



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CC-2025/06

**MISTRAL VS9
(Software v9.2.3.5 / Hardware IP9001 & IP9010)**

Paris, le 12 Février 2025

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

Vincent STRUBEL

[ORIGINAL SIGNE]



AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CC-2025/06
Nom du produit	MISTRAL VS9
Référence/version du produit	Software v9.2.3.5 / Hardware IP9001 & IP9010
Conformité à un profil de protection	<i>(aucun).</i>
Critère d'évaluation et version	Critères Communs version 3.1 révision 5
Niveau d'évaluation	EAL4 augmenté ALC_FLR.3
Développeur	THALES SIX GTS FRANCE 110 avenue du Marechal Leclerc 49300 Cholet, France
Commanditaire	THALES SIX GTS FRANCE 110 avenue du Marechal Leclerc 49300 Cholet, France
Centre d'évaluation	OPPIDA 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;"><p>Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.3.</p></div><div style="text-align: center;"><p>Ce certificat est reconnu au niveau EAL4 augmenté de ALC_FLR.3.</p></div></div>

PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.cyber.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit.....	6
1.2.1	Introduction	6
1.2.2	Services de sécurité.....	6
1.2.3	Architecture	6
1.2.4	Identification du produit.....	6
1.2.5	Cycle de vie	7
1.2.6	Configuration évaluée	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation	8
2.2	Travaux d'évaluation	8
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	8
2.4	Analyse du générateur d'aléa.....	8
3	La certification	9
3.1	Conclusion.....	9
3.2	Restrictions d'usage	9
3.3	Reconnaissance du certificat.....	10
3.3.1	Reconnaissance européenne (SOG-IS).....	10
3.3.2	Reconnaissance internationale critères communs (CCRA).....	10
ANNEXE A.	Références documentaires du produit évalué	11
ANNEXE B.	Références liées à la certification	12

1 Le produit

1.1 Présentation du produit

Le produit évalué est « MISTRAL VS9, Software v9.2.3.5 / Hardware IP9001 & IP9010 » développé par THALES SIX GTS FRANCE.

Il s'agit d'un équipement de chiffrement IPsec dont la mission est de protéger les flux réseaux sensibles lors de leur transit sur des réseaux publics ou non maîtrisés.

1.2 Description du produit

1.2.1 Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits à la section 2.2.3 « *TOE Functionalities* » de la cible de sécurité [ST].

1.2.3 Architecture

Le produit est constitué du *firmware* VS9 chargé sur une plateforme hardware, comme décrit en Figure 3 de la cible de sécurité.

Les architectures de déploiement possibles de la TOE sont présentées en section 2.2.1 « *Architecture of the Mistral system* » de la cible de sécurité [ST].

1.2.4 Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée des produits est identifiable par les éléments en réponse à la commande « show system » (voir [GUIDES]), dont les valeurs attendues sont spécifiées en Table 1 de la cible de sécurité.

1.2.5 Cycle de vie

Le cycle de vie du produit est décrit à la section 2.2.6 « *TOE lifecycle* » de la cible de sécurité [ST].

Le produit a été développé sur les sites mentionnés au 4.4.2.4 de la cible de sécurité.

1.2.6 Configuration évaluée

Le certificat porte sur les configurations permises par les [GUIDES], pour les produits tels qu'ils sont identifiés en 1.2.4 du présent rapport.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [ANSSI Crypto], pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires subit un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3 Reconnaissance du certificat

3.3.1 Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



3.3.2 Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires², des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none">- <i>Security Target for MISTRAL VS9</i>, reference 63535113-306, revision AF, 14 janvier 2025. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none">- <i>Security Target for MISTRAL VS9</i>, reference 63535113-Lite-306, revision AF.
[RTE]	<p><i>Evaluation Technical Report, Project : NOROIT</i>, Reference : OPPIDA/CESTI/NOROIT/RTE, version 1.3, 23 janvier 2025.</p>
[ANA_CRY]	<p><i>Cryptographic mechanisms analysis report</i>, MISTRAL – NOROIT, reference OPPIDA/CESTI/CC/NOROIT/CRYPTO GW, version 1.0, 30 septembre 2024.</p>
[CONF]	<p>Liste_de_configuration_des_sources_GW_Mistral-VS9, ref. 67423842-000, version E, 8 septembre 2023</p>
[GUIDES]	<p>Les guides du produit sont [Instal-IP9001], [MU-IP9001], [UM-IP9001], [Instal-IP9010], [MU-IP9010], [UM-IP9010], [Instal-MMC], [MMC-Install], [MU-MMC] et [UM-MMC] listés en Table 5 de la cible de sécurité [ST].</p>

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none">- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.