



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2014/91

Logiciel Mistral IP version 2.0.84

Paris, le 22 décembre 2014

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

Guillaume POUPARD
[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.anssi@ssi.gouv.fr

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

<i>Référence du rapport de certification</i>	ANSSI-CC-2014/91
<i>Nom du produit</i>	Logiciel Mistral IP
<i>Référence/version du produit</i>	Version 2.0.84
<i>Critères d'évaluation et version</i>	Critères Communs version 3.1 révision 4
<i>Niveau d'évaluation</i>	EAL 3 augmenté ALC_FLR.3, AVA_VAN.3
<i>Développeur</i>	Thales Communications 110 Avenue du Maréchal Leclerc BP 70945 49309 Cholet
<i>Commanditaire</i>	Thales Communications 4 avenue des Louvresses 92230 Gennevilliers, France
<i>Centre d'évaluation</i>	Amossys 4 bis allée du bâtiment, 35000 Rennes, France
<i>Accords de reconnaissance applicables</i>	 

Préface

La certification

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 Premier ministre 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 matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Identification du produit</i>	6
1.2.3. <i>Services de sécurité</i>	6
1.2.4. <i>Architecture</i>	7
1.2.5. <i>Cycle de vie</i>	9
1.2.6. <i>Configuration évaluée</i>	10
2. L’EVALUATION	11
2.1. REFERENTIELS D’EVALUATION	11
2.2. TRAVAUX D’EVALUATION	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	11
2.4. ANALYSE DU GENERATEUR D’ALEAS	11
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D’USAGE	12
3.3. RECONNAISSANCE DU CERTIFICAT	13
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	13
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	13
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	14
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	15
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est le logiciel du chiffreur IP, version 2.0.84, embarqué sur le boîtier matériel Mistral, version 1.2.00, développé par Thales Communications.

Le produit, 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.

Deux modes de chiffrement sont disponibles :

- le mode simple renforcé qui assure uniquement le chiffrement de la charge utile des paquets IP (ce mode de chiffrement ne permet pas d'assurer la protection contre le rejeu) ;
- le mode tunnel qui permet le chiffrement complet des paquets IP dont notamment des en-têtes.

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. Identification du produit

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

La version certifiée du produit est identifiable par les éléments suivants :

- la version de l'appliquatif 2.0.84 ;
- la version du boîtier matériel : 1.2.00.

Lors du démarrage de la TOE, un message permettant d'identifier la version du logiciel apparaît sous forme d'une bannière d'accueil. Le résultat de la commande « *show version* » fournit également la version du logiciel et du boîtier.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection du flux de données en confidentialité ;
- la protection du flux de données en intégrité ;
- l'authentification des données échangées et la protection contre le rejeu ;
- l'authentification mutuelle des équipements de chiffrement ;
- l'administration locale et la supervision de l'équipement ;
- l'effacement d'urgence ;
- le stockage des données locales sécurisé ;
- la journalisation des événements.

1.2.4. Architecture

Le chiffreur s'insère dans une architecture plus large qui se compose de stations de gestion locale (SGL) et d'un centre d'élaboration de clés (CEC). Le produit est également en relation avec des équipements externes pour assurer sa supervision ou sa configuration.

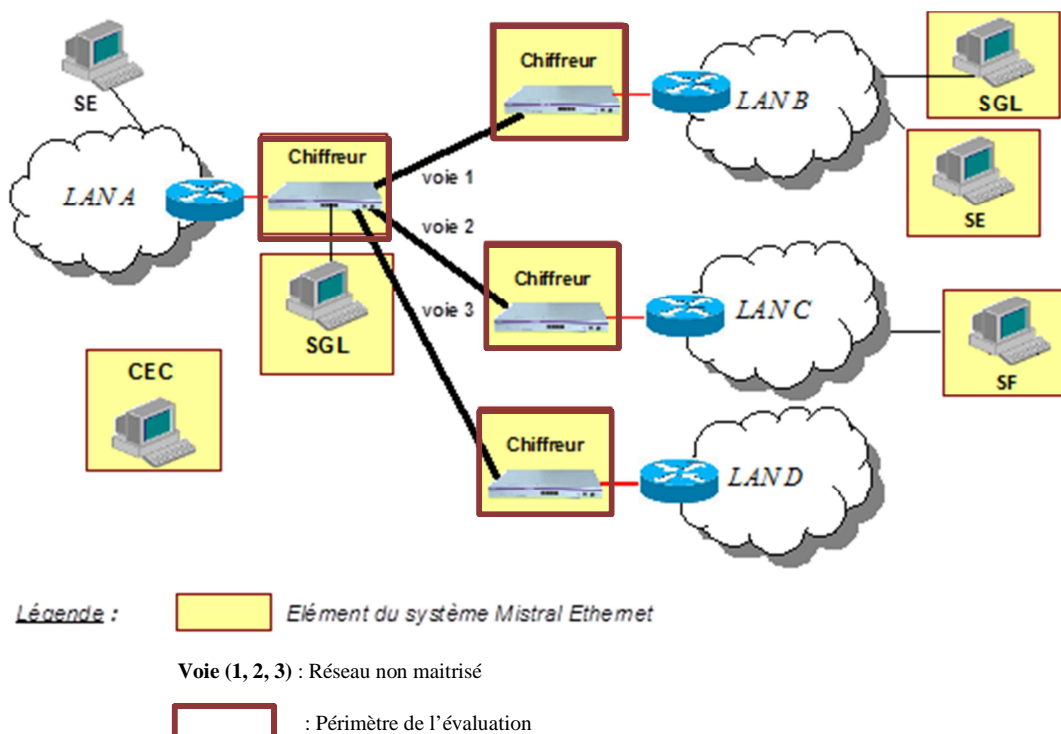


Figure 1: Architecture du système Mistral IP

Le produit est un équipement de chiffrement de type « passerelle VPN (*Virtual Private Network*) ». Placé en coupure des réseaux, il chiffre et déchiffre les paquets IP échangés avec l'extérieur au travers d'un tunnel IPsec (*Internet Protocol Security*). Les mécanismes mis en œuvre par le boîtier sont transparents pour les flux utilisateurs.

Le boîtier est administrable et configurable via une Interface de Gestion Locale (IGL), accessible localement en ligne de commande ou via la Station de Gestion Locale située sur un réseau local d'administration dédié.

Un serveur TFTP doit être mis à disposition du système Mistral pour effectuer les mises à jour *firmware* du boîtier. Il s'agit de la station nommée Serveur de Fichiers (SF).

La station de supervision (SE) permet la supervision des boîtiers Mistral IP. Elle est équipée d'un logiciel de supervision SNMP (*Simple Network Management Protocol*) et permet de superviser les boîtiers à distance via le protocole SNMP et les requêtes ICMP (*Internet Control Message Protocol*) supportées.

Le Centre d'Élaboration des Clés est une station hors ligne qui dispose d'un logiciel permettant d'élaborer des clés PSK (« *Pre-Shared Key* ») utilisées pour authentifier les boîtiers.

La TOE est la partie logicielle du boîtier Mistral IP. Ce dernier se compose d'un boîtier matériel et d'un OS Linux hébergeant l'applicatif.

Le schéma ci-dessous illustre l'architecture logique du produit.

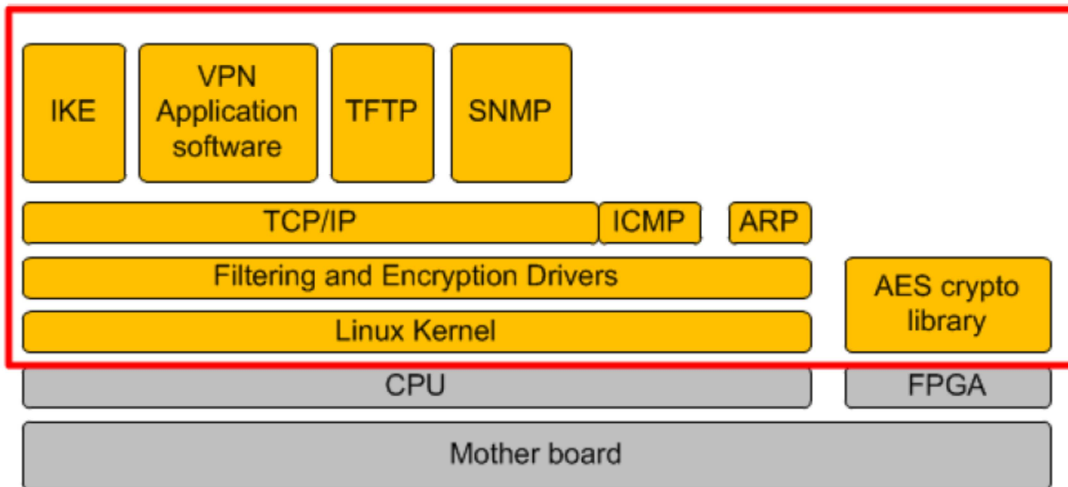


Figure 2: Architecture logique de la TOE

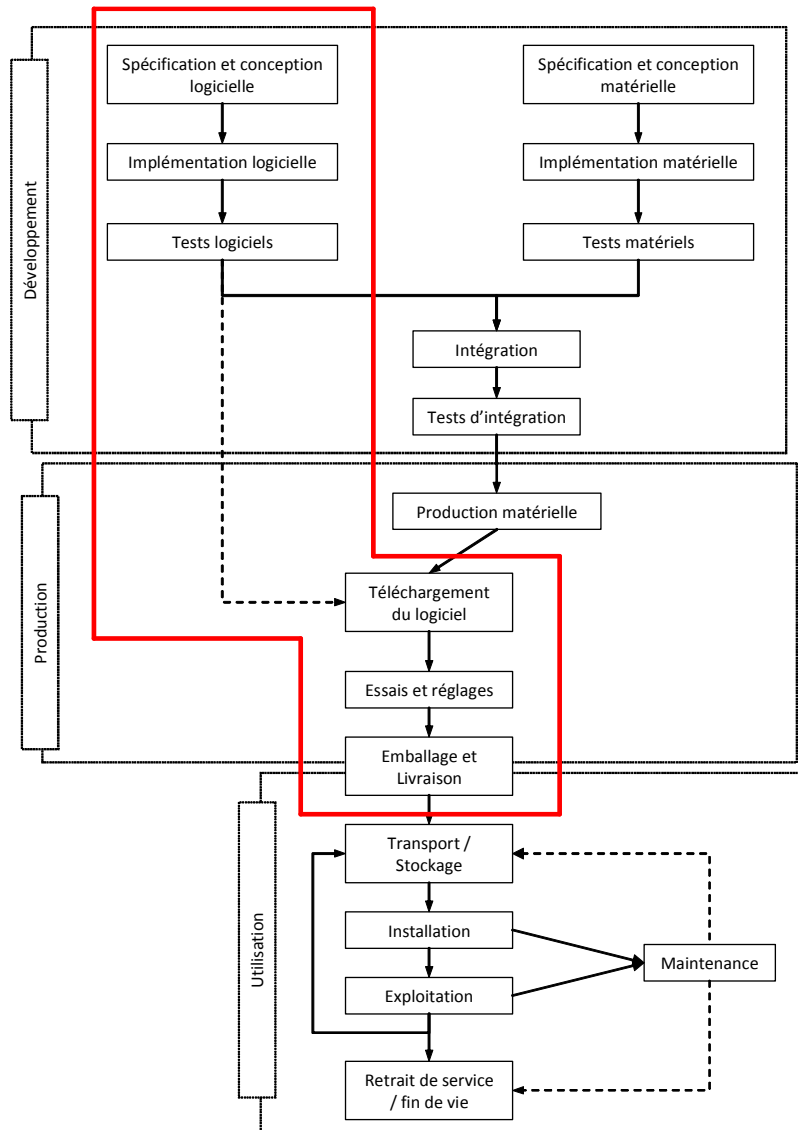
La TOE utilise les versions des composants sur étagères suivants :

- « Kernel Linux », version 2.6.38 ;
- « OpenSSL », version 0.9.8g ;
- « UBoot », version 1.3.4 ;
- « DBus », version 1.2.20 ;
- « DBus-glib », version 0.8 4 ;
- « NetSNMP », version 5.4.2 ;

Tous les autres éléments appartenant au système Mistral (SGL, CEC) sont considérés comme hors périmètre de l'évaluation.

1.2.5. Cycle de vie

Le cycle de suivi du produit est le suivant :



Les phases du cycle de vie analysées dans le cadre de cette évaluation correspondent à celles détournées en rouge dans la figure précédente.

Les sites correspondants à ces phases sont les suivants :

- **Thales Communications & Security**
Site de Cholet
 110 Av Maréchal Leclerc
 49300 Cholet
 France

- **Thales Communications & Security**

- **Site de Gennevilliers**

- 4 Av des Louvresses
92230 Gennevilliers
France

L'ensemble des phases du cycle de vie du produit dans le cadre de cette évaluation se déroule sur le site de Cholet, à l'exception du développement de la partie crypto qui a lieu sur le site de Gennevilliers.

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les rôles suivants définis dans la cible de sécurité :

- les administrateurs du produit ;
- les administrateurs en charge de la plate-forme de gestion locale ;
- les administrateurs en charge de la plate-forme de supervision.

Il n'y a pas à proprement parler d'utilisateurs de la TOE définis dans la cible autre 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 de l'équipement comprenant la librairie cryptographique embarquée dans le FPGA (*Field Programmable Gate Array*).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 novembre 2014, 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 obtenus ont fait l'objet d'un rapport d'analyse [EXP-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. 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 AVA_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Le produit comporte des générateurs d'aléas entrant dans le périmètre d'évaluation. Ces générateurs ont fait l'objet d'une analyse. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que les générateurs ne souffrent pas de défauts majeurs de conception. Conformément au document [REF], la sortie des générateurs matériels de nombres aléatoires subit un retraitement algorithmique de nature cryptographique.

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 logiciel « Mistral IP, version 2.0.84, embarqué dans le boîtier matériel, version 1.2.00 » 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 ALC_FLR.3 et AVA_VAN.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], notamment :

- associer les ports des éventuels commutateurs et concentrateurs de manière statique à l'adresse MAC des équipements qu'ils desservent ;
- bloquer toutes les fonctions de supervision depuis le réseau chiffré en privilégiant une supervision depuis l'interface de gestion locale ;
- privilégier l'utilisation du mode tunnel ;
- ne pas utiliser le mode « simple renforcé » ;
- s'assurer de la conformité des clés générées par le CEC aux recommandations de l'ANSSI ;
- s'assurer de la conformité des mécanismes de signature de mise à jour du logiciel.

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. 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 [CC RA].

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 EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

² Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	3	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	2	Architectural design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	3	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	3	3	Implementation representation CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	1	1	Identification of security measures
	ALC_FLR									3	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	1	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	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	3	3	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p><i>Security Target of Mistral IP Encryption Device</i> Référence : 62 625 250 – 306 ; Version : P ; Date : 29/10/2014.</p>
[RTE]	<p><i>EVALUATION TECHNICAL REPORT</i> Référence : ETR-PEPITO2-1.00 ; Version : 1.00 ; Date : 04/11/2014.</p>
[EXP-CRY]	<p><i>Expertise des mécanismes cryptographiques</i> Référence : CRY-PEPITO2-1.00 ; Version : 1.00 ; Date : 03/11/2014.</p>
[CONF]	<p><i>Plan de développement équipement - Système de chiffrement Mistral IP et ETHERNET</i> Référence : 62 572 558 – 544 ; Version : O ; Date : 08/08/2014.</p> <p><i>Index de Configuration Développement Mistral VS8</i> Référence : 62 908 115 – 085 ; Version : S ; Date : 28/10/2014.</p>
[GUIDES]	<p>Guide d'installation du produit :</p> <p><i>Procédure d'essai réglage personnalisation</i> Référence : 62 908 104 – 072 ; Version : C ; Date : 16/14/2014.</p> <p>Guide d'utilisation du produit :</p> <p><i>TRC7546-IO Mistral Net - Manuel Utilisateur</i> Référence : 62 908 103 – 108 ; Version : F ; Date : 22/10/2014.</p>

Annexe 3. 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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CCRA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, Septembre 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr .