



**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 30 mai 2025
N° 00916 /ANSSI/SDE/NP

DECISION DE QUALIFICATION D'UN PRODUIT

**TRUSTWAY PROTECCIO
VERSION V194/X194**

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° 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 des systèmes d'information ;
- 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 1^{er} ;

- 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-2025/09 du 31/03/2025 ;
- VU le dossier de demande de qualification déposé par BULL SAS ;

DÉCIDE :

- Art. 1^{er} – Le produit « TRUSTWAY PROTECCIO » en version « V194/X194 », ci-après désigné « le produit », fourni par BULL SAS, ci-après désigné « le fournisseur », 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 est agréé pour la protection d'informations marquées Diffusion Restreinte, ou classifiées Restreint UE/UE Restricted dans un contexte national uniquement, ou classifiées Diffusion Restreinte OTAN/NATO Restricted 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 V194/X194 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, règlement modifié par le règlement (UE) n°2024/1183, sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.
- Art. 4 – Le maintien de cette décision est conditionné au respect par le fournisseur des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.
- Art. 5 – La présente décision est valable 3 ans.

 Vincent Strubel

Annexe

Conditions et limites de la qualification.

Références

- [1]. Rapport de certification ANSSI-CC-2025/09 du 31/03/2025 ;
- [2]. Trustway Proteccio - Security Target – reference PCA4_P142, version 1.09 – 26/11/2024
- [3]. Installation and user's guide – reference 86 A2 76FH, version 71 – Novembre 2024, ou, Manuel d'installation et d'utilisation – Référence 86 F2 76FH, version 71 – Novembre 2024
- [4]. Developers' Guide – reference 86 A2 75FH, version 70 – October 2024
- [5]. Enabling PP5 compliance mode – reference 86 XY 05GA, version 03 – August 2024
- [6]. Migration of Trustway Proteccio software to V193/X193 and higher – reference 86 A2 02GA, version 3, 03/07/2024
- [7]. 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 et d'agrément 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 le rapport [1] sont respectés.
- C2. Les restrictions d'usage figurant dans le rapport [1] sont respectées.
- C3. Les recommandations figurant dans les guides du produit référencés dans le rapport [1] sont respectées.
- C4. La configuration pour la conformité au PP-419221-5 est respectée dans le cadre d'une utilisation comme dispositif de signatures qualifiées (QSCD) en local ou à distance au titre du règlement eIDAS.
- C5. Les conditions d'utilisation établies au chapitre 4.2 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 ;
 - 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 identifiés 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 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 ;
- 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).

C6. Les exigences de l'ANSSI en matière de choix et de dimensionnement des mécanismes cryptographiques [7] 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

C7. L'installation et l'utilisation s'effectue en suivant strictement les guides [3], [4], [5], [6].

Limite(s)

L1. Seules les fonctions identifiées dans [2] au chapitre « 5.2 - Security objectives for the TOE » sont couvertes par la présente décision de qualification