PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/01

AVSE v1_1

Paris, le 30 janvier 2006.

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[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 2006/01

AVSE v1_1

Développeur : KOTIO

Critères Communs version 2.2

EAL2 Augmenté
(AVA_VLA.2)

Commanditaire : KOTIO

Centre d'évaluation : OPPIDA

Préface

La certification

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

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

Les procédures de certification sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le module AVSE (Autorité de Vérification de Signature Electronique) v1_1 développé par KOTIO.

1.2. Développeur

KOTIO

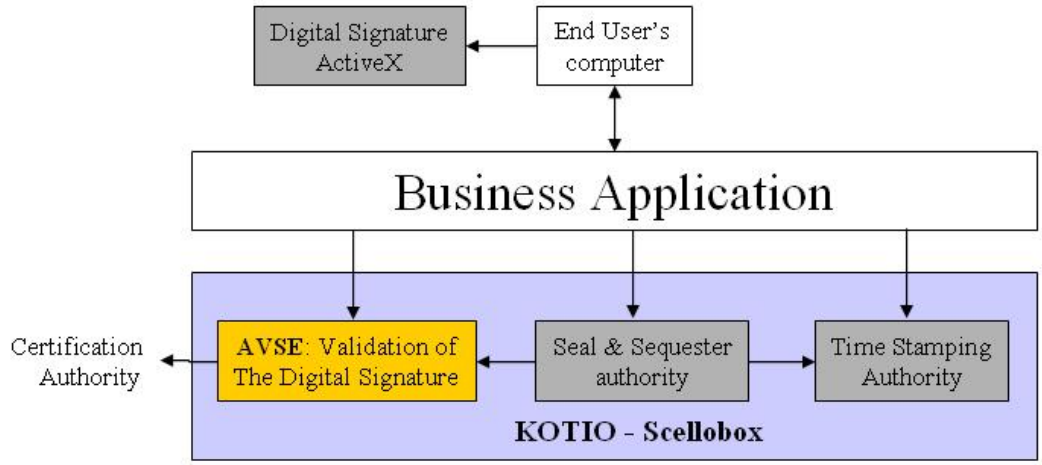
96, avenue du Général Leclerc

92100 Boulogne Billancourt

1.3. Description du produit évalué

1.3.1. Architecture

La TOE s'intègre dans le produit plus complet nommé Scellobox, et s'interface avec les logiciels clients de la façon suivante :



Le module AVSE doit être installé dans l'environnement suivant :

- Linux Red Hat 9 ;
- Apache HTTP server, V 1.3.28 ;
- modules ModSSL and OpenSSL ;
- mySQL 4.0 ;
- SUN JDK 1.4.2_04.

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

1. développement du module AVSE (KOTIO) ;
2. installation du module AVSE (client) ;
3. utilisation du module AVSE.

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend les éléments suivants :

- la fonction de vérification d'un fichier de signature au format XML-DSIG ;
- la fonction de vérification d'une balise de signature au format XML-DSIG ;
- la fonction de vérification d'un certificat X509 pour une date ;
- la fonction permettant de garantir l'origine de la réponse fournie à l'application appelante ;
- la fonction permettant de tracer des demandes et réponses faites par l'AVSE ;
- la fonction de gestion et vérification des CRL en place ;
- la fonction de vérification technique du format d'une signature électronique RSA-SHA1.

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

- le système d'exploitation et l'application Apache, en particulier les modules d'authentification ;
- le mécanisme de contrôle d'accès au code de la TOE, aux données de configuration et aux enregistrements d'audit.

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

KOTIO

96, avenue du Général Leclerc

92100 Boulogne Billancourt

2.3. Centre d'évaluation

Oppida

4-6 rue du Vieil Etang
Bâtiment B
78180 Montigny le Bretonneux

2.4. Rapport technique d'évaluation

L'évaluation s'est déroulée du 22 avril 2005 au 23 janvier 2006.

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
+ AVA_VLA.2	Independent vulnerability analysis

2.6.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

KOTIO

96, avenue du Général Leclerc

92100 Boulogne Billancourt

Des procédures de gestion de configuration permettent de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite de Kotio à Boulogne Billancourt. (cf Annexe 1)

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

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

2.6.3. L'évaluation de la conception du produit

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

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :
- Audit data generation (FAU_GEN.1);
- Action in case of possible data loss (FAU_STG.3);
- Cryptographic key access (FCS_CKM.3);
- Cryptographic operation (FCS_COP.1) / Signature verification;
- Cryptographic operation (FCS_COP.1) / SHA-1;
- Basic data authentication (FDP_DAU.1);
- Export of user data without security attributes (FDP_ETC.1);
- Import of user data without security attributes (FDP_ITC.1);
- Inter-TSF basic TSF data consistency (FPT_TDC.1) / Timestamps;
- Inter-TSF basic TSF data consistency (FPT_TDC.1) / XML DSIG files.

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

Classe ADV: Développement		Verdicts
ADV_FSP.1	Informal functional specification	Réussite
ADV_HLD.1	Descriptive high-level design	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 site de KOTIO et leurs clients.

Les procédures d'installation analysées permettent d'obtenir la configuration évaluée du produit.

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

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

2.6.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les clients de KOTIO et comme utilisateurs les utilisateurs finaux.

L'évaluateur a analysé les guides d'administration et 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.

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

La cible de sécurité n'identifie aucun mécanisme probabiliste ou combinatoire non cryptographique. Il n'y a donc pas de niveau de résistance intrinsèque.

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 plate-forme suivante :

- Linux Red Hat 9 ;
- Apache HTTP server, V 1.3.28 ;
- modules ModSSL and OpenSSL ;
- mySQL 4.0 ;
- SUN JDK 1.4.2_04.

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_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 n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et 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] :

- le module AVSE doit être exécuté dans un environnement sécurisé ;
- les listes de révocation doivent être mises à jour régulièrement ;
- un dispositif d'horodatage externe logiciel ou matériel doit être fourni ;
- les administrateurs ne sont pas hostiles ;
- l'accès au code de la TOE, aux données de configuration, aux listes de révocation et aux enregistrements d'audits est limité aux administrateurs ;
- les messages ne doivent pas être hachés avec l'algorithme MD5.

Annexe 1. Visite du site de développement de la société KOTIO à Boulogne Billancourt

Le site de la société KOTIO situé à Boulogne Billancourt, a fait l'objet d'une visite par l'évaluateur les 31 août 2005 et 7 septembre 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le produit AVSE v1_1.

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

- ACM_CAP.2 ;
- ADO_DEL.1.

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

Annexe 2. 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 3. Références documentaires du produit évalué

[CONF]	Gestion de configuration de l'AVSE v1.4b du 21/11/2005
[GUIDES]	Procédures de livraison de la TOE v1.1a du 09/09/2005 Guide d'installation et d'administration du produit AVSE ADO_IGS.1 AGD_ADM.1 v1.2 du 16/09/2005.
[RTE]	Rapport technique d'évaluation, référence OPPIDA/CESTI/SAPHIR/RTE/2 version 2.0 du 19/01/2006.
[ST]	« Security Target Description Electronic Signature Verification Authority – AVSE Project » Cible de sécurité CC niveau EAL2+ - v1.1 du 01/06/2005.
[Visite]	Rapport de visite d'audit, référence OPPIDA/CESTI/SAPHIR/DOC.002/1.0, version 1.0 du 13/09/2005.

Annexe 4. 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.

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.pm.gouv.fr