PREMIÈRE 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 15 DEC. 2022
N° 2650 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

Gateway IPsec MISTRAL VS9

THALES SIX GTS France SAS
SIRET n° 383 470 937 00194
4, avenue des Louvresses
92230 GENNEVILLIERS

Pièces constitutives de la décision de qualification :
Fiche 1 : Description du produit
Fiche 2 : Versions du produit
Fiche 3 : Conditions et limites de la qualification
Fiche 3 : Base documentaire de la qualification

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information,

Vu 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, notamment son article 9 ;

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 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu l'Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles.

Vu l'instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne ;

Vu l'instruction générale interministérielle n° 2100 du 1er décembre 1975 sur l'application en France du système de sécurité de l'organisation du traité de l'atlantique nord ;

Vu le processus de qualification d'un produit,

Vu le processus d'agrément d'un produit,

Décide que :

Art. 1er – Le produit fourni par la société Thales Six GTS France SAS portant le nom « MISTRAL GATEWAY IPSEC » et dont les versions sont identifiées en fiche 2 respecte les règles fixées par les décrets n° 2010-112 du 2 février 2010 et n° 2015-350 du 27 mars 2015 est qualifié au niveau standard sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 3.

Art. 2 – Le produit dont les versions sont identifiées en fiche 2 est agréé pour la protection des informations marquées ***Diffusion Restreinte, Restreint OTAN/NATO Restricted*** et classifiées au niveau ***Restreint UE/EU Restricted.*** Les dates d'échéance des agréments figurent en fiche 2.

Art. 3 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

Fiche 1

Description du produit

Désignation et versions

Le produit qualifié est la solution matérielle et logicielle ***MISTRA***L en versions spécifiées en fiche 2, fournie par l'entreprise THALES.

Figure n°1 – Boîtier du MISTRAL

Présentation générale

Le système MISTRAL assure la sécurisation des données échangées à l'intérieur des réseaux locaux privés (LAN) ou sur des réseaux étendus (WAN).
Basé sur les technologies VPN (Réseaux Privés Virtuels) IPsec, il offre l'ensemble des services de sécurité indispensables à tout déploiement d'applications sécurisées sur les réseaux IP.
Il est conçu principalement pour sécuriser les réseaux d'entreprises, les réseaux bancaires et les réseaux d'organismes étatiques sur lesquels transitent des informations sensibles.

Le système MISTRAL permet de sécuriser les données de réseaux informatiques intégrant potentiellement un grand nombre de Gateways IPsec MISTRAL dont la fonction est de protéger les accès à des sites de dimensionnements différents, allant de un seul à plusieurs centaines de postes (LAN d'entreprise). Pour cela, les administrateurs disposent d'un centre de gestion (MISTRAL Management Center), qui peut être réparti sur plusieurs instances, et qui assure la gestion et la supervision des parcs de Gateways IPsec MISTRAL.

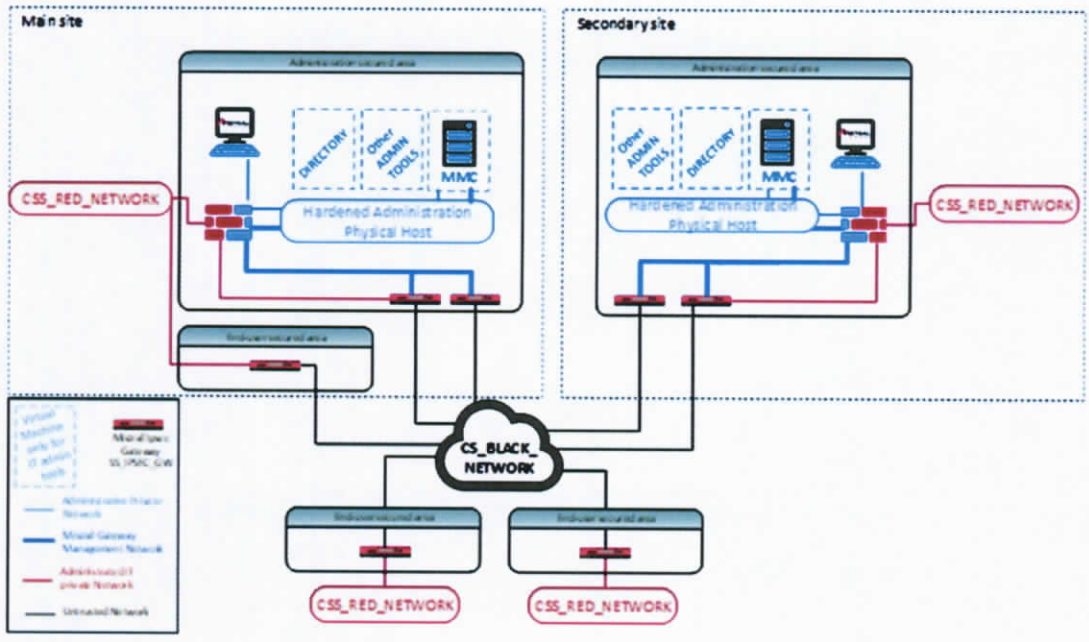

Figure 2 - Architecture type MISTRAL

Le centre de gestion (MMC) peut être intégré à des centres de gestion existants, ou bien dédié à l'administration des Gateways IPsec MISTRAL.

La Gateway IPsec MISTRAL fournit les services de protection des flux réseaux IP lors de leur transit sur des réseaux qui ne sont pas considérés de confiance pour leur niveau de sensibilité ou sur des réseaux dits a-confidentiels.
Les services offerts sont les suivants :

- Protection des flux usagers
  - Protection des flux IPv4 en confidentialité, intégrité, authenticité et anti-rejeu, à l'aide de tunnels IPsec ESP
  - Configuration de politiques de sécurité (Security Policies) fines avec filtrage des flux
- Protection des flux de gestion
  - Protection supplémentaire des flux de gestion des flux IPv4 en confidentialité, intégrité, authenticité et anti-rejeu, de bout-en-bout, par encapsulation TLS
- Protection interne
  - Cloisonnement des domaines
  - Stockage et effacement sécurisé
  - Boot sécurisé
  - Autotests PBIT et IBIT
  - Génération des journaux d'événements
- Gestion à distance
  - Supervision
  - Inventaire et reconfiguration des parcs
  - Gestion des clés et des certificats
  - Mises à jour sécurisées
  - Remontée des journaux d'événements

Fiche 2

Versions du produit

Version du matériel	Version du logiciel	Date de début de la qualification standard	Date de fin de la qualification standard
IP9001	9.0.7.x (avec x ≥ 2)	1er août 2021	1er août 2024

Version du matériel	Version du logiciel	Date de début de l'agrément ***Diffusion Restreinte***	Date de fin de l'agrément ***Diffusion Restreinte***
IP9001	9.0.7.x (avec x ≥ 2)	1er août 2021	1er juin 2023

Version du matériel	Version du logiciel	Date de début de l'agrément Restreint ***UE et Restreint OTAN***	Date de fin de l'agrément ***Restreint UE et Restreint OTAN***
IP9001	9.0.7.x (avec x ≥ 2)	1er août 2021	1er août 2024

Fiche 3

Conditions et limites de la qualification

Conditions

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 ainsi 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 installés 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 du MMC doit être maintenu en condition de sécurité par l'application régulière des corrections de sécurité empêchant l'utilisation de vulnérabilités exploitables.

Limites

La décision de qualification est valide sous réserve du respect de la limite d'utilisation suivante :

L1. Seules les fonctions de sécurité décrites dans la cible de sécurité sont couvertes par la présente décision de qualification.

Fiche 4

Base documentaire de la qualification

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
[PROCESS_AGREMENT]	Processus d'agrément des produits de sécurité n°001047/SGDSN/DCSSI/SDR du 16 mai 2003.
[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 https://www.legifrance.fr
[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

[RTE]	Rapport technique d'évaluation - référence : OPPIDA/CESTI/POULEN/RTE - version : 2.0 - en date du 09/06/2021 Rapport d'analyse des mécanismes cryptographiques - référence : OPPIDA/CESTI/POULEN/CRYPTO/3.0 - version : 3.0 - en date du 18/01/2021

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification, référence : ANSSI-CC-2021/32 en date du 28 juin 2021.
[CRYPTO]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques,_annexée au Référentiel général de sécurité (RGS_B1), disponible sur www.ssi.gouv.fr. - version : 2.03 - en date du 21 février 2014

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_INSTALL]	Guide d'installation rapide [MISTRAL Series 9000-IP9001] - référence : 65471286-108 - version : B
[GUIDE_UTIL]	Mistral Management Center (MMC) manuel utilisation - Référence : 67147242-108 - Version : B Gateway IPSEC Mistral (IP9001) MU - Référence : 67147240-108 - Version : F
[CDS]	Security Target for Mistral VS9.0 Gateway Software (CDS) - référence : 63535113- 306 - version : L

Diffusion interne (par messagerie)

ANSSI DIR – SDE – PSS – DST– DAT – BQA – DIT – Eloise Descarpentrie - chrono informatique.