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 16 NOV. 2016
N° 4834 /ANSSI/SDE

QUALIFICATION AU NIVEAU STANDARD

TRC7546-I0 version 8.2.1.2
THALES COMMUNICATIONS AND SECURITY

Références :
[1] Processus de qualification d'un produit de sécurité –niveau standard-, version 1.2.
[2] Cible de sécurité du MISTRAL IP *ENCRYPTION DEVICE*, référence 63 295 297 - 306 -A Lite du 21/07/2016.
[3] Rapport de certification ANSSI-CC-2016/42.
[4] Guide d'installation du produit, Réf : 62 908 104 - 072 - F du 16/07/2015 et Guide d'utilisation du produit TRC7546-I0 Mistral Net Version système V8.2.1, Réf : 62 999 647 - 108 -B de septembre 2015.

Le produit qualifié est composé du logiciel MISTRAL IP v2.1.2 pour MISTRAL IP dans sa version système 8, embarqué dans un équipement MISTRAL V5M v1.2.00, et est dénommé par la référence TRC7546-I0 version 8.2.1.2. Cet équipement permet la protection des flux IP entre une ou plusieurs enclaves.

Cette qualification s'applique uniquement au mode de chiffrement « IPsec tunnel », également dénommé « ESP-MISTRAL », seul mode de l'équipement capable d'assurer la protection des flux de données en confidentialité, intégrité, authentification et anti-rejeu et d'assurer l'authentification mutuelle des équipements.

Conformément au processus de qualification en première référence et sur la base :

- de la cible de sécurité, en deuxième référence ;
- du rapport de certification, en troisième référence ;

et sous réserve que :

- 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 [2], et suive les recommandations se trouvant dans les guides [4] ;
- l'opérateur s'assure que le « contrôle de l'anti-rejeu » est bien activé ;
- l'opérateur s'assure que les adresses MAC des équipements associées aux ports des commutateurs et concentrateurs reliés à l'équipement sont configurés de manière statique;

- l'opérateur s'assure que le Centre d'Elaboration des Clés (CEC) soit configuré de telle sorte que le rafraichissement par l'aléa physique se fasse périodiquement lors de son fonctionnement, et non uniquement à l'allumage de la machine ;
- en mode distribué, l'opérateur s'assure de la disponibilité dans des délais compatibles avec l'usure des clefs des éléments du système - CEC et Centre de Gestion (CG) - participant au renouvellement des clefs ;
- l'opérateur bloque toutes les fonctions de supervision depuis le réseau chiffré en privilégiant une supervision depuis l'interface de gestion locale ;

j'atteste que le TRC7546-I0 version 8.2.1.2 en mode « ESP-MISTRAL» atteint le niveau de qualification standard.

Cette qualification porte sur les modes distribué et négocié pour les clés de session. L'emploi du mode négocié (protocole IKEv2) est cependant à privilégier autant que possible, car il permet un meilleur traitement des problématiques d'usure et de renouvellement de clés.

Ce produit est agréé pour la protection d'informations marquées *Diffusion Restreinte* ou classifiées au niveau *Diffusion Restreinte* OTAN, *Restreint UE/UE Restricted* ou EUROCOR *Diffusion Restreinte*.

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

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information