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-2008/44

Module de signature FASTSignature

Paris, le 17 décembre 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-2008/44

Nom du produit

Module de signature FASTSignature

Référence/version du produit

Version 1.1

Conformité à un profil de protection

PP/nc0504 [PP-ACSE]

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)

DICTAO

152 avenue de Malakoff, 75016 Paris, France

Commanditaire

CDC FAST

195 boulevard Saint Germain, 75007 Paris, France

Commanditaire

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 le « Module de signature FASTSignature, Version 1.1 » développé par DICTAO.

La cible d'évaluation est le module logiciel FASTSignature permettant de créer des signatures électroniques au format européen XAdES sur un document au format XML, en s'appuyant sur un dispositif de création de signature (SCDev[1]) effectuant les calculs cryptographiques mettant en œuvre la clé privée du signataire. La signature électronique XAdES créée est elle-même structurée au format XML et est directement insérée dans le document XML.
Le module FASTSignature se présente sous la forme d'un contrôle ActiveX. Il est exécuté suite à son appel par une page web (nommée par la suite application appelante). Son exécution se fait au travers du navigateur Internet dans lequel la page web se trouve.
Les documents signés par le module FASTSignature sont au format XML sous forme canonique (suivant l'algorithme C14N exclusif sans conservation de commentaires), format invariant par nature. Le module réalise l'affichage de ces documents grâce à une transformation du contenu XML du document en HTML. La correspondance entre les balises XML et leur équivalent en HTML est effectuée à l'aide d'une table de correspondance. Dans le cas où la TOE ne peut pas afficher le document, elle arrête le processus de signature.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection [PP-ACSE].

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 grâce au fichier « FASTSignature.inf », inclus dans l'archive « FASTSignature.cab ». A noter que les versions des deux DLL constitutives du module sont identiques à celle de ce module.
La signature de l'archive peut être vérifiée à l'aide d'un navigateur web.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la présentation, au signataire, du document à signer aux formats XML ou HTML (F.Présentation_Document) ;
- la sélection, par l'application appelante, d'une politique de signature et la mise en œuvre de celle-ci (F.Applique_Politique_Signature) ;

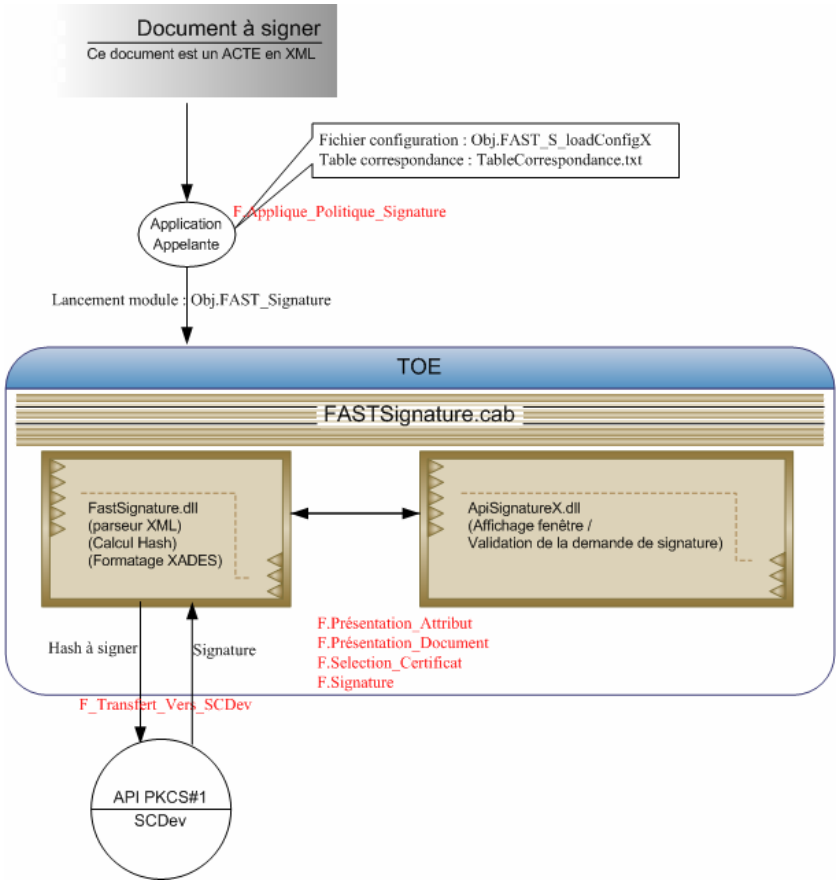
[1] Signature Creation Device, dispositif de création de signature

- la sélection, par le signataire, du certificat de signature à utiliser en fonction de la politique de signature sélectionnée (F.Transfert_vers_SCDev, F.Sélection_Certificat) ;
- la présentation, au signataire, des attributs de signature associés à la politique de signature sélectionnée (F.Présentation_attributs) ;
- la signature des données brutes au format XML sous forme canonique (conformément à l'algorithme C14N exclusif sans conservation de commentaires [XML-C14EXC]) et encodé en UTF-8 correspondant au document initialement présenté (F.Transfert_vers_SCDev, F. Signature).

1.2.3. Architecture

Le module est constitué de l'archive « FASTSignature.cab » qui contient les deux DLL[1] suivantes :

- FASTSignature.dll : comprenant le parseur XML, le calcul du hash et le formatage XADES. Cette DLL joue le rôle d'API : elle fournit les interfaces programmatiques qui permettent à l'application appelante (donc la page web) de jouer le rôle d'interface entre le signataire et le module FASTSignature (sélection du document à signer, sélection de la politique de signature à appliquer…) ;
- APISignatureX.dll : comprenant l'affichage de la fenêtre et la validation de la demande de signature, cette DLL correspond à l'interface graphique du module.



[1] Dynamic Link Library, bibliothèque de liens dynamiques

Les éléments suivants, hors périmètre de cette évaluation, sont nécessaires au fonctionnement du module FASTSignature :

- système d'exploitation : Windows Server 2003 et Windows XP ;
- navigateur internet : Internet Explorer 6.0 ;
- dispositifs de création de signature : SCDev logiciel du navigateur ou carte à puce Axalto Cyberflex Access e-gate 32K USB associée au lecteur ActiveCard ;
- application appelante.

1.2.4. Cycle de vie

Le cycle de vie du module est le suivant :

- le module est développé sur le site de DICTAO à Paris ;
- il est ensuite fourni, avec sa documentation d'intégration, aux développeurs des applications appelantes qui intègrent ce module.

Le produit a été développé sur le site suivant :

Site de développement de DICTAO

152 avenue de Malakoff
75016 Paris
France

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les développeurs des applications appelantes et les gestionnaire des machines hôtes du module FASTSignature, et comme utilisateurs du produit les signataires (utilisateurs finaux de l'application appelante).

1.2.5. Configuration évaluée

Le certificat porte sur les quatre environnements d'exploitation suivants :

- Windows XP / Internet explorer 6/ SCDev logiciel du navigateur ;
- Windows XP / Internet explorer 6/ Carte à puce Axalto Cyberflex Access e-gate 32K USB et lecteur ActiveCard ;
- Windows Server 2003 / Internet explorer 6/ SCDev logiciel du navigateur ;
- Windows Server 2003 / Internet explorer 6/ Carte à puce Axalto Cyberflex Access e-gate 32K USB et lecteur ActiveCard.

Les tests, réalisés dans le cadre de cette évaluation, ont été menés sur tous ces environnements. Une application appelante a également été fournie au CESTI par le développeur pour réaliser ses tests.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 2.2 [CC2.2], à la méthodologie d'évaluation définie dans le manuel CEM [CEM2.2], et aux interprétations numéros 86, 146, 192, 220, 227, 228, 232, 243 (voir commoncriteriaportal.org).
Ces critères et cette méthodologie d'évaluation, associés à ces interprétations, sont équivalents aux **Critères Communs version 2.3** [CC2.3] et [CEM2.3].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 5 décembre 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 (listés dans la cible de sécurité [ST]) a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés atteignent le niveau de robustesse standard tel que défini dans le référentiel cryptographique de la DCSSI [REF-CRY].

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 « Module de signature FASTSignature, Version 1.1» 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], notamment :

- la mise en œuvre de mesures de protection sur la machine hôte (OE.Machine_Hôte) ;
- l'authentification du signataire et la génération des signatures et à l'aide d'un SCDev (OE.Dispositif_De_Création_De_Signature) ;
- la gestion d'un canal de communication intègre entre SCDev et machine hôte (OE.Communication_TOE/SCDev) ;
- la confidentialité et l'intégrité des données d'authentification transmises au SCDev. (OE.Protection_Données_Authentification_Signataire) ;
- la présence du signataire entre l'instant où il manifeste son intention de signer et celui où il entre les données d'authentification permettant d'activer la clé de signature (OE.Présence_Du_Signataire) ;
- la vérification par les administrateurs de l'application appelante de l'authenticité des politiques de signature avant qu'elles ne soient utilisées par la TOE (OE.Authenticité_Origine_Politique_Signature) ;
- la confiance nécessaire envers l'administrateur de sécurité de la TOE et le développeur de l'application appelante (OE.Administrateur_De_Sécurité_Sûr, OE.Développeur_ Application_Appelante_Sûr) ;
- le développement de l'application appelante conformément au guide de développement [GUIDES-dev] (OE.Application_Appelante_Sûre) ;
- la mise en œuvre par l'administrateur de sécurité de mécanismes de contrôle d'intégrité des services et des paramètres de la TOE. (OE.Intégrité_Services) ;
- la protection en intégrité des paramètres transmis à la TOE par le serveur web depuis lequel sont chargées l'application appelante et la TOE (OE.Communication_Web).

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**	Identification 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 : - « Module de signature FASTSignature », réf. dictao_cdc_fastsig_CibleDeSécurité, version 3.1 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Cible de sécurité (publique) » réf. cdcfast_fastsig_CibleDeSécurité_publique, version 1.0
[RTE]	Rapport technique d'évaluation : - « Rapport technique d'évaluation- Projet FAST », réf. OPPIDA/CESTI/FAST/RTE/1.0, version 1.0
[ANA-CRY]	« Cotation de mécanismes cryptographiques – Qualification standard FASTSignature », N°1834/SGDN/DCSSI/SDS/Crypto, 21 août 2008
[CONF]	« Liste de configuration ACM_CAP- projet FASTSignature », réf. : dictao_cdc_fastsig_anx07, version 24.0
[GUIDES]	Guide d'installation et d'intégration du produit ([GUIDES-dev]) : - « Module de signature client FASTSignature version 1.1 – Guide d'intégration », réf. dictao_cdc_fastsig_gu03_guideintégration, version 4.0 Guide d'administration du produit : - « Module de signature client FASTSignature version 1.1 – Guide d'administration », réf. dictao_cdc_fastsig_gu02_guideadministration, version 3.1 Guide d'utilisation du produit : - « Module de signature FASTSignature version 1.1 – Guide d'utilisation », réf. dictao_cdc_fastsig_gu01_guideutilisation, version 3.1
[PP-ACSE]	Profil de Protection « Application de création de signature », version 1.0, référence PP-ACSE, PP/nc0504, 15 février 2005, voir www.ssi.gouv.fr
[XML-C14EXC]	W3C Recommandation - Exclusive XML Canonicalization, version 1.0 http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/

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.
[CC2.2]	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.
[CEM2.2]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC2.3]	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.
[CEM2.3]	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 courante, voir www.ssi.gouv.fr.