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 10/03/2025
N° 381/ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

TRUSTWAY IP PROTECT
VERSION 6.01.X
AVEC X ≥ À 17

BULL SAS

RCS 642 058 739

Rue Jean Jaurès
78340 Les Clayes-sous-Bois
France

Pièces constitutives de la décision de qualification :
Fiche 1 : Description du produit
Fiche 2 : Périmètre de qualification et d'agrément
Fiche 3 : Conditions, limites de la qualification et recommandations
Fiche 4 : 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 ;

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 ;

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-2024/32 du 25 novembre 2024 ;

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

Décide :

Art. 1er – Le produit « TRUSTWAY IP PROTECT » et dont les versions sont identifiées en fiche 2, ci-après désigné « le produit », fourni par BULL SAS, ci-après désigné « le fournisseur », respecte les règles fixées par les décrets n° 2010-112 du 2 février 2010 et n° 2015-350 du 27 mars 2015 et est qualifié au niveau standard 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 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. 4 – Le fournisseur applique les engagements spécifiés dans le courrier d'accompagnement de cette présente décision.

Art. 5 – La présente décision est valable trois ans.

18/3/2025 | 18:23 CET

Vincent Strubel

Fiche 1

Description du produit qualifié et agréé

Le produit dans ses conditions qualifiées, permet d'interconnecter un ou plusieurs réseaux de confiance via l'instanciation d'un ou de plusieurs tunnels VPN (*Virtual Private Network*). Il est admis que ces tunnels peuvent faire transiter des informations jusqu'au niveau Diffusion Restreinte[1] lorsque le produit est utilisé dans ses conditions d'usage (voir fiche 2).

Les composants suivants font partie de l'infrastructure de gestion des chiffreurs :

- Le Trustway Domain Manager (TDM) est l'outil de configuration et supervision nécessaire à la définition et l'application des politiques de sécurité sur les différents équipements de chiffrement.
- La Station de Personnalisation Client (SPC) est l'outil de personnalisation client des équipements de chiffrement Trustway. Elle s'accompagne d'une clé USB permettant la personnalisation initiale du chiffreur.

L'ensemble de ces éléments sont décrits dans la cible de sécurité [2].

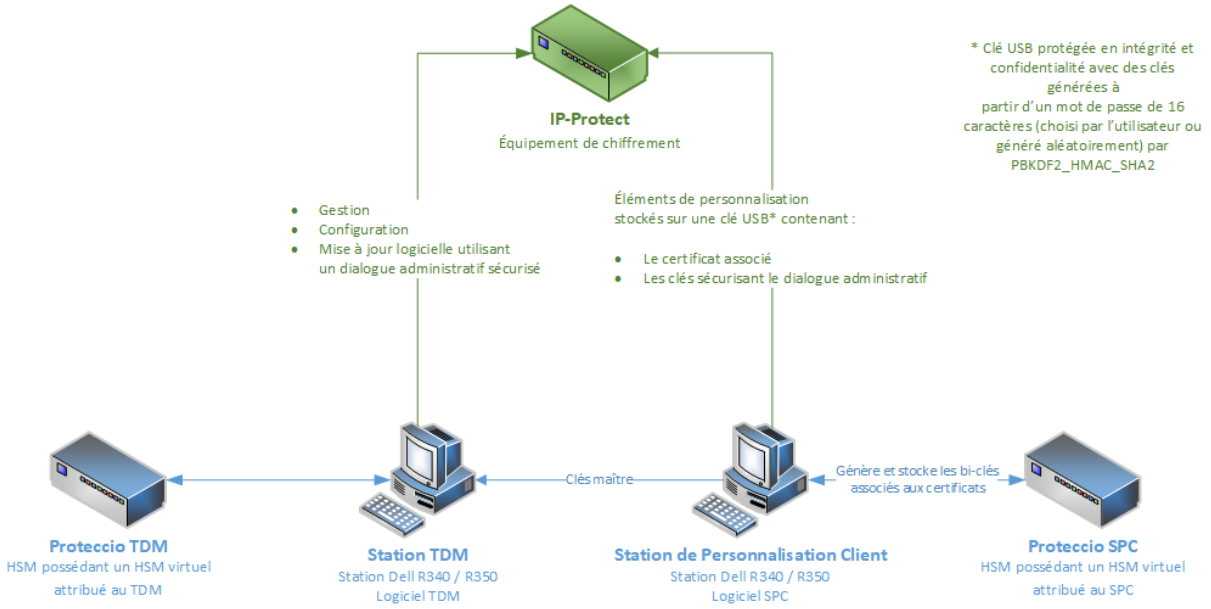

Schéma simplifié de l'infrastructure de gestion

[1] Voir Instruction interministériel relative à la protection des systèmes d'informations sensibles II901 disponible sur https://www.legifrance.gouv.fr/

Fiche 2

Périmètre de qualification et d'agrément

1. En usage

Le produit qualifié et agréé est le chiffreur dénommé Trustway IP PROTECT et configuré en mode « Full IPSEC DR » conformément à la cible de sécurité [2].
Les fonctionnalités comprises dans le périmètre de qualification et d'agrément sont décrites dans le rapport [1].

2. Infrastructure de gestion

L'infrastructure de gestion comprenant les composants TDM et SPC n'est pas comprise dans le périmètre de qualification et d'agrément. En revanche, l'ANSSI impose des conditions d'emploi relatives à ces composants (voir fiche 3). Il convient pour l'autorité d'emploi, de s'assurer du respect de ces conditions.

Tout autre composant ou interconnexion non mentionné dans cette présente fiche n'est pas compris dans le périmètre de qualification et d'agrément.
L'autorité d'emploi du produit qualifié et agréé est responsable de l'analyse et de l'identification des risques induits par l'usage et/ou l'interconnexion de tout autre composant.

3. Versions qualifiées du chiffreur « Trustway IP Protect »

<table>
<tr><th>Numéro de produit</th><th>Ports réseaux</th><th>Famille</th><th>Modèles associés</th><th>Version logiciel</th></tr>
<tr><td>76682879</td><td>4 ports 1 Gb</td><td>Light</td><td>IE5L-4, IE20L-4, IE50L-4</td><td rowspan="7">6.01.x

(Avec x ≥à 17)

x correspond aux corrections d'anomalies rétro compatible n'entrainant pas de modification relative aux fonctionnalités</td></tr>
<tr><td>76682591</td><td>4 ports 1 Gb</td><td>4 ports</td><td>IE50-4, IE100-4, IE300-4</td></tr>
<tr><td>76682592</td><td>8 ports 1 Gb</td><td>8 ports</td><td>IE50-8, IE100-8, IE300-8</td></tr>
<tr><td>76682593</td><td>8 ports 1 Gb</td><td colspan="2">IE900-8</td></tr>
<tr><td>76682594</td><td>8 ports 1 Gb et 8 ports 10 Gb</td><td colspan="2">IE1800-16</td></tr>
<tr><td>76683056</td><td>4 ports 10 Gb</td><td colspan="2">IE10G-4</td></tr>
</table>

Fiche 3

Conditions, limites de la qualification et recommandations.

Condition(s)

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

C1. L'autorité d'emploi doit s'assurer que le **chiffreur** respecte ses conditions d'emploi conformément à la cible de sécurité [1], notamment, sans s'y limiter* :

- le chiffreur est déployé en mode « FULL IPSEC DR » ;
- les hypothèses d'environnement sont respectées (il s'agit des hypothèses A.AUDIT, A.ALARME, A.ADMIN, A.LOCAL, A.MAITRISE_CONFIGURATION, A.CRYPTO).

* Ces éléments sont mis en exergues afin de faciliter la lecture pour l'autorité d'emploi. Le descriptif détaillé se trouve dans le rapport [1] ainsi que l'ensemble du corpus associé. L'autorité d'emploi doit demander ces éléments afin de pouvoir mettre en œuvre le produit dans ses conditions de certification.

Par ailleurs, l'autorité d'emploi doit s'assurer que l'administration du chiffreur soit effectuée via un port d'administration dédié.

C2. L'autorité d'emploi doit s'assurer que les restrictions d'usage figurant dans le rapport [1] sont respectées.

C3. L'autorité d'emploi doit s'assurer que les recommandations figurant dans les guides du produit référencés dans le rapport [1] sont respectées si elles existent.

C4. Concernant le **TDM** et le **SPC**, l'autorité d'emploi doit s'assurer :

- que le TDM et le SPC sont inclus dans le périmètre d'un système d'information homologué au moins au niveau Diffusion Restreinte [4] ;
- que les administrateurs sont informés de leurs droits et devoirs ;
- que les administrateurs sont formés à l'état de l'art en matière SSI ;
- de disposer de documents reflétant fidèlement l'état courant des systèmes d'information qu'ils administrent, notamment des cartographies du SI (physique, système, réseau, applications) faisant notamment apparaître clairement les interconnexions avec l'extérieur ;
- de mener régulièrement une analyse de risque sur le TDM et le SPC dans leur contexte et environnement d'utilisation, la fréquence de mise à jour de l'analyse de risque est à justifier selon le contexte ;
- que le TDM est positionné dans une zone d'administration, au sens du guide ANSSI [5] ;
- que le SPC est déconnecté de tout réseau et stocké physiquement dans un local protégé ;
- que le TDM et le SPC respectent les recommandations applicables à des postes d'administration au sens du guide ANSSI [5] ;
- que le TDM et le SPC sont gérés par l'autorité d'emploi et non par un sous-traitant ;

- que et le SPC n'a pas accès à Internet ou à tout autre réseau tiers non maîtrisé ;
- que le TDM et le SPC sont durcis conformément à [3]. L'autorité d'emploi doit notamment, sans s'y limiter, mettre en œuvre le *SecureBoot*. Il est recommandé que le durcissement soit effectué par le fournisseur du produit à la livraison. Les évolutions de durcissement comprises dans le périmètre de la qualification et de l'agrément doivent être réalisées par un travail conjoint entre le fournisseur du produit (devoir de conseil) et l'autorité d'emploi ;
- que les mots de passe fournis à la livraison sont modifiés, que les comptes sont dédiés par administrateur ;
- que les administrateurs utilisent par défaut des comptes d'administration individuels, qui sont réservés aux actions d'administration ;
- de définir une politique de gestion et d'analyse des journaux d'évènements prenant en compte les capacités spécifiées dans le guide [3] ;
- par prévention, d'avoir identifié et prévu des scénarios de remédiation en cas de compromission du TDM ou du SPC. Ces scénarios sont documentés et connus des administrateurs.

Limite(s)

L1. Seules les fonctions du chiffreur identifiées dans le rapport [1] sont couvertes par la présente décision de qualification.

L2. L'évolution des composants TDM et SPC doivent faire l'objet d'une mise à jour de l'analyse de risque de l'autorité d'emploi afin de prendre en compte ces évolutions et risques éventuels.

L3. Tout autre composant hormis le TDM et le SPC mentionné dans la cible de sécurité [2] ou dans les guides associés ne sont pas compris dans le périmètre de qualification et d'agrément. L'autorité d'emploi du produit qualifié et agréé est responsable de l'analyse et de l'identification des risques induits par l'usage et/ou l'interconnexion de tout autre composant.

Recommandation(s)

R1. Il est recommandé que l'autorité d'emploi demande et prenne connaissance de l'ensemble des documents précisés dans la fiche 4 ainsi que des sous-ensembles de documents qui y sont spécifiés.

R2. Il est recommandé que l'autorité d'emploi garde un lien privilégié avec le fournisseur du produit tout au long du cycle de vie de celui-ci (livraison, maintenance, évolution), notamment en cas de détection de vulnérabilités.

Fiche 4

Base documentaire pour la qualification

Référence(s)

[1]. Rapport de certification ANSSI-CC-2024/32 du 25 novembre 2024 ;

[2]. Cible de sécurité Trustway IP Protect – référence TW/IPP/IP Protect_Cible de sécurité/CI, version 1.22 du 9 septembre 2024 ;

[3]. Durcissement TDM et SPC, version 1.3 à demander à BULL SAS ;

[4]. Instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'information sensibles, version en vigueur, disponible sur https://www.legifrance.gouv.fr.

[5]. Recommandations relatives à l'administration sécurisée des SI, ANSSI, disponible sur https//www.cyber.gouv.fr.