PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2012/26

AdSigner v5.0.0.1

Paris, le 4 juin 2012

Le directeur général de l'agence nationale
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 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 et de la sécurité 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.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2012/26**
Nom du produit **AdSigner**
Référence/version du produit **Version 5.0.0.1**
Conformité à un profil de protection **[PP ACSE] Application de création de signature électronique, version 1.7**
Critères d'évaluation et version **Critères Communs version 3.1 révision 3**
Niveau d'évaluation **EAL 3 augmenté** **ALC_FLR.3, AVA_VAN.3**
Développeur **Dictao** **152 avenue de Malakoff, 75116 Paris, France**
Commanditaire **Dictao** **152 avenue de Malakoff, 75116 Paris, France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**
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 modifié. 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 le module « AdSigner version 5.0.0.1 » développé par la société Dictao.

Le module AdSigner5 permet la création de signature électronique au format XML, avec l'extension XAdES, en s'appuyant sur un dispositif de création de signature (SCDev – *Signature Creation Device*) externe. Le module peut signer des documents au format texte brut ou HTML, et effectue lui-même l'interprétation du document HTML et son affichage.

Le module fait partie d'un système global de création de signature électronique, incluant l'application et le dispositif de création de signature. Ce dernier est le seul à posséder la clé privée du signataire et à pouvoir l'utiliser pour des opérations cryptographiques.

Le module AdSigner est exécuté au sein d'une page web (l'application appelante). Le document à signer est transmis au module par l'intermédiaire de la page web sous forme de paramètre.

1.2. Description du produit

1.2.1. Introduction

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]. Cette conformité est de type démontrable.

1.2.2. Identification du produit

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

Le module AdSigner5 est composé d'un fichier .jar qui s'exécute si une machine virtuelle Java est installée sur la plateforme hôte.

La version certifiée du produit est identifiable par les éléments suivants :

- le nom de l'archive .jar comporte le numéro de version (Dictao_AdSigner5_RELEASE_5.0.0.1.jar) ;
- l'archive .jar contient à la racine un fichier VERSION contenant le nom et la version de la TOE ;
- lorsque la TOE est exécutée, le nom et la version de la TOE apparaissent dans la console Java (Dictao AdSigner5 version 5.0.0.1).

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la spécification, pour l'application appelante, des paramètres de la politique de signature et du format du document (texte brut ou HTML) ;
- la mise en oeuvre de la politique de signature ;
- la présentation des attributs de signature au signataire ;
- la présentation du document à signer au signataire ;
- le contrôle de la stabilité de la sémantique du document à signer ;
- la sélection, par le signataire, d'un certificat dans la liste des certificats disponibles sur le SCDev et conformes à la politique de signature ;
- la signature électronique de document ;
- la vérification que la signature générée par le SCDev est bien au format PKCS#1 et que cette signature est valide de manière cryptographique.

1.2.4. Architecture

Le produit est constitué des composants suivants :

- un composant de présentation des attributs de signature au signataire ;
- un composant de présentation du document à signer ;
- un composant de sélection du certificat qui récupère la liste des certificats stockés et disponibles dans le SCDev puis filtre cette liste selon la politique de signature avant de la présenter au signataire ;
- un composant de gestion de la politique de signature qui applique la politique de signature spécifiée par l'application appelante pendant le processus de signature ;
- un composant de détection de l'environnement d'exécution qui permet la sélection du sous-composant qui sera utilisé pour se connecter au *middleware* du SCDev ;
- un composant de contrôle de l'invariance de la sémantique du document ;
- un composant de hachage qui calcule la valeur du *hash* des données à signer ;
- un composant de formatage de la signature qui crée la signature XML de la signature électronique XAdES ;
- un composant fournissant une interface avec le SCDev.

La figure ci-dessous donne une vue d'ensemble de la cible d'évaluation (TOE – *Target of Evaluation*) et de son environnement :

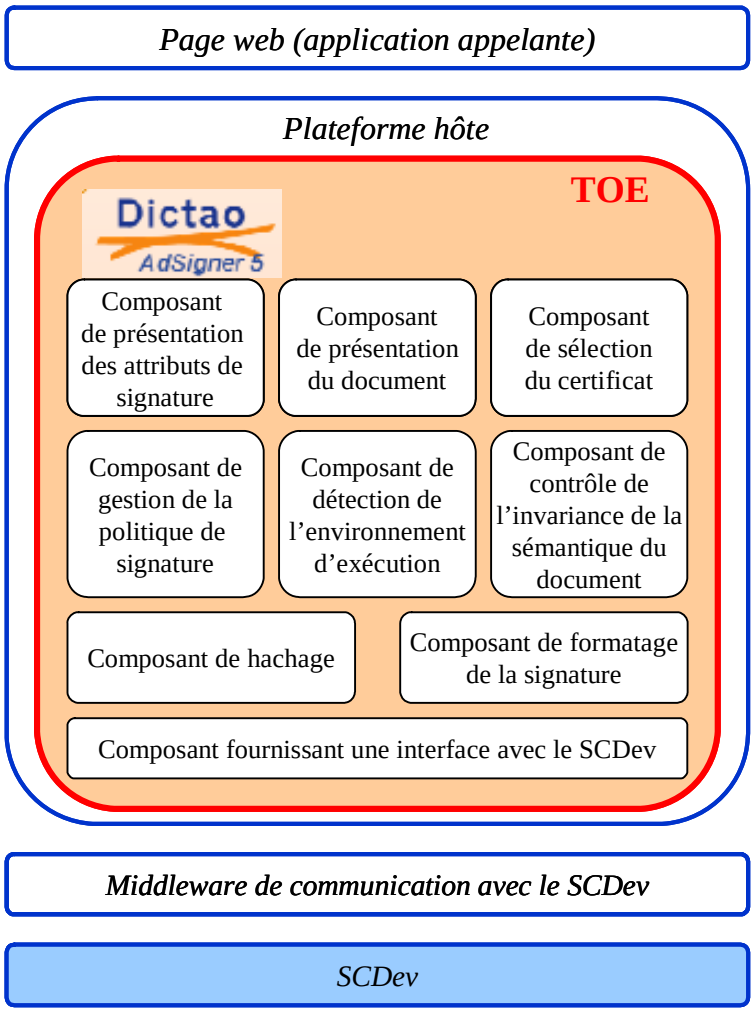

Figure 1 - Architecture de la TOE

Les éléments suivants, hors périmètre de cette évaluation, sont nécessaires au fonctionnement de la TOE :

- l'application appelante sur laquelle est intégrée la TOE ;
- la plateforme hôte, qui est constituée :
  - d'un système d'exploitation choisi parmi les suivants :
    Windows XP SP3 ;
    Windows Vista SP2+ ;
    Windows Seven SP1 ;
    Ubuntu Linux 9.04 ;
  - d'un navigateur web choisi comme suit :

Navigateur	Windows	Linux
Internet Explorer 7+	X	
Firefox 3+	X	X
Chrome 12+	X	

  - d'une machine virtuelle Java (JRE en version 1.5 ou 1.6) ;
- le middleware de communication avec le SCDev ;
- le SCDev. Le dispositif de création de signature peut être une carte à puce, un token USB ou un composant logiciel. Cependant, afin de satisfaire les exigences sur la

création de signature électronique, au sens de la directive européenne 1999/93/CE et du décret français n° 2001-272 du 30 mars 2001 sur la signature électronique, le SCDev doit être un SSCD (*Secure Signature Creation Device* – Dispositif sécurisé de création de signature), c'est-à-dire une carte à puce.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés par Dictao ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

Dictao

152 avenue de Malakoff
75116 Paris
France

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les développeurs et les administrateurs de l'application appelante, et comme utilisateurs du produit les signataires.

1.2.6. Configuration évaluée

Le certificat porte sur les quatre configurations suivantes :

Configuration 1 :

- système d'exploitation : Microsoft Windows XP SP3 ;
- navigateur : Firefox 3.6.27 ;
- environnement : Oracle JRE 1.6.31 ;
- middleware IAS ECC : version 2.0.20 (32 bits) ;
- TOE : AdSigner 5.0.0.1.

Configuration 2 :

- système d'exploitation : Microsoft Windows Vista SP2 ;
- navigateur : Chrome 17 (17.0.963.66 m) ;
- environnement : Oracle JRE 1.6.31 ;
- middleware IAS ECC : version 2.0.20 (32 bits) ;
- TOE : AdSigner 5.0.0.1.

Configuration 3 :

- système d'exploitation : Microsoft Windows Seven SP1 ;
- navigateur : Internet Explorer 8.0 ;
- environnement : Oracle JRE 1.6.31 ;
- middleware IAS ECC : version 2.0.20 (64 bits) ;
- TOE : AdSigner 5.0.0.1.

Configuration 4 :

- système d'exploitation : Ubuntu 9.04 ;
- navigateur : Firefox 3.0.8+nobinonly-0ubuntu3 ;
- environnement : Oracle JRE 1.6.31 ;
- middleware IAS ECC : version 2.0.8 ;
- TOE : AdSigner 5.0.0.1.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [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 23 mai 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et conclut que les mécanismes analysés sont conformes aux exigences du référentiel cryptographique de l'ANSSI.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI.

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.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

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 « AdSigner version 5.0.0.1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- (OE.Host_Platform) les mesures suivantes doivent être appliquées à la plateforme hôte :
    - la plateforme hôte doit être protégée contre les virus ;
    - les échanges entre la plateforme hôte et d'autres machines via un réseau ouvert doivent être contrôlés et limités par un pare-feu ;
    - l'accès aux fonctions d'administration de la plateforme hôte doit être restreint aux seuls administrateurs de celle-ci ;
    - l'installation et la mise à jour de logiciels sur la plateforme hôte doit être sous le contrôle de l'administrateur ;
    - le système d'exploitation de la plateforme hôte doit refuser l'exécution d'applications téléchargées ne provenant pas de sources sûres ;
    - la plateforme hôte doit être synchronisée avec une source de temps fiable ;

- (OE.SCDev) le SCDev doit avoir au moins pour fonction de générer effectivement la signature à partir des éléments communiqués par la TOE et être en charge de l'authentification du signataire ;

- (OE.TOE/SCDev_Communications) l'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le SCDev doit être capable de gérer un canal de communication garantissant l'intégrité et l'exclusivité de la communication ;

- (OE.Signatory_Authentication_Data_Protection) les composants logiques ou physiques, permettant au signataire de s'authentifier auprès du SCDev pour qu'il active la clé privée de signature correspondant au certificat sélectionné, doivent assurer la confidentialité et garantir l'intégrité des données d'authentification au moment de leur saisie et tout au long du transfert de ces données vers le SCDev ;

- (OE.Signatory_Presence) le signataire doit être présent entre le moment où il manifeste son intention de signer et celui où il entre les données d'authentification permettant d'activer la clé de signature ;

- (OE.Signature_Policy_Origin) l'administrateur de l'application appelante doit s'assurer de l'authenticité de l'origine des politiques de signature avant qu'elles ne soient utilisées par la TOE ;

- (OE.Trusted_Calling_Application) l'application appelante doit être de confiance ;

- (OE.Trusted_Calling_Application_Developer_and_Administrator) le développeur et l'administrateur de l'application appelante doivent être de confiance, formés à l'utilisation de la TOE et disposer des moyens nécessaires pour exécuter leurs tâches ;

- (OE.Services_Integrity) l'environnement de la TOE doit fournir à l'application appelante et à son administrateur les moyens de contrôler l'intégrité des services et des paramètres de la TOE ;

- (OE.Web_Communications) le canal de communication entre la plateforme hôte, sur laquelle s'exécute la TOE, et le serveur web, depuis lequel est téléchargée l'application appelante et sur lequel est hébergée la TOE, doit garantir l'intégrité des paramétres d'entrée de la TOE ;

- (OE.Web_Server) le serveur web hébergeant la TOE et l'application appelante doit garantir l'intégrité de la TOE et de l'application appelante ;

- le signataire doit contrôler l'heure et la date du système au moment de la signature de son document.

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 2010 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 E3 Elémentaire et CC EAL4. 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'Autriche, l'Espagne, la Finlande, la France, 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, le Pakistan, les Pays-Bas, la République de Corée, 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	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation 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**	1	**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 : - Security Target AdSigner 5 signature module Référence : dictao_adsigner_TSS Version 1.7 du 23/05/2012 Dictao. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target AdSigner 5 signature module Référence : dictao_adsigner_TSS_Public Version 1.2 Dictao.
[RTE]	Rapport technique d'évaluation – Projet AS5 Référence : OPPIDA/CESTI/AS5/RTE Version 2.0 du 23/05/2012 OPPIDA.
[ANA-CRY]	Cotation de mécanismes cryptographiques – Qualification AdSigner5, Référence : 823/ANSSI/ACE datée du 30 mars 2012, ANSSI.
[CONF]	Liste de configuration AdSigner 5 Référence : dictao_adsigner_ALC_CMS Version 3.0 du 23/09/2011 Dictao.
[GUIDES]	Guide d'administration du produit : - AdSigner5 – Guide Administration AGD_PRE Référence : dictao_adsigner5_AGD_PRE Version 5.1 du 06/10/2011 Dictao. Guide d'utilisation du produit : - AdSigner5 – Guide Utilisation AGD_OPE Référence : dictao_adsigner5_AGD_OPE Version 1.9 du 06/10/2011 Dictao.
[PP ACSE]	Profil de protection « Application de création de signature électronique », référence PP-ACSE-CCv3.1, version 1.7 du 2 mars 2011. *Certifié par l'ANSSI le 21 mars 2011 sous la référence ANSSI-CC-PP-2008/05-M01*.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.