Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CC-2016/62

# Stormshield Data Security - Fonction de chiffrement transparent de fichiers

Version 9.1.2, *Build* 0688

*Paris, le 23 septembre 2016*

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

# Avertissement

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

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

Toute correspondance relative à ce rapport doit être adressée au :

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

certification@ssi.gouv.fr

*Référence du rapport de certification*

# ANSSI-CC-2016/62

*Nom du produit*

## Stormshield Data Security - Fonction de chiffrement transparent de fichiers

*Référence/version du produit*

## Version 9.1.2, *Build* 0688

*Conformité à un profil de protection*

## Sans Objet

*Critères d'évaluation et version*

## Critères Communs version 3.1 révision 4

*Niveau d'évaluation*

## EAL3 augmenté

**ALC_FLR.3, AVA_VAN.3**

*Développeur(s)*

**STORMSHIELD**

**1, place Verrazzano, 69009 Lyon, France**

*Commanditaire*

**STORMSHIELD**

**10, rue Marceau, 92130 Issy-Les-Moulineaux, France**

*Centre d'évaluation*

**OPPIDA**

**4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**

*Accords de reconnaissance applicables*

**CCRA**

**Le produit est reconnu au niveau EAL2 et ALC_FLR.3.**

**SOG-IS**

**Le produit est reconnu au niveau EAL3 et ALC_FLR.3.**

# Préface

## La certification

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

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

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

# Table des matières

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est « Stormshield Data Security – Fonction de chiffrement transparent de fichiers », version 9.1.2, *build* 0688 développé par *STORMSHIELD*.

*Stormshield Data Security* (en abrégé SDS) est une solution de sécurité pour poste de travail sous Windows qui préserve la confidentialité de données, stockées ou échangées par voie de messagerie.

## 1.2. Description du produit

### *1.2.1. Introduction*

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

### *1.2.2. Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable en faisant un clic-droit sur l'icône SDS dans la barre de tâches :

- version 9.1.2 ;
- *build* 0688.

Ces informations apparaissent comme le montre l'écran ci-dessous, à la ligne « **Stormshield Data Security Suite 9.1.20688 ».**

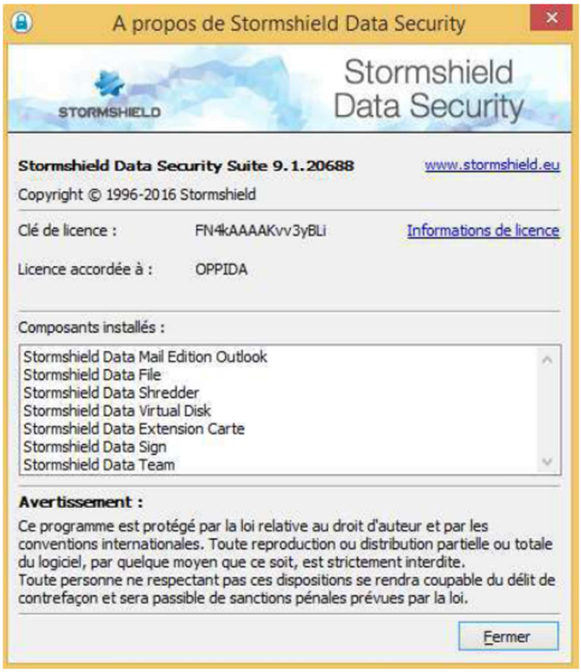


Figure 1 : Version du produit

### *1.2.3. Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- l'authentification des utilisateurs ;
- la protection en intégrité et en confidentialité de fichiers ;
- la protection des règles de sécurité partagées ;
- la vérification du statut des certificats électroniques ;
- la protection des comptes utilisateurs ;
- la protection en confidentialité du fichier d'échange du système (*swap*) ;
- la protection en confidentialité de disques virtuels ;
- la génération de journaux d'évènements ;
- l'administration de fonctions de sécurité ;
- la vérification de l'intégrité et de l'authenticité de la politique téléchargée ;
- le cloisonnement de sessions *Stormshield Data Security* ;
- la sauvegarde et la restauration de fichiers.

### *1.2.4. Architecture*

SDS réalise le chiffrement transparent de fichiers en s'intégrant au noyau Windows et en s'insérant dans l'architecture des systèmes de fichier (*FileSystem*) selon une technique de « filtre » présentée par le schéma suivant :

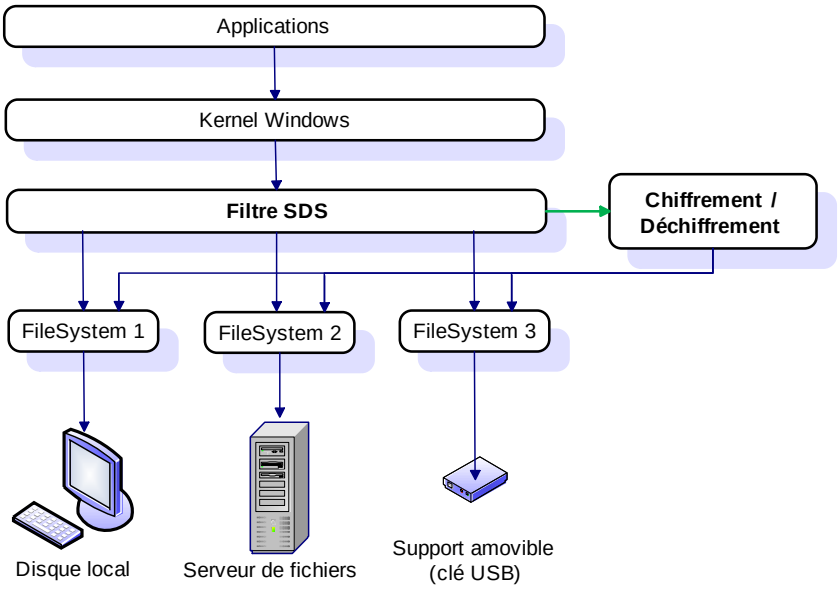


Figure 2 : Fonctionnement de Stormshield Data Security

Le périmètre logique d'évaluation (TOE[1]) est constitué de l'ensemble des composants logiciels suivants :

- le module « SDS Crypto » est une interface cryptographique conforme au standard PKCS#11[2]. Les clés de l'utilisateur peuvent être stockées soit dans une carte à puce, soit sur un dispositif matériel cryptographique ;

[1] *Target Of Evaluation.*
[2] Interface de périphérique cryptographique.

- le « noyau SDS » assure l'authentification de l'utilisateur, surveille l'activité du poste, offre des fonctions de haut niveau d'accès aux clés, contient un annuaire de certificats de confiance, et contrôle la non-révocation des certificats utilisés ;
- le composant « Chiffrement transparent » assure
  - la définition des règles de sécurité (via notamment une extension de l'explorateur) ;
  - et l'application de ces règles ;
- les composants installés au niveau du noyau du système d'exploitation (mode *kernel*) assurent le chiffrement de fichiers et du *swap*.

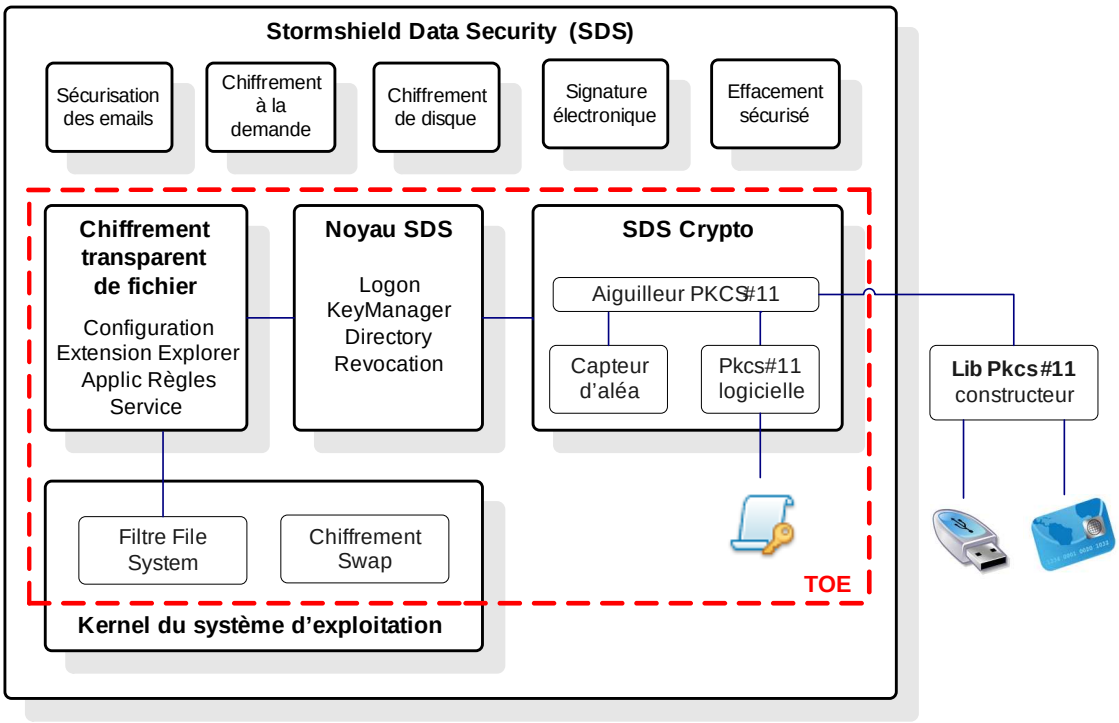


Figure 3 : Périmètre de la TOE

Les éléments suivants sont hors évaluation :

- la librairie PKCS#11 du constructeur du dispositif matériel ;
- le système d'exploitation Microsoft Windows.

### *1.2.5. Cycle de vie*

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés sur le site de *STORMSHIELD* à LYON ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

***STORMSHIELD DATA SECURITY***

1, place Verrazzano
69006 Lyon
France

Pour l'évaluation, l'évaluateur a considéré les rôles suivants définis dans la cible de sécurité :

- l'administrateur de la sécurité (administrateur SDS) définit la politique de sécurité. Si les comptes des utilisateurs sont gérés par *Stormshield Data Security Authority Manager*, l'administrateur de la sécurité crée également les comptes des utilisateurs ;
- l'administrateur système (administrateur *Windows*) se charge de l'installation à partir d'un *master* préparé par l'administrateur de la sécurité. Ce *master* comprend un fichier de configuration globale. Si les clés des utilisateurs sont fournies par une IGC[1] d'entreprise, le *master* comprend également une politique "modèle" utilisée pour la création des comptes directement sur le poste de travail ;
- l'utilisateur conformément à la règle de sécurité fixée par l'administrateur système, est autorisé à accéder à un dossier, voire en modifier ses règles.

### *1.2.6. Configuration évaluée*

Le certificat porte sur l'application est « Stormshield Data Security – Fonction de chiffrement transparent de fichiers », version 9.1.2, *build* 0688 évaluée sur deux systèmes d'exploitation différents à savoir « Windows Seven Ultimate Service Pack1 64 bits » et « Windows 8.1 Enterprise 64 bits ».
Conformément à la cible de sécurité [ST], la plateforme réseau ci-après a été mise en place pour procéder à l'évaluation.

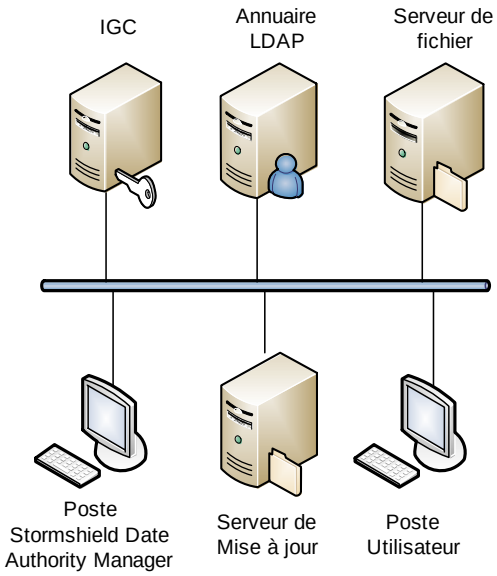


Figure 4 : Plateforme de test pour l'évaluation de la TOE

[1] Infrastructure de Gestion de Clés cryptographiques.

Cette plateforme est constituée des éléments suivants :

- un poste utilisateur sous les systèmes d'exploitation Microsoft suivants : « Windows Seven Ultimate Service Pack 1 64 bits » et « Windows 8.1 Enterprise 64 bits ». Sur ce poste est installé le logiciel « Stormshield Data Security version 9.1 » ;
- un dispositif middleware « OBERTHUR AWP 4.5.1 » ;
- un lecteur de cartes à puce « OMNIKEY CARDMAN 3121 » ;
- des cartes à puce « OBERTHUR Cosmo64 RSA v5.2 » ;
- un poste d'administration sous le système d'exploitation « Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 ». Sur ce poste est installé le logiciel « Stormshield Data Authority Manager version 9.1 » ;
- une IGC, pour la production de clés et de cartes à puce ;
- un serveur de fichier sous le système d'exploitation « Microsoft Windows Server 2008 Enterprise Service Pack 1 ». Ce serveur partage via le protocole CIFS[1], des dossiers hébergés sur une partition NTFS[2] ;
- un annuaire LDAP[3] pour la publication des certificats X.509 des collaborateurs ;
- un serveur pour le déploiement des mises à jour de la politique de sécurité.

[1] *Common Interface File System.*
[2] *New Technology File System.*
[3] *Lightweigth directory Access protocol.*

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

## 2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 septembre 2016, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être suivies :

- l'usage des chiffrements DES 64, 3DES 128, 192, RC2 40, 128, 256, RC4 64, 128, 256, RC5 40, 64, 128, 256 n'est pas recommandé bien que le produit le permette ;
- il en est de même pour le calcul d'empreinte à partir de MD2, MD5, SHA-1 ;
- des modules RSA de taille au moins égale à 2048 bits doivent être utilisés.

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

## 2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires du produit a été évalué. Comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie de son alimentation subit un retraitement de nature cryptographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Stormshield Data Security – Fonction de chiffrement transparent de fichiers », version 9.1.2, *build* 0688 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

## 3.2. 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 d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment pour définir les politiques de sécurité et les paramétrages associés. A noter également qu'il est recommandé de préférer les comptes accessibles depuis un dispositif de sécurité pour pouvoir bénéficier de la sécurité du support physique.

## 3.3. Reconnaissance du certificat

### *3.3.1. Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :


[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

### *3.3.2. Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs.
La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

# Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 3+ | Intitulé du composant |
| **ADV Développement** | ADV_ARC | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Security architecture description |
| | ADV_FSP | **1** | **2** | **3** | **4** | **5** | 5 | **6** | **3** | Functional specification with complete summary |
| | ADV_IMP | | | | **1** | 1 | **2** | 2 | | |
| | ADV_INT | | | | | **2** | **3** | 3 | | |
| | ADV_SPM | | | | | | **1** | 1 | | |
| | ADV_TDS | | **1** | **2** | **3** | **4** | **5** | **6** | **2** | Architectural design |
| **AGD Guides d'utilisation** | AGD_OPE | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Operational user guidance |
| | AGD_PRE | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Preparative procedures |
| **ALC Support au cycle de vie** | ALC_CMC | **1** | **2** | **3** | **4** | 4 | **5** | 5 | **3** | Authorisation controls |
| | ALC_CMS | **1** | **2** | **3** | **4** | **5** | 5 | 5 | **3** | Implementation representation CM coverage |
| | ALC_DEL | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Delivery procedures |
| | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 | **1** | Identification of security measures |
| | ALC_FLR | | | | | | | | **3** | Systematic flaw remediation |
| | ALC_LCD | | | **1** | 1 | 1 | 1 | **2** | **1** | Developer defined life-cycle model |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 | | |
| **ASE Evaluation de la cible de sécurité** | ASE_CCL | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Conformance claims |
| | ASE_ECD | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Extended components definition |
| | ASE_INT | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | ST introduction |
| | ASE_OBJ | **1** | **2** | 2 | 2 | 2 | 2 | 2 | **2** | Security objectives |
| | ASE_REQ | **1** | **2** | 2 | 2 | 2 | 2 | 2 | **2** | Derived security requirements |
| | ASE_SPD | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Security problem definition |
| | ASE_TSS | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | TOE summary specification |
| **ATE Tests** | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 | **2** | Analysis of coverage |
| | ATE_DPT | | | **1** | 1 | **3** | 3 | **4** | **1** | Testing: basic design |
| | ATE_FUN | | **1** | 1 | 1 | 1 | **2** | 2 | **1** | Functional testing |
| | ATE_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** | **2** | Independent testing: sample |
| **AVA Estimation des vulnérabilités** | AVA_VAN | **1** | **2** | 2 | **3** | **4** | **5** | 5 | **3** | Focused vulnerability analysis |

# Annexe 2. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- SDS - NOÉ - Cible de Sécurité, référence NOE/Cible, version 2.3 du 15/09/2016, *STORMSHIELD DATA SECURITY*. |
| [RTE] | Rapport technique d'évaluation, référence OPPIDA/CESTI/NOE/RTE, version 2.0 du 14/09/2016, *OPPIDA*. |
| [ANA-CRY] | Cotation des mécanismes cryptographiques Stormshield Data Security, référence OPPIDA/CESTI/NOE/CRYPTO/1.1, version 1.1 du 26/06/2015, *OPPIDA*. |
| [EXP-CRY] | Expertise de l'implémentation cryptographique, référence OPPIDA/CESTI/NOE/CRYPTO/1.1, version 1.1 du 06/10/2015, *OPPIDA*. |
| [CONF] | Liste de configuration du produit :<br>- DES - Gestion de la configuration, référence DES/ORG/Configuration, version 2.5 du 06/04/2016, *STORMSHIELD DATA SECURITY*. |
| [GUIDES] | Guide d'installation du produit :<br>- GUIDE D'INSTALLATION ET DE MISE EN OEUVRE, STORMSHIELD DATA SECURITY SUITE, référence sds-fr-sds_suite-guide_d_installationv9.1.2, version 9.1.2 d'avril 2016, *STORMSHIELD DATA SECURITY*.<br>Guide d'administration du produit :<br>- STORMSHIELD DATA SECURITY SUITE, référence sds-fr-sds_suite-guide_d_administration-v9.1.2, version 9.1.2 d'avril 2016, *STORMSHIELD DATA SECURITY*.<br>Guide d'utilisation du produit :<br>- STORMSHIELD DATA AUTHORITY MANAGER référence sds-fr-sd_authority_manager- guide_d_utilisation-v9.1.2, version 9.1.2 d'avril 2016, *STORMSHIELD DATA SECURITY* ;<br>- STORMSHIELD DATA TEAM, Chiffrement transparent et partagé, référence sds-fr-sd_team-guide_d_utilisation-v9.1.2, version 9.1.2 d'avril 2016, *STORMSHIELD DATA SECURITY*. |

# Annexe 3. 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. | |
| [CER/P/01] | Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>Part 1: Introduction and general model,<br>septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001;<br>Part 2: Security functional components,<br>septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002;<br>Part 3: Security assurance components,<br>septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,<br>septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004. |
| [CC RA] | Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014. |
| [SOG-IS] | « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee. |
| [REF] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr. |
| | Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr. |
| | Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr. |