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-2010/53

TrustySign version 4.1.4

Paris, le 26 août 2010

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-2010/53**
Nom du produit **TrustySign**
Référence/version du produit **Version 4.1.4**
Conformité à un profil de protection **Néant**
Critères d'évaluation et version **Critères Communs version 3.1 révision 2**
Niveau d'évaluation **EAL 3 augmenté** **ALC_FLR.3**
Développeur **C.S.** **22 avenue Galilée, 92350 Le Plessis-Robinson, France**
Commanditaire **C.S.** **22 avenue Galilée, 92350 Le Plessis-Robinson, 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 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 logiciel « TrustySign Version 4.1.4 » développé par la société C.S.

La cible d'évaluation (TOE – *Target of Evaluation*) est une application permettant à la fois :
- de créer des signatures électroniques en s'appuyant sur un dispositif de création de signature (dénommé SCDev) effectuant les calculs cryptographiques mettant en œuvre la clé privée du signataire ;
- de vérifier une signature électronique d'un document ;
- de chiffrer/déchiffrer un document pour un ou plusieurs destinataires ;
- de gérer les politiques de signature et de chiffrement applicables aux opérations de sécurité ;
- d'administrer et de configurer la cible d'évaluation.

1.2. Description du produit

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 de l'application TrustySign (version 4.1.4) est identifiable par le menu ' ? -> A propos' de l'interface.
Ce numéro de version est également disponible à travers l'interface du panneau de configuration de Windows listant les programmes installés, ou encore à travers le nom du fichier en .jar présent dans le répertoire d'installation (TrustySign-4.1.4.jar).

Le logiciel TrustyAdmin version 1.1.2 est également utilisé pour l'administration des politiques de signature et de chiffrement.
La version de l'application TrustyAdmin est identifiable de la même façon que l'application TrustySign.

1.2.2. Services de sécurité

La cible d'évaluation offre les services suivants :
- l'authentification de l'utilisateur avant toute action de signature ou de déchiffrement ;
- la réalisation d'une signature (ou d'une sur-signature ou d'une co-signature) suivant les standards CMS, XMLDSIG ou XADES ;
- la vérification de la signature d'un fichier dans le format CMS, XMLSIG ou XADES et l'extraction du document d'origine ;
- l'horodatage des signatures suivant les standards CADES-T, ou XADES-T par interrogation d'un système d'horodatage externe ;
- le chiffrement dans le format CMS ou XML_Enc d'un ou plusieurs documents ;
- le déchiffrement dans le format CMS ou XML_Enc d'un ou plusieurs documents ;

- l'authentification de l'administrateur de sécurité avant toute action de gestion des politiques ;
- la visualisation des politiques disponibles ;
- l'ajout ou la suppression de politiques ;
- la sélection des politiques applicables ;
- la gestion des paramètres relatifs aux composants externes à la cible d'évaluation, qui contiennent les clés secrètes et les données d'authentification.

La TOE permet également de lancer une application de visualisation, permettant au signataire de visualiser le document à signer et au vérificateur de visualiser le document dont la signature est à vérifier.

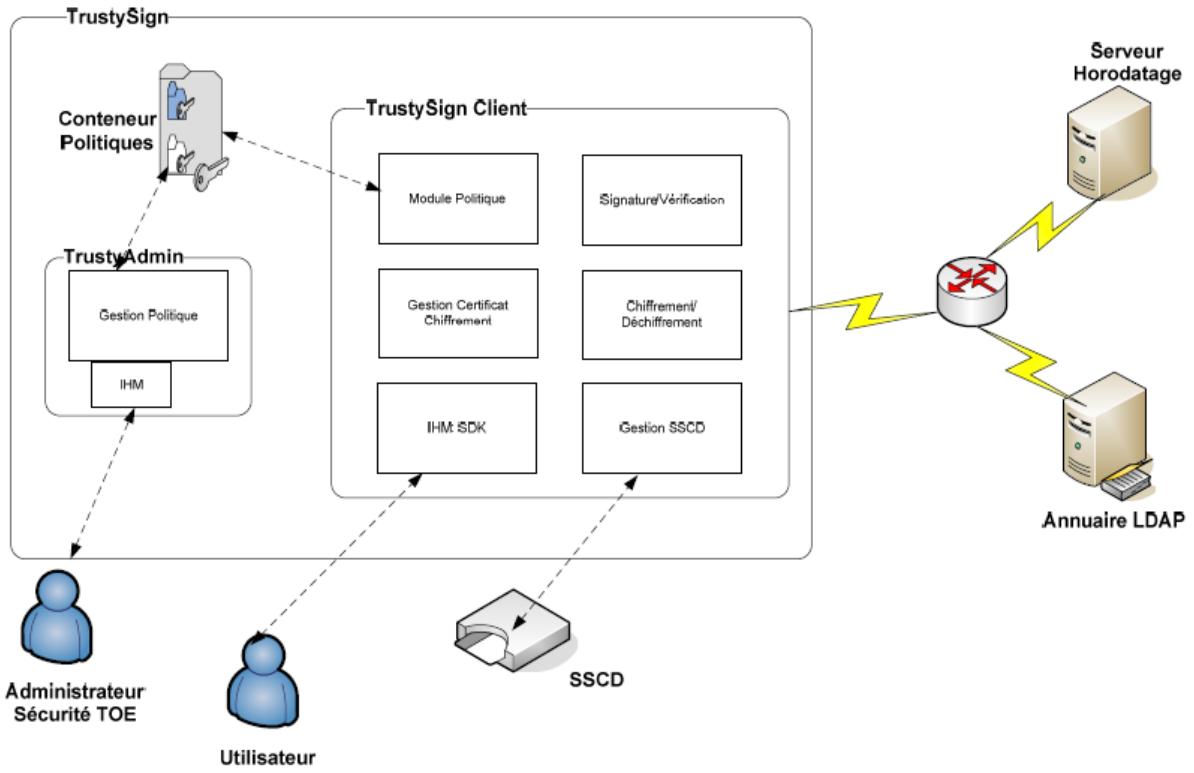
1.2.3. Architecture

Le produit TrustySign est constitué d'une composante client et d'une composante d'administration.

La composante TrustySign Client représente la partie principale de la TOE. Elle prend en charge des services de signature/vérification et de chiffrement/déchiffrement. Pour réaliser ces services, TrustySign Client met à la disposition des utilisateurs une interface sous la forme d'une IHM (Interface Homme Machine) et un SDK (*Software Development Kit* – Kit de développement logiciel) pour l'intégration dans un autre logiciel (progiciel métier par exemple). TrustySign Client réalise les opérations de sécurité conformément aux paramètres définis dans les politiques de signature et de chiffrement. Ces politiques sont incluses dans un fichier conteneur protégé en intégrité.

Pour permettre une gestion simple de ces politiques, TrustySign dispose d'une composante d'administration indépendante (TrustyAdmin) permettant de gérer les politiques de signature et de chiffrement définissant le pilotage des opérations de sécurité.

La figure ci-dessous donne une vue d'ensemble de la TOE :



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

- la communication (envoi de fichiers signés, chiffrés, …) au destinataire ;
- la visualisation (la TOE ne contient pas d'application de visualisation).

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés par C.S. ;
- 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 :

C.S.

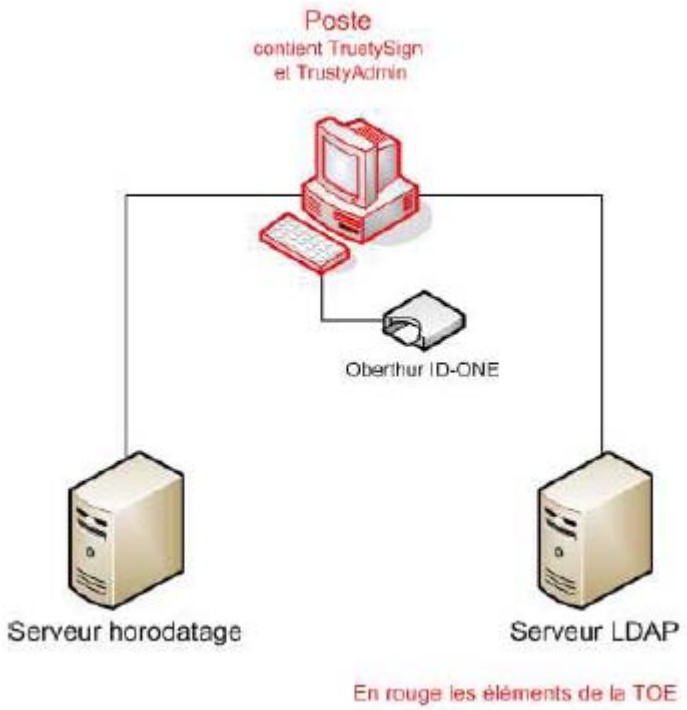
22 avenue Galilée
92350 Le Plessis-Robinson
France

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit l'administrateur de sécurité de la TOE qui a pour prérogative de gérer les biens sensibles de la TOE et ses paramètres de configuration.

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit les utilisateurs qui interagissent avec la TOE pour signer, vérifier, chiffrer ou déchiffrer un ou plusieurs documents selon une politique de signature ou de chiffrement. L'utilisateur peut être un être humain ou un système automatisé.

1.2.5. Configuration évaluée

La plateforme de tests mise en œuvre par le CESTI correspond à la configuration suivante :



Le certificat porte sur la configuration suivante du poste client :

- système d'exploitation : Microsoft Windows Vista SP1 ;
- SCDev : Oberthur ID-ONE classic card ;
- environnement : JRE 1.6.0.20 (6 update 2) ;
- TOE : TrustySign 4.1.4 et TrustyAdmin 1.1.2.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 2** [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 21 juin 2010, 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 les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques [REF-CRY], [REF-KEY] et [REF-AUT] n'a pas été réalisée par l'ANSSI. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé.

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 « TrustySign Version 4.1.4 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 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 :

- (OE.Machine_Hôte) les mesures suivantes doivent être appliquées à la machine hôte :
  - la machine hôte doit être protégée contre les virus ;
  - les échanges entre la machine 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 machine hôte doit être restreint aux seuls administrateurs de celle-ci ;
  - l'installation et la mise à jour de logiciels sur la machine hôte doit être sous le contrôle de l'administrateur ;
  - le système d'exploitation de la machine hôte doit refuser l'exécution d'applications téléchargées ne provenant pas de sources sûres ;

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

- (OE.Présentation_Document) le système dans lequel s'insère la TOE doit posséder des applications de visualisation ;

- (OE.Contrôle_Sémantique_Document) l'environnement de la TOE doit fournir un module capable de déterminer si la sémantique du document signé/à signer est soit bien invariante, soit stable, soit n'a pas pu être vérifiée. Ce module doit communiquer le statut de son analyse à la TOE ;

- (OE.Authenticité_Origine_Politique_Signature) les administrateurs de la TOE doivent s'assurer de l'authenticité de l'origine des politiques de signature avant qu'elles ne soient utilisées par la TOE ;

- (OE.Administrateur_De_Sécurité_Sûr) l'administrateur de sécurité de la TOE doit être de confiance, formé à l'utilisation de la TOE et disposer des moyens nécessaires à la réalisation de son activité ;

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

- (OE.Fournitures_Des_Données_De_Validation) l'environnement de la TOE doit lui fournir les données de validation nécessaires à la vérification de la signature.

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 :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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[1], 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 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 configuration management coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification if 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**	**2**	**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	**2**	Vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité Critères Communs TrustySign v4 Référence : CSSI/HLS/TRUSTY/FR/7/0057, version 2.0 du 01/06/2010 CS
[RTE]	Rapport technique d'évaluation – Projet NAMMU Référence : OPPIDA/CESTI/NAMMU/RTE du 16/06/2010 OPPIDA
[CONF]	Liste de configuration 4.1.4 Référence : CSSI/HLS/TRUSTY/FR/10/0034, version 1.0 du 04/06/2010 CS
[GUIDES]	Guide d'administration du produit : - TrustySign 4 Manuel d'administration Référence : CSSI/HLS/TRUSTY/FR/8/0061, version 1.8 du 07/05/2010 CS - Description SDK Java, TrustySign 4 Référence : CSSI/HLS/TRUSTY/FR/9/0123, version 1.5 du 07/05/2010 CS Guide d'utilisation du produit : - TrustySign 4 Manuel d'utilisation Référence : CSSI/HLS/TRUSTY/FR/8/0070, version 2.0 du 07/05/2010 CS

Annexe 3. Références liées à la certification

Décret 2002-535 modifié 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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[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, voir www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr