PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Le Directeur général

Paris, le 25/10/2024
N° 1778/ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU RENFORCE

TRUSTWAY PROTECCIO
VERSION V167/X170

BULL SAS

RCS 642 058 739

Rue Jean Jaurès
78340 Les Clayes-sous-Bois
France

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 ;

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 4 janvier 2023 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. STRUBEL (Vincent) ;

Vu le processus de qualification d'un produit, version en vigueur ;

Vu le rapport de certification, ANSSI-CC-2024/13, 02/07/2024 ;

Vu le dossier de demande de qualification déposé par BULL SAS,

Décide :

Art. 1er – Le produit fourni par la société BULL SAS portant le nom « TRUSTWAY PROTECCIO » en version V167/X170 respecte les règles fixées par le décret n° 2015-350 du 27 mars 2015 et est qualifié au niveau renforcé sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.

Art. 2 – Le produit fourni par la société BULL SAS portant le nom « TRUSTWAY PROTECCIO » en version V167/X170 est agréé pour la protection d'informations marquées Diffusion Restreinte sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.

Art. 3 – Le produit fourni par la société BULL SAS portant le nom « TRUSTWAY PROTECCIO » en version V167/X170 est apte à mettre en œuvre des clés cryptographiques de services de confiance tels que définis à l'article 3 du règlement (UE) n°910/2014, sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.

Art. 4 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

Art. 5 – La présente décision est valable jusqu'au 1er juillet 2025.

4/11/2024 | 18:52 CET

Vincent Strubel

Annexe

Conditions et limites de la qualification.

Références

[1]. Rapport de certification ANSSI-CC-2024/13, 02/07/2024 ;

[2]. TrustWay Proteccio – Security Target LITE, reference PCA4_0152_CIB_Security_target_lite_EN, version 1.2, 31/05/2024.

[3]. Installation_and_user_guide, référence 86 F2 76 FH, version 25.1, Septembre 2023 ;

[4]. Developper's Guide_ATOS, référence : 86 A2 75 FH, version 27, juin 2023 ;

[5]. Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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 objectifs de sécurité sur l'environnement définis dans la cible de sécurité référencée dans [2] doivent être respectés.

C2. Les restrictions d'usage figurant dans le rapport [1] doivent être respectées.

C3. Les recommandations figurant dans les guides du produit référencés dans le rapport [1] doivent être respectées.

C4. Les conditions d'utilisation établies au chapitre 3.2 de [1] doivent être respectées, en particulier :

- le HSM doit être mis en œuvre sur un réseau dédié ;
- les postes depuis lesquels le HSM est administré doivent être dédiés à cet usage ;
- les applications clientes autorisées à communiquer avec le HSM via le réseau doivent être inventoriées préalablement au déploiement du produit ;
- des mesures techniques et organisationnelles doivent être mises en œuvre afin de garantir que seules les personnes autorisées accèdent physiquement au HSM lors de son stockage, de son transport, de son exploitation ou de sa maintenance ;
- le certificat électronique permettant au HSM de s'authentifier auprès des applications clientes via le protocole TLS doit être généré par l'entité ayant fait l'acquisition du produit puis déployé localement sur chaque application cliente ;
- les applications clientes doivent être configurées pour authentifier via le protocole TLS le HSM à l'aide de ce certificat électronique déployé localement et refuser toute communication en cas d'échec de cette authentification ;
- les certificats électroniques permettant aux applications clientes de s'authentifier auprès du HSM via le protocole TLS doivent être générés individuellement pour chaque application cliente ;

- les applications clientes doivent s'authentifier par certificat électronique auprès du HSM via le protocole TLS à l'aide du certificat électronique déployé localement ;
- les fonctions et attributs PKCS#11 associés à chaque clé cryptographique mise en œuvre par le HSM doivent impérativement être identifiées par l'entité ayant fait l'acquisition du produit en s'appuyant sur le manuel développeur [4] ;
- seuls les fonctions et attributs PKCS#11 associés à chaque clé cryptographique mise en œuvre par le HSM doivent être activés ;
- des mesures techniques et organisationnelles doivent être mises en place afin d'empêcher tout accès non autorisé au HSM via le réseau, que cet accès soit direct ou indirect (par rebond via l'application cliente par exemple).

C5. Les exigences de l'ANSSI en matière de choix et de dimensionnement des mécanismes cryptographiques [5] doivent être respectées et notamment :

- la taille des modules RSA doit être d'au moins 2048 bits pour une utilisation jusqu'en 2030 et 3072 bits au-delà ;
- la taille des courbes elliptiques ECDSA doit être d'au moins 256 bits;
- une même clé cryptographique ne doit être affectée qu'à un seul usage ;
- les fonctions de hachage MD5 et SHA-1 ne doivent pas être utilisées dans le cadre de la signature électronique quel que soit l'algorithme de signature (RSA ou ECDSA) ; les fonctions de hachage SHA 256, SHA384, SHA512 peuvent être utilisées ;
- l'algorithme de chiffrement symétrique DES ne doit pas être utilisé.

C6. L'installation et l'utilisation s'effectue en suivant strictement le guide [2].

Limite

L1. Seules les fonctions identifiées dans [2] au chapitre « 5.1 - Security objectives for the TOE » sont couvertes par la présente décision de qualification.