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

Bureau Qualification et Agrément

Paris, le 24 NOV. 2017
N° 9926/ANSSI/SDE/PSS/BQA

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

***STORMSHIELD ENDPOINT SECURITY*, version 7.2.06 – *build* 29579**
Fonctionnalité de « chiffrement de données à la volée sur mémoire de masse », dite « chiffrement de surface »
pour poste utilisateur : *WINDOWS XP* pro SP3 32 bits et *WINDOWS SEVEN ENTREPRISE* SP1 64 bits ;
pour poste serveur : *WINDOWS SERVER* 2008 SP2.

STORMSHIELD

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions et limites de la qualification.

Fiche 3 : Base documentaire de la qualification.

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

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [RGS] ;

Vu le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale [LPM] ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1er ;

Vu le décret du 27 mars 2017 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Décide :

Art. 1er – La fonctionnalité « *chiffrement de données à la volée sur mémoire de masse* » du produit ***STORMSHIELD ENDPOINT SECURITY*** en version 7.2.06 *build* 29579 fourni par la société *STORMSHIELD* respecte les règles fixées par les décrets n° 2010-112 du 2 février 2010 [RGS] et n° 2015-350 du 27 mars 2015 [LPM] ainsi que le *processus* de qualification d'un produit [*PROCESS_QUALIF_PROD*], et est qualifiée au niveau standard, sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – La fonctionnalité « chiffrement de données à la volée sur mémoire de masse » du produit *StormShield Endpoint Security* en version 7.2.06 ***build*** 29579 est agréée pour la protection des informations *Diffusion Restreinte* ou classifiées au(x) niveau(x) *Diffusion Restreinte OTAN* ou *Restreint UE/EU Restricted.*

Art. 3 – La fonctionnalité « chiffrement de données à la volée sur mémoire de masse » du produit *StormShield Endpoint Security* version 7.2.06 ***build*** 29579 est conforme au profil de protection PP-CDISK-CCv3.1 version 1.4 d'août 2008 [PP].

Art. 4 – La présente décision est valable pour une durée de 3 ans.

Art. 5 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le chapitre VII du *processus* de qualification d'un produit [*Process_Qualif_Prod*].

Fiche 1

Description du produit

Désignation et versions

Le produit qualifié est la fonctionnalité « chiffrement de données à la volée sur mémoire de masse » de la solution *StormShield Endpoint Security* version 7.2.06 *build* 29579 développée par *StormShield*.

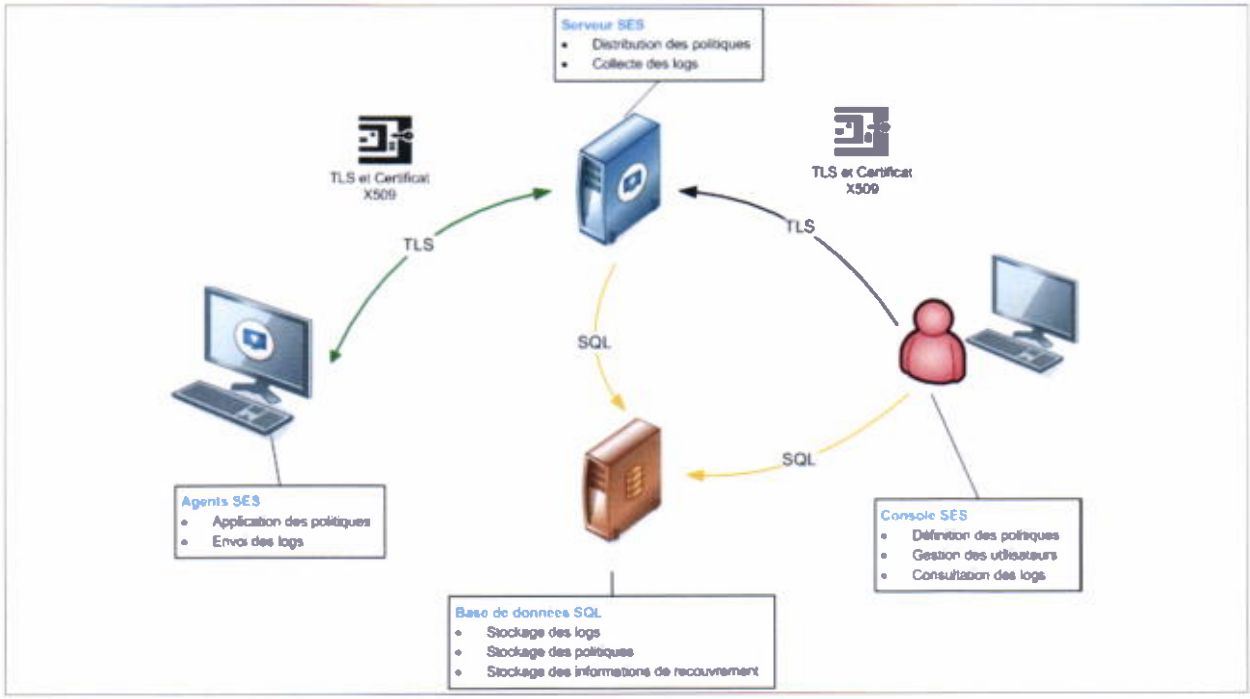

Figure 1. Produit StormShield Endpoint Security, version 7.2.06 build 29579

Présentation générale

La solution *StormShield Endpoint Security* version 7.2.06 *build* 29579 est une solution logicielle de sécurité. Elle permet de protéger les serveurs et postes de travail, et offre, par sa fonctionnalité de chiffrement de données à la volée sur mémoire de masse, les services de sécurité suivants :

- le chiffrement initial ;
- l'authentification unique ;
- le recouvrement ;
- la notion d'invité ;
- l'hibernation.

Elle se compose :

- côté poste client :

- d'un résident *BIOS* qui gère l'authentification de l'utilisateur et le lancement de *WINDOWS* ;
- d'un *driver WINDOWS* qui assure le chiffrement/déchiffrement du disque ;
- de services, communs à tous les modules fonctionnels de *STORMSHIELD*, qui assurent sous *WINDOWS* :
  - l'application de la politique de sécurité et l'enregistrement des journaux ;
  - les communications sécurisées avec le serveur (téléchargement de la politique de sécurité, transmission des journaux) ;
  - toutes les fonctions interactives : changement de mot de passe, consultation locale des journaux, etc. ;

- coté serveur :
  - des modules qui fournissent les clés de chiffrement et les mots de passe de recouvrement, et qui en assurent le stockage sécurisé dans la base de données ;
- du logiciel installé sur un CD de recouvrement.

Fiche 2

Conditions et limites de la qualification

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

C1. Les restrictions d'usage figurant aux chapitres 2.3 et 3.2 du rapport de certification [*CERTIF*] soient bien respectées.

C2. Les guides d'installation, d'administration et utilisateurs [*GUIDES*] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie.

C3. L'utilisateur du produit s'assure du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [CDS].

C4. Les conditions suivantes relatives aux choix et au dimensionnement des mécanismes cryptographiques sont respectées :

- l'algorithme AES avec une taille de clé de 256 bits est recommandé ;
- la taille des modules RSA doit être d'au moins 2048 bits, avec un exposant public strictement supérieur à 65536, pour une utilisation ne dépassant pas 2030 et d'au moins 3072 bits au-delà de 2030.

Limites

L1. Seuls les services décrits dans la fiche 1 sont couverts par la présente décision de qualification.

Fiche 3

Base documentaire de la qualification	

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, version en vigueur. Disponible sur http://www.ssi.gouv.fr/qualification-processus
[RGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Disponible sur http://www.legifrance.gouv.fr.
[LPM]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Disponible sur http://www.legifrance.gouv.fr.

Documents rédigés par le centre d'évaluation

[RTE]	Rapport technique d'évaluation, référence : OPPIDA/CESTI/KIBO/RTE/2.0 en date du : 10/04/2017
[EXP-CRY]	Expertise de l'implémentation des mécanismes cryptographiques, référence : OPPIDA/CESTI/KIBO/CRYPTO/1.0, en date du : 22/03/2017

Référentiels et standards

[PP]	Profil de protection « Application de chiffrement de données à la volée sur mémoire de masse » référence : PP-CDISK-CCv3.1, version 1.4 en date du : août 2008

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification, référence : ANSSI-CC-2017/25 en date du : 07/06/2017

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE]	*STORMSHIELD ENDPOINT SECURITY*, Guide d'administration, référence : ses-fr-guide_d_administration-v7.2, en date du : mars 2017
[CDS]	Cible de sécurité, *STORMSHIELD ENDPOINT SECURITY* – Cible de sécurité EAL3+ - version 1.9a,référence : KIBO/Cible, en date du : 11/07/2017