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*

Paris, le 25 janvier 2016

N° 198/ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU RENFORCÉ

HSM TRUSTWAY PROTECCIO *(ATOS/BULL)*

HSM TRUSTWAY PROTECCIO Entry Level (EL)
Matériel : 1.05.03 - 76681604-004D/76681604-005
Système : X130, Module de sécurité : V128

HSM TRUSTWAY PROTECCIO High Range (HR)
Matériel : 1.05.03 - 76681610-004D/76681604-005
Système : X130, Module de sécurité : V128

Annexe : Références.

La ressource cryptographique HSM[1] TRUSTWAY PROTECCIO développée par la société *ATOS/BULL* se présente sous la forme d'un boitier qui offre, via une interface PKCS#11 accessible sur son interface réseau Ethernet, les services cryptographiques suivants : gestion de clés cryptographiques (génération, stockage, sauvegarde, restauration, destruction), création et vérification de signatures électroniques, chiffrement et déchiffrement symétrique et asymétrique de messages, création et vérification de codes d'authentification de messages et calcul de condensés.

Le HSM TRUSTWAY PROTECCIO existe en deux gammes (*High Range* et *Entry Level*) offrant des débits cryptographiques différents.

Eu égard au rapport de certification [5] et conformément au processus de qualification d'un produit de sécurité [1], j'atteste que ce produit, dans ces deux gammes, atteint le niveau de qualification renforcé, sous réserve :

- du respect du guide d'installation et d'utilisation du HSM [6] ;
- du respect des conditions d'utilisation établies au chapitre 3.2 de [5], et notamment :
  - 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,

[1] *Hardware Security Module*.

    - 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 certificats électroniques permettant aux applications clientes de s'authentifier auprès du HSM via le protocole TLS doivent être générés pour 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 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 identifiés par l'entité ayant fait l'acquisition du produit en s'appuyant sur le manuel développeur [7],
    - 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 une application cliente par exemple) ;
- du respect des exigences de l'ANSSI en matière de choix et de dimensionnement des mécanismes cryptographiques [4] 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 200 bits pour une utilisation jusqu'en 2020 et 256 bits au-delà,
    - 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 SHA256, SHA384, SHA512 peuvent être utilisées,
    - l'algorithme de chiffrement symétrique DES ne doit pas être utilisé.

En outre, la conformité du produit au profil de protection [8] permet d'attester de l'aptitude du produit à satisfaire les exigences :

- du référentiel général de sécurité [2] pour le niveau trois étoiles (***) ;
- du règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement eIDAS [3]. À ce titre, le produit est donc déclaré apte à stocker et mettre en œuvre des clés cryptographiques d'autorités de certification, de signature électronique à distance, d'authentification ou de chiffrement dans le cadre de [2] et [3].

Le produit est de plus déclaré apte à la génération et à la protection de clés destinées à la protection d'informations sensibles de niveau *Diffusion Restreinte*, ou classifiées au niveau *Diffusion Restreinte OTAN*, *Restreint UE/EU Restricted*, ou *Diffusion Restreinte EUROCOR*.

Cette qualification est valable pour une durée de 3 ans. Elle pourra être prolongée par la mise sous surveillance du produit certifié.

Signé : Contre-amiral Dominique RIBAN, Directeur général adjoint

Annexe

Références

[1]. Processus de qualification au niveau renforcé, version 1.0 (disponible sur www.ssi.gouv.fr).

[2]. Référentiel général de sécurité, versions 1.0 et 2.0.

[3]. Règlement européen n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

[4]. Annexe B1 du RGS, Mécanismes cryptographiques - règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014.

[5]. Rapport de certification ANSSI-CC-2015/46, HSM Trustway Proteccio, version 1.03.05 (X130/V128), ANSSI, 23 octobre 2015.

[6]. Trustway Proteccio – Manuel d'installation et d'utilisation, référence 86F276FH09, février 2015.

[7]. Trustway Proteccio – Manuel développeur, référence 86F275FH14, septembre 2015.

[8]. Cryptographic Module for CSP Signing Operations with Backup, Protection profile reference : prEN 14167-2 :2012.