PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/11

Applatoo version 1.2.4

Paris, le 25 avril 2005.

Le Directeur central de la sécurité des systèmes d'information

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

Synthèse

Rapport de certification 2005/11

Produit : Applatoo version 1.2.4

Développeur : France Telecom R&D

Critères Communs version 2.2

EAL2 Augmenté
(ADV_HLD.2, ADV_LLD.1, ADV_IMP.1, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1, AVA_MSU.1, AVA_VLA.2)

Commanditaire : France Telecom R&D

Centre d'évaluation : Silicomp-AQL

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 Applatoo version 1.2.4 développé par France Telecom R&D.

1.2. Développeurs

France TELECOM R&D

38-40, rue du Général Leclerc
92764 Issy les Moulineaux Cedex 9
France

Ilex

51 boulevard Voltaire
92600 Asnières-sur-Seine
France

1.3. Description du produit évalué

1.3.1. Architecture

La cible d'évaluation est un produit logiciel, développé en Java, offrant des fonctionnalités de sécurité destinées à être utilisées par des applications de plus haut niveau.

Le produit offre les fonctionnalités suivantes :
- génération de la clef de session ;
- chiffrement symétrique avec la clef de session (Triple DES, AES, RC6, IDEA) ;
- chiffrement asymétrique de la clef de session à l'aide de la clef publique (RSA, DSA avec padding PKCS#1) ;
- déchiffrement symétrique du document à l'aide de la clef de session (Triple DES, AES, RC6, IDEA) ;
- génération du condensat du document (SHA-1) ;
- déchiffrement asymétrique du condensat à l'aide du certificat public de l'émetteur (RSA, DSA avec padding PKCS#1) ;
- comparaison du condensat vérifié avec celui réalisé.

Les fonctions de signature et de déchiffrement asymétrique (qui nécessitent des clefs privées) seront fournies par les ressources sur lesquelles s'appuie APPLATOO : cartes à puces (Axalto, Oberthur, Rainbow-ikey, ActivCard, Crypto-Hardware), modules logiciels (CAPI, Netscape, PKCS#11, PKCS#12).

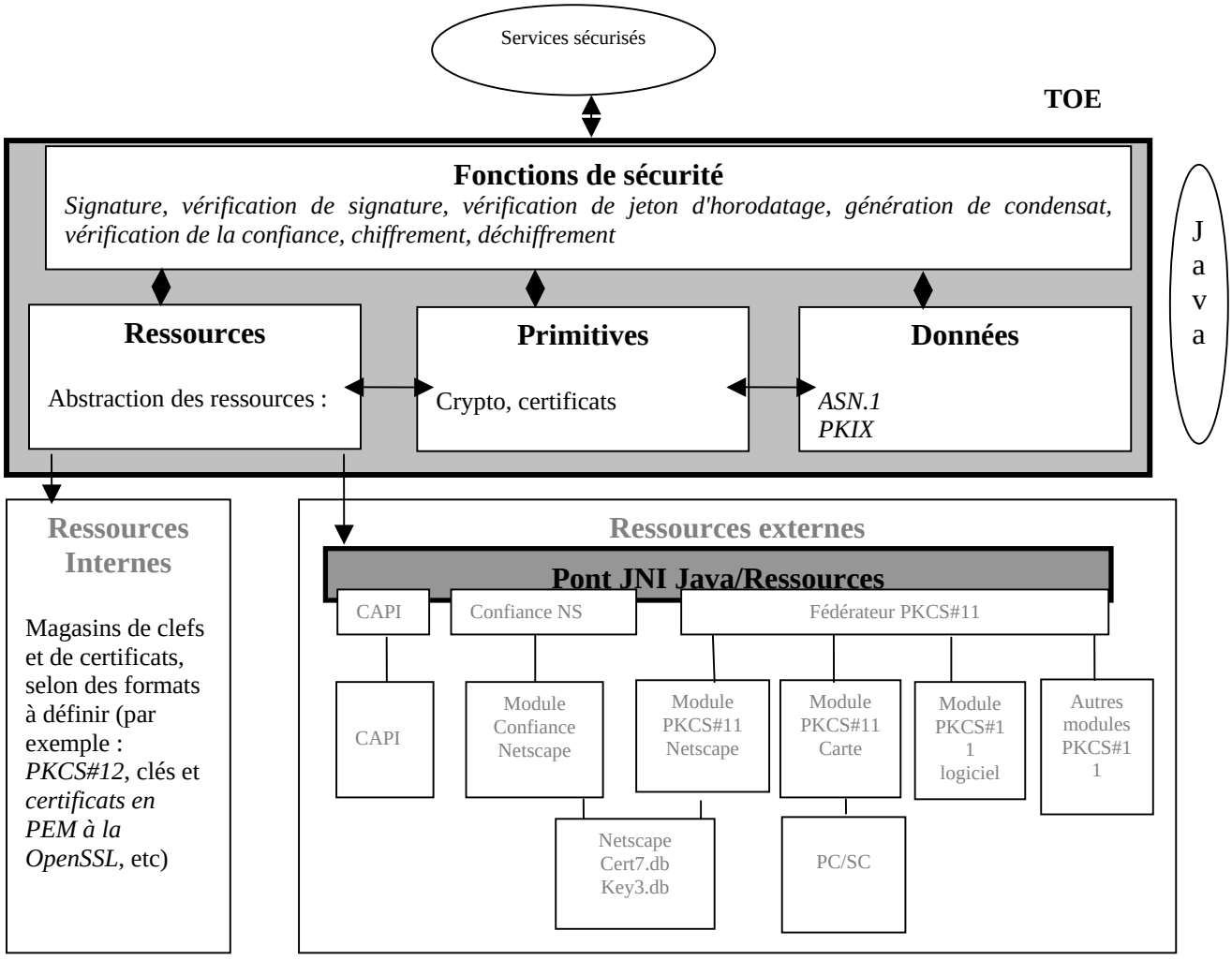
1.3.2. Périmètre et limites du produit évalué

Le produit évalué comprend les éléments suivants :

- un module d'interface permettant de développer les fonctions de signature et vérification de signature, de chiffrement et déchiffrement et de génération de condensat ;
- un module permettant l'abstraction des ressources cryptographiques (clefs et certificats) ;
- un module fournissant les algorithmes cryptographiques (chiffrement, hachage) ;
- un module mettant en oeuvre les différents formats utilisés au sein du produit (PKCS#7, X509…) ;
- un pont JNI (Java Native Interface) permettant la communication entre les ressources externes (CAPI, Confiance NS, fédérateur PKCS#11) et l'environnement Java.

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

- ressources internes (magasins de clefs et de certificats, selon des formats à définir (par exemple : PKCS#12, clés et certificats en PEM à la OpenSSL, etc)) ;
- ressources externes (CAPI, Module Confiance Netscape, Module PKCS#11 Netscape, Module PKCS#11 Carte, Module PKCS#11 Logiciel, Autres modules PKCS#11) ;
- la machine virtuelle Java.



1.3.3. Environnement d'utilisation

Deux modes d'utilisation sont possibles suivant le service sécurisé développé à l'aide de la TOE : mode servlet (exécution sur un serveur) ou mode applet (exécution à l'aide d'un navigateur sur un client).

Les environnements supportés par le produit sont décrits dans la cible d'évaluation [ST].

Les environnements installés et testés par l'évaluateur sont les suivants :

- mode client :
    - Windows 98 avec Netscape 4.78 et carte Axalto;
    - Windows 98 avec Mozilla 1.4 et carte Axalto;
    - Windows 2000 avec Netscape 4.75 et carte Axalto;
    - Windows 2000 avec Mozilla 1.2.1 et carte Axalto;
    - Windows 2000 avec Internet explorer 6.0 et carte Axalto;
    - Linux 2.4 avec Mozilla 1.1;
    - MacOS X avec Mozilla 1.1;
- mode serveur :
    - Linux 2.4 avec moteur de servlets Tomcat 4.2.

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

France TELECOM R&D

38-40, rue du Général Leclerc
92764 Issy les Moulineaux Cedex 9
France

2.3. Centre d'évaluation

Silicomp – AQL

1 rue de la châtaigneraie
CS 51766
35517 Cesson Sévigné
France

2.4. Rapport technique d'évaluation

L'évaluation s'est déroulée du 26 mai 2004 au 21 mars 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 EAL2[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL2	Structurally tested
+ ADV_HLD.2	Security enforcing high-level design
+ ADV_LLD.1	Descriptive low-level design
+ ADV_IMP.1	Subset of the implementation of the TSF
+ ALC_DVS.1	Identification of security measures
+ ALC_FLR.3	Systematic flaw remediation
+ ALC_TAT.1	Well-defined development tools
+ AVA_MSU.1	Examination of guidance
+ AVA_VLA.2	Independent vulnerability analysis

2.6.2. L'évaluation de l'environnement de développement

Le produit est développé sur les sites suivants :

France Telecom R&D
38-40, rue du Général Leclerc
92764 Issy les Moulineaux Cedex 9
France,

et

Ilex
51 boulevard Voltaire
92600 Asnières-sur-Seine
France.

L'évaluateur a confirmé que les mesures de sécurité définies pour l'environnement de développement du produit évalué sont appliquées.

La vérification de l'application des procédures analysées a été effectuée lors des visites des sites de France Telecom R&D à Issy-les-Moulineaux et d'Ilex à Asnières-sur-Seine (cf Annexe 1 et Annexe 2).

L'évaluateur a 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.

[1] Annexe 3 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

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.2	Configuration items	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) et conception de haut-niveau (HLD). Pour la partie du produit réalisant des opérations cryptographiques (classe FCS), cette analyse a aussi porté sur la conception de bas-niveau (LLD) et la représentation de l'implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- FCS_COP.1 Cryptographic operation [chiffrement/déchiffrement asymétrique];
- FCS_COP.1 Cryptographic operation [chiffrement/déchiffrement symétrique];
- FCS_COP.1 Cryptographic operation [génération de condensats];
- FCS_CKM.1 Cryptographic key generation [génération de clefs de session];
- FCS_CKM.3 Cryptographic key access [chiffrement/déchiffrement externe et accès aux certificats];
- FMT_MTD.3 Secure TSF data [vérification de la chaîne de confiance].

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.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.1	Subset of the 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 :

- entre le sous-traitant Ilex à Asnières-sur-Seine et le site de développement de France Telecom R&D à Issy-les-Moulineaux ;
- entre le site de développement de France Telecom R&D à Issy-les-Moulineaux et l'intégrateur du produit évalué.

L'installation du produit correspond à la copie de fichiers et à la collecte des ressources externes.

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

2.6.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, l'évaluateur a considéré comme utilisateurs les l'intégrateur du produit évalué. Il a également été considéré qu'il n'y avait pas d'administrateur.

L'évaluateur a analysé les guides d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

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 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 un échantillon représentatif des plates-formes de tests listées dans la cible de sécurité [ST] (voir 1.3.3).

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

Classe ATE: Tests		**Verdicts**
ATE_COV.1	Evidence of coverage	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.

La cible de sécurité n'identifie aucun mécanisme probabilistique ou combinatoire non cryptographique.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur la même plate-forme que les tests indépendants.

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	Misuse	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 (listés dans la cible de sécurité [ST]) a été analysée par la DCSSI. Les mécanismes analysés atteignent le niveau de robustesse standard tel que défini dans le référentiel cryptographique de la DCSSI [CRY].

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.

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] :

- l'environnement d'utilisation doit assurer l'intégrité du code de la TOE par un mécanisme technique ;
- les certificats de confiance présents sur le poste (et qui permettent de remonter une chaîne de confiance) doivent être issus de chaînes sûres ;
- les ressources cryptographiques utilisées doivent permettre d'effectuer un chiffrement asymétrique dont la nature ne permet pas de révéler la clef privée de chiffrement. Ce chiffrement s'effectue sur un condensat ;
- les ressources cryptographiques utilisées doivent permettre d'effectuer un déchiffrement asymétrique dont la nature ne permet pas de révéler la clef privée de déchiffrement. Ce déchiffrement s'effectue sur une clef de session ;
- les ressources cryptographiques utilisées doivent assurer l'intégrité et la confidentialité des clefs privées ;
- les mesures de sécurité des ressources cryptographiques utilisées et de leur environnement doivent permettre de limiter l'accès aux services de chiffrement asymétrique aux utilisateurs et entités TI autorisées ;
- la confiance dans les mesures de sécurité des ressources et de leur environnement doit être au moins équivalente à un niveau deux étoiles PRIS [PRIS] ;
- les services de la plate-forme sur laquelle la TOE s'exécute contrôlent l'accès en lecture et écriture en zone mémoire où sont stockés les DS et CSD, et ils contrôlent l'accès en écriture en zone mémoire où sont stockés les DTBS et DTBSR ;
- les mesures de sécurité de l'environnement d'utilisation garantissent l'intégrité et la confidentialité des données échangées entre la TOE et les ressources externes ainsi qu'entre la TOE et les différents magasins de certificats.

3.3. Reconnaissance européenne (SOG-IS)

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

3.4. 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.

Annexe 1. Visite du site de développement de la société France Telecom à Issy-les-Moulineaux

Le site de développement de la société France Telecom, situé à Issy-les-Moulineaux, a fait l'objet d'une visite par l'évaluateur le 8 novembre 2004 pour s'assurer de l'application des procédures de sécurité de l'environnement de développement du produit Applatoo version 1.2.4.

Ces procédures ont été fournies et analysées dans le cadre de la tâche d'évaluation ALC_DVS.1.

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

Annexe 2. Visite du site de développement de la société Ilex à Asnières-sur-Seine

Le site de développement de la société Ilex, situé à Asnières-sur-Seine, a fait l'objet d'une visite par l'évaluateur le 9 novembre 2004 pour s'assurer de l'application des procédures de sécurité de l'environnement de développement du produit Applatoo version 1.2.4.

Ces procédures ont été fournies et analysées dans le cadre de la tâche d'évaluation ALC_DVS.1.

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

[ST]	• APPLATOO – CIBLE DE SÉCURITÉ Référence : DTL/SSR/284.03/LF/Livrable 1.2.a version 1.12 • APPLATOO – CIBLE DE SÉCURITÉ – version publique Référence : DTL/SSR/284.03/LF/Livrable 1.2.aa
[RTE]	Rapport technique d'évaluation Référence CNT263-RTE01-3.01, version : 3.01
[CONF]	Procédures de gestion de configuration Référence : DTL/SSR/284.03/LF/Livrable 1.2.l, version du 16/09/04
[GUIDES]	• FAQ Référence : DTL/SSR/284.03/LF/Livrable 1.2.p, version du 18/01/05 • How To Référence : DTL/SSR/284.03/LF/Livrable 1.2.q, version du 01/09/04
[Visite]	Rapport de visite Référence : CNT263-RAU01-1.00, version : 1.00

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 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.
[CRY]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.02 du 19/11/04.
[PRIS]	Politique de référencement intersectorielle de sécurité, www.adae.gouv.fr.

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