
PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

# Rapport de certification DCSSI-2008/09

# Boîtier MISTRAL TRC 7535 V4.6.1

*Paris, le 10 mars 2008*

*Le Directeur central de la sécurité des systèmes d'information*

Patrick Pailloux
[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 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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

*Référence du rapport de certification*

**DCSSI-2008/09**

*Nom du produit*

**Boîtier MISTRAL TRC 7535 V4.6.1**

*Référence/version du produit*

**Version du boîtier matériel : v4. Version logicielle : V4.6.1.2**

*Conformité à un profil de protection*

**Néant**

*Critères d'évaluation et version*

**Critères Communs version 2.3**

**conforme à la norme ISO 15408:2005**

*Niveau d'évaluation*

**EAL 3 augmenté**

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

***appliqués aux exigences FCS**

*Développeur*

**Thales Communications**

**160, boulevard de Valmy, BP82, 92704 Colombes cedex, France**

*Commanditaire*

**Thales Communications**

**110, avenue du Maréchal Leclerc, 49300 Cholet, France**

*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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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

Le produit évalué est le boîtier MISTRAL TRC 7535 V4.6.1, développé par Thales Communications.

Le MISTRAL TRC 7535 est un boîtier de chiffrement qui assure 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). Basé sur les technologies VPN (Réseaux Privés Virtuels), il offre un ensemble de services de sécurité nécessaire 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 évalué

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 :

- le boîtier MISTRAL TRC 7535 version 4, incluant une carte électronique spécifique, et disposant d'une interface série, Ethernet, d'un lecteur de carte à microprocesseur (CAM), ainsi que d'une interface d'effacement d'urgence ;
- le logiciel VPN IP version 4.6.1.2 embarqué dans le boîtier ;
- le logiciel embarqué dans la ressource cryptographique (FPGA) AES v2.0 ;
- le logiciel CGM version 6.1.2 qui interagit avec un boîtier MISTRAL TRC 7535 frontal, permettant la protection des flux de gestion des autres boîtiers.

Ces éléments peuvent être vérifiés : le boîtier comporte une étiquette qui mentionne le type du boîtier ainsi que les références du module cryptographique embarqué, et le logiciel d'administration permet de vérifier la version du logiciel embarqué.

### *1.2.2. Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- gestion des paramètres de configuration ;
- gestion des politiques de sécurité et des associations de sécurité ;
- gestion des clés de chiffrement ;
- gestion des flux clairs ;
- filtrage des flux réseau ;
- chiffrement des flux réseau ;
- télégestion ;
- gestion des alarmes ;

- gestion des accès par le port série ;
- gestion de l'interface CAM ;
- effacement d'urgence ;
- gestion des flux avec les Mistral Nomades.

### *1.2.3. Architecture*

Le boîtier constitué des éléments identifiés au §1.2.1 s'utilise au sein d'une architecture réseau pouvant être schématisé selon la figure 1 :

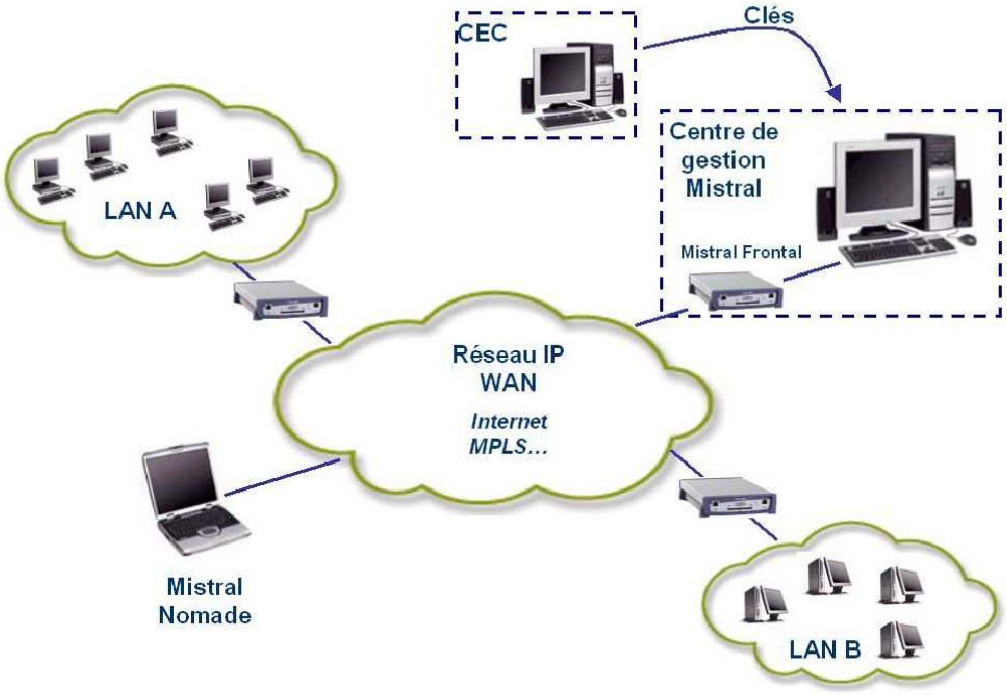


**Figure 1 – Architecture d'utilisation**

Sur ce schéma, on identifie différents équipements optionnels ne faisant pas partie du périmètre de l'évaluation :

- le logiciel Mistral nomade ;
- le centre d'élaboration de clés (CEC) qui permet de générer les clés certifiées du système.

Les diverses fonctionnalités de ce système sont décrites dans la cible de sécurité [ST], dans le guide d'installation et d'utilisation du boîtier ainsi que dans le guide d'utilisation du CGM (cf. [GUIDES]).

### *1.2.4. Cycle de vie*

Le cycle de vie du produit est le suivant :

- la partie cryptographique du code du produit est développée par Thales Communications sur le site de Colombes ;
- le produit est développé par Thales Communications sur le site de Cholet ;
- l'assemblage du produit est délégué à un sous-traitant ;

- les produits assemblés sont ensuite renvoyés à Thales Communications (site de Cholet), qui peut vérifier l'intégrité du produit avant livraison aux clients finaux.

### *1.2.5. Configuration évaluée*

Le certificat porte sur le boîtier MISTRAL TRC 7535 V4.6.1 avec algorithme de chiffrement AES, et télé administré par le logiciel CGM v6.1.2, ce dernier devant être protégé par un boîtier Mistral frontal, comme indiqué sur la figure 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 [CEM].

## 2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du boîtier MISTRAL TRC 7535 en version 4.5.2.2, certifié en 2005 sous la référence 2005/13 (cf. [2005/13]).

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 5 mars 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Ils 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 VLA 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 « Boîtier MISTRAL TRC 7535 V4.6.1 » 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

Administrateur de confiance

- Les administrateurs du produit doivent être des personnels de confiance et doivent être formés à son utilisation.

Mise en application de la politique de sécurité

- 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 œuvre par la TOE par rapport à cette politique.

Contrôle d'accès physique au produit

- L'organisme doit placer le produit dans un environnement sécurisé qui prévient tout accès physique non autorisé à celui-ci.

Contrôle d'accès physique aux CAM

- L'organisme doit gérer les CAM du produit de manière à prévenir tout accès physique non autorisé à celles-ci.

Renouvellement des clés

- L'organisme doit renouveler périodiquement les clés cryptographiques utilisées par le produit via le CGM.

Contrôle d'accès physique au CGM

- L'organisme doit placer le CGM dans un environnement sécurisé qui prévient tout accès physique non autorisé à celui-ci.

Contrôle d'accès physique au CEC

- L'organisme doit placer le CEC dans un environnement sécurisé qui prévient tout accès physique non autorisé à celui-ci.

Installation du produit en coupure des réseaux

- L'organisme doit placer le boîtier Mistral en coupure des réseaux à protéger, afin de garantir qu'aucun flux réseau ne peut contourner le boîtier.

Canal sécurisé entre le CGM et le produit

- Le CGM communique avec les boîtiers Mistral qu'il supervise via un boîtier configuré en mode « boîtier frontal », afin d'utiliser les services de sécurité de ce boîtier pour protéger les flux d'administration. Le frontal est connecté directement au CGM.

Environnement logiciel hébergeant l'hyperterminal

- Le terminal servant à l'administration du produit 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 du produit lors de son administration locale (clé de base, clé de trafic,...)[1].

Protection logique du poste CGM

- L'utilisateur doit s'authentifier sur le poste avant d'accéder au logiciel CGM.

Connexion entre le poste CGM et le boîtier mistral Frontal

- Le poste CGM doit être connecté directement au boîtier Mistral (la TOE) frontal.

De plus, pour tout produit offrant des services VPN, la DCSSI recommande d'utiliser le mode « tunnel » uniquement.

## 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 1999 permet la reconnaissance, par les pays signataires de l'accord[2], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. 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 CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[3], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux

[1] On privilégiera la configuration par télégestion/CAM plutôt que l'administration locale par console.
[2] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.
[3] 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, la République de Corée, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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 :

# 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 |
| **ACM Gestion de configuration** | ACM_AUT | | | | **1** | 1 | **2** | 2 | | |
| | ACM_CAP | **1** | **2** | **3** | **4** | 4 | **5** | 5 | **3** | Authorisation 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** | **1** | Developer defined life-cycle model |
| | 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** | **1** | Testing: high-level 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_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 |

# Annexe 2. Références documentaires du produit évalué

| | |
|---|---|
| [2005/13] | Rapport de certification 2005/13 - Boîtier MISTRAL TRC 7535 version 4.5.2.2, 30 mai 2005, SGDN/DCSSI. |
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- Cible de sécurité Mistral (CDS) MISTRAL TRC735 EAL3+, Référence : 61 485 069 – 805 révision L Thales Communications<br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- Cible de sécurité Mistral (CDS) MISTRAL TRC735 EAL3+ - version Lite, Référence : 61 485 069 – 805 révision M Thales Communications |
| [RTE] | Rapport Technique d'Evaluation, Projet SIROCCO2, Référence : OPPIDA/CESTI/SIROCCO2/RTE/1.0 du 03/03/08 |
| [ANA-CRY] | Rapport d'analyse cryptographique SIROCCO2, N° 66/SGDN/DCSSI/SDS/Crypto du 14 janvier 2008, SGDN/DCSSI |
| [CONF] | Mistral v4 – Plan de développement équipement (EDP), Référence : 62 061 737- 567, révision –B Thales Communications |
| [GUIDES] | - TRC 7535 Mistral v4.6.1, Manuel utilisateur (SUM), Référence : 61 484 290 AF, 108 fr révision A – (février 2008) Thales Communications<br>- Centre de Gestion Mistral, Manuel utilisateur (CGM_SUM), Référence : 46 250 239 05 – 108 Ind –E (juillet 2007) Thales Communications |

# Annexe 3. Références liées à la certification

| | |
|---|---|
| Décret 2002-535 du 18 avril 2002 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 :<br>Part 1: Introduction and general model,<br>August 2005, version 2.3, ref CCMB-2005-08-001;<br>Part 2: Security functional requirements,<br>August 2005, version 2.3, ref CCMB-2005-08-002;<br>Part 3: Security assurance requirements,<br>August 2005, version 2.3, ref CCMB-2005-08-003.<br><br>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,<br>August 2005, version 2.3, ref CCMB-2005-08-004.<br>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 2.0, April 1999, Management Committee of Agreement Group. |
| [REF-CRY] | Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto. |