Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Schéma français

d'évaluation et de certification

de la sécurité des technologies de l'information

Rapport de certification 2002/26

M>Tunnel 2.5

Février 2003

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

CERTIFICAT 2002/26

M>Tunnel 2.5

(référence MT25-B43-08)

Développeur : EADS Telecom

Critères Communs

EAL2 Augmenté

(ADV_HLD.2, ALC_LLD.1*, AVA_VLA.2)

*appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

Commanditaire : EADS Telecom

Centre d'évaluation : AQL - Groupe Silicomp

Le 7 février 2003,

Le Directeur central de la sécurité
des systèmes d'information
Henri Serres

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information publié au journal officiel de la République française le 19 avril 2002.

Ce produit a été évalué par un centre d'évaluation de la sécurité des TI conformément aux Critères Communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée du produit dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Chapitre 1

Présentation

Executive Summary

1.1 Objet

Purpose

1 Ce document est le rapport de certification du produit "M>Tunnel 2.5"

This document is the certification report of the "M>Tunnel 2.5" product

2 Ce produit est développé par la société EADS Telecom :

The developer of the target of evaluation is EADS Telecom:

- EADS Telecom
  Rue Jean-Pierre Timbaud
  PC26B
  78392 Bois d'Arcy Cedex
  France.

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

This evaluation has been performed in conformance with Common Criteria [CC] and with the methodology defined in the CEM [CEM].

4 La cible d'évaluation atteint le niveau d'assurance EAL 2 augmenté des composants d'assurance suivants tirés de la partie 3 des Critères Communs :

The target of the evaluation reaches the EAL 2 assurance level augmented with the following Common Criteria Part 3 components:

- ADV_HLD.2 "Security enforcing high-level design",
- ADV_LLD.1* "Descriptive low-level design",
- AVA_VLA.2 "Independant vulnerability analysis",

* Le composant ADV_LLD.1 a été appliqué au sous-ensemble de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS "Cryptographic support".

** The ADV_LLD.1 component has been applied to the part of the TOE that responds to the functional requirements of the FCS class "Cryptographic support".*

1.2 Contexte de l'évaluation

Evaluation Context

5 L'évaluation s'est déroulée de juin 2002 à novembre 2002.

The evaluation has been carried out from June 2002 to November 2002.

6 Le commanditaire de l'évaluation est EADS Telecom :

The sponsor of the evaluation is EADS Telecom:

- EADS Telecom
  Rue Jean-Pierre Timbaud
  PC26B
  78392 Bois d'Arcy Cedex
  France.

7 L'évaluation a été réalisée par le Centre d'Evaluation de la Sécurité des Technologies de l'Information de AQL - Groupe Silicomp :

The evaluation has been performed by the Information Technology Security Evaluation Facility of AQL - Groupe Silicomp:

- AQL - Groupe Silicomp
  Rue de la Châtaigneraie
  B.P. 51766
  78392 Cesson-Sevigné cedex
  France.

Chapitre 2

Description de la cible d'évaluation

Description of the Target of Evaluation

2.1 Périmètre de la cible d'évaluation

Scope of the Target of Evaluation

8 La cible d'évaluation est le produit "M>Tunnel 2.5", ce produit permet la création de réseaux privés virtuels (VPN). Le produit est constitué des éléments suivants :

The target of evaluation is the "M>Tunnel 2.5" product, this product ensures the creation of virtual private networks (VPN). The product consists of the following elements:

- Le M>Tunnel Master est le point de configuration central du réseau privé virtuel. Sur le M>Tunnel Master sont définies les informations sur la configuration et les groupes d'accès.

  The M>Tunnel Master is the central configuration point of the virtual private network. The informations related to configuration and access groups are defined on the M>Tunnel Master.

- Les M>Tunnel Gateways sont les extrémités du tunnel pour les réseaux auxquels ils sont connectés. Dans la configuration d'une organisation de réseaux privés virtuels, les M>Tunnel Gateways téléchargent les informations de configuration à partir du M>Tunnel Master et créent les politiques de tunnel.

  M>Tunnel Gateways are the tunnel's edges for the networks to which they are connected. In the configuration of virtual private networks, M>Tunnel Gateways download configuration informations from M>Tunnel Master and create the tunnel's policies.

- Les M>Tunnels Clients téléchargent des informations à la fois à partir du M>Tunnel Master et des M>Tunnel Gateways : à partir du M>Tunnel Master, les informations relatives aux certificats (autorité de certification, liste de révocation) et la liste des M>Tunnel Gateways en cohérence avec le groupe d'accès de l'utilisateur ; à partir des M>Tunnel Gateways, les politiques M>Tunnel.

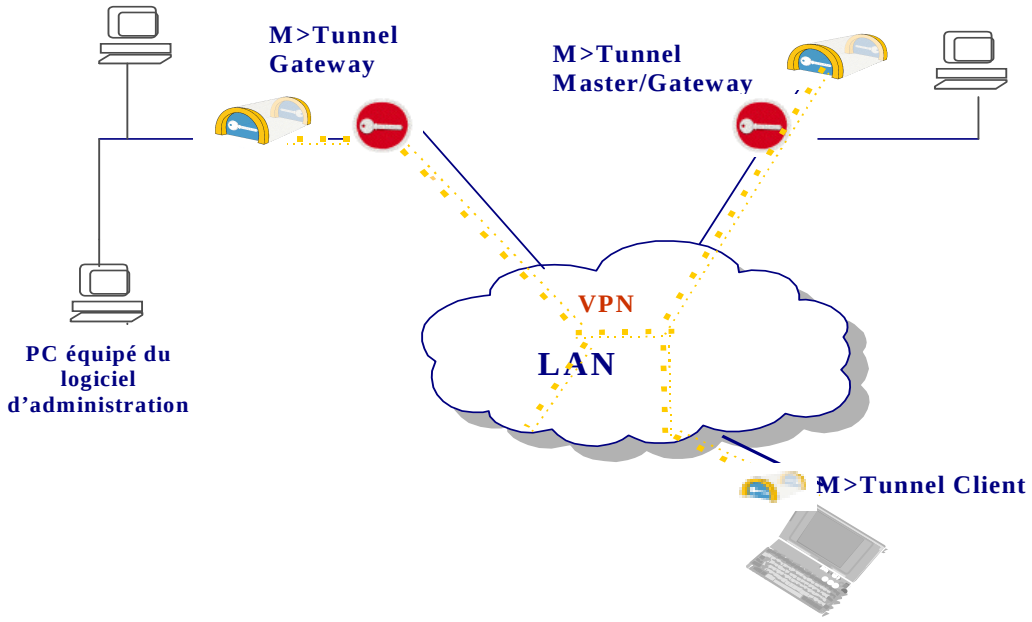
  M>Tunnel Clients download informations from the M>Tunnel Master and from M>Tunnel Gateways: from the M>Tunnel Master, informations related to certificates (certification authority, revocation list) and the M>Tunnel Gateways' list compliant with the user's access group; from the M>Tunnel Gateways, the M>Tunnel policies.

- Le logiciel d'administration M>Admin permet la gestion des équipements M>Tunnel Master et M>Tunnel Gateway ainsi que l'administration de la politique de chiffrement.

  The administration software ensures the management of M>Tunnel Master and M>Tunnel Gateway equipment as well as the administration of the ciphering policy.

9 Le schéma suivant montre un exemple de répartition de ses différents éléments de la cible d'évaluation :

The diagram below shows and example of the organisation of the different elements of the TOE:



10 Les tunnels VPN sont établis de M>Tunnel Gateway à M>Tunnel Gateway ou de M>Tunnel Gateway à M>Tunnel Client. Au niveau de chaque M>Tunnel Gateway, les fonction de sécurité mettent en oeuvre une politique de filtrage (autorisation/ refus) et de chiffrement des paquets sur la base des adresses IP, des numéros de protocole (ICMP, UDP, TCP,...) et des numéros de ports (TCP/UDP) des paquets, ainsi que des champs des certificats numériques présentés par les M>Tunnel Gateways ou les M>Tunnel Clients.

The VPN tunnels are established from M> Tunnel Gateway to M> Tunnel Gateway or from M> Tunnel Gateway to M> Tunnel Client. On each M>Tunnel Gateway, security functions operate filtering policy (authorization/refusal) and cyphering policy based on IP addresses, protocol number (ICMP, UDP, TCP,...) and packet's port numbers (TCP/UDP), as well as the numeric certificates' fields submitted by the M> Tunnel Gateways or the M> Tunnel Clients.

2.2 Identification des éléments de la cible d'évaluation

Identification of the TOE's elements

11 La cible d'évaluation correspond aux versions suivantes des différents éléments :

The TOE corresponds to the following versions of the different elements:

- M>Tunnel Master & M>Tunnel Gateway (MTG25B4308) avec les patchs (MCO13B4302, MTG25B4301, MTG25B4302, MTG25B4303, MTG25B4304) et leur système d'exploitation BSD/OS 4.3 (bsdi-i386-4.3-01) ;

  M>Tunnel Master & M>Tunnel Gateway (MTG25B4308) and patches (MCO13B4302, MTG25B4301, MTG25B4302, MTG25B4303, MTG25B4304) and their operating system BSD/OS 4.3 (bsdi-i386-4.3-01) ;

- M>Tunnel Client (MTC254W3202) pour Windows 2000 ;
  M>Tunnel Client (MTC254W3202) for Windows 2000 ;

- M>Admin (MAD401JVA02) pour Windows 2000.
  M>Admin (MAD401JVA02) for Windows 2000.

2.3 Mode d'utilisation de la cible d'évaluation

Target of Evaluation Mode of Operation

12 La cible d'évaluation est évaluée dans la configuration suivante :

The target of evaluation is evaluated in following configuration:

- 1 M>Tunnel Master installé sur le même ordinateur qu'un M>Tunnel Gateway ;
  1 M>Tunnel Master installed on the same computer than a M>Tunnel Gateway;
- 2 M>Tunnel Gateways installés chacun sur un ordinateur équipé de la version du système d'exploitation BSD/OS 4.3 fournie par EADS Telecom ;
  2 M>Tunnel Gateways installed on computer equipped with the version of the BSD/OS 4.3 operating system delivered by EADS Telecom;
- 1 M>Tunnel Client installé sur un poste nomade équipé du système d'exploitation Windows 2000 (version 5.0.2195 Service Pack 2) et d'un lecteur de carte à puce ;
  1 M>Tunnel Client installed on a laptop computer equipped of the Windows 2000 (version 5.0.2195 Service Pack 2) operating system and a smart card reader;
- Le logiciel d'administration, couplé avec un M>Tunnel Client, installés sur un ordinateur équipé du système d'exploitation Windows 2000 (version 5.0.2195 Service Pack 2) et d'un lecteur de carte à puce.
  The administration software, linked with a M>Tunnel Client, installed on a computer equipped of the Windows 2000 (version 5.0.2195 Service Pack 2) operating system and a smart card reader.

2.4 Fonctions de sécurité

Security Functions

13 Les fonctions de sécurité de la cible d'évaluation sont décrites dans la cible de sécurité [ST], elles concernent les points suivants :

The security functions of the target of evaluations are described in the security target [ST], they deal with the following points:

- Politique de chiffrement et de filtrage basée sur l'adresse IP, le numéro de protocole, les ports source et destination des paquets mettant en œuvre les fonctions suivantes, selon le paramétrage :

  Cyphering and filtering policy based on IP dress, protocol number, source and destination ports of packets doing the following function, depending on parameters:

  - identification et authentification de chaque extrémité d'un tunnel par émission de certificat X.509 et utilisation d'un protocole de défi mutuel (challenge / response) ;

identification and authentication of each tunnel edge by a X.509 certificate emission and the use of a challenge/response protocol;

- génération de clés de session automatisée et sécurisée sur la base des aléas du challenge / response ;
  automatic and secured session key generation based on challenge response random numbers;
- renégociation périodique de la clé de session à l'initiative de l'une ou l'autre des extrémités du tunnel, en fonction du temps écoulé et/ou du volume échangé ;
  session key periodic renegotiation order by one or the other edge of the tunnel related to time or volume of information;
- authentification (intégrité) ;
  authentication (integrity);
- chiffrement (confidentialité) ;
  cyphering (confidentiality);
- rejet de paquets si la politique ne les autorise pas ;
  packets rejecting if not authorized by the policy;

- Protection des sessions d'administration à distance du M>Tunnel Master et des M>Tunnel Gateways par chiffrement et authentification des paquets ;

  M>Tunnel Master and M>Tunnel Gateways distant administration session protection by cyphering and authentication of packets;

- Identification et authentification des administrateurs par login / mot de passe ;

  Administrators identification and authentication by login/password;

- Contrôle d'accès aux fonctions d'administration :

  Access control to administration functions:

  - démarrage des logiciels M>Tunnel Master et M>Tunnel Gateway ;
    M>Tunnel Master and M>Tunnel Gateway start-up;
  - gestion des politiques de chiffrement et de filtrage ;
    cyphering and filtering policies management;
  - mise à jour des CRL ;
    CRL update;

- Imputabilité et audit :

  Imputability and audit:

  - enregistrement des événements relatifs à la sécurité et des données d'imputabilité associées (adresses IP ou identifiants utilisateurs) ;
    recording of security events and relative data (IP address or users identificators);
  - protection des fichiers d'événements contre les modifications non autorisées et le bourrage ;
    events files protection against unauthorized modification and jamming;
  - filtrage pour l'audit des événements ;
    filtering for events audit;

- Stockage sécurisé des fichiers de politique de chiffrement et de filtrage, des CRL et des fichiers de configuration ;

Secured storage of cyphering and filtering policies files, CRL and configuration files;

- Chiffrement et détection des modifications des fichiers de politique de chiffrement et de filtrage, des CRL et des fichiers de configuration lors de leur transit entre deux composants ;

  Cyphering and detection of the modification of cyphering and filtering policies files, CRLs and configuration files when going from one component to another;

- Auto-vérification au démarrage de l'intégrité des fichiers exécutables des logiciels M>Tunnel Master, M>Tunnel Gateway et M>Tunnel Client.

  Start-up self-verification of the integrity of M>Tunnel Master, M>Tunnel Gateway and M>Tunnel Client executable files.

2.5 Guides d'utilisation

Guidance Document

14 Les guides d'utilisation et d'administration de la cible d'évaluation disponibles sont :

The available guidance documents of the target of evaluation are:

- M>Tunnel Administrator's Guide V2.5, réf: 200-400-2002005 du 01/10/ 2002,
- M>Tunnel System Administration Guide V2.5, réf: 200-400-2002-006 du 04/11/2002,
- User guide, aide en ligne M>Tunnel Client, réf: 200-400-2002025 du 06/11/ 2002.

Chapitre 3

Résultats de l'évaluation

Evaluation Results

3.1 Exigences de sécurité d'assurance

Security Assurance Requirements

15 La cible d'évaluation a été évaluée au niveau EAL 2 augmenté des composants d'assurance suivants, tirés de la partie 3 des Critères Communs [CC] : ADV_HLD.2, ADV_LLD.1* et AVA_VLA.2.

The target of evaluation has been evaluated at the EAL2 assurance level augmented with the following Common Criteria Part 3 components: ADV_HLD.2, ADV_LLD.1 and AVA_VLA.2.

Assurance class	Assurance components
Security Target	ASE Security target evaluation
Configuration management	ACM_CAP.2 Configuration items
Delivery and operation	ADO_DEL.1 Delivery procedures ADO_IGS.1 Installation, generation , and start-up procedures
Development	ADV_FSP.1 Informal functional specification **>ADV_HLD.2 Security enforcing high-level design** **>ADV_LLD.1 Descriptive of low-level design, limited to the part of the TOE implementing FCS functional requirements** ADV_RCR.1 Informal correspondance demonstration
Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_SOF.1 Strength of TOE security functions **>AVA_VLA.2 Independent vulnerability analysis**

> EAL2 augmentations

16 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.

For all the above assurance requirements, a «pass» verdict has been issued by the evaluator.

17 Les travaux d'évaluation qui ont été menés sont décrits dans le Rapport Technique d'Evaluation [RTE].

The evaluation tasks which have been done are described in the Evaluation Technical Report [RTE].

18 Le niveau de résistance des fonctions s'appuyant sur des mécanismes de nature probabilistique ou permutationnelle de la cible d'évaluation, composant AVA_SOF, est élevé (SOF-high).

The strength of probabilistic and permutational mechanisms of the TOE, AVA_SOF component, is SOF-high.

19 Les mécanismes de nature cryptographique ont été évalués par la Direction centrale de la sécurité des systèmes d'information. Ils sont compatibles avec le niveau de résistance visé.

The cryptographic mechanisms have been evaluated by the Direction Centrale de la Sécurité des Systèmes d'Information. Their strength is compatible with the level to be reached.

3.2 Tests fonctionnels et de pénétration

Functional and penetration testing

20 Le développeur a fourni sa documentation de test fonctionnel du produit.

The developer of the target of evaluation has provided its test documentation.

21 L'évaluateur a réalisé de son côté des tests fonctionnels pour s'assurer par échantillonnage que les fonctions de sécurité fonctionnent effectivement.

The evaluator has performed independent tests to check by sampling that the TOE security functions perform as specified.

22 L'évaluateur a mené une analyse de vulnérabilités, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élémentaire (composant AVA_VLA.2) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation. Ces objectifs sont décrits dans la cible de sécurité [ST], ils concernent principalement les aspects suivants :

The evaluator lead a vulnerability analysis, confirmed by penetration testing, to ensure that an attacker with a low attack potential (AVA_VLA.2 assurance requirements) cannot bypass the security objectives for the target of evaluation. These security objectives are described in the security target [ST], it can be summarised as follow:

- la cible d'évaluation ne met en oeuvre un tunnel que pour les utilisateurs autorisés,
  a tunnel can only be initialized by the TOE for authorized users
- la cible d'évaluation doit appliquer les politiques de chiffrement et de filtrage définie par l'administrateur,
  the TOE must apply cyphering and filtering policies defined by the administrator,
- la cible d'évaluation ne permet qu'aux administrateurs autorisés d'utiliser les fonctions de sécurité du logiciel d'administration,
  the TOE only allows authorized administrators to use administration software security functions,
- la cible d'évaluation doit se protéger contre les actions non-intentionnelles de modification des mécanismes de sécurité,
  the TOE must protect itself against non-intentional actions on security mechanisms,
- la cible d'évaluation doit fournir une vérification de cohérence sur les politiques de chiffrement et de filtrage,
  the TOE must supply a coherence verification on cyphering and filtering policies,

- la cible d'évaluation doit pouvoir rejeter un paquet IP signé ayant été modifié,
  the TOE must be able to reject a signed IP packet that has been modified,
- la cible d'évaluation doit pouvoir chiffrer les paquets IP transitant sur le réseau,
  the TOE must be able to cypher IP packets passing through the network,
- la cible d'évaluation doit protéger le transfert des clés de session,
  the TOE must protect session key transfer,
- la cible d'évaluation doit empêcher un utilisateur d'un tunnel d'accéder aux informations transitant sur un autre tunnel,
  the TOE must prevent a tunnel user to access to information passing through another tunnel,
- la cible d'évaluation doit être capable de renouveler, automatiquement et de façon sûr, les clés de session selon des critères paramétrables,
  the TOE must be able to automatically and securely renew session keys according to defined criteria,
- M>Tunnel Gateway et M>Tunnel Master doivent pouvoir fonctionner même s'il n'y a plus de liaison avec la station d'administration,
  M>Tunnel Gateway and M>Tunnel Master must be able to work even if they are not connected to the administration station,
- la cible d'évaluation doit être capable de gérer les cas d'erreurs de manipulation lors de la mise en œuvre d'un tunnel ou lors de la négociation des clés de session,
  the TOE must be able to manage manipulation errors during the initialization of a tunnel or during session keys negotiation,
- toutes les informations liées aux politiques de chiffrement et de filtrage ainsi que la configuration et transitant sur un réseau non sûr doivent être sécurisées, ces informations doivent être stockées sur le poste de l'utilisateur et utilisées en cas de rupture de la communication avec le M>Tunnel Master.
  all the information linked to the cyphering and filtering policies, as well as the configuration passing through a non-reliable network must be secured, this information must be stored on the user's computer and used in case of communication failure with the M>Tunnel Master.

Chapitre 4

Certification

Certification

4.1 Verdict

Verdict

23 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL 2 augmenté des composants d'assurance suivants tirés de la partie 3 des Critères Communs [CC] :

The present report certifies that the target of evaluation satisfies to the requirements of the EAL 4 assurance level augmented with the following Common Criteria Part 3 components [CC]:

- ADV_HLD.2 "Security enforcing high-level design",
- ADV_LLD.1* "Descriptive low-level design",
- AVA_VLA.2 "Independent vulnerability analysis".

* Le composant ADV_LLD.1 n'a été appliqué qu'au sous-ensemble de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS "Cryptographic support".

** The ADV_LLD.1 component has been applied to the part of the TOE that responds to the functional requirements of the FCS class "Cryptographic support".*

4.2 Restrictions

Restriction

24 La cible d'évaluation doit être utilisée dans sa configuration précisée au chapitre 2 et conformément aux procédures d'utilisation et d'administration prescrites dans la cible de sécurité [ST].

The target of evaluation shall be used in the configuration described in the chapter 2 and shall be used in the environment described in the security target [ST].

25 Les recommandations du développeur exprimées dans les guides d'utilisation doivent impérativement être respectées.

The requirements present in the user and administrator guidance shall be respected.

26 La cible d'évaluation doit être configurée et utilisée avec les restrictions suivantes :

The target of evaluation must be configured and used with the following restrictions:

- les algorithmes de chiffrements utilisés sont Triple-DES ou AES ;
  the cryptographic algorithm used are Triple-DES or AES;
- le seuil de renégociation des clés est inférieur à 150.000 paquets ;
  the key renegotiation threshold is inferior to 150,000 packets;
- le service de sécurité ESP authentifié est utilisé ;
  ESP authenticated security service is used;

- le délai maximum de renégociation des clés est de 30 minutes.
  the maximimun delay for key renogotiation is 30 minutes.
- les modulos des clés publiques RSA, fournies par la PKI, doivent tous être différents,
  RSA public keys modulos, given by the PKI, must be different,
- sur toutes les Gateway et tous les clients l'option "bloquer le trafic inconnu" doit être activée,
  on all Gateways and on all clients, option "block unknown traffic" must be activated,
- sur tous les clients l'option "permettre la sauvegarder du code PIN de la carte" doit être désactivée,
  on all clients, option "rmember card PIN code" must be disabled,
- la politique de distribution des certificats doit exclure l'utilisation des tokens soft pour les clients,
  certificates distribution policy must exclude the use of soft tokens for clients,
- les groupes d'accès associés à chaque politique doivent refléter strictement les utilisateurs ayant le droit de négocier la politique,
  access groups associated to each policy must strictly identify the users having the right to negotiate that policy,
- les procédures de sécurité de l'environnement d'exploitation impliquent que les utilisateurs ayant accès aux données sensibles signalent le plus rapidement possible la perte ou le vol de leur carte et que le certificat que porte celle-ci soit révoqué dans les meilleurs délais au niveau du Master (mise à jour de la CRL),
  exploitation environment security procedures imply that users having access to sensitive data immediately inform loose or theft of their card and that the card certificate be revoked by the Master (CRL update),
- la configuration (paramètres) de M>Tunnel Client doit ne pouvoir être définie qu'au niveau de M>Admin par la fonctionnalité de déploiement associée à l'interface d'exploitation du Master,
  M>Tunnel Client parameters must only be defined from M>Admin with the deployment functionality of the Master exploitation interface,
- interdire la modification en local par l'administrateur du poste (flag 'userisadmin'),
  unable local modification by the computer administrator of the 'userisadmin' flag,
- au cas où des services applicatifs seraient installés sur les Gateways et accessibles sans utiliser IPSec (grâce à une politique de filtrage les autorisant explicitement), les mesures de sécurité appliquées aux logiciels qui fournissent ces services doivent garantir qu'ils ne peuvent servir à obtenir d'accès root sur les Gateways,
  in case of application service are installed on Gateways and accessible without using IPSec (explicitly authorized by a filtering policy), security measures applied to this application must guaranty that they cannot give a root access on Gateways,
- M>Tunnel Client s'appuyant sur des fonctionnalités de sécurité propres à Windows 2000, une vigilance particulière devra être accordée à la configuration des machines disposant d'un client M>Tunnel, pour qu'un utilisateur ne puisse pas obtenir des droits d'administration sur son ordinateur,
  as M>Tunnel Client relies on Windows 2000 security functionalities, computer configuration for M>Tunnel Clients must be carefully done, so the user cannot gain administrator rights on its computer,
- les services Qpopper et IMAPd sur les Gateways et le Master doivent être désactivés.
  Qpopper and IMAPd services on Gateways and Master must be disabled.

27 La version certifiée de la cible d'utilisation doit être configurée en respectant le guide de recommandations de mise en oeuvre de ces contraintes [CONT]

The certified version of the target of evaluation must be configured in conformance to the guide that specify how to set up theses restriction [CONT].

4.3 Certification

Certification

28 Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information, publié au journal officiel de la République française le 19 avril 2002.

This certificate is issued within the scope of the «décret 2002-535» of April 18th, 2002 dealing with the evaluation and the certification of the security provided by IT product and systems. The text of the «décret» was published april 19th, 2002 in the «journal officiel de la République française».

29 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

Certification is not in itself a recommendation of the product. It does not guaranty that the certified product is totally exempt of exploitable vulnerabilities: it still remains a residual probability that exploitable vulnerabilities have not been discovered: this probability is as low as the assurance level is high.

4.4 Reconnaissance internationale

International recognition

30 Afin de d'éviter les certifications multiples d'un même produit dans différents pays, il existe des accords de reconnaissance des certificats ITSEC et Critères Communs.

In order to avoid multiple certification of the same product in different countries, a mutual recognition of ITSEC and CC certificates was agreed.

31 Ce certificat répond aux exigences des accords suivants :

This certificate meets the requirements of the following agreements:

4.4.1 SOG-IS

32 L'accord SOG-IS [SOG-IS] sur la reconnaissance des certificats ITSEC est applicable depuis mars 1998. Cet accord a été signé par 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. Cet accord a ensuite été étendu aux certificats Critères Communs pour tous les niveaux d'évaluation (EAL1 - EAL7).

The SOGIS-Agreement [SOG-IS] on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates based on the CC was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

4.4.2 CC MRA

33 Un arrangement (Common Criteria Arrangement) [MRA] sur la reconnaissance des certificats basés sur les évaluations jusqu'au niveau EAL4 a été signé en mai 2000. Cet arrangement a été signé par l'Allemagne, l'Australie, l'Autriche, le Canada, l'Espagne, les Etats-Unis, la Finlande, la France, la Grèce, Israël (en novembre 2000), l'Italie, la Norvège, la Nouvelle-Zélande, les Pays-Bas, le Royaume-Uni et la Suède (juin 2002).

An arrangement (Common Criteria Arrangement) [MRA] on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. The arrangement was signed by the national bodies of Australia, Austria, Canada, Finland, France, Germany, Greece, Israel (november 2000), Italy, The Netherlands, New Zealand, Norway, Spain, Sweden (june 2002), United Kingdom and the United States.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	Addition d'un ou de plusieurs composants d'assurance de la partie 3 des CC à une échelle prédéfinie d'assurance ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou par son environnement.
Cible d'évaluation (TOE)	Produit ou système et documentation associée pour (administrateur et utilisateur) qui est l'objet d'une évaluation.
Cible de sécurité	Ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Paquet de composants d'assurance extraits de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	Ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

Références

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- Part 1 : Introduction and general model, august 1999, version 2.1, réf : CCIMB-99-031 ;
- Part 2 : Security functional requirements, august 1999, version 2.1, réf : CCIMB-99-032 ;
- Part 3 : Security assurance requirements, august 1999, version 2.1, réf : CCIMB-99-033.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

[ST] M>Tunnel 2.5 - cible de sécurité, version 1.16 du 4 novembre 2002, réf: 100-400-2002001, EADS Defence & Security Networks.

[CONT] M>Tunnel 2.5 - Contraintes d'emploi, version 1.1 du 07 janvier 2003, EADS Defence & Security Networks.

[RTE] Rapport Technique d'Evaluation, version 4.01 du 19 novembre 2002, réf: EAD001-RTE01-4.01, AQL - Groupe Silicomp.

[MRA] ARRANGEMENT on the Recognition of Common Criteria Certificates In the field of Information Technology Security, mai 2000.

[SOG-IS] «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification 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 07 SP

certification.dcssi@sgdn.pm.gouv.fr