Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2011/78

Suite MISTRAL IP :
version 7.0.2 pour TRC 7535, version 7.0.1 pour TRC 7539-11-A
et leur centre de gestion CGM version 7.0.1

Paris, le 18 janvier 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ 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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2011/78

Nom du produit

Suite MISTRAL IP :
version 7.0.2 pour TRC 7535, version 7.0.1 pour TRC 7539-11-A et leur centre de gestion CGM version 7.0.1

Référence/version du produit

Conformité à un profil de protection

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 3 augmenté

ADV_IMP.1*, ADV_LLD.1*, ALC_FLR.3, ALC_TAT.1*, AVA_VLA.2

***appliqués aux exigences FCS**

Développeur(s)

Thales Communications & Security
160, boulevard de Valmy
BP82
92704 Colombes Cedex

Commanditaire

Thales Communications & Security
160, boulevard de Valmy
BP82
92704 Colombes Cedex

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr

Accords de reconnaissance applicables

CCRA

SOG-IS

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

1.1. Présentation du produit

La « **Suite MISTRAL IP : version 7.0.2 pour TRC 7535, version 7.0.1 pour TRC 7539-11-A et leur centre de gestion CGM version 7.0.1»,** ci-après appelée « suite logicielle MISTRAL », est composée d'applications développées par Thales Communications & Security :

- l'application VPN IP version 7.0.2 embarquée dans le boitier TRC 7535 incluant un FPGA qui dispose de fonctions cryptographiques TDES (128 bits) et AES (128 et 256 bits). Cette application est encore appelée application VPN IP version **4**[1].7.0.2 ;
- l'application VPN IP version.7.0.1 embarquée dans le boitier TRC 7539-11-A qui dispose de fonctions cryptographiques AES (128 et 256 bits). Cette application est encore appelée application VPN IP version **6a** [2].7.0.1 ;
- l'application Centre de Gestion Mistral (CGM) version 7.0.1 nécessaire au contrôle et à l'administration des MISTRAL TRC 7535 et TRC 7539-11-A.

La suite logicielle MISTRAL intégrée dans les boitiers MISTRAL TRC7535 et TRC 7539-11-A permet, en mode usuel, au système MISTRAL d'assurer la sécurisation des données échangées à l'intérieur des réseaux locaux privés (LAN) ou lors des interconnexions de réseaux locaux sur un réseau extérieur (WAN).
En mode inversé, le système MISTRAL assure également le passage d'un flux de confiance moindre au travers d'un réseau de confiance plus élevé, en canalisant ces flux dans des VPN (Réseaux Privés Virtuels) étanches.
Basé sur les technologies VPN 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.

1.2. Description du produit

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

1.2.1. 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 :

- CGM : menu « à propos du centre de gestion » ;
- TRC 7535 : commande « confg » ou test de présence à partir du centre de gestion ;
- TRC 7539-11-A : commande « confg » ou test de présence à partir du centre de gestion.

[1] le 4 traduisant implicitement que l'application VPN IP version 7.0.2 est embarquée dans le boitier TRC 7535.
[2] le 6a traduisant implicitement que l'application VPN IP version 7.0.1 est embarquée dans le boitier TRC 7539-11-A.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la gestion des paramètres de configuration ;
- la gestion des politiques de sécurité et des associations de sécurité ;
- la gestion des clés de chiffrement ;
- la gestion des flux clairs ;
- le filtrage des flux réseaux ;
- le chiffrement des flux réseaux ;
- la télégestion ;
- le téléchargement des logiciels ;
- la gestion des alarmes ;
- la gestion des accès par le port série ;
- la gestion de l'interface CAM[3] ;
- la gestion des fichiers de configuration sécurisée ;
- l'effacement d'urgence ;
- la gestion des flux avec les postes Nomade.

1.2.3. Architecture

L'architecture MISTRAL peut ainsi être représentée par les figures suivantes :

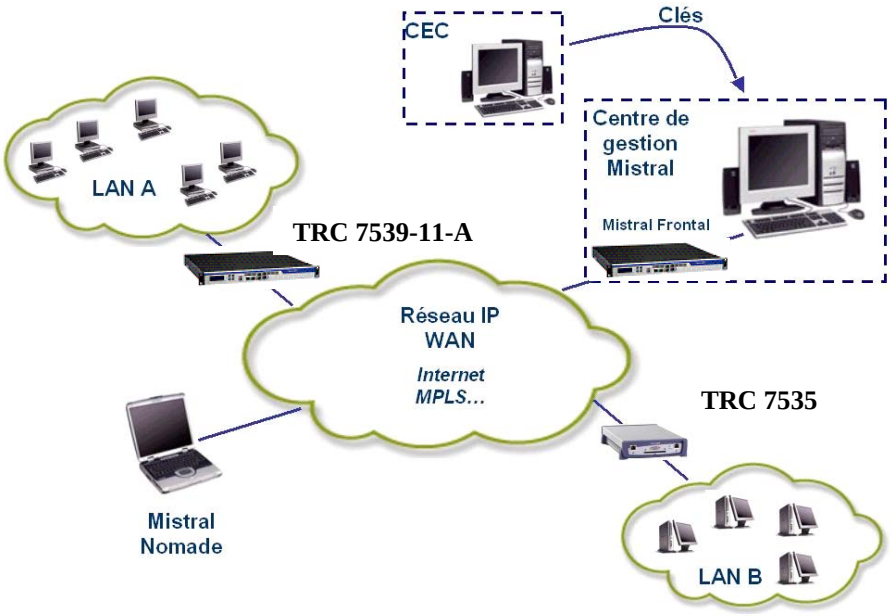


Figure 1 : Présentation du système Mistral (mode usuel)

[3] Carte A Microprocesseurs

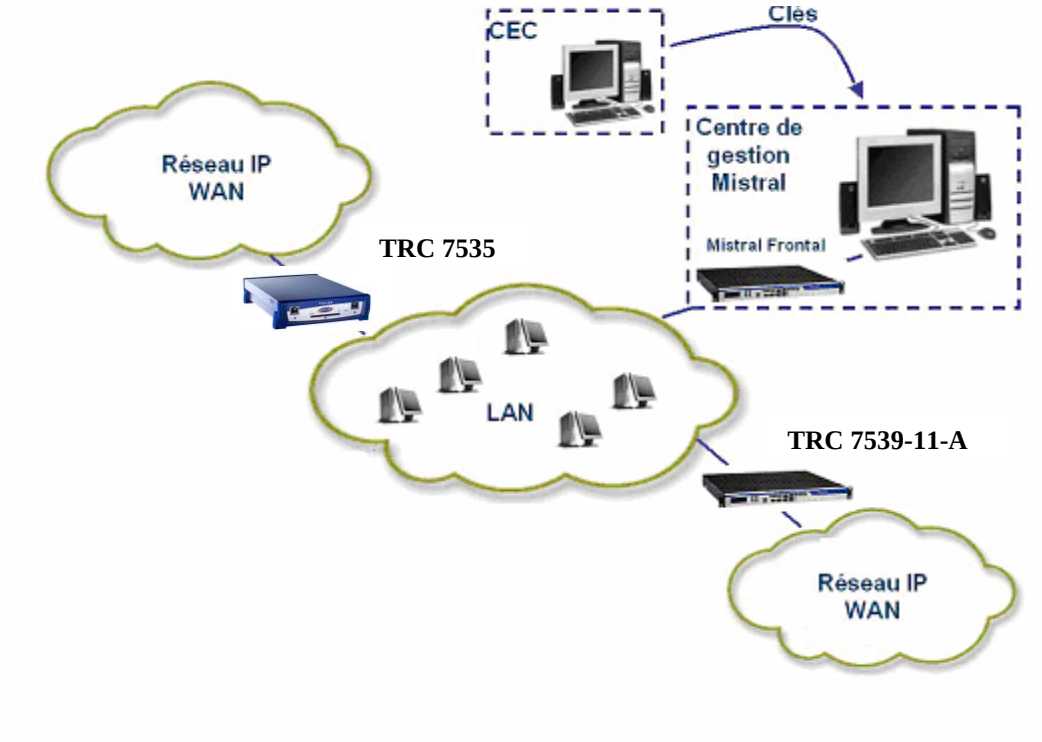
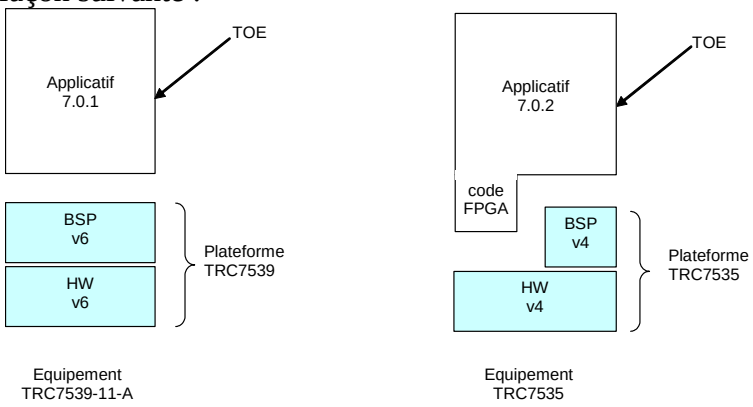


Figure 2 : Présentation du système Mistral (tunnel inversé)

La cible d'évaluation (TOE) est la suite logicielle MISTRAL constituée des éléments suivants :

- le logiciel VPN IP version 4.7.0.2 pour MISTRAL TRC 7535 et le programme du FPGA intégré ;
- le logiciel VPN IP version 6a.7.0.1 pour MISTRAL TRC 7539-11-A ;
- le logiciel de gestion version 7.0.1 qui interagit avec un boitier MISTRAL frontal (TRC 7535 ou TRC 7539-11-A).

La TOE au sein des produits MISTRAL TRC 7535 et TRC 7539-11-A peut être représentée de la façon suivante :



avec BSP : couche d'abstraction (drivers) hors TOE.
HW : plateforme *hardware* (v6 pour TRC 7539-11-A et v4 pour TRC 7535) hors TOE.

1.2.4. Cycle de vie

Le produit a été développé sur les sites suivants :

- pour ce qui concerne le développement logiciel de la partie cryptographique et sa documentation :

  Thales Communications & Security

  Site de Colombes

  160 Boulevard de Valmy
  92704 Colombes Cedex
  France

- pour ce qui concerne le développement logiciel et sa documentation :

  Thales Communications & Security

  Site de Cholet

  110 Av Maréchal Leclerc
  49300 CHOLET
  FRANCE

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

- les personnes responsables du maintien en condition opérationnelle de la TOE ;
- les mainteneurs : personnels de Thalès qui possèdent les droits administrateur, et qui peuvent mettre à jour les logiciels de la TOE, sur site ou après retour usine.

1.2.5. Configuration évaluée

Le certificat porte sur la suite MISTRAL composée des applications décrites au chapitre 1.1.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [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 12 janvier 2012, 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-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Le mode de chiffrement CBC avec un IV constant ou à l'aide d'un IV[4] potentiellement prédictible n'est pas conforme aux exigences du référentiel cité ci-dessus. Cependant, dans le cadre du processus de qualification standard du produit, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY] : ces 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_VLA visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas n'est pas conforme au référentiel technique de l'ANSSI [REF-CRY].
Néanmoins, l'utilisation de ce générateur pseudo-aléatoire dans le contexte de la génération d'IVs pour le mode « tunnel » pour lequel il est utilisé n'introduit pas de vulnérabilité.

[4] *initialization vector* : vecteur d'initialisation

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 « Suite MISTRAL IP: version 7.0.2 pour TRC 7535, version 7.0.1 pour TRC 7539-11-A et leur centre de gestion CGM version 7.0.1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté.

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 :

- l'organisme doit recruter des personnels de confiance comme administrateurs de la TOE et les former à l'utilisation de la TOE (OE.Adm_No_Evil) ;
- les administrateurs de la TOE doivent être formés et sensibilisés à la sécurité. Ils doivent appliquer la politique de sécurité du système d'information et vérifier périodiquement la conformité des règles de chiffrement et de filtrage mises en oeuvre par la TOE par rapport à cette politique (OE.Appli_Politique) ;
- l'organisme doit placer la TOE dans un environnement sécurisé qui prévient tout accès physique non autorisé à celle-ci (OE.TOE_Phys_Acs) ;
- l'organisme doit gérer les CAM de la TOE de manière à prévenir tout accès physique non autorisé à celles-ci (OE.CAM_Phys_Acs[TRC7535]) ;
- l'organisme doit véhiculer de façon sécurisée les Codes Porteurs des fichiers de configuration sécurisés, du poste du CGM à la TOE, de manière à en garantir la confidentialité. L'organisme doit utiliser des canaux différents pour la diffusion des fichiers de configuration sécurisés et des Codes Porteurs associés. Il doit finalement détruire les fichiers de configuration sécurisés et code porteurs associés, après injection dans la TOE (OE.FIC_Canaux_CP[TRC7539]) ;
- l'organisme doit renouveler périodiquement les clés cryptographiques utilisées par la TOE, ceci via le CGM (OE.Key_Renew) ;
- l'organisme doit placer le CGM dans un environnement sécurisé qui prévient tout accès physique non autorisé à celui-ci (OE.CGM_Phys_Acs) ;
- l'organisme doit placer le CEC dans un environnement sécurisé qui prévient tout accès physique non autorisé à celui-ci (OE.CEC_Phys_Acs) ;
- l'organisme doit placer la TOE en coupure des réseaux à protéger, afin de garantir qu'aucun flux réseau ne peut contourner la TOE (OE.TOE_Install) ;
- le CGM communique avec les TOE qu'il supervise, via une TOE configurée en mode « boitier frontal », afin d'utiliser les services de sécurité de cette TOE pour protéger

les flux d'administration. Le Frontal est connecté directement au CGM (OE.CGM_Channel) ;
- le terminal servant à l'administration de la TOE via son port console doit être protégé de tout dispositif tant matériel que logiciel (key logger matériel, cheval de Troie,...) permettant de capturer des éléments secrets de la configuration de la TOE lors de son administration locale (clé da base, clé de trafic,...) (OE.PC_Hyperterminal) ;
- l'utilisateur doit s'authentifier sur le poste avant d'accéder au logiciel CGM (OE.CGM_Acs_Control) ;
- le poste CGM doit être connecté directement au boîtier Mistral (la TOE) frontal (OE.CGM_Frontal).

Enfin, l'utilisateur de la suite MISTRAL devra s'assurer que :
- dans le cas d'une architecture avec un seul CGM, l'accès à la base de données MySQL du CGM est restreint à l'usage local ;
- dans le cas d'une architecture avec plusieurs CGM, un mécanisme de contrôle de flux assurant que seuls les CGM sont autorisés à accéder à la base de données est mis en place ;
- le boitier TRC 7539-11-A est, notamment en mode transport, toujours utilisé avec une clé avec usure.

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[5], 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 :

[5] 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.

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 signataires[6], 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 :

[6] 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.

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
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Autorisation controls
	ACM_SCP			**1**	**2**	**3**	3	3	**1**	TOE CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1***	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1***	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Indentification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3	**1***	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**		
	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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

*appliqués aux exigences FCS.

Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible De Sécurité (CDS) MISTRAL TRC7535/TRC7539, référence 61 485 069 805, version X du 22 décembre 2011.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation, référence OPPIDA/CESTI/SIROCCO3/RTE du 12 janvier 2012.
[ANA-CRY]	Cotation de mécanismes cryptographiques Projet SIROCCO3, référence : 2890/SGDN/ANSSI/DR du 18 novembre 2009, ANSSI.
[EXP-CRY]	Rapport de tests SIROCCO3, référence OPPIDA/CESTI/SIROCC3/TEST/1.0 du 5 juillet 2011, OPPIDA.
[CONF]	- Document de Description de Version (VDD) pour le CSCI Boîtier Mistral du système MISTRAL, référence. 61 484 104 AF - 498, version M du 17/01/2011 ; - Document de Description de Version (VDD) Centre de Gestion MISTRAL, référence 46 250 239 05 - 498, version N du 17/09/2010 ; - Document de Description de Version (VDD) pour le CSCI Boîtier Mistral du système MISTRAL, référence 62 138 883 - 498, version F du 17/01/2011 ; - EDP : Annexe de l'EDP MISTRAL, référence DLJ/TCF/RSS/SSI/PREST/el,09/0041/COM du 24 avril 2009.
[GUIDES]	- Manuel utilisateur Centre de Gestion MISTRAL, Version 7.0.1, référence 46 250 239 05-108 ind-L-fr, THALES COMMUNICATIONS & SECURITY ; - *User guide MISTRAL Management Center, Version 7.0.1, reference 46 250 239 05-108 ind-L-gb*, THALES COMMUNICATIONS & SECURITY ; - Manuel utilisateur MISTRAL, Version 4.7.0, référence 61 484 290 AG-108-fr rev -D, Mai 2011, THALES COMMUNICATIONS & SECURITY ; - *TRC7535 Mistral v4.7.0 User guide, reference 61 484 290 AG-108-fr rev -D, May 2011*, THALES COMMUNICATIONS & SECURITY ; - TRC7539-series Mistral v6x.7.0 Manuel Utilisateur, référence 62 203 862-108-fr rev -F, Mai 2011, THALES COMMUNICATIONS & SECURITY ; - *TRC7539-series Mistral v6x.7.0 User guide, reference* 62 203 862-108-en *rev -F, May 2011*, THALES COMMUNICATIONS & SECURITY.

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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.10 du 24 août 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr