Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/13

Boîtier MISTRAL TRC 7535 version 4.5.2.2

Paris, le 30 mai 2005

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/13

Produit : Boîtier MISTRAL TRC 7535 version 4.5.2.2

Développeur(s) : Thalès Communications

Critères Communs version 2.2

EAL3 Augmenté
(ADV_LLD.1*, ADV_IMP.1*, ALC_FLR.3, ALC_TAT.1, AVA_VLA.2)
*appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

Commanditaire : Thalès Communications

Centre d'évaluation : Oppida

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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle 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 :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle 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] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.
[2] En novembre 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède et la Turquie.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le boîtier de chiffrement MISTRAL TRC 7535 en version 4.5.2.2 développé par Thalès Communications.

1.2. Développeur

Thalès Communications

160 Boulevard de Valmy,
BP82,
92704 Colombes Cedex.

et

Thalès Communications

110 avenue du Maréchal Leclerc
49300 Cholet.

1.3. Description du produit évalué

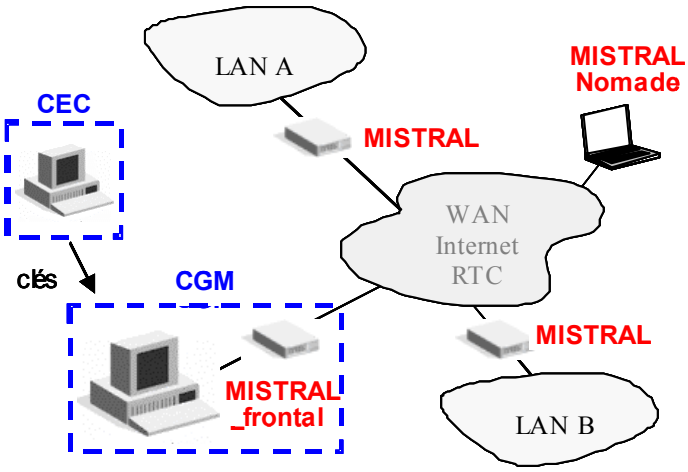
1.3.1. Architecture

Le produit est constitué des 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 4.5.2.2 embarqué dans le boîtier ;
- le logiciel embarqué dans de la ressource cryptographique (FPGA) 3DES v1.0, ou AES v1.0 ;
- le système d'exploitation PSOS (hors périmètre).

Il s'agit d'un équipement de chiffrement des réseaux IP sensibles. Placé en coupure sur le réseau, il chiffre (et déchiffre) les données échangées avec l'extérieur. Il possède également une fonction de filtrage simple pour protéger les équipements internes. Le chiffrement s'effectue avec l'algorithme AES ou 3DES.

Le boîtier s'utilise au sein d'une architecture du type :



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

- le logiciel Mistral nomade ;
- le centre de Gestion Mistral (CGM) qui permet d'administrer un ensemble de boîtiers Mistral ;
- 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 [GUIDES], ainsi que dans le guide d'utilisation du CGM [CGM].

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

- la partie cryptographique du code du produit est développée par Thalès Communications sur le site de Colombes ;
- le produit est développé par Thalès Communications sur le site de Cholet ;
- l'assemblage du produit est délégué à un sous-traitant ;
- les produits assemblés sont ensuite renvoyés à Thalès Communications (site de Cholet), qui peut vérifier l'intégrité du produit avant livraison aux clients finaux.

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend 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 4.5.2.2 embarqué dans le boîtier ;
- le logiciel embarqué dans une ressource cryptographique (FPGA), 3DES v1.0, ou AES v1.0.

Les éléments suivants ne font donc pas partie du périmètre d'évaluation :

- le système d'exploitation PSOS ;
- le centre de Gestion Mistral (CGM) et le logiciel Mistral nomade ;
- le centre d'élaboration de clés (CEC).

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Commanditaire

Thalès Communications

160 Boulevard de Valmy
BP82
92704 Colombes Cedex

2.3. Centre d'évaluation

Oppida

4-6 avenue du vieil étang
Bâtiment B
78180 Montigny le Bretonneux

Adresse électronique : cesti@oppida.fr

2.4. Rapport technique d'évaluation

L'évaluation s'est déroulée du 7 octobre 2004 au 25 mai 2005.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.5. Evaluation de la cible de sécurité

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

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		Verdicts
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite

ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.6. Evaluation du produit

2.6.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL3[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL3	Methodically tested and checked
+ ADV_LLD.1[2]	Descriptive low-level design
+ ADV_IMP.1[2]	Subset of the implementation of the TSF
+ ALC_FLR.3	Systematic flaw remediation
+ ALC_TAT.1	Well-defined development tools
+ AVA_VLA.2	Independent vulnerability analysis

2.6.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

Thalès Communications

160 Boulevard de Valmy
BP82
92704 Colombes Cedex

et

Thalès Communications

110 avenue du Maréchal Leclerc

49300 Cholet

L'assemblage du produit est sous-traité, mais cette étape n'est pas considérée comme une phase sensible du développement.

L'évaluateur a confirmé que les mesures de sécurité définies pour l'environnement de développement du produit évalué sont définies.
La vérification de l'application des procédures analysées a été effectuée lors des visites des sites de Thalès Communications à Colombes et à Cholet (cf Annexe 1 et Annexe 2).

[1] Annexe 3 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].
[2] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

L'évaluateur a également vérifié que :
- le produit évalué est identifié de façon unique ;
- cette identification est indiquée sur le produit ;
- les éléments constitutifs du produit évalué sont identifiés de façon unique ;
- les éléments constitutifs du produit évalué sont gérés par un système de gestion de configuration. Le système garanti que seules des modifications autorisées sont appliquées au éléments constitutifs.

Des procédures de correction d'anomalies décrivent la manière dont toute anomalie découverte sera suivie et corrigée, ainsi que la diffusion des informations et corrections relatives à ces anomalies, tant que le produit est maintenu par le développeur. Ces procédures ont été évaluées, bien que le respect de ces procédures ne puisse pas être déterminé au moment de l'évaluation.

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_CAP.3	Authorisation controls	Réussite
ACM_SCP.1	TOE CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.1	Identification of security measures	Réussite
ALC_FLR.3	Systematic flaw remediation	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.6.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD)[1], implémentation (IMP)[1].

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :
- Security alarms (FAU_ARP.1),
- Potential violation analysis (FAU_SAA.1),
- Cryptographic key distribution (FCS_CKM.2),
- Cryptographic key destruction (FCS_CKM.4),
- Cryptographic operation (FCS_COP.1),
- Complete access control (FDP_ACC.2),
- Security attributes based access control (FDP_ACF.1),
- Subset information flow control (FDP_IFC.1),
- Simple security attributes (FDP_IFF.1),
- Import of user data without security attributes (FDP_ITC.1),
- Full residual information protection (FDP_RIP.2),
- Basic data exchange confidentiality (FDP_UCT.1),

[1] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

- Data exchange integrity (FDP_UIT.1),
- Authentication failures handling (FIA_AFL.1),
- User authentication before any action (FIA_UAU.2),
- User identification before any action (FIA_UID.2),
- Management of security functions behaviour (FMT_MOF.1),
- Management of security attributes (FMT_MSA.1),
- Secure security attributes (FMT_MSA.2),
- Static attribute initialisation (FMT_MSA.3),
- Management of TOE security functions data (FMT_MTD.1),
- Security management roles (FMT_SMR.1),
- Anonymity (FPR_ANO.1),
- Abstract machine testing (FPT_AMT.1),
- Inter-TSF confidentiality during transmission (FPT_ITC.1),
- Inter-TSF detection of modification (FPT_ITI.1),
- Replay detection (FPT_RPL.1),
- Manual recovery (FPT_RCV.1),
- TSF testing (FPT_TST.1),
- Trusted Path (FTP_TRP.1).

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_FSP.1	Informal functional specification	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1[1]	Descriptive low-level design	Réussite
ADV_IMP.2[1]	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.6.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit sur le site de Cholet le 27 Avril 2005.

Ces procédures spécifient la procédure sécurisée de livraison du produit aux clients.

L'installation du produit correspond à la phase d'utilisation du produit. Les procédures analysées [GUIDES] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.1	Delivery procedures	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

[1] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

2.6.5. L'évaluation de la documentation d'exploitation

Du point de vue de l'évaluation, les administrateurs sont :

- les personnes en charge de l'installation et de la configuration des boîtiers Mistral, ainsi que du démarrage du boîtier. Elles s'authentifient par CAM « utilisateur ». Les guides livrés à ces administrateurs [GUIDES] ont été fournis pour évaluation ;
- le mainteneur du produit qui est un personnel de Thalès pouvant mettre à jour les logiciels du produit sur site ou après retour usine, en s'authentifiant à l'aide de CAM « téléchargement logiciel et téléchargement cryptographique ».

Du point de vue de l'évaluation, les utilisateurs sont les personnes transmettant des données via le VPN mis en place par les administrateurs. L'usage du VPN est transparent pour les utilisateurs et il n'y a donc pas de guide utilisateur spécifique.
Le logiciel d'administration CGM ne fait pas partie du périmètre d'évaluation. Il a néanmoins été installé sur la plate-forme de test pour les besoins de l'évaluation. Le guide administrateur utilisé pour son installation et son utilisation est donné sous la référence [CGM].

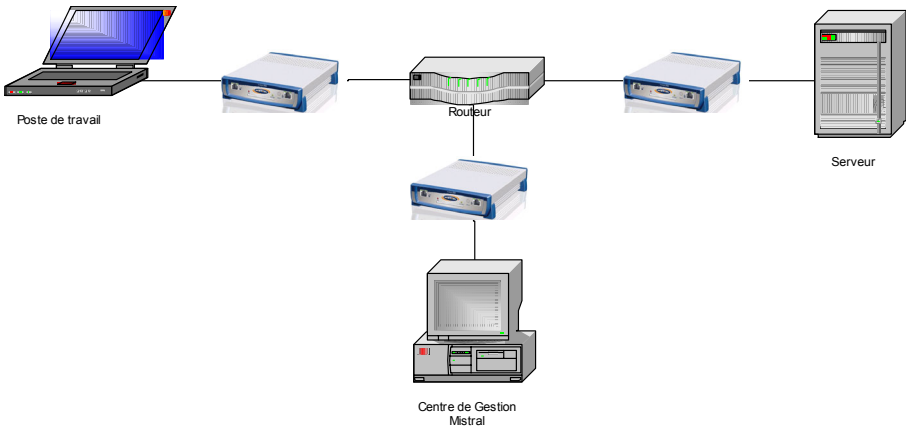
Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.6.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.
L'évaluateur a réalisé ses tests fonctionnels indépendants sur la plate-forme suivante :



La plate-forme est constituée d'un routeur constituant le réseau non sécurisé, d'une plate-forme d'administration protégée par un boîtier Mistral en coupure, de deux réseaux sensibles (un avec un serveur, l'autre avec un poste de travail), chacun étant protégé par un boîtier Mistral en coupure, de références suivantes :

- Boîtier TRC 7535 v4
- Logiciel embarqué v1 (AES et 3DES)
- Logiciel VPN IP 4.5.2.2

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		Verdicts
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.6.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Seule la fonction de protection par mot de passe de l'accès console (pour l'administration locale du boîtier) a fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de cette fonction est jugé élevé : SOF-high.

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit. L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
Cette analyse a été complétée par des tests sur la plate-forme décrite au paragraphe 2.6.6.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau élémentaire.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		Verdicts
AVA_MSU.1	Examination of guidance	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent vulnerability analysis	Réussite

2.6.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation, décrits dans le rapport technique d'évaluation [RTE], permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

3.3. Exigences pour l'environnement d'exploitation

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [GUIDES] :

Administrateur de confiance

- L'organisme doit recruter des personnels de confiance comme administrateurs du produit et les former à l'utilisation du produit.
- Les administrateurs du produit 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 le produit 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, ceci 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.

Environnement logiciel hébergeant l'hyperterminal

- 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 de base, clé de trafic,...)[1].

3.4. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.5. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4.

[1] On privilégiera la configuration par télégestion/CAM plutôt que l'administration locale par console.

Annexe 1. Visite du site de développement de la société Thalès Communications à Cholet

Le site de développement de la société Thalès Communications situé au 110, avenue du Maréchal Leclerc, 49300, Cholet, a fait l'objet d'une visite par l'évaluateur le 27 avril 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le boîtier de chiffrement MISTRAL TRC 7535 en version 4.5.2.2.

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_CAP.3 ;
- ALC_DVS.1 ;
- ADO_DEL.1 ;
- ALC_FLR.3.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. Visite du site de développement de la société Thalès Communications à Colombes

Le site de développement de la société Thalès Communications situé au 160 Boulevard de Valmy, BP82, 92704 Colombes Cedex, a fait l'objet d'une visite par l'évaluateur le 24 mai 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le boîtier de chiffrement MISTRAL TRC 7535 en version 4.5.2.2.

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_CAP.3 ;
- ALC_DVS.1 ;
- ADO_DEL.1 ;
- ALC_FLR.3.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 3. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 4. Références documentaires du produit évalué

[CGM]	Manuel utilisateur – Centre de gestion Mistral version 5.2, Référence : 46 250 239 05 - 108 – ind-A-fr, Thalès Communications
[CONF]	Chapitre 6, paragraphe 1.3 et 3.1 du document : Mistral VS5.2 – Plan de développement équipement, Référence : 56 685 952 01 – 311, révision –B du 31/01/2005 Thalès Communications
[GUIDES]	TRC 7535 – Mistral v4.5.2 - Manuel Utilisateur, Référence : 61 484 290AC – 108 – fr rev C, Thalès Communications
[RTE]	Rapport Technique d'Evaluation, Référence : OPPIDA/CESTI/SIROCCO/RTE/1 Oppida
[ST]	Mistral TRC 7535 – Cible de sécurité (CDS) - EAL3+, Référence : 61 485 069 code 805, révision H, Thalès Communications
[Visite]	Visite relative aux livraisons : • Rapport intermédiaire ADO_DEL, Référence : OPPIDA/CESTI/SIROCCO/ADO_DEL/4.0 Oppida Visite relative à la sécurité du développement : • Rapport intermédiaire ALC_DVS, Référence : OPPIDA/CESTI/SIROCCO/ALC_DVS/4.0 Oppida Visite relative à la procédure de gestion des anomalies : • Rapport intermédiaire ALC_FLR, Référence : OPPIDA/CESTI/SIROCCO/ALC_FLR/3.0 Oppida

Annexe 5. 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: Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[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.

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
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr