



PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/09

Appliance MISTRAL TRC 7535 V4.6.1

Paris, 10th of March 2008

Courtesy Translation



Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.

Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.



Any correspondence about this report has to be addressed to:

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
France

certification.dcssi@sgdn.gouv.fr

Reproduction of this document without any change or cut is authorised.



<i>Certification report reference</i>	DCSSI-2008/09
<i>Product name</i>	Appliance MISTRAL TRC 7535 V4.6.1
<i>Product reference</i>	Hardware revision: v4. Software revision : V4.6.1.2
<i>Protection profile conformity</i>	None
<i>Evaluation criteria and version</i>	Common Criteria version 2.3 compliant with ISO 15408:2005
<i>Evaluation level</i>	EAL 3 augmented ADV_LLD.1*, ADV_IMP.1*, ALC_FLR.3, ALC_TAT.1*, AVA_VLA.2 *applied to FCS functional requirements
<i>Developer</i>	Thales Communications 160, boulevard de Valmy, BP82, 92704 Colombes cedex, France
<i>Sponsor</i>	Thales Communications 160, boulevard de Valmy, BP82, 92704 Colombes cedex, France
<i>Evaluation facility</i>	Oppida 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France Phone: +33 (0)1 30 14 19 00, email : cesti@oppida.fr
<i>Recognition arrangements</i>	 

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.



Content

1. THE PRODUCT	6
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION	6
1.2.1. <i>Product identification</i>	6
1.2.2. <i>Security services</i>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Life cycle</i>	7
1.2.5. <i>Evaluated configuration</i>	8
2. THE EVALUATION.....	9
2.1. EVALUATION REFERENTIAL	9
2.2. EVALUATION WORK	9
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	9
3. CERTIFICATION.....	10
3.1. CONCLUSION	10
3.2. RESTRICTIONS.....	10
3.3. RECOGNITION OF THE CERTIFICATE.....	11
3.3.1. <i>European recognition (SOG-IS)</i>	11
3.3.2. <i>International common criteria recognition (CCRA)</i>	11
ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....	12
ANNEX 2. EVALUATED PRODUCT REFERENCES	13
ANNEX 3. CERTIFICATION REFERENCES	14

1. The product

1.1. Presentation of the product

The evaluated product is the appliance MISTRAL TRC 7535 V4.6.1 developed by Thales Communications.

The MISTRAL TRC 7535 is an appliance performing encryption and authentication allowing the protection of information exchanged within local area network (LAN) or through local networks interconnection on a wide area network (WAN). Based on VPN technologies (Virtual Private Network), the appliance offers several security services required for any security application used over IP network.

The product is built mainly to address and secure corporate, banking or governmental networks.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

The certified version of the product can be identified by the following elements:

- The hardware appliance TRC 7535 version 4, including an specific electronic card with a serial and Ethernet interfaces, a card reader (CAM), and an interface for emergency deletion of critical assets,
- The VPN IP software version 4.6.1.2 embedded in the appliance,
- The software embedded in the cryptographic module (FPGA) AES v2.0,
- The software for remote administration (CGM) version 6.1.2 that communicates with a front-end appliance MISTRAL TRC 7535, allowing the protection of communication between the CGM and other Mistral appliances.

These elements can be checked by the users: the appliance is physically labelled with its type and reference of the embedded cryptographic module, and the CGM allows checking the version of the embedded software in any Mistral appliance.

1.2.2. Security services

The product provides mainly the following security services:

- Configuration management,
- Security policy and security associations management,
- Keys management,
- Clear text flows management,
- Flows filtering,
- Flows encryption,
- Remote administration,
- Alarm management,

- Serial port access control,
- CAM access control,
- Emergency deletion,
- Management of the flows with roaming users.

1.2.3. Architecture

The appliance is made of the elements identified in §1.2.1 used within the following typical network architecture:

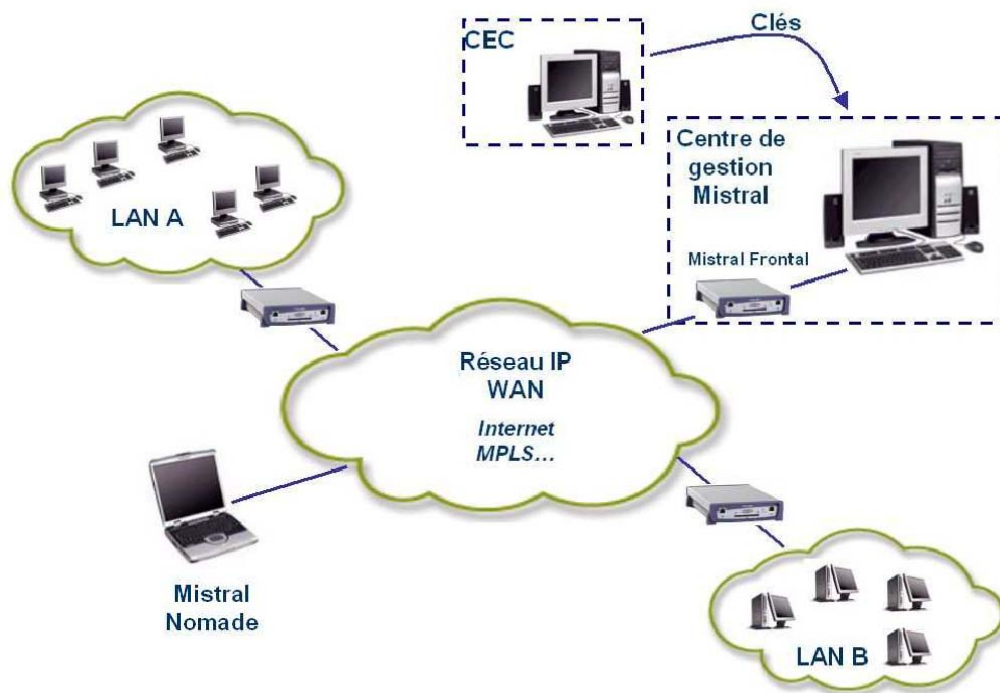


Figure 1 – Typical architecture

On this picture, different optional equipments are identified, that are not included in the scope of evaluation:

- The software for roaming users;
- The key management facility (CEC) allowing the generation of certified keys for the system.

The functionalities of this architecture are described in the security target [ST] and in guidance of the appliance and of the CGM (cf. [GUIDES]).

1.2.4. Life cycle

The product's life cycle is the following:

- The cryptographic source code is developed by Thales Communications on its premises in Colombes,
- The product is designed and developed by Thales Communications on its premises in Cholet,
- The assembly of the final product is performed by a sub-contractor,
- The final products are sent back to Thales Communications (Cholet) that can check the integrity of the products before final delivery to customers.

1.2.5. Evaluated configuration

This certificate covers the Mistral appliance used with AES encryption algorithm, and managed by the software CGM v6.1.2, the latter being protected by a front-end Mistral appliance, as shown in figure 1.



2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].

2.2. Evaluation work

The evaluation relies on the evaluation results of the MISTRAL TRC 7535 version 4.5.2.2 product certified in 2005 under the reference 2005/13 (cf. [2005/13]).

The evaluation technical report [ETR], delivered to DCSSI the 5th of March 2008, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are “**pass**”.

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has been analysed by DCSSI. The results are stated in the cryptographic analysis report [ANA-CRY] and have been taken into account in the evaluator vulnerability analysis that did not evidence any exploitable vulnerability.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product “Appliance MISTRAL TRC 7535 V4.6.1” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 3 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the operational environmental security objectives summarized in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

Trusted Administrators

- The administrators of the product shall be trusted and shall be appropriately trained.

Enforcing the security policy

- The administrators shall be trained and be aware of security. They shall apply the information system security policy and check on a regular basis the conformity of encryption and filtering rules enforced by the product with this security policy.

Physical access control to the product

- The organism shall put the product in a secure environment preventing from any unauthorized physical access.

Physical access control to the CAM

- The CAM shall be protected in term of unauthorized physical access.

Keys renewal

- The organism shall renew on a regular basis cryptographic keys used in the product, using the CGM for that purpose.

Physical access control to the CGM

- The organism shall put the CGM in a secure environment preventing from any unauthorized physical access.

Physical access control to the CEC

- The organism shall put the CEC in a secure environment preventing from any unauthorized physical access.

Installation at a point of convergence of networks

- The organism shall install the product at the separation point between the networks to be protected, in order to ensure that no network stream can bypass the product.

Secure channel between the CGM and the product



- The CGM configures the Mistral appliances through a front-end Mistral, in order to use the latter to protect the administrative flow. The front-end Mistral is directly connected to the CGM.

Software environment hosting the hyperterminal

- The terminal used to configure the product through the “consol” port shall be protected from any hardware or software device (key logger, trojan...) that could allow capturing secrets elements of the product configuration, during its local configuration (base key, traffic key...)¹.

Logical protection of the CGM workstation

- The users shall be authenticated on the CGM workstation before using the CGM software.

Connexion between the CGM workstation and the front-end Mistral appliance

- The CGM workstation shall be connected directly to the front-end Mistral appliance.

In addition, for any product offering VPN services, the DCSSI recommends to use the product in tunnel mode only.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement², of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:



3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries³, of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:



¹ The configuration through remote administratio/CAM administration shall be the preferred one.

² The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

³ The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Classe	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Name of the component
ACM Configuration management	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 Delivery and operation	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 Development	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 Guidance	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 Life-cycle support	ALC_DVS			1	1	1	2	2	1	Identification 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 Vulnerability assessment	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



Annex 2. Evaluated product references

[2005/13]	Certification report 2005/13 - Boîtier MISTRAL TRC 7535 version 4.5.2.2, 30 May 2005, SGDN/DCSSI.
[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> - Cible de sécurité Mistral (CDS) MISTRAL TRC735 EAL3+, Reference: 61 485 069 – 805 revision L Thales Communications <p>For the needs of publication, the following security target has been provided and validated in the evaluation:</p> <ul style="list-style-type: none"> - Cible de sécurité Mistral (CDS) MISTRAL TRC735 EAL3+ - version Lite, Reference: 61 485 069 – 805 revision M Thales Communications
[ETR]	Rapport Technique d'Evaluation, Projet SIROCCO2, Reference: 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), Reference: 62 061 737- 567, révision –B Thales Communications
[GUIDES]	<ul style="list-style-type: none"> - TRC 7535 Mistral v4.6.1, Manuel utilisateur (SUM), Reference: 61 484 290 AF, 108 fr révision A – (février 2008) Thales Communications - Centre de Gestion Mistral, Manuel utilisateur (CGM_SUM), Reference: 46 250 239 05 – 108 Ind –E (juillet 2007) Thales Communications

Annex 3. Certification references

Decree number 2002-535 dated 18 th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, 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. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international 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]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14 th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR