument les relations entre les biens sensibles susmentionnés et leurs exigences de sécurité.

	Confidentialité	Intégrité	Disponiblité	Authenticité
A. AUTHENTICATION_FACTOR	X			
A. ACU_DASSNET_COM	X	X	X	X
A. ACU_DATA	X	X	X	

	Confidentialité	Intégrité	Disponiblité	Authenticité
A. ACU_READER_COM	X	X	X	X
A. DASSNET_DATA	X	X	X	
A. READER_DATA	X	X	X	

Figure 13. Correspondance de sécurité des biens sensibles

4.3 Hypothèses

Cette section établit un ensemble de considérations, concernant l'environnement dans lequel la TOE fonctionnera, qui sont prises pour acquises. Pour l'évaluation, les hypothèses suivantes sont prises en compte sur l'environnement d'exécution.

Identifier	Description
AS. ADMINISTRATOR	Le personnel chargé de gérer chaque partie de la TOE est correctement formé, conscient des exigences de sécurité de son rôle et dépourvu de toute intention malveillante.
AS. USER_CARD	Chaque ICC d'identification que l'on tente de valider par la TOE est un ICC MIFARE DESFire EV2 valide. Chacune de ces cartes est utilisée par son propriétaire légitime et jamais par un tiers. Les informations contenues dans chacune des cartes sont chiffrées, sécurisées et inaccessibles à tout agent autre qu'un lecteur légitime. Les clés stockées dans le SAM du MT sont correctement protégées par cryptage et inaccessibles à un acteur malveillant. Les communications établies entre le SAM du MT et les cartes utilisateurs afin d'authentifier les utilisateurs sont protégées par le protocole DESFire.

Identifier	Description
AS. DASSNET_ENVIRONMENT	Les communications entre le serveur DASSnet et ses clients s'effectuent au sein de l'installation que la TOE vise à protéger et sont hors de portée d'éventuels acteurs malveillants. Les machines utilisées dans la partie DASSnet du système exécutent n'importe quel système d'exploitations qui suit les recommandations faites par le développeur comme indiqué dans la section *3.4 Environnement opérationnel technique.* En termes de dépendances, le produit est entièrement fonctionnel par lui-même et ne nécessite la présence d'aucun autre matériel, logiciel ou microprogramme dans le système afin de développer correctement ses fonctionnalités. Environnement opérationnel technique : avoir DASSnet installé sur un OS à jour, contenir un logiciel correctement mis à jour et ne contenir aucune forme de logiciel malveillant.
AS. PIN_ASSIGNMENT	Lors de l'utilisation du lecteur EVOpass20K, le code PIN est attribué à chaque porteur de badge et est donc sous le contrôle de l'utilisateur final. Il est communiqué au titulaire de la carte par un échange direct et confidentiel.
AS. SECURE_INSTALLATION	Tous les éléments de la TOE qui ne sont pas accessibles au public sont protégés contre tout accès physique non autorisé. C'est-à-dire, chaque partie de la TOE sauf le lecteur. Les unités de contrôle d'accès sont installées dans une pièce sécurisée accessible uniquement au personnel autorisé et formé. En conséquence, toutes les informations qui y sont stockées restent inaccessibles par altération physique de cette partie de la TOE. Les machines serveur et client exécutant le logiciel DASSnet sont installées dans une salle sécurisée accessible uniquement au personnel autorisé.

Identifier	Description
AS. SAM	Les SAM sont des modules certifiés. Les informations contenues dans les SAM sont correctement chiffrées. La procédure de validation des SAM est effectuée en suivant les meilleures pratiques de sécurité ainsi que les manuels de Dorlet.
AS. READER_PROTECTION	Les lecteurs ICC sont installés de manière à ce que chaque accès à l'installation sécurisée soit contrôlé. Il est également supposé que les lecteurs soient installés de manière à ne pas être exposé (câbles et autres pièces matérielles)
AS. ISOLATION	Tous les éléments du système sont connectés entre eux via un réseau TCP/IP sécurisé de type VLAN dédié, la configuration d'accès depuis l'extérieur est restreinte et sécurisée, conformément à [TOE-INSTALL].
AS. SECURE_INTEGRATION	Les intégrations pour la videosurveillance et la détection se font sur des systèmes sûrs ayant leurs librairies à jour et sans vulnérabilités connues, conformément à [TOE-INSTALL]. Pour rappel, elles sont désactivées pour l'évaluation.

Figure 14. Tableau des hypothèses

4.4 Menaces

Cette section décrit tous les facteurs de menace possibles pouvant entraîner le dysfonctionnement de la violation d'un ou plusieurs éléments sensibles de la TOE.

Les attaquants considérés sont les suivants :

- A1. Attaquant sur le réseau de gestion (entre le Dassnet et les ACU) ;
- A2. Attaquant sur le réseau entre l'ACU et le lecteur ;
- A3. Attaquant disposant d'un accès physique au lecteur.

La menace d'un attaquant physique disposant d'un accès physique au Dassnet et ACU est couverte par la protection organisationnelle (en hypothèse) et la protection matérielle (***SF. Fonction anti-effraction***).

Chaque entrée de la *Figure 15. Tableau des menaces* constitue une menace de sécurité possible qui pourrait éventuellement affecter la TOE. La *Figure 16. La correspondance actif-menace* contient un résumé de la relation entre chaque menace et les actifs qu'elle pourrait

potentiellement compromettre. Chacune de ces menaces est atténuée soit par une fonction de sécurité, soit par une hypothèse sur l'environnement opérationnel.

Identifiant	Menace
T. ACU_DASSNET_MITM	Un attaquant (A1) pourrait tenter de se positionner au milieu de la communication entre le serveur DASSnet et l'unité de contrôle d'accès et tenter d'accéder et/ou de modifier la communication capturée (***A. ACU_DASSNET_COM***).
T. ACU_READER_MITM	Un attaquant (A2) pourrait tenter de se positionner au milieu de la communication entre le lecteur EVOpass et l'unité de contrôle d'accès et tenter d'accéder et/ou de modifier la communication capturée (***A. ACU_READER_COM***).
T. BRUTE_FORCE	Un attaquant (A3) pourrait utiliser des techniques de force brute sur les mécanismes d'authentification de la TOE afin d'obtenir des informations d'identification valides (***A. AUTHENTICATION_FACTOR***).
T. COERCION	Un attaquant (A3) pourrait tenter d'accéder au système en forçant un utilisateur légitime par la coercition à utiliser son code PIN, exposant ainsi ces informations d'identification et accordant l'accès à un acteur illégitime(***A. AUTHENTICATION_FACTOR***).
T. DATA_EXTRACTION	Un attaquant (A3) pourrait tenter d'extraire les données stockées dans les différentes parties de la TOE accessibles publiquement (***A. READER_DATA***).
T. DENIAL_OF_SERVICE	Un acteur malveillant (A1, A2) pourrait tenter d'interrompre le flux de communication habituel entre les différentes parties de la TOE interrompant ainsi le bon fonctionnement du système.
T. READER_SAM_MITM	Un attaquant (A3) pourrait tenter de se positionner au milieu de la communication entre le lecteur EVOpass et le SAM qui y est installé et tenter d'accéder et/ou de modifier la communication capturée.
T. READER_TAMPERING	Un attaquant (A3) pourrait tenter de modifier le comportement normal du lecteur ICC pour compromettre le

Identifiant	Menace
	système par la divulgation ou la modification d'informations gérées par le lecteur.
T. REPLAY	Un attaquant (A2) pourrait s'emparer d'informations issues du processus de communication entre les cartes d'identification et les lecteurs et tenter de les reproduire.

Figure 15. Tableau des menaces

	A. AUTHENTICATION_FACTOR	A. ACU_DASSNET_COM	A. ACU_DATA	A. ACU_READER_COM	A. DASSNET_DATA	A. READER_DATA	A.MANIPULATED_KEYS
T. ACU_DASSNET_MITM		X					
T. ACU_READER_MITM				X			
T. BRUTE_FORCE	X						
T. COERCION	X						
T. DATA_EXTRACTION			X			X	
T. DENIAL OF SERVICE		X		X			
T. READER_SAM_MITM						X	X
T. READER_TAMPERING						X	X
T. REPLAY						X	

Figure 16. Correspondance actif-menace

4.5 Fonctions de sécurité de la TOE

Chacune des sous-sections suivantes définit une fonction de sécurité offerte par la TOE ainsi que la spécification des menaces qu'elle contribue à atténuer. La relation entre les fonctions de sécurité et les menaces qu'elles atténuent est résumée dans la *Figure 17. Justification des menaces et des mesures d'atténuation*.

4.5.1 SF. Protection des communications ACU – DASSnet

Les communications entre le logiciel de gestion DASSnet et l'unité de contrôle d'accès sont protégées par un schéma de cryptage symétrique. L'ACU échange une clé AES-128 avec le logiciel de gestion via des méthodes cryptographiques asymétriques. À la fin de ce processus, toutes les communications ultérieures entre ces deux éléments sont chiffrées. Cela signifie que toutes les données d'authentification, d'utilisateur et de gestion partagées entre l'ACU et le DASSnet dans le cadre du fonctionnement normal de la TOE sont chiffrées.

De plus, l'intégrité des messages échangés entre les différentes parties de la TOE est vérifiée en utilisant le mode Galois/Compteur de l'algorithme AES.

En outre, les connexions sont rejetées en cas d'échec du processus d'échange de clés.

En cas d'indisponibilité du DASSnet, l'ACU est autonome et stocke les journaux pour retransmission au DASSnet au retour de la connexion.

4.5.2 SF. Protection des communications ACU – Lecteur

Les communications entre l'ACU et le lecteur sont chiffrés à tout moment à l'aide d'un chiffrement symétrique. Le TM de l'ACU et le lecteur (LT) échangent une clé 128-AES à l'aide de la cryptographie asymétrique et cette clé est utilisée dans toutes les communications ultérieures pour chiffrer et déchiffrer les échanges. Par conséquent, toutes les informations transmises dans le canal ACU-EVOpass sont protégées.

De plus, l'intégrité des messages échangés entre les différentes parties de la TOE est vérifiée en utilisant le mode Galois/Compteur de l'algorithme AES.

4.5.3 SF. Protection PIN

Les lecteurs EVOpass20K et EVOpass40K ICC se protègent contre les acteurs malveillants qui peuvent effectuer différentes sortes d'attaques sur l'interface du clavier. Ces mesures de sécurité consistent en une protection contre les attaques par force brute et une protection des utilisateurs contraints.

La protection contre la force brute est déclenchée après cinq tentatives d'authentification infructueuses et se bloquera. Après cela, le lecteur est bloqué pendant quelques minutes avant d'accepter d'autres tentatives d'authentification, rendant ainsi impraticables les attaques par force brute réussies.

La protection des utilisateurs contraints fonctionne comme un moyen de protéger le système contre un attaquant qui peut forcer un utilisateur avec des informations d'identification légitimes à lui accorder l'accès. Dans cette situation, un utilisateur peut entrer un code d'intimidation au lieu du code valide afin d'alerter le système de la menace et de déclencher des mesures pour empêcher l'attaque.

4.5.4 SF. Fonction anti-effraction

La TOE assure une protection contre les tentatives d'effraction physique sur certaines de ses parties : Les lecteurs EVOpass. La protection contre la falsification physique fait face à des menaces liées à la manipulation directe du lecteur lui-même. Lors de la détection d'une tentative d'effraction, le système est alerté et des mesures d'arrêt peuvent être appliquées en conséquence. Une tentative de déplacer le lecteur EVOpass de sa position d'installation d'origine déclenche une alarme du système et révélerait la présence d'un attaquant.

En plus des mesures organisationnelles pour protéger les unités ASDx, ces boîtiers déclenchent une alarme à l'échelle du système lors de la détection de la tentative de sabotage.

4.5.5 SF. Fonction anti-retour

La TOE enregistre les informations recueillies par chaque lecteur afin de contrôler l'utilisation des cartes dans l'établissement. Par conséquent, lorsqu'un utilisateur se voit accorder l'accès, sa carte reste dans l'impossibilité d'accéder une deuxième fois jusqu'à ce qu'un événement de sortie soit enregistré.

De cette manière, l'antipassback interdit à un agent malveillant de reproduire l'entrée donnée lors d'un processus d'authentification valide pour se voir accorder l'accès. Cette fonctionnalité est hautement configurable et peut être définie pour des lecteurs et des cartes particulières.

5 Justification

Dans cette partie, les menaces affectant la TOE sont brièvement décrites ainsi que les protections mises en place pour les contrer.

Un schéma des menaces et leurs atténuations correspondantes est présenté à la *Figure 17. Justification des menaces et des atténuations.*

Menace	Atténuations
T. ACU_DASSNET_MITM	Cette menace affecte les communications entre l'unité de contrôle d'accès et le DASSnet (A. ACU_DASSNET_COM). Pour atténuer cette menace, la TOE présente ***SF. Protection des communications ACU-DASSnet*** qui consiste à établir un canal sécurisé pour protéger toutes les communications.
T. ACU_READER_MITM	Cette menace consiste en l'interception ou la manipulation des communications entre l'unité de contrôle d'accès et le lecteur (***A. ACU_READER_COM***). Ces communications sont protégées par la TOE à travers ***SF. Protection des communications ACU - lecteur*** qui chiffre toutes les données partagées par ces deux éléments.
T. BRUTE_FORCE	Un attaquant pourrait tenter de s'authentifier avec un ensemble d'informations d'identification valides possibles jusqu'à ce qu'il obtienne l'accès. Pour prévenir ce type d'attaques la TOE présente ***SF. Protection PIN*** qui bloque les mécanismes d'authentification après un nombre de 5 tentatives infructueuses.
T. COERCION	Cette menace consiste à forcer un propriétaire légitime de carte et utilisateur de la TOE à fournir des identifiants valides à un acteur malveillant. La coercition des utilisateurs est empêchée grâce la présentation de la carte plus de 5 secondes sur le lecteur qui déclencheraient des alarmes de coercition dans le système. De même, lors qu'il y a la présence d'un clavier l'utilisateur tapera '#' ou '*'+ le Code PIN (***SF. Protection PIN***).
T. DATA_EXTRACTION	Dans le sens d'un accès direct aux données que la TOE stocke, un attaquant ne peut présenter une menace que sur la possibilité d'accéder physiquement à la TOE et de la falsifier. ***SF. Fonction anti-effraction*** empêche l'accès non autorisé à ces parties de la TOE.
T. DENIAL OF SERVICE	Cette menace consiste à tenter d'entraver les communications entre les différentes parties de la TOE afin d'interrompre son fonctionnement régulier. Cette menace est maîtrisée par ***SF.***

Menace	Atténuations
	Protection des communications ACU-DASSnet et ***SF. Protection des communications ACU-Lecteur***.
T. READER_SAM_MITM	La communication entre le lecteur EVOpass et le SAM qui y est installé est également sujette à des manipulations malveillantes. Étant donné qu'une manipulation physique du lecteur est nécessaire pour accéder aux communications entre le lecteur et le SAM, cette menace est atténuée par ***SF. Fonction anti-effraction*** qui détecterait la tentative d'effraction.
T. READER_TAMPERING	De par la nature de leur fonction, les lecteurs sont positionnés dans des lieux publics de l'établissement dont ils visent à contrôler l'accès. Par conséquent, les menaces qui affectent cette partie de la TOE sont liées à la falsification physique du lecteur, ce qui pourrait potentiellement conduire à la divulgation de données sensibles. Pour protéger les lecteurs de cette variété d'attaques, ils disposent de protections physiques qui alertent le système en cas de tentative de falsification (***SF. Fonction anti-effraction***).
T. REPLAY	Un vecteur d'attaque qui affecte les lecteurs et ne nécessite pas de manipulation physique est l'attaque par relecture. Ce type d'attaque consiste à répéter une performance d'authentification valide afin d'accorder l'accès à un deuxième acteur malveillant à l'aide des informations d'identification capturées à partir de la première authentification valide. Cette menace est atténuée par la ***SF. Fonction anti-retour***, qui empêche les données de la carte d'être réutilisées une fois qu'un utilisateur en a obtenu l'accès, de même un mécanisme anti-replay qui consiste à incrémenter un compteur et ne permet pas de renvoyer une commande chiffrée qui ne serait pas incrémenté.

Figure 17. Justification des menaces et des mesures d'atténuation

Plus d'informations sur les mécanismes cryptographiques présents dans les canaux de communication de la TOE sont disponibles dans **[DORLET-CRYPTO]**.