PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-2009/29

Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ, version 8.0.1.1

Paris, le 29 juillet 2009

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

Le contre-amiral Michel Benedittini,
directeur général adjoint
[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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

Référence du rapport de certification

ANSSI-2009/29

Nom du produit

Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ

Référence/version du produit

Version 8.0.1.1

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 3 augmenté

ALC_CMC.4, ALC_CMS.4, ALC_FLR.3, AVA_VAN.3

Développeur(s)

NETASQ

3 rue Archimède, 59650 Villeneuve d'Ascq, France

Commanditaire

NETASQ

3 rue Archimède, 59650 Villeneuve d'Ascq, France

Centre d'évaluation

Silicomp AQL

1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France

Tél : +33 (0)2 99 12 50 00, mél : cesti@aql.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 :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ**,** version 8.0.1.1 **»** développée par la société NETASQ.

Ce produit offre des fonctionnalités de type firewall regroupant filtrage, détection d'attaques, gestion de la bande passante, gestion de la politique de sécurité, audit, imputabilité et authentification forte des utilisateurs. Il offre également des fonctionnalités VPN (*Virtual Private Network* – Réseau Privé Virtuel : chiffrement et authentification) implémentant le protocole ESP (*Encapsuling Security Payload*) en mode tunnel du standard IPSec, sécurisant ainsi la transmission de données entre des sites distants.

1.2. Description du produit

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

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Une étiquette, collée sur chacun des boîtiers, indique son modèle, son numéro de série, le code d'activation web du client et un code barre contenant ce même numéro de série.

Une autre étiquette, collée sur le carton d'emballage dans lequel se trouvent le boîtier et le CD-ROM contenant le logiciel d'administration, indique la version logicielle installée sur le firewall.

En se connectant via l'application Firewall Manager, fournie dans le CD-ROM d'installation du boîtier appliance, le Manager affiche à l'écran le modèle, le numéro de série et la version du boîtier. Le numéro de version du logiciel installé est indiqué par le logiciel d'administration en fond d'écran ainsi que dans le menu « Aide ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- le filtrage des flux entre les équipements ;
- l'identification et l'authentification des utilisateurs ;
- le chiffrement (au niveau VPN) ;
- l'établissement des associations de sécurité ;
- la journalisation, l'audit et les alarmes ;
- la prévention des intrusions ;
- le contrôle d'accès aux opérations d'administration de la sécurité ;
- la sauvegarde et la restauration ;
- la protection des sessions d'administration.

1.2.3. Architecture

La suite logicielle est composée des parties logicielles suivantes :

Composant	TAG
IPS-Firewall	8.0.1.1
Suite d'administration (Manager, Reporter, Monitor)	8.0.1

L'**IPS-Firewall** s'exécute sur un boîtier appliance connecté à la station d'administration distante au travers d'un réseau.

Le package **NETASQ Administration Suite (IHM)**, qui s'exécute sur la station d'administration, est constitué de trois interfaces graphiques :
- **NETASQ Unified Manager**, qui permet l'administration et la configuration des firewalls NETASQ ;
- **NETASQ Real-Time Monitor**, qui permet la supervision et le monitoring d'un ou plusieurs firewalls ;
- **NETASQ Event Reporter**, qui permet l'analyse des traces et le reporting.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :
- **Développement** : développement de la cible d'évaluation ;
- **Déploiement** : mise à disposition du produit aux clients ;
- **Installation** : conformité aux recommandations fournies par NETASQ ;
- **Exploitation** : suivi du produit au jour le jour lorsqu'il est en production avec remontée éventuelle de bugs ;
- **Rebus** : destruction d'un produit obsolète ou défaillant.

Seules les phases de développement et de déploiement (réalisées par NETASQ) ont été évaluées.
Les phases d'installation, d'exploitation et de rebus sont réalisées par le client.

Le produit a été développé sur le site suivant :

NETASQ

3 rue Archimède
59650 Villeneuve d'Ascq
France

L'évaluateur a considéré comme administrateurs du produit les personnes réalisant les opérations d'administration de la sécurité et responsables de leur exécution conformément aux guides [GUIDES], et comme utilisateurs du produit les personnes utilisant des ressources informatiques des réseaux de confiance protégés par le produit depuis d'autres réseaux de confiance ou depuis des réseaux non maîtrisés.

La définition des profils administrateurs est du ressort d'un administrateur spécial, le « super-administrateur », qui intervient exclusivement lors des phases d'installation et de maintenance et est le seul habilité à se connecter, via la console locale, sur les boîtiers. Il doit être le seul responsable de l'accès dans les locaux où sont stockés les boîtiers.

1.2.5. Configuration évaluée

La configuration évaluée correspond :

- au logiciel IPS-Firewall version 8.0.1.1 exécuté sur les modèles de boîtiers appliance firewall-VPN F200 et U250 ;
- à la suite d'administration NETASQ version 8.0.1 installée sur un poste de travail sous Windows XP SP3.

Les éléments constitutifs de la cible d'évaluation sont indiqués sur la figure suivante, aux côtés de l'ensemble de la plate-forme de test mise en œuvre par le développeur :

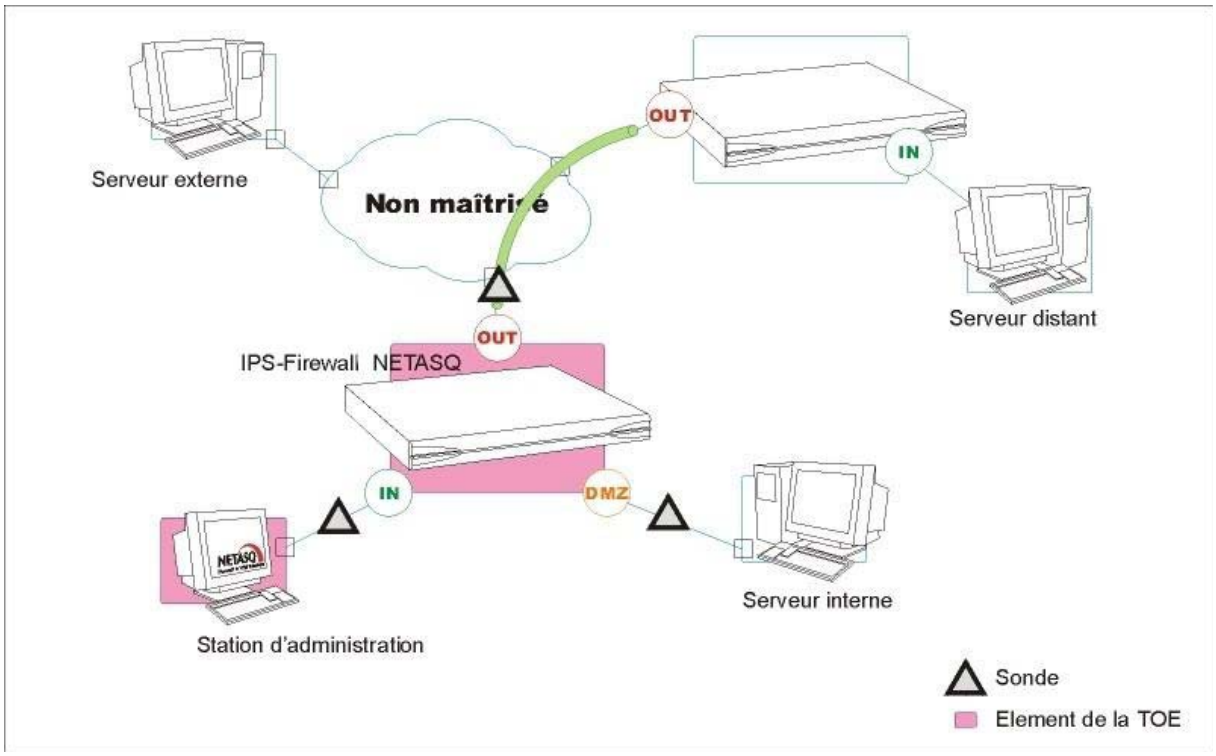

Figure 1 - Eléments constitutifs de la cible d'évaluation

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 juillet 2009, 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 l'ANSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de l'ANSSI (Cf. [REF-CRY]).

Dans le cadre du processus de qualification standard, une analyse des mécanismes cryptographiques a été réalisée par le CESTI [EXP-CRY]. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN 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 la « Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ, version 8.0.1.1 » soumise 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 :

- les boîtiers appliances doivent être installés et stockés conformément à l'état de l'art concernant les dispositifs de sécurité sensibles ;
- les boîtiers appliances doivent être installés de façon à constituer les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information ;
- les équipements réseaux avec lesquels le produit établit des tunnels VPN doivent être protégés de manière équivalente aux boîtiers appliances ;
- les stations d'administration à distance doivent être sécurisées, maintenues à jour de toutes les vulnérabilités connues, installées dans des locaux à accès protégé et doivent être exclusivement dédiées à l'administration de la cible d'évaluation et au stockage des données ;
- les postes sur lesquels s'exécutent les clients VPN des utilisateurs autorisés doivent être protégés de manière équivalente aux stations d'administration distantes ;
- les mots de passe des utilisateurs et des administrateurs doivent être gérés par une politique de création et de contrôle des mots de passe ;
- les administrateurs doivent être des personnes de confiance, compétentes et formées, disposant des moyens nécessaires à l'accomplissement de leurs tâches ;
- le super-administrateur doit être le seul à être habilité à se connecter, via la console locale, sur les boîtiers ;
- la politique de contrôle des flux d'informations à mettre en oeuvre doit être définie, pour tous les équipements des réseaux de confiance à protéger, de manière complète, stricte, correcte et non ambiguë ;
- la cible d'évaluation ne doit pas dépendre de services externes « en ligne » pour l'application de la politique de contrôle des flux d'information ;
- à part l'application des fonctions de sécurité, les boîtiers appliances ne doivent pas fournir de service réseau autre que le routage et la translation d'adresse ;

- les algorithmes cryptographiques et les tailles de clés correspondant aux options spécifiées dans la cible de sécurité [ST §5.2.5], rappelées ici, doivent être utilisées (en prenant en compte la modification suivante : pour la signature et l'élaboration des clés, il est recommandé d'adopter une clé de 2048 bits au moins pour l'algorithme Diffie-Hellman) :

Opération cryptographique	***Algorithme***	***Taille des clés***
Signature et élaboration de clés	Diffie-Hellman	~~1536~~, 2048, 3072, 4096
Chiffrement / déchiffrement asymétrique	RSA	2048, 4096
Hachage univoque	HMAC-SHA1	160
	SHA2	256, 384, 512
Chiffrement / déchiffrement symétrique des paquets VPN	AES	128, 192, 256
	Triple DES	168
	Blowfish	128 à 256
	CAST	128
Chiffrement / déchiffrement symétrique des sessions d'administration	AES	128
Contrôle des sessions d'administration	HMAC-SHA1	160

L'administrateur du produit certifié devra également suivre les recommandations suivantes :
- protéger par chiffrement du carnet d'adresses, dans le logiciel Manager, les informations de login et de mots de passe ;
- activer systématiquement la protection en intégrité dans les flux IPSec ;
- utiliser la protection en intégrité HMAC-SHA1 dans les flux IPSec ;
- utiliser des moyens d'authentification (clés prépartagées, clés publiques) suivant les règles et recommandations de [REF-CRY] pour l'authentification des échanges de clés dans le cadre de l'exécution du protocole IKE (*Internet Key Exchange*) ;

Pour l'authentification des utilisateurs, si une base LDAP externe est utilisée, le serveur distant hébergeant la base LDAP doit être protégé suivant l'état de l'art. Plus précisément, on cherchera à :
- assurer la confidentialité des informations véhiculées par le protocole LDAP, en chiffrant les communications entre l'annuaire LDAP et l'IPS-Firewall au moyen du protocole SSL. Le serveur LDAP externe doit être à l'écoute sur le port TCP 636 (port par défaut pour les communications LDAP) ;
- créer un compte administrateur spécifique permettant à l'IPS-Firewall de se connecter sur le serveur LDAP externe en restreignant la lecture/écriture sur les seuls champs nécessaires à l'IPS-Firewall ;
- choisir un algorithme de hachage suivant les règles et recommandations de [REF-CRY] pour les mots de passe stockés.

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[1], 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 CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] 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 Royaume-Uni et la Suède.

[2] 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, le Pakistan, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	**2**		
	ADV_INT					**2**	**3**	**3**		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance, procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Development tools CM coverage
	ALC_DEL		**1**	1	**1**	1	1	**1**	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	2	**3**	3	**4**	**1**	Testing: basic 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_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Firewalls NETASQ – Cible de sécurité Suite logicielle IPS-Firewall Version 8 Référence : NA_ASE_ciblesec_v8, version 1.4 du 15/04/2009 NETASQ
[RTE]	Rapport technique d'évaluation – Projet JOCELYNE Référence : NTQ004-Jocelyne-RTE, version 4.01 du 24/07/2009 Silicomp-AQL
[ANA-CRY]	Cotation de mécanismes cryptographiques – Projet JOCELYNE Référence : 1644/SGDN/DCSSI/ACE du 26 juin 2009 SGDN/DCSSI
[EXP-CRY]	Analyse des mécanismes cryptographiques – Projet JOCELYNE Référence NTQ004-AMC, version 1.02 du 24/07/2009 Silicomp-AQL
[CONF]	Liste en configuration Référence : NA_ALC_sources_liste_v8, version 1.0 du 12/01/2009 NETASQ
[GUIDES]	Guide d'utilisation de l'interface Manager : - NETASQ UNIFIED MANAGER V8.0 – Manuel d'utilisation et de configuration Référence : FRUG0907-V1.2_NUMANAGER-V8.0, version 1.2 de juillet 2009 NETASQ Guide d'utilisation de l'interface Monitor : - NETASQ REAL6TIME MONITOR V8.0 - Manuel d'utilisation et de configuration Référence : FRUG0901-V1.1_NRMONITOR-V8.0, version 1.1 de janvier 2009 NETASQ Guide d'utilisation de l'interface Reporter : - NETASQ EVENT REPORTER V8.0 – Manuel d'utilisation et de configuration Référence : FRUG0901-V1.1_NEREPORTER-V8.0, version 1.1 de janvier 2009 NETASQ

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 : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, revision 2, ref CCMB-2007-09-004.
[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, version courante, voir www.ssi.gouv.fr