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-2021/32

Logiciel Mistral Gateway IPSec (version 9.0.7.2)

Paris, le 28 juin 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

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 présupposées 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

Référence du rapport de certification **ANSSI-CC-2021/32**
Nom du produit **Logiciel Mistral Gateway IPSec**
Référence/version du produit **version 9.0.7.2**
Conformité à un profil de protection Sans objet
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 3 augmenté** ALC_FLR.3, AVA_VAN.3
Développeur **THALES** 4 avenue des Louvresses 92230 Gennevilliers France
Commanditaire **THALES** 4 avenue des Louvresses 92230 Gennevilliers France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3. **SOG-IS** Ce certificat est reconnu au niveau EAL3 augmenté de FLR.3.

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.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Logiciel Mistral Gateway IPSec, version 9.0.7.2 » développé par THALES.

Ce produit est le logiciel embarqué dans les boîtiers TRC7540-2. L'ensemble constitué par le boîtier et son logiciel embarqué est commercialisé sous la référence IP9001. Le produit final est un équipement de chiffrement de niveau réseau (couche 3 du modèle OSI) assurant la protection des paquets IP. Il offre des services de protection de données échangées sur des liens d'interconnexions de réseaux locaux avec un réseau tiers non maîtrisé.

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.

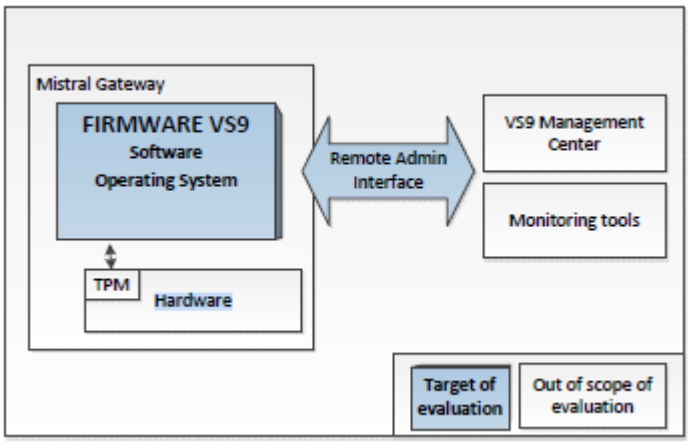
1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection du flux de données en confidentialité, intégrité, et anti-rejeu via IPSec en mode tunnel ESP ;
- la protection des flux d'administration via TLS ;
- l'administration et la supervision en local ou à distance ;
- la gestion des certificats et des clés ;
- le stockage sécurisé des données locales ;
- le démarrage sécurisé ;
- l'effacement sécurisé ;
- la mise à jour sécurisée du logiciel ;
- l'autotests ;
- la supervision ;
- la journalisation des événements.

1.2.3 *Architecture*

Le chiffreur est destiné à être utilisé avec un équipement d'administration dédié appelé *Management Center* (ou MMC), qui n'est pas inclus dans le périmètre de l'évaluation, comme le montre la figure ci-après.



Une infrastructure à clés publiques est également requise pour fournir les certificats nécessaires au bon fonctionnement du produit.

Le produit est enfin en relation avec des équipements externes THALES lors de sa production en usine avant livraison (ce processus étant dans le périmètre de l'évaluation).

La section 2.1.1 de [ST] précise les architectures de déploiement possibles de la TOE.

1.2.4 *Identification du produit*

La version de logiciel peut être obtenue via la commande « *show system* », qui doit retourner les versions suivantes :

- *OS Name : IP9001* ;
- *Machine : TRC7540-2* ;
- *OS Release : 9.0.7.2 ;*
- *Build : 1613729699.*

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit dans la section 2.2.6 de [ST]. L'évaluation a porté sur l'intégralité des activités effectuées sur les sites de THALES, jusqu'à (et incluant) la phase de *Packaging* et *Delivery*. Ces activités de développement, fabrication et maintenance impliquent les deux sites suivants :

THALES GENNEVILLIERS 4 avenue des Louvresses, 92622 Gennevilliers Cedex	**THALES CHOLET** 110 Av du Maréchal Leclerc, 49300 Cholet

Comme précisé dans [ST], les deux utilisateurs U.ROLE_GW_OPERATOR et U.ROLE_SYS_ADMIN sont considérés comme administrateurs lors de l'évaluation. Il n'y a pas à proprement parler d'utilisateurs de la TOE définis dans la cible autres que les administrateurs. En effet, les fonctions de chiffrement de flux fournies par le produit sont transparentes pour un utilisateur en bout de chaîne.

1.2.6 *Configuration évaluée*

Le certificat porte sur la partie logicielle fonctionnant sur le boîtier dans la version précisée au paragraphe 1.2.4.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 5 [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 11 juin 2021, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'évaluation visé.

2.4 Analyse du générateur d'aléas

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [REF]. Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'évaluation 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 « Logiciel Mistral Gateway IPSec, version 9.0.7.2 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants AVA_VAN.3 et ALC_FLR_3.

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'accord[1], 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 :

Le présent certificat est reconnu par le SOG-IS au niveau EAL3 augmenté de ALC_FLR.3.

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

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

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2] , 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 :

Le présent certificat est reconnu par le CCRA au niveau EAL2 augmenté de ALC_FLR.3.

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

ANNEXE A. Niveau d'évaluation du produit [CCv3.1R5]

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	*Security architecture description*
	ADV_FSP	1	2	3	4	5	5	6	**3**	*Functional specification with complete summary*
	ADV_IMP				1	1	2	2		
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**2**	*Architectural design*
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	*Operational user guidance*
	AGD_PRE	1	1	1	1	1	1	1	**1**	*Preparative procedures*
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**3**	*Authorisation controls*
	ALC_CMS	1	2	3	4	5	5	5	**3**	*Implementation representation CM coverage*
	ALC_DEL		1	1	1	1	1	1	**1**	*Delivery procedures*
	ALC_DVS			1	1	1	2	2	**1**	*Identification of security measures*
	ALC_FLR								**3**	*Systematic flaw remediation*
	ALC_LCD			1	1	1	1	2	**1**	*Developer defined life-cycle model*
	ALC_TAT				1	2	3	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	*Conformance claims*
	ASE_ECD	1	1	1	1	1	1	1	**1**	*Extended components definition*
	ASE_INT	1	1	1	1	1	1	1	**1**	*ST introduction*
	ASE_OBJ	1	2	2	2	2	2	2	**2**	*Security objectives*
	ASE_REQ	1	2	2	2	2	2	2	**2**	*Derived security requirements*
	ASE_SPD		1	1	1	1	1	1	**1**	*Security problem definition*
	ASE_TSS	1	1	1	1	1	1	1	**1**	*TOE summary specification*
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	*Analysis of coverage*
	ATE_DPT			1	2	3	3	4	**1**	*Testing: basic design*
	ATE_FUN		1	1	1	1	2	2	**1**	*Functional testing*
	ATE_IND	1	2	2	2	2	2	3	**2**	*Independent testing: sample*
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**3**	*Focused vulnerability analysis*

ANNEXE B. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target for Mistral VS9.0 Gateway Software (CDS), ref. 63535113-306, version L. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target for Mistral VS9.0 Gateway Software (CDS), ref. 63535113-306, version L lite.
[RTE]	Rapport technique d'évaluation : - OPPIDA/CESTI/POULEN/RTE version 2.0 du 09/06/2021.
[GUIDES]	GUIDE D'INSTALLATION RAPIDE [MISTRAL Series 9000-IP9001], ref. 65471286-108, version B ; MISTRAL MANAGEMENT CENTER (MMC) manuel utilisation, ref. 67147242-108, version B ; GATEWAY IPSEC MISTRAL (IP9001) MU, ref. 67147240-108, version F de mars 2021.

ANNEXE C. 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]	Procédure ANSSI-CC-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, ANSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.