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 25/03/2025
N° 564/ANSSI/SDE/NP

DECISION DE QUALIFICATION D'UN PRODUIT

GATEWAY IPSEC MISTRAL
VERSION VS9.2.3.X (AVEC X ≥ 5)

THALES SIX GTS FRANCE SAS
SIRET N° 383 470 937 00194

4, avenue des Louvresses
92230 GENNEVILLIERS
FRANCE

Pièces constitutives de la décision de qualification :

Fiche 1 : Base documentaire de la qualification et l'agrément
Fiche 2 : Versions du produit concernées par la qualification et l'agrément DR
Fiche 3 : Conditions et limites de la qualification et l'agrément DR

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 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 l'instruction interministérielle relative à la protection des systèmes d'information sensibles n° 901/SGDSN/ANSSI ;

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

VU le rapport de certification ANSSI-CC-2025/06 du 12/02/2025 ;

VU le dossier de demande de qualification déposé par THALES SIX GTS FRANCE,

DÉCIDE :

Art. 1er – Le produit « GATEWAY IPSEC MISTRAL » en version « VS9.2.3.X AVEC X≥5 », ci-après désigné « le produit », fourni par THALES SIX GTS FRANCE, 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 *Restreint 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 – La présente décision est valable trois ans.

26/3/2025 | 08:45 CET

Vincent Strubel

Fiche 1

Base documentaire de la qualification et de l'agrément

Références

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, référence QUAL-PROD-PROCESS, version en vigueur. Disponible sur https://www.ssi.gouv.fr/qualification-processus
[RGS]	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. Disponible sur www.ssi.gouv.fr/rgs
[II 901]	Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles. Disponible sur https://www.legifrance.gouv.fr/.
[IGI 2102]	Instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne

Documents rédigés par le centre d'évaluation

[CRYPTO]	Rapport d'analyse des mécanismes cryptographiques du MMC OPPIDA/CESTI/2024/CC/NOROIT/ CRYPTO_MMC/1.0 du 14/11/2024 Rapport de conformité IPSEC-DR OPPIDA/DOC/2023/FQR/2319/1.0 du 22/12/2023 Rapport d'analyse des mécanismes crypto de la passerelle OPPIDA/CESTI/CC/NOROIT/CRYPTO GW VERSION 1.0 du 30/09/2024
[RTE]	Rapport Audit de code OPPIDA/DOC/2024/FRF/1752/1.1 du28/06/2024 Rapport d'audit de configuration OPPIDA/DOC/2024/FRF/1721/1.4 du 02/08/2024 Rapport de Tests d'Intrusion OPPIDA/DOC/2024/FRF/1708/1.2 du 15/07/2024 RTE de l'évaluation de la passerelle OPPIDA/CESTI/NOROIT/RTE 1.3 du 23/01/2025

[CERTIF]	Certificat ANSSI-CC-2025/06 EAL4 Augmenté (ALC_FLR.3) du 12/02/2025

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_INSTALL]	Guide d'installation rapide Mistral séries 9000-IP9001 - Référence : 65471286-108 - Version : D, janvier 2022 Guide d'installation rapide Mistral séries 9000-IP9010 - Référence : 68720460-108 - Version : A, avril 2023 Manuel d'installation Mistral Management Center - Référence : 67417122-067 - Version : C, septembre 2024
[GUIDE_UTIL]	Manuel d'utilisation Mistral Management Center - Référence : 67147242-108 - Version : F, septembre 2024 Manuel d'utilisation Gateway IPsec MISTRAL IP9001 Référence : 67147240-108 - Version : K, septembre 2024 Manuel d'utilisation Gateway IPsec MISTRAL IP9010 Référence : 68720459-108 - Version : B, septembre 2024
[CDS]	Security Target for Mistral VS9 Gateway Software (CDS) - Référence : 63535113- 306 - Version : AF du 14/01/2025

Fiche 2

Versions du produit concernées par la qualification et l'agrément

Version du matériel	Version du logiciel
IP9001 et IP9010	9.2.3.X (avec X ≥ 5)

Fiche 3

Conditions et limites de la qualification et de l'agrément

Condition(s)

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 consignes de sécurité indiquées dans les guides d'administration [GUIDE_INSTALL] et utilisateurs [GUIDE_UTIL] sont mises en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout au long de son cycle de vie.

C2. Les objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans les cibles de sécurité [CDS] sont strictement respectés.

C3. Tous les utilisateurs sont formés et entrainés à l'usage des produits MISTRAL selon les besoins opérationnels.

C4. Les administrateurs sont informés de la politique de sécurité du système d'information, et doivent contrôler que les règles de filtrage et de chiffrement qui sont implémentées sont conformes avec la politique de sécurité.

C5. Les Gateways IPsec sont installées dans un environnement sécurisé qui protège de tout accès physique non autorisé.

C6. Les dispositifs de configuration locale par liaison USB sont identifiés et utilisés uniquement par des administrateurs. Les mesures organisationnelles mises en place pour le transfert des données de configuration des Gateways IPsec assurent l'intégrité de ces dispositifs.

C7. Le renouvellement des certificats d'authentification, est fait régulièrement par le biais du MMC en cohérence avec leur durée de validité.

C8. Le MMC et l'IGC externe de gestion des certificats sont installés dans un environnement sécurisé qui empêche tout accès physique non autorisé.

C9. L'installation des Gateways IPsec est bien en coupure du flux de communication, interdisant toute possibilité de contournement de l'équipement.

C10. Le canal de télégestion des Gateways IPsec MISTRAL installées en dehors du réseau d'administration se fait via un VPN IPsec d'administration établi avec une Gateway IPsec MISTRAL installée en bordure du réseau d'administration.

C11. Les terminaux utilisés pour la gestion en local des Gateways IPsec sont durcis et protégés contre les attaques qui pourraient mener à une fuite d'information liées aux biens sensibles (clés, topologie, configuration …).

C12. L'accès au logiciel MMC est restreint conformément aux règles de contrôle d'accès du réseau d'administration de l'organisation utilisatrice.

C13. Le contrôle d'accès aux bases de données internes des MMC doit limiter leur consultation aux seuls utilisateurs locaux ayant les droits d'accès au système d'exploitation du MMC.

C14. Le système d'exploitation et l'ensemble des technologies utilisées par le MMC doivent être maintenus en condition de sécurité par l'application régulière des corrections de sécurité empêchant l'utilisation de vulnérabilités exploitables.

Limite(s)

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