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 DCSSI-2008/38

ExaProtect Security Management Solution (SMS)

Paris, le 27 novembre 2008

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.dcssi@sgdn.gouv.fr

Référence du rapport de certification

DCSSI-2008/38

Nom du produit

ExaProtect Security Management Solution (SMS)

Référence/version du produit

Version 2.7.3.5

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 2 augmenté

ADV_HLD.2, ADV_IMP.1*, ADV_LLD.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1, AVA_VLA.2

***appliqués aux exigences FCS**

Développeur(s)

ExaProtect

149 boulevard Stalingrad, 69100 Villeurbanne, France

Commanditaire

ExaProtect

149 boulevard Stalingrad, 69100 Villeurbanne, France

Centre d'évaluation

Oppida

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

Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr

Accords de reconnaissance applicables

CCRA **SOG-IS**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

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

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

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « ExaProtect Security Management Solution (SMS)**,** Version 2.7.3.5 » développé par ExaProtect.

Le produit ExaProtect SMS permet de répondre aux besoins de supervision de la sécurité. On peut résumer ces besoins de la manière suivante :

- gérer un grand nombre de dispositifs de sécurité répartis sur l'ensemble du système d'information ;
- traiter la grande masse d'information générée par les dispositifs ;
- enrichir les événements (réduction des faux positifs, prise en compte du contexte « métier ») ;
- corréler les événements provenant de différents dispositifs et générer des alertes ;
- automatiser le processus de diagnostic ;
- attirer l'attention de l'expertise humaine sur la menace la plus importante ;
- proposer des contre-mesures lorsque c'est possible ;
- fournir une vue synthétique et globale sur le risque et la menace.

Ces services sont réalisés par les deux composants principaux ExaProtect Security Management Agent (**SMA**) et ExaProtect Security Management Platform (**SMP**). L'analyse des événements de sécurité et la configuration de la solution sont réalisées via la console ExaProtect Security Management Console (**SMC**) depuis un poste avec un navigateur Web.

1.2. Description du produit évalué

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

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par les éléments suivants :

- version : 2.7.3.5 ;
- numéro de build : 390 ;
- numéro de commit : 16754.

Ces informations sont identifiables via la fenêtre « About » de la console SMC.
Le numéro de version du produit est également indiqué sur la page d'accueil de la console SMC.

La version des agents installés est disponible dans le fichier *version* présent dans le répertoire *ExaProtect Technology\ESMA 2.7.3.3\config* sur le poste où est installé l'agent.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- identification et authentification des utilisateurs qui se connectent à la console du produit ExaProtect SMS afin de gérer les alertes ;
- gestion des profils utilisateurs et accord des droits en fonction d'une table de droits ;
- protection et contrôle d'accès aux fichiers de paramétrage du serveur ;
- protection et contrôle d'accès aux tables des bases de données du serveur ;
- collecte des événements et des logs bruts des équipements et ceux internes au fonctionnement de l'agent ;
- collecte des événements internes au fonctionnement du serveur SMP ;
- audit des événements collectés au niveau des agents et du serveur ;
- synchronisation de la configuration des agents au démarrage et également à la demande d'un utilisateur autorisé ;
- prévention d'une rupture de liaison avec l'agent ;
- confidentialité et intégrité des échanges entre le serveur et ses agents ;
- confidentialité et intégrité des échanges entre la console et le serveur ;
- confidentialité et intégrité des archives de logs bruts.

1.2.3. Architecture

La figure ci-dessous présente la vision globale du concept ExaProtect SMS et les services fournis par le produit :

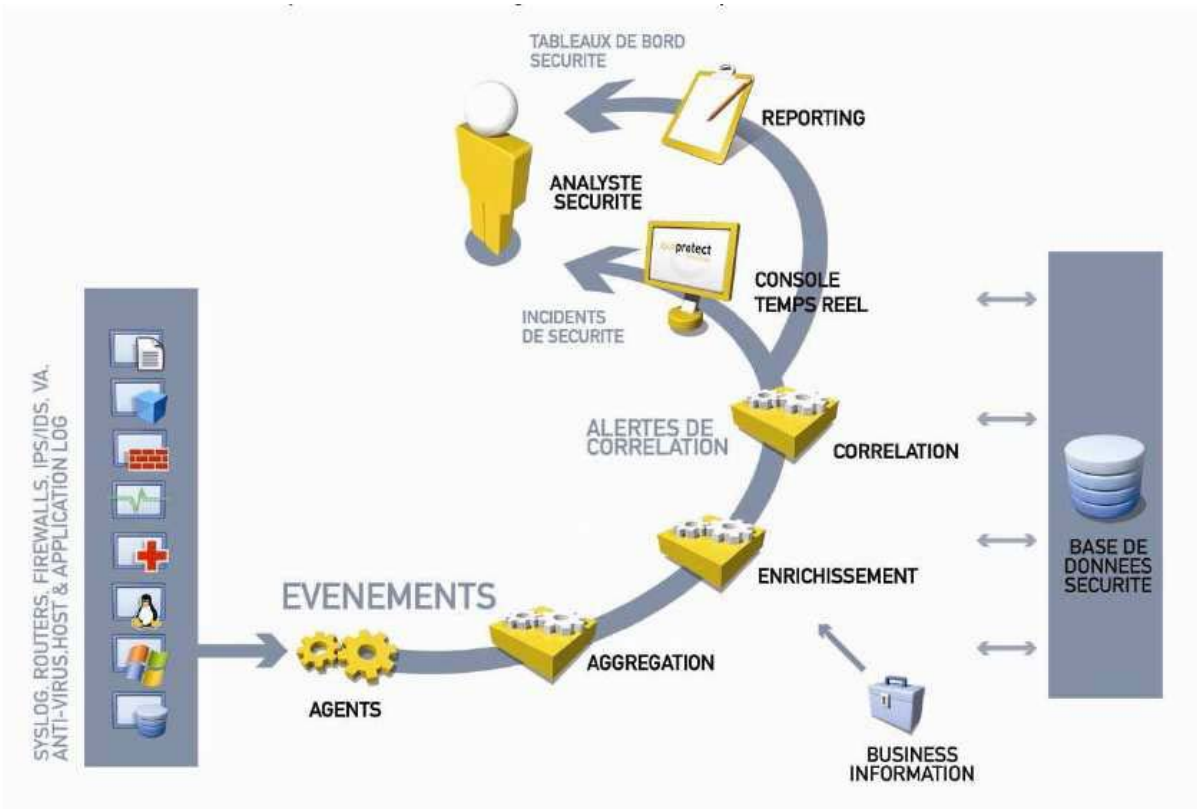

Figure 1 - Cas d'utilisation de la TOE

Le schéma ci-dessous présente le périmètre de l'évaluation associé aux composants du produit :

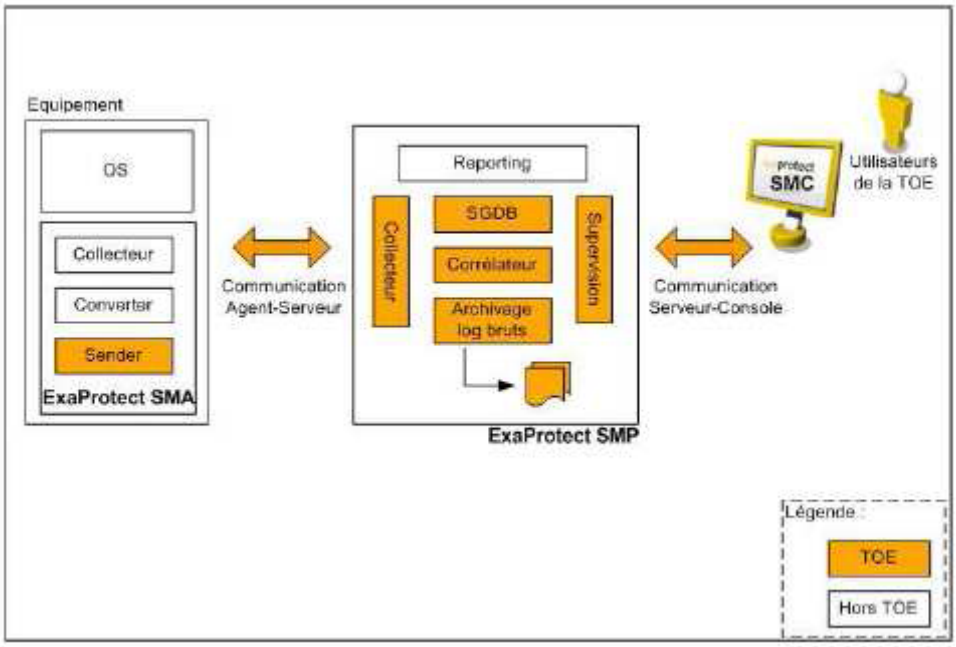

Figure 2 - Architecture de la TOE

Le SGDB mentionné dans la figure ci-dessus correspond au système de gestion de bases de données.

Le périmètre d'évaluation est le suivant :

- la collecte des événements et logs bruts par le serveur SMP envoyés par l'agent SMA ;
- l'application des règles de corrélation d'événements en vue de générer des alertes de sécurité ;
- l'analyse des alertes de sécurité au travers de fonctions d'audit accessibles via la console SMC ;
- les communications entre les agents et le serveur ;
- les communications entre la console et le serveur, y compris le mécanisme d'authentification et de contrôle d'accès des utilisateurs ;
- l'archivage des logs bruts issus des équipements.

Les éléments suivants ne font pas partie du périmètre de l'évaluation :

- les mécanismes de « reporting » à partir des événements et des alertes de sécurité stockées dans la base de données ;
- la collecte des entrées de log sur l'équipement, leur communication vers un agent et leur transformation en événements et logs bruts ;
- la pertinence des règles et heuristiques utilisées par le corrélateur pour générer les alertes.

1.2.4. Cycle de vie

Le produit a été développé sur le site suivant :

ExaProtect Innovation

149 boulevard Stalingrad
69100 Villeurbanne
France

La procédure de livraison du matériel et des certificats est décrite dans la figure ci-dessous. Le certificat permet à un client de télécharger les patchs, les mises à jour et la documentation du produit.

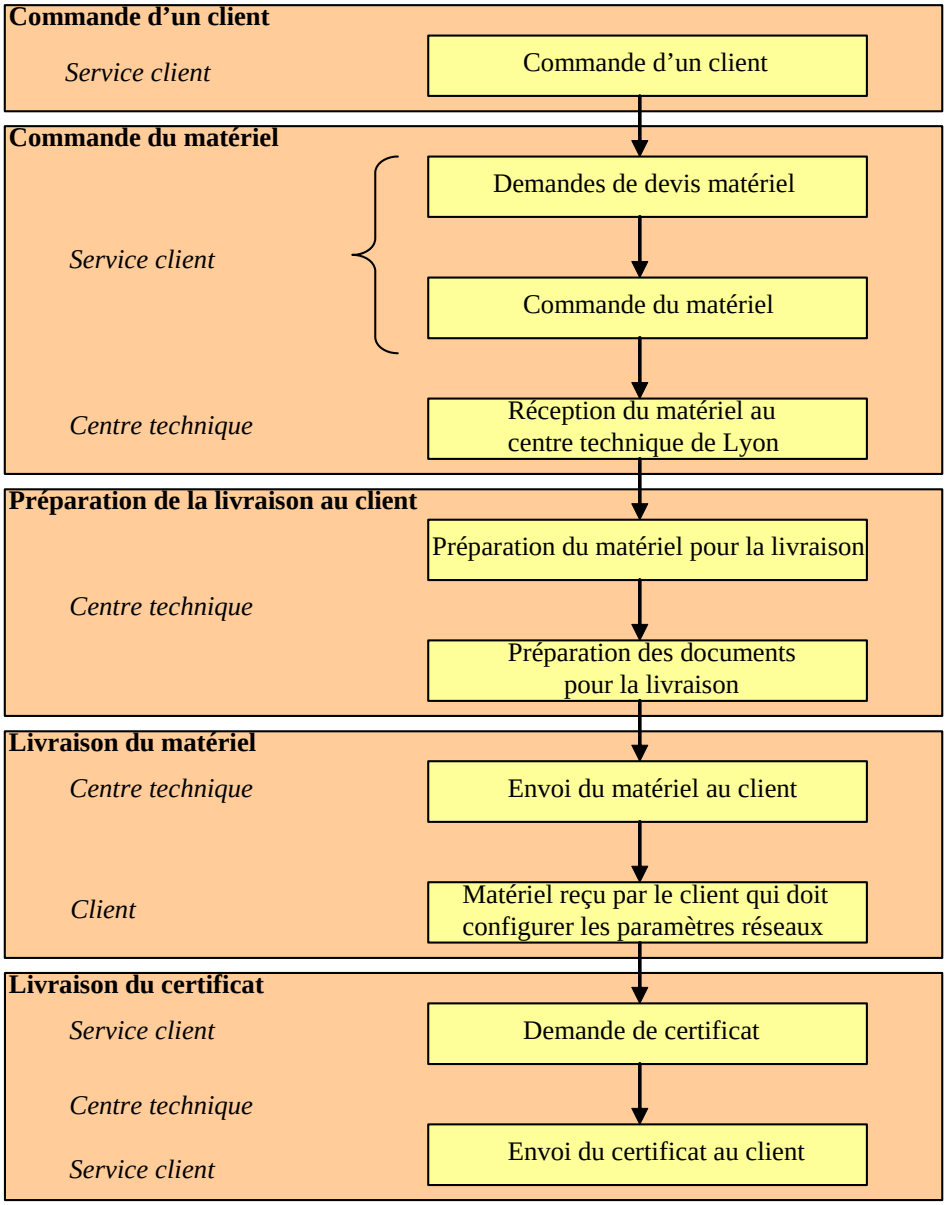

Figure 3 - Procédure de livraison

Pour l'évaluation, l'évaluateur a considéré comme « administrateurs du produit » les « administrator » qui visualisent/acquittent les alertes, activent/configurent les agents et configurent les règles de corrélation, et les « superuser » qui ont les mêmes privilèges que les « administrator » mais qui peuvent en plus créer/configurer les comptes utilisateurs/administrateurs. L'évaluateur a considéré comme « utilisateurs du produit » les « viewer » qui visualisent les alertes et les « analyst » qui visualisent/acquittent les alertes et peuvent également activer/désactiver un agent (mais pas le configurer).

1.2.5. Configuration évaluée

Le **serveur SMP** se présente sous la forme d'une *appliance* constituée du système d'exploitation Red Hat Enterprise Linux 3.0, ainsi que des applications suivantes :

- application SMP 2.7.3.5 ;
- serveur Tomcat 5.5.17 ;
- base de données MySQL 5.0.38 ;
- Java SDK 1.5.0-08 ;
- application GnuPG 1.2.1-20.

Un **agent SMA** est constitué des éléments suivants :

- application SMA 2.7.3.5 (application Java identique quelle que soit le système) ;
- Java runtime JRE 1.5.0-06 (exécutable dépendant du système sur lequel est installé l'agent).

Les **agents SMA** sont supportés sur les systèmes d'exploitation suivants :

- Linux : RedHat 7.1 ou supérieur, RedHat Enterprise Linux 3.0 ou supérieur, Debian 3.0 (kernel 2.4) ou supérieur ;
- Windows XP, 2000, 2003 ;
- SUN-Solaris 2.8 ou supérieur ;
- DEC TRU64 4.0f ou supérieur ;
- IBM-AIX 5.1 ou supérieur.

La **console SMC** est accessible depuis un navigateur web type Mozilla Firefox 1.5 ou supérieur ou Internet Explorer 6.0. L'évaluateur a réalisé ses tests a partir d'un navigateur web Mozilla Firefox 2.0.0.5.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 30 septembre 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] qui ont révélé que l'algorithme DSA utilisé pour la signature des données archivées n'atteint pas le niveau standard. Afin de remédier à cela, une recommandation figure dans les guides [GUIDES] indiquant de séquestrer la clé publique de signature des archives de manière sûre.
L'ensemble des autres résultats du rapport d'analyse des mécanismes cryptographiques [ANA-CRY] ont été pris en compte dans l'analyse de vulnérabilités indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau VLA visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « ExaProtect Security Management Solution (SMS), Version 2.7.3.5 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 2 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]. Il devra notamment suivre les recommandations rappelées ci-après :

1. OE.PROTECT_HARDWARE. Le poste d'accès à la console SMC et le serveur SMP doivent être installés dans un local sécurisé.

2. OE.EXPORT_BASE. Dans le cadre du service d'archivage des logs bruts, il est supposé que les moyens permettant le déchiffrement et la vérification de la signature des archives hors de la TOE sont gérés de manière sûre.

3. OE.TRUE_AGENT. La TOE doit se reposer sur des agents qui transforment de façon fiable et cohérente les entrées de log remontées par les équipements.

4. OE.ADM_NO_EVIL. L'organisme doit recruter des personnels de confiance comme administrateurs des systèmes d'exploitation qui hébergent les agents ExaProtect SMA et comme administrateurs du serveur ExaProtect SMP.

5. OE.HOST_CLEAN. Les équipements sur lesquels sont installés les agents SMA doivent être sécurisés selon des procédures de durcissement et mis à jour en fonction des vulnérabilités spécifiques découvertes sur le système d'exploitation et les applications installées sur ces équipements.

6. OE.SERVER_CLEAN. L'appliance sur laquelle le serveur SMP est installé ne doit pas contenir d'autres services (applications tierces) que ceux installés initialement.

7. OE.USR_AWARE. Les utilisateurs de la TOE doivent être formés à l'utilisation de la TOE et être sensibilisés à la sécurité, en particulier aux conséquences de leurs actes lorsqu'ils traitent et acquittent des alertes.

8. OE.CRYPTO. La TOE doit utiliser des mécanismes cryptographiques conformes au référentiel de la DCSSI pour les produits qualifiés au niveau « standard ».

9. OE.QUALIF. La TOE doit être évaluée au niveau EAL2+ correspondant à une qualification au niveau standard.

10. OE.TIME. Le temps de référence de la TOE doit être synchronisé avec une base de temps à disposition par l'environnement.

11. OE.FIREWALL. L'environnement de la TOE doit inclure un dispositif de filtrage des communications placé devant le serveur ExaProtect SMP.

12. OE.CTL_AGENT_ASSETS. Les systèmes sur lesquels les agents sont installés doivent mettre en œuvre un contrôle d'accès sur les ressources des agents (fichiers de paramétrage, bi-clé).

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, 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 2+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**2**	Configuration items
	ACM_SCP			**1**	**2**	**3**	3	3		
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1***	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1***	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Indentification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3	**1***	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**1**	Evidence coverage
	ATE_DPT			**1**	1	**2**	2	**3**		
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

*appliqués aux exigences FCS.

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité ExaProtect Security Management Solution Référence SMSSecurityTarget.fr, version 1.8 du 15/07/2008 ExaProtect
[RTE]	Rapport technique d'évaluation – Projet JOUBARBE Référence : OPPIDA/CESTI/JOUBARBE/RTE/1.0 du 30/09/2008 OPPIDA
[ANA-CRY]	Cotation des mécanismes cryptographiques – Projet JOUBARBE, N°1228/SGDN/DCSSI/SDS/Crypto du 26/05/2008 SGDN/DCSSI
[CONF]	Liste de configuration de la version 2.7.3 Référence : ConfigListSMS273-fr, version 1.3 du 22/09/2008 ExaProtect
[GUIDES]	Guide d'installation du produit : - SMA Installation Guide Référence : udoc-00616-en, version 6 du 23/04/2008 ExaProtect - SMP Installation Guide Référence : udoc-00614-en, version 7 du 23/04/2008 ExaProtect Guide d'administration du produit : - SMS Administration Guide Référence : udoc-00632-en, version 3 du 23/04/2008 ExaProtect Guide d'utilisation du produit : - SMC User Guide Référence : udoc-00613-en, version 5 du 22/04/2008 ExaProtect

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, 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. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.