Cible de sécurité CSPN

Difenso Core System (DCS)

Titre	: Cible de sécurité CSPN - Difenso Core System
Version	: v2.6 du 19/01/2017
Référence	: DIFENSO-DCS-ST_v2.6.docx

Tableau de suivi des modifications

Date	Version	Evolution
29/11/2015	1.0	Première version
03/06/2016	2.0	Serveur DCS en mode « appliance » avec le HSM TrustWay
02/07/2016	2.1	Modification du document suite aux premiers retours du CESTI Quarkslab
10/10/2016	2.2	Modification du document suite aux retours du CESTI Quarkslab
03/11/2016	2.4	Modification du document pour prise en compte remarques ANSSI CSPN
12/01/2017	2.5	Modification du document pour permettre sa publication
19/01/2017	2.6	Modification du format de la cible sécurité

Table des matières

Table des Figures

Table des Tableaux

1 Identification du Produit

Organisation éditrice	Difenso
Lien vers l'organisation	https://www.difenso.com
Nom commercial du produit	Difenso Core System (DCS)
Numéro de la version évaluée	1.1.0
Catégorie du produit	Identification, authentification et contrôle d'accès Chiffrement

2 Argumentaire du produit

Difenso propose deux types de services :

1. Service de chiffrement de données « à la volée » : Difenso permet de protéger en Confidentialité et Intégrité les données destinées à être stockées ou traitées par un service distant de type « Software as a Service » (SaaS) ;

2. Service de chiffrement de données « à la demande » : Difenso permet de protéger en Confidentialité et Intégrité les données manipulées par des applications internes aux Clients. Cette protection est assurée par la mise à disposition d'un service de protection « à la demande » de type web services.

Les solutions Difenso permettent un accès transparent aux données manipulées vers et en provenance des services distants.

La *Figure 1* ci-dessous présente les composants des solutions Difenso.

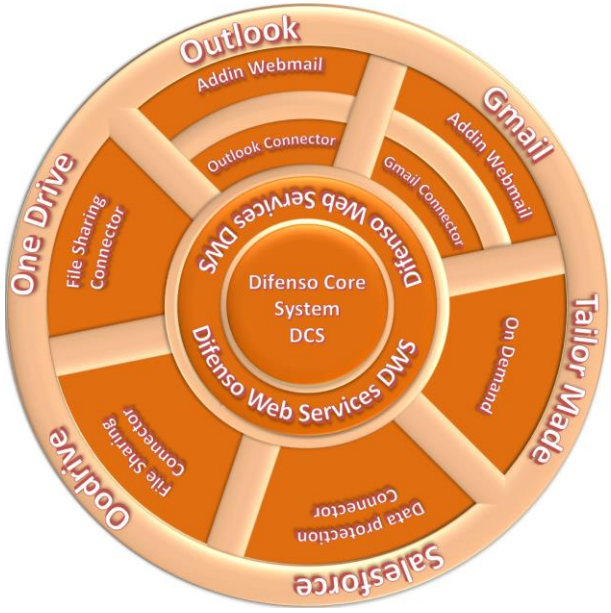

Figure 1 : composants des solutions Difenso

L'architecture logicielle des solutions Difenso est donc composée des éléments suivants :

- **Difenso Core System (DCS)** : cœur cryptographique des solutions Difenso, ce composant est en charge des opérations cryptographiques et se présente sous la forme d'une librairie cryptographique appelée par un composant nommé Difenso Web Services (DWS).
  Le DCS s'appuie sur un Hardware Security Module (HSM) pour toutes les opérations cryptographiques (chiffrement, déchiffrement).
- **Difenso Web Services (DWS)** : seul composant intégrant le DCS. Le DWS est appelé par des connecteurs ou des applications tierces.

- **Connecteurs logiciels et applications tierces** : éléments mis à disposition des utilisateurs, ces connecteurs et applications tierces sont autorisés à envoyer des requêtes au DWS.
  Nota : Dans certains cas, un composant logiciel supplémentaire (add-in) peut être nécessaire. Ces add-ins sont installés sur les postes des utilisateurs et dialoguent avec leurs connecteurs respectifs.

Précision importante : le détail de ces briques techniques des solutions Difenso est présenté afin d'en faciliter la compréhension mais ne vient pas en contradiction à la cible de certification décrite dans le paragraphe « 2.6 Description du périmètre d'évaluation du produit ». L'objectif est de faire certifier progressivement les différentes briques constitutives des solutions Difenso en commençant par l'élément central : le Difenso Core Sytem (DCS).

2.1 Principales opérations réalisées par le produit

Le produit concerné par la cible de sécurité est le Difenso Core System (DCS) qui se présente sous la forme d'une librairie cryptographique qui réalise les principales opérations suivantes : chiffrement et déchiffrement des données qui lui sont transmises par l'appelant.

Les chapitres suivants visent à décrire le fonctionnement des opérations réalisées par le DCS et se limitent au strict périmètre des données reçues par le DCS, de leur traitement et de l'envoi de la réponse au système appelant (DWS).

2.1.1 Chiffrement des données

Le chiffrement des données suit le processus suivant :

1. Envoi par l'appelant des informations nécessaires au chiffrement (données « en clair » ainsi que certaines données techniques) ;
2. Envoi par le DCS auprès du HSM d'une requête pour obtenir une clé cryptographique ;
3. Envoi par le HSM d'une clé cryptographique ;
4. Chiffrement par le DCS des données ;
5. Envoi de la donnée chiffrée par le DCS au HSM pour signature ;
6. Envoi de la signature par le HSM au DCS ;
7. Envoi par le DCS au système appelant (le DWS) des données chiffrées ainsi que de certaines données techniques (dont la signature).

Cette cinématique est résumée dans la *Figure 2*.

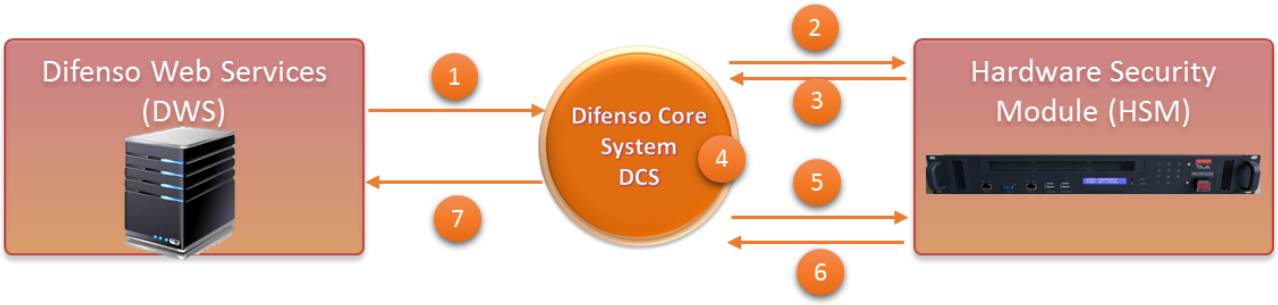

Figure 2 : processus de chiffrement des données

2.1.2 Déchiffrement des données

Le déchiffrement des données suit le processus suivant :

1. Envoi par l'appelant des informations nécessaires au déchiffrement (données chiffrées ainsi que certaines données techniques) ;
2. et 3. Echanges entre le DCS et le HSM des informations nécessaires à la vérification de l'intégrité des données chiffrées ;
4. Vérification par le DCS de l'intégrité des données chiffrées reçues ;
5. Envoi par le DCS auprès du HSM d'une requête pour obtenir la clé de déchiffrement ;
6. Envoi par le HSM de la clé de déchiffrement ;
7. Déchiffrement par le DCS de la donnée chiffrée ;
8. Envoi par le DCS au système appelant de la donnée déchiffrée.

Cette cinématique est résumée dans la Figure 3.

Figure 3 : processus de déchiffrement des données

2.2 Description de l'environnement prévu pour l'utilisation du produit

2.2.1 Ecosystème Difenso

Le Difenso Core System (DCS) s'utilise au sein d'un écosystème complet allant du poste de travail de l'utilisateur jusqu'au lieu de stockage des données. La Figure 4 présente les interactions entre les composants de l'écosystème Difenso et représente les couches applicatives et logicielles de l'écosystème.

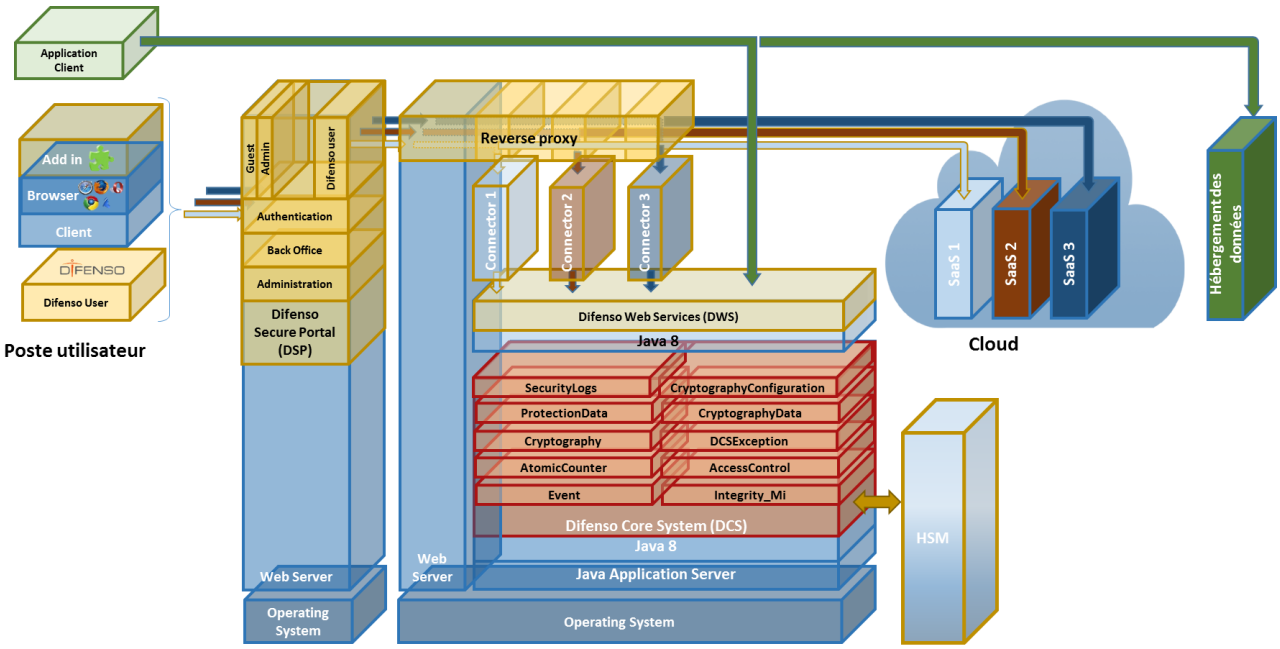

Figure 4 : écosystème Difenso

Selon le périmètre défini au paragraphe « 2.6 Description du périmètre d'évaluation du produit de la cible de sécurité », les composants constitutifs de la cible sont représentés sur la *Figure 5* (seule l'interface avec le HSM est dans le périmètre).

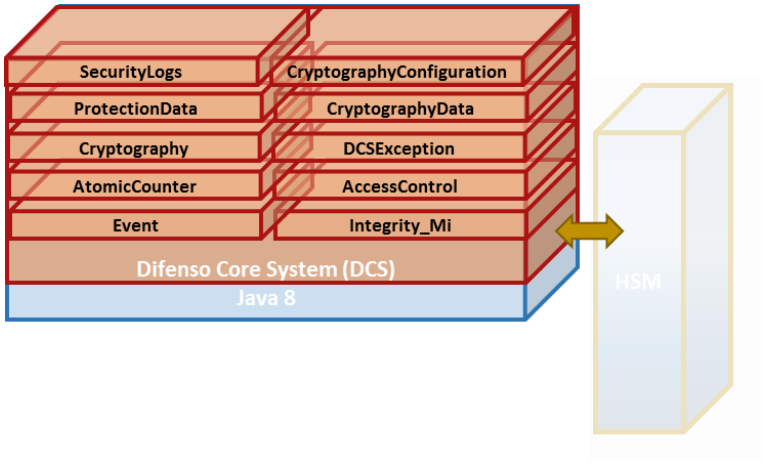

Figure 5 : modules constitutifs du Difenso Core System (DCS)

2.2.2 Difenso Core System (DCS)

Ce composant supporte les services sensibles de sécurisation de l'écosystème Difenso et assure les opérations de chiffrement, de protection et de déchiffrement / vérification d'une donnée. Pour réaliser ces opérations, le DCS s'appuie sur 10 modules présentés en *Figure 6*.

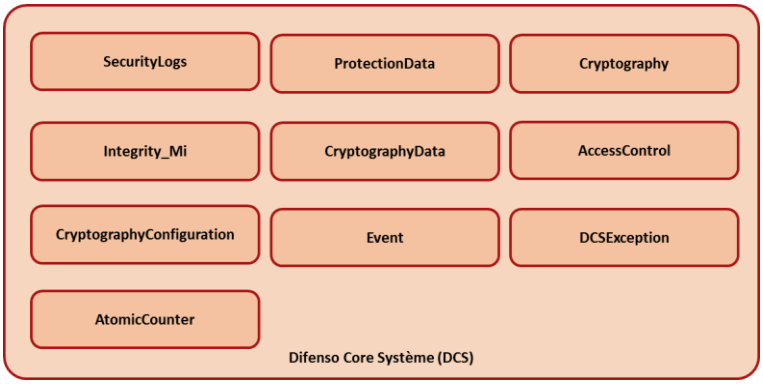

Figure 6 : Difenso Core System

2.2.2.1 Module SecurityLog

Ce module fournit un service transverse au Difenso Core System (DCS) qui a en charge :

- La création des logs dans un format approprié ;
- L'horodatage ;
- La création d'un identifiant de la trace ;
- L'ajout d'une signature de l'ensemble des informations à tracer.

2.2.2.2 Module ProtectionData

Ce module est le point d'entrée du composant Difenso Core System (DCS). Il permet d'orchestrer l'ensemble des actions nécessaires à la protection des données. Il va ainsi s'assurer des opérations cryptographiques à apporter aux données transmises par le DWS (chiffrement, déchiffrement).

Ce module orchestre l'ensemble des actions nécessaires pour :

- Protéger des données ;
- Accéder à des données protégées ;
- Obtenir la signature symétrique d'une donnée chiffrée ;
- Obtenir l'intégrité d'une nouvelle liste d'autorisation d'une donnée protégée ;
- Obtenir une trace opposable ;
- Obtenir la version d'une trace ;
- Vérifier la signature d'une trace ;
- Vérifier l'intégrité de la liste des autorisations d'une donnée protégée.

2.2.2.3 Module Cryptography

Ce module réalise les opérations de chiffrement, déchiffrement des données et de signature symétrique des données qui lui sont présentées :

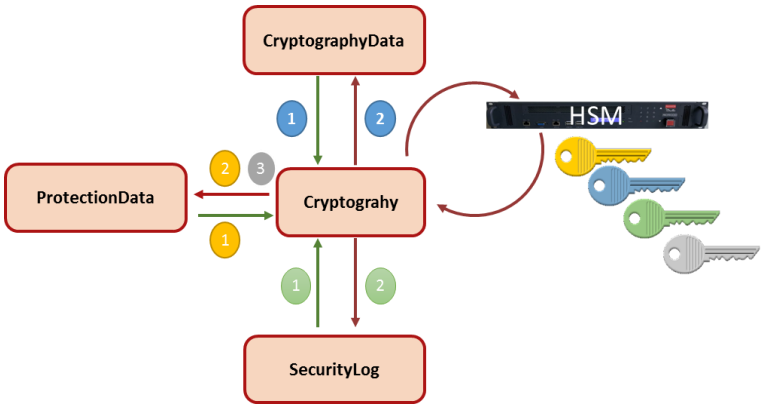

Figure 7 : schéma du module « Cryptography »

Le module Cryptography est appelé par :

- « ProtectionData » ;
- « SecurityLog » ;
- « CryptographyData » .

Pour chiffrer, déchiffrer, signer les données et les traces et garantir l'intégrité des listes d'autorisation.

2.2.2.4 Module AccessControl

Ce module assure la validité de l'intégrité de l'ensemble des éléments associés à la clé, permettant ainsi de garantir que le propriétaire de la donnée, la liste des destinataires, ainsi que tous les éléments techniques nécessaires n'ont pas été altérés.

De plus ce module vérifie qu'un utilisateur est autorisé à accéder à la donnée.

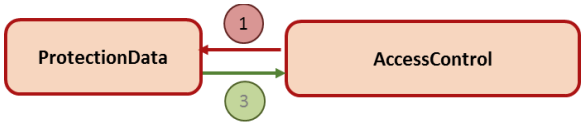

Figure 8 : schéma du module « Access Control »

2.2.2.5 Module AtomicCounter

Ce module permet de mettre à disposition du DCS un compteur qui s'incrémente automatiquement à chaque appel. Ce module est appelé par le module « SecurityLog ».

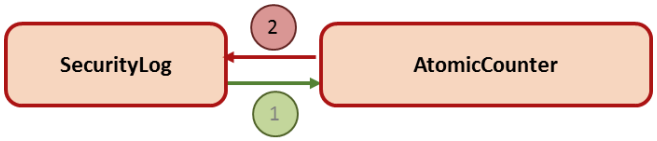

Figure 9 : schéma du module « AtomicCounter »

2.2.2.6 Module Event

Ce module définit les messages qui seront affichés par le module « SecurityLog ». Les événements sont, notamment, relatifs aux accès, aux logs, aux vérifications d'intégrité, à la protection des données.

2.2.2.7 Module CryptographyConfiguration

Ce module permet de transmettre la configuration cryptographique qui sera utilisée par le module « Cryptography ».

2.2.2.8 Module CryptographyData

Ce module permet de fournir une structure fournissant des critères sur les Mac integrity Mi (module integrity).

2.2.2.9 Module DCSException

Ce module est utilisé pour remonter une exception en cas d'erreur ou de problème technique.

2.2.2.10 Module Integrity_Mi

Ce module permet de réaliser une sérialisation en format adapté de différentes informations relatives au Mac integrity Mi (module integrity).

Cette sérialisation est ensuite signée par le module « Cryptography ». Nous obtenons ainsi l'intégrité de la liste des autorisations.

2.3 Description des hypothèses sur l'environnement

- H1 : le composant DCS est déployé sur un serveur physique dédié (HSM) dans une zone de confiance du SI.
- H2 : le serveur DCS est installé suivant les guides d'intégration, de sécurité et d'administration.
- H3 : le serveur DCS exécute les seuls services nécessaires au fonctionnement du composant. Le système d'exploitation et les services sont maintenus à jour.
- H4 : les comptes des utilisateurs de la solution Difenso sont configurés conformément à la politique de sécurité du SI.
- H5 : le HSM est un composant de confiance du SI, il est supposé réaliser les fonctions cryptographiques attendues suivants ses spécifications. Il est administré suivant ses guides de sécurité et d'administration et n'est pas considéré comme un vecteur d'attaque.
- H6 : le composant DCS peut être uniquement sollicité par le DWS.
- H7 : le composant DCS est seulement responsable de la génération des clés de chiffrement de chaque donnée, mais non de leur stockage sécurisé dans la base de données.
- H8 : le composant DCS n'est ni responsable de la génération des clés permanentes du serveur et du HSM, ni de leur stockage sécurisé, ni de leur gestion (révocation, renouvellement).
- H9 : la bibliothèque Java étant directement importée par le DWS et s'exécutant avec les mêmes droits, la sécurité du DCS repose intrinsèquement sur la sécurité du DWS qui a en effet accès au keystore du serveur et à son mot de passe, ainsi qu'à l'interface du HSM et à son mot de passe.

2.4 Description des dépendances

Le serveur DCS nécessite les dépendances suivantes :

- Matérielle :
  - HSM TrustWay Proteccio version OEM d'Atos/Bull, certifié Critères Communs EAL4+ (certificat N° ANSSI-2016/07) ;
- Logicielle :
  - Système appelant le DCS (DWS) ;
  - Base de données MariaDB.

2.5 Description des utilisateurs et rôles typiques

Il y a deux types d'acteurs impliqués dans l'utilisation du produit :

- U1 : les programmeurs chargés de l'intégration du DCS au sein du serveur DCS. Ces acteurs ne sont pas considérés comme malveillants ;
- U2 : le composant appelant autrement dit le DWS.

2.6 Description du périmètre d'évaluation du produit

Les éléments suivants sont considérés dans le périmètre d'évaluation du composant DCS :

- Le composant DCS en charge du contrôle d'accès et de la cryptographie avec les composants :
  - « Cryptography » : réalise les opérations de chiffrement, déchiffrement des données et de signature symétrique des données qui lui sont présentées ;
  - « AccessControl » : assure la validité l'intégrité de l'ensemble des éléments associés à la clé ;
  - « ProtectionData » : coordonne les fonctions de protection des données ;
  - « SecurityLogs » : en charge de la traçabilité des opérations réalisées avec signature des enregistrements ;
  - « AtomicCounter » : permet de mettre à disposition du DCS un compteur qui s'incrémente automatiquement à chaque appel ;
  - « DCSException » : remonte une exception en cas d'erreur ou de problème technique ;
  - « CryptographyData » : fournit les éléments nécessaires au opérations cryptographiques (random_Mi, initial_Value_Mi, ident_Mi, ciphered_Mi, integrity_Mi) ;
  - « CryptographyConfiguration » : transmet la configuration cryptographique qui sera utilisée par le module « Cryptography » ;
  - « Event » : définit les messages qui seront affichés par le module « SecurityLog » ;
  - « Integrity_Mi » : réalise les sérialisations en JSON.
- Interface avec le HSM.

Tandis que les éléments suivants sont hors périmètre :

- La base de données ;
- Le Difenso Web Services (DWS)

3 Description de l'environnement technique de fonctionnement

3.1 Matériel compatible ou dédié

Le composant DCS est déployé sur l'Appliance HSM TrustWay Proteccio (version OEM) d'Atos/Bull.

3.2 Système d'exploitation retenu

Le composant DCS est exécuté sur un système d'exploitation Linux (Debian 7) avec notamment un environnement d'exécution Java 1.8 (JRE), un serveur d'application web Play Framework et une interface avec le HSM.

4 Description des biens sensibles que le produit doit protéger

Les biens sensibles à protéger par le composant DCS sont :

- B1 : Données sensibles du client transmises et reçues des services distants ;
- B2 : Journal d'évènements des opérations réalisées par le DCS.

Les biens sensibles suivants ne relèvent pas de la responsabilité de la cible à elle seule, le composant DCS. Tout au plus il faut veiller à ce que la cible ne mette pas en danger ces biens dans leur utilisation, mais elle ne peut en garantir à elle seule la protection au sein de la solution Difenso :

- B3 : Les clés de 256 bits générées dans le HSM et utilisées par le DCS ;
- B4 : Les clés de 256 bits générées et utilisées par le DCS ;

Les biens sensibles suivants sont considérés comme hors périmètre :

- B5 : Les informations d'authentification des utilisateurs aux services distants ;
- B6 : Les identifiants au service Difenso sont à protéger par la solution Difenso.

5 Description des menaces

Les modèles d'attaques pris en compte pour la conception du Difenso Core System (DCS) partent du principe qu'il faut protéger la confidentialité et l'intégrité des données stockées sur le SaaS.

De plus, nous émettons l'hypothèse qu'un utilisateur ayant été authentifié par le SaaS est un utilisateur légitime.

Dans la description des attaques, des vecteurs et des menaces, nous appelons « base de données principale » la base de données contenant les enregistrements identi_Mi, random_Mi, initial_Value_Mi, ident_Prop, list_Ident_Dest_Mi, integrity_Mi.

Le modèle de sécurité du DCS a été établi à partir des vecteurs d'attaques suivants :

- Attaquant ayant des droits légitimes Difenso, et les utilisant pour se connecter au service
- Attaquant ayant un accès légitime au SaaS, mais non utilisateur Difenso
- Attaquant ayant des droits administrateurs sur le SaaS, pouvant observer les chiffrés et ayant la possibilité de les modifier
- Attaquant réussissant une intrusion sur le système Difenso (hors DCS) afin de récupérer la base de données principale
- Attaquant réussissant une intrusion sur le système Difenso (hors DCS), et modifiant la base de données principale
- Attaquant interceptant le flux de données entre Difenso et le SaaS
- Attaquant ayant récupéré tous les chiffrés de tous les SaaS
- Attaquant « in-the-middle » modifiant les chiffrés à la volée dans un flux de communication entre Difenso et le SaaS

Le modèle de sécurité du composant Difenso Core System (DCS) a été établi à partir des menaces suivantes :

- **M1 : Un attaquant récupère sur le système Difenso la base de données principale hors DCS contenant les informations sur les données afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur Difenso.**

  Cet utilisateur n'a besoin d'un accès qu'en lecture seule sur la base de données. Il ne doit pouvoir obtenir comme information que la liste des personnes autorisées.

- **M2 : Un attaquant capturant en dehors du DCS des données chiffrées afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur.**

  Cet attaquant ne doit pas pouvoir obtenir d'information sur le contenu des données. Même s'il capture toutes les données chiffrées émises.

- **M3 : Un attaquant effectuant une escalade de privilège sur le système Difenso afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur.**

  Cet attaquant aurait accès aux interfaces du serveur DCS et à la base de données principale hors du périmètre de la cible de certification du DCS. Cependant, nous avons conçu le système pour que sans donnée chiffrée, il ne puisse rien obtenir d'autre que des listes expéditeurs/destinataires. Par exemple il ne doit pas être capable d'obtenir des contenus de données.

- **M4 : Un attaquant tentant de récupérer les clés stockées sur le serveur DCS en observant les flux d'entrée/sortie du DCS.**

  Nul ne doit être capable d'obtenir les clés principales stockées dans le DCS (HSM ou SERVER) en observant le DCS en boite noire, ou en interagissant avec les interfaces de celui-ci.

- **M5 : Un attaquant ayant la main sur la base de données principale souhaite générer ou modifier une ligne de cette base donnant un MAC integrity_Mi valide.**

  Nul ne doit être capable de générer ou modifier une ligne de cette base donnant un MAC integrity_Mi valide, sans les clés du DCS.

- **M6 : le journal d'évènements est accessible à un attaquant souhaitant l'altérer.**

  On supposera que cet accès ne donne pas d'autres droits sur le serveur DCS. Par exemple l'attaquant s'en prend à un journal une fois celui-ci extrait et stocké hors du DCS.

- **M7 : l'attaquant, en mesure de solliciter le composant DCS, via une API fonctionnellement équivalente au DWS, souhaite altérer le journal d'évènements.**

- **M8 : Un attaquant effectuant une cryptanalyse des primitives cryptographiques**.

  Nous utilisons des primitives et des gestions de clés préconisées par les documents de l'ANSSI.

- **M9 : Un attaquant ayant effectué une escalade de privilège sur le serveur DCS, ayant de plus accès aux interfaces du DCS et possédant en outre une ou des données chiffrées.**

  Cet attaquant pourra déchiffrer ce(s) donnée(s).

Les menaces ci-dessous ne sont pas prises en compte dans la cible de sécurité. Soit elles sont considérées comme trop difficiles à mettre en œuvre soit hors du périmètre de la cible sécurité. Cependant, elles sont discutées dans le document décrivant les spécifications cryptographiques :

- **M10 : Un utilisateur utilise ses droits légitimes Difenso afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur.**

  Cet utilisateur ne doit avoir la capacité que d'accéder en lecture et écriture à ses données, et n'obtenir aucune information sur le contenu des données des autres utilisateurs. Même dans le cas où il posséderait le chiffré de données destinés à un autre utilisateur.

- **M11 : Un utilisateur du SaaS utilise son accès au Saas afin de compromettre la confidentialité ou l'intégrité des données d'un utilisateur Difenso.**

  Cet utilisateur n'ayant pas de droits d'utiliser le service Difenso ne devrait pas avoir le droit d'accéder ou modifier des données (clairs ou chiffrés) qui ne lui sont pas destinés.

- **M12 : Un attaquant modifiant les requêtes envoyées au DCS par le SaaS ou par l'utilisateur, afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur.**

  Cet attaquant ne doit pas pouvoir obtenir des informations sur les données chiffrées qui ne lui sont pas destinés.

- **M13 : Un attaquant maîtrisant le SaaS modifie des fichiers chiffrés Difenso afin de forger un chiffré valide, ou de modifier un chiffré existant pour en faire un chiffré valide.**

  Nul ne doit être capable de forger un chiffré valide, ni de modifier un chiffré existant pour en faire un chiffré valide différent sans posséder les clés du DCS.

- **M14 : Un attaquant effectuant une escalade de privilègse sur le Difenso Core System DCS.**

- **M15 : Utilisateur usurpant le compte Difenso d'un autre utilisateur**

  L'authentification étant portée par les connecteurs, cette menace est hors du périmètre de la cible.

- **M16 : Un attaquant ayant la main sur le SaaS pourra effacer ou corrompre (pour les rendre illisibles) des données chiffrées par Difenso.**

  Ceci ne fait pas partie de la cible de sécurité. De même qu'un attaquant modifiant les flux entre le SaaS et Difenso pourra effacer ou corrompre (pour les rendre illisibles) ces flux.

6 Description des fonctions de sécurité

6.1 F1 : Protection des données échangées

Le composant DCS est en charge de la protection des données échangées au sein des flux de donnée entre le client et le service distant.

En prétraitement des données en claires avant leur chiffrement, il y a possibilité de supprimer certaines balises HTML ainsi que des caractères d'échappement.

En post traitement des données chiffrées après leur chiffrement, certains indicateurs internes spécifiques sont créés.

Le chiffrement de la donnée est basé sur un algorithme standard : AES 256 en mode CBC, en s'appuyant sur la clé générée et le vecteur d'initialisation aléatoire. Des librairies cryptographiques JAVA certifiées sont utilisées.

Une signature de la donnée chiffrée est générée par le HSM. Différents traitements internes sont effectués sur ces signatures pour des raisons d'administration interne de la solution.

Les API utilisées pour le HSM Bull sont les API PKCS#11 fournies par le constructeur.

Dès la fin des opérations de chiffrement :

- Un « identifiant » de la clé est sauvegardée dans la base protégée ;
- Les données chiffrées sont retransmises directement vers le service cible (poste de travail de l'utilisateur ou service disant).

La fonction de déchiffrement consiste à vérifier le droit d'accès à la clé de déchiffrement, à utiliser cette dernière pour déchiffrer et transmettre l'information non chiffrée.

6.2 F2 : Audit des activités

Les activités du composant DCS sont journalisées et stockée sur le composant DSP. Les journaux de sécurité sont contenus dans un fichier spécifique et sont signés.

Le format d'un évènement contient les éléments nécessaires à sa gestion.

Ce journal d'évènement est accessible seulement au compte applicatif qui a les droits en lecture/écriture ainsi qu'au compte *root*. Le compte administrateur n'a qu'un droit de lecture. L'outil de contrôle d'intégrité (AIDE) vérifié l'intégrité des fichiers de journalisation.

Un ID du serveur est enregistré afin de déterminer de quelle machine proviennent les traces.

6.3 Synthèse des protections contre les menaces identifiées

Le tableau suivant présente une synthèse des mécanismes de protection mis en œuvre par le composant DCS.

Menace	Protection	Fonction de sécurité associée
M1 : Un attaquant récupère sur le système Difenso la base de données principale hors DCS contenant les informations sur les données afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur Difenso.	Cet utilisateur n'a besoin d'un accès qu'en lecture seule sur la base de données. Il ne doit pouvoir obtenir comme information que la liste des personnes autorisées. Les informations contenues dans la base de données ne permettent pas à elles seules d'obtenir le déchiffré d'une donnée chiffrée. De plus, les informations utilisées pour assurer la confidentialité et l'intégrité des données sont protégées par le HSM.	F1
M2 : Un attaquant capturant en dehors du DCS des données chiffrées afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur.	Cet attaquant ne doit pas pouvoir obtenir d'information sur le contenu des données. Même s'il capture toutes les données chiffrées émises. Les algorithmes de chiffrement et de signature utilisés par Difenso sont ceux préconisés par l'ANSSI et le NIST.	F1
M3 : Un attaquant effectuant une escalade de privilège sur le système Difenso afin de compromettre la confidentialité ou l'intégrité des données d'un autre utilisateur.	Cet attaquant aurait accès aux interfaces du serveur DCS et à la base de données principale hors du périmètre de la cible de certification du DCS. Cependant, nous avons conçu le système pour que sans donnée chiffrée, il ne puisse rien obtenir d'autre que des listes expéditeurs/destinataires. Par exemple il ne doit pas être capable d'obtenir des contenus de données.	F1
M4 : Un attaquant tentant de récupérer les clés stockées sur le serveur DCS en observant les flux d'entrée/sortie du DCS.	Nul ne doit être capable d'obtenir les clés principales stockées dans le DCS (HSM ou SERVER) en observant le DCS en boite noire, ou en interagissant avec les interfaces de celui-ci. Les algorithmes de chiffrement et de signature utilisés par Difenso sont ceux préconisés par l'ANSSI et le NIST.	F1
M5 : Un attaquant ayant la main sur la base de données principale souhaite générer ou modifier une ligne de cette base donnant un MAC integrity_Mi valide.	Nul ne doit être capable de générer ou modifier une ligne de cette base donnant un MAC integrity_Mi valide, sans les clés du DCS. Les données stockées en base sont serialisées en JSON et signées par le HSM.	F1

Menace	Protection	Fonction de sécurité associée
M6 : le journal d'évènements est accessible à un attaquant souhaitant l'altérer.	On supposera que cet accès ne donne pas d'autres droits sur le serveur DCS, pour respecter M12. Par exemple l'attaquant s'en prend à un journal une fois celui-ci extrait et stocké hors du DCS. Les traces sont serialisées en JSON, elles contiennent une date, un compteur et sont signées par le HSM. Hors périmètre de la cible, le serveur DCS externalisera de manière périodique la sauvegarde des traces sur un serveur distant.	F2
M7 : l'attaquant, en mesure de solliciter le composant DCS, via une API fonctionnellement équivalente au DWS, souhaite altérer le journal d'évènements.	Seul le DCS a accès au journal d'évènements, chaque nouvel évènement contient un ID unique et la date de création et le tout signé par le HSM. Hors périmètre de la cible, le serveur DCS externalisera de manière périodique la sauvegarde des traces sur un serveur distant.	F2
M8 : Un attaquant effectuant une cryptanalyse des primitives cryptographiques.	Nous utilisons des primitives et des gestions de clés préconisées par les documents de l'ANSSI.	F1
M9 : Un attaquant ayant effectué une escalade de privilège sur le serveur DCS, ayant de plus accès aux interfaces du DCS et possédant en outre une ou des données chiffrées.	Cet attaquant pourra déchiffrer ce(s) donnée(s).	F1 et F2

Tableau 1 - synthèse des protections contre les menaces

7 Glossaire et acronymes

Terme	Définition
« Software as a Service » (SaaS)	« Software as a Service » (SaaS) est un modèle d'exploitation des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur.
Protocole TLS	Transport Layer Security (TLS) est un protocole de sécurisation des échanges sur Internet
HSM	Un Hardware Security Module HSM (Module Matériel de Sécurité) est un matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques.
Nombre pseudo aléatoire	Un générateur de nombres pseudo-aléatoires, pseudorandom number generator (PRNG) en anglais, est un algorithme qui génère une séquence de nombres présentant certaines propriétés du hasard. Les nombres sont supposés être suffisamment indépendants les uns des autres.
Vecteur d'initialisation	Un vecteur d'initialisation (en anglais initialization vector ou IV) est un bloc de bits combiné avec le premier bloc de données lors d'une opération de chiffrement.
MAC	Un code d'authentification de message (MAC, Message Authentication Code) est un code accompagnant des données dans le but d'assurer l'intégrité de ces dernières, en permettant de vérifier qu'elles n'ont subi aucune modification.
Difenso Core System (DCS)	Gestion du contrôle d'accès et de la cryptographie.

FIN DU DOCUMENT