PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2021/33

Zed!
(Version Q.2020.1)

Paris, le 13 juillet 2021

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti 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 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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2021/33**
Nom du produit **Zed!**
Référence/version du produit **Version Q.2020.1**
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 3 augmenté** ALC_FLR.3, AVA_VAN.3
Développeur **Prim'X Technologies S.A.** SKY 56, 18 Rue du Général Mouton-Duvernet 69003 Lyon, France
Commanditaire **Prim'X Technologies S.A.** SKY 56, 18 Rue du Général Mouton-Duvernet 69003 Lyon, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3. **SOG-IS** Ce certificat est reconnu au niveau EAL3 augmenté de FLR.3.

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Zed!, Version Q.2020.1 » développé par Prim'X Technologies S.A..

Zed! est un produit de sécurité pour postes de travail opérant sous Windows, Linux et Mac. Il se présente comme un produit autonome. Son rôle est de permettre aux utilisateurs de fabriquer des conteneurs de fichiers compressés et chiffrés. Le produit intègre par ailleurs un mécanisme de contrôle de l'intégrité des fichiers stockés dans les conteneurs. Ces conteneurs sont destinés à servir d'archive, ou, plus généralement, de pièce-jointe chiffrée dans des courriers électroniques échangés dans une société.

Zed! se décline en différents packages :
- l'édition standard, qui contient le produit complet ;
- l'édition limitée (appelé «Zed! Edition Limitée»), gratuite, libre de distribution et d'usage, qui permet aux correspondants de lire le contenu des conteneurs (moyennant la fourniture d'une clé d'accès) et d'en extraire les fichiers. Le correspondant a également le droit de modifier le contenu du conteneur (enlever, ajouter des fichiers) pour pouvoir le renvoyer à l'émetteur d'origine. L'édition limitée ne lui permet pas, cependant, de créer de nouveaux conteneurs ou de modifier les accès prévus par le créateur original du conteneur. L'édition limitée se présente sous la forme d'un simple exécutable (zedle.exe), facile à transporter, et qui évite d'avoir à effectuer une installation ;
- Zed! est également incorporé dans les différents produits de la gamme ZoneCentral.

Dans le cadre de cette évaluation seules l'édition standard et l'édition limitée, toutes les deux installées sous Windows 10, ont été prises en compte.

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.

1.2.2 *Services de sécurité*

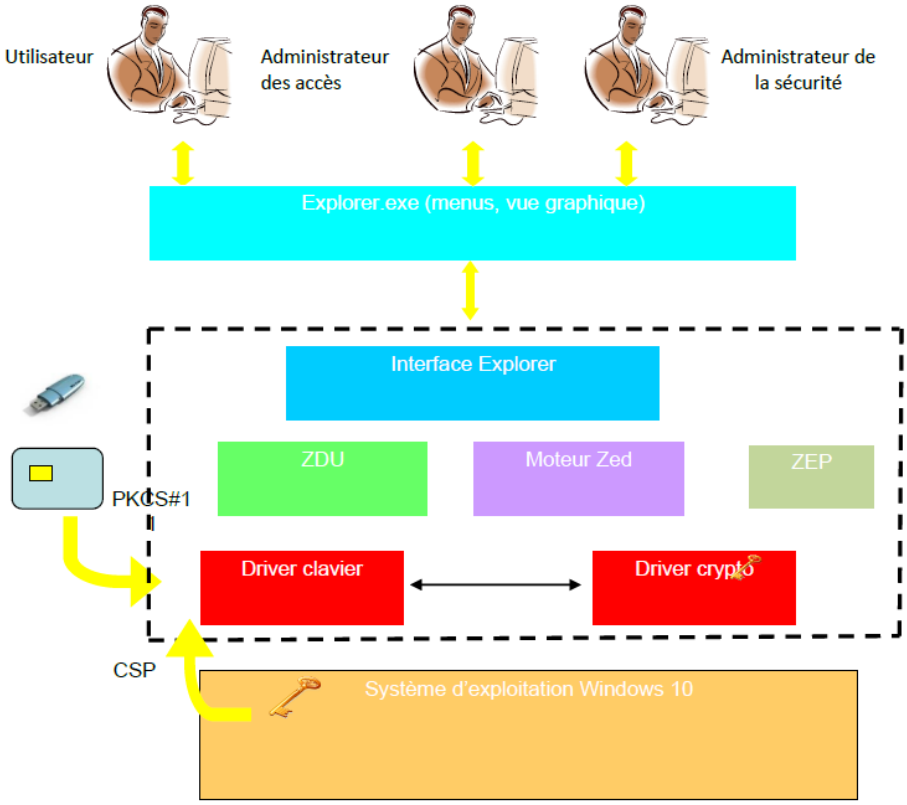
Les principaux services de sécurité fournis par le produit sont :
- la protection des conteneurs chiffrés notamment lors de leur ouverture que ce soit pour la lecture, le remplissage ou la gestion des accès ;
- la gestion de la saisie du mot de passe et sa dérivation en une clé d'accès ;
- la gestion de la saisie du code confidentiel du fichier de clés ;
- la gestion de la saisie du code confidentiel du *token* logique ;
- la conservation dans le conteneur de fichiers et dossiers sous forme chiffrée avec la possibilité de masquer leurs noms ;
- le contrôle de l'intégrité lors de l'ouverture d'un fichier ;
- la protection des différentes clés ;
- la protection de chaque vecteur d'initialisation spécifique à chacun des fichiers ;
- la vérification, avant leur application, des politiques définies par l'administrateur de la sécurité (version standard uniquement) ;

- la vérification de l'intégrité du fichier de contrôle. Ce fichier contient le libellé du conteneur, un identifiant unique, des informations de gestion et les clés de chiffrement du conteneur ;
- la vérification d'intégrité du fichier dit « catalogue ». Ce dernier contient les fichiers applicatifs du conteneur avec leurs positions dans l'arborescence, les tailles originales, les horodatages, etc.

1.2.3 *Architecture*

Le produit Zed! se décline en deux packages :
- l'édition standard contient le produit complet ;
- l'édition limitée est une version « bridée » de l'édition standard.

Zed! Edition Standard.

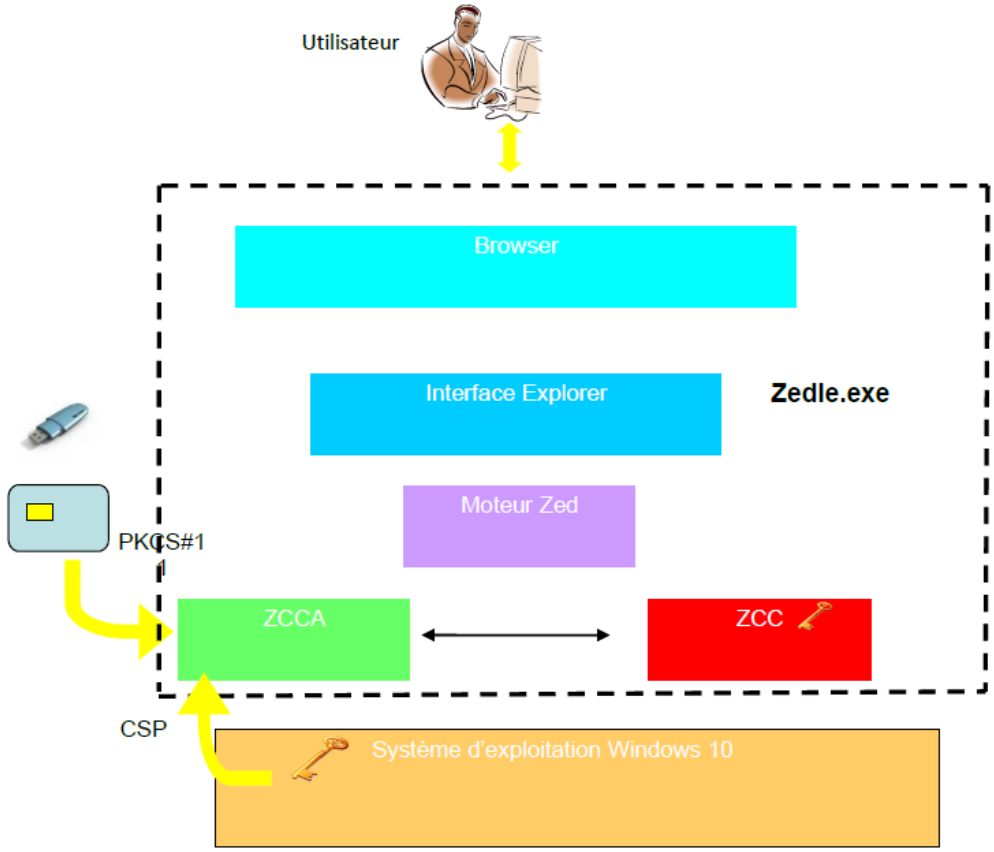


Cette figure présente l'architecture du produit dans sa version « standard » (TOE délimitée par les pointillés) ainsi que ses principaux composants :
- le module « Interface Explorer » implémente les interfaces Shell de Windows permettant de gérer les menus et la vue graphique accessibles à partir de l'explorateur Windows ;
- le module « ZDU » est un « *daemon* » utilisateur instancié pour chaque session utilisateur Windows qui pointe les clés des utilisateurs générées par le produit via l'entrée d'un mot de passe, l'interface PKCS#11, le *Cryptographic Service Provider* (CSP) ou le *Cryptographic Next Generation* (CNG) ;
- le service « ZEP » contrôle la signature des politiques ;
- le module « Moteur Zed » coordonne les différents traitements ;

- le « *driver crypto* » implanté en mode *Kernel*, est le centre cryptographique de Zed! « Edition Standard » : il gère les clés de conteneurs et exécute les différentes opérations de calcul. Les clés générées ne sortent jamais du produit ;
- le « *driver clavier* » est un filtre de saisie clavier : il intercepte à très bas niveau les mots de passe et codes confidentiels saisis de façon à ce que leurs valeurs restent confinées le plus bas possible dans le système.

Zed! Edition Limitée.

Zed! Edition Limitée est une déclinaison du produit Zed! Edition Standard.



La figure ci-dessus présente l'architecture du produit dans sa version « limitée » (TOE délimitée par les pointillés) ainsi que ses principaux composants :

- le module « *Browser* » émule l'Explorer Windows ;
- le module « *Interface Explorer* » permet de gérer les menus et la vue graphique ;
- le module « Moteur Zed » coordonne les différents traitements ;
- le module « ZCC » est le centre cryptographique de Zed! « Edition Limitée » : il gère les clés et exécute les opérations de calcul. Ici, « ZCC » est un applicatif alors que le « *driver crypto* » de Zed! « Edition Standard » est implanté en mode *Kernel* ;
- le module « ZCCA » pointe les clés des utilisateurs générées par le produit via l'entrée d'un mot de passe, l'interface PKCS#11 ou le CSP.

1.2.4 *Identification du produit*

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

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

- Edition standard :
  - nom du package : Setup Zed! Q.2020.1 x64.exe ;
  - valeur de la signature : 04 20 65 BF 61 34 AF 5C 42 92 1B E1 1A FD CD D4 29 CC E4 6F E3 12 F5 70 27 B9 CF 0E F7 1B 9E 17 00 C1.
- Edition limitée :
  - nom du package : zedle Q.2020.1 x64.exe ;
  - valeur de la signature : 04 20 9A 31 5F 24 07 54 36 D3 20 6B 5D 4F 08 12 F2 2D CA 4E A2 CD CA A8 D2 15 D4 93 0C DF 70 F1 F1 B4.

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés sur le site de Prim'X Technologies à Lyon ;
- 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 :

Prim'X Technologies S.A

Immeuble Sky56 (PRIM'X)

18 Rue du Général Mouton-Duvernet

69003 LyonFrance

1.2.6 *Configuration évaluée*

Les produits « Edition Standard » et « Edition Limitée » ont été évalués sur le système d'exploitation Windows 10 (64 bits).

La cible d'évaluation correspond à « Zed! Edition Standard » et « Zed! Edition Limitée » en version exécutable avec les politiques de sécurité activées en section 2.3.3.1 de la cible de sécurité [CIBLE].

Le produit intégré dans « ZoneCentral » ne fait pas partie du périmètre de l'évaluation.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 5 [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 14 décembre 2020, 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 a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI.

Les 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.3 visé.

2.4 Analyse du générateur d'aléas

Le générateur de nombres aléatoires du produit a été évalué. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Comme requis dans le référentiel cryptographique de l'ANSSI [REF], sa sortie subit un retraitement de nature cryptographique.

Les 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.3 visé.

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 « Zed!, Version Q.2020.1 » 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].

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 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Le présent certificat est reconnu par le SOG-IS au niveau EAL3 augmenté de ALC_FLR.3

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

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 EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Le présent certificat est reconnu par le CCRA au niveau EAL2 augmenté de ALC_FLR.3.

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Niveau d'évaluation du produit CCv3.1R5

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	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	**3**	*Focused vulnerability analysis*

ANNEXE B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - PRIMX-ZED ! Q.2020 Cible de sécurité (PX185856r8 v1r8), octobre 2020
[RTE]	Rapport technique d'évaluation : - Rapport technique d'évaluation, référence OPPIDA/CESTI/CC/ZED6.2/RTE, version 1.0 du 14 décembre 2021
[ANA-CRY]	Rapport d'analyse des mécanismes cryptographique, version 3.0 du 10 mai 2021
[CONF]	Liste de configuration du produit : - PRIMX-Zed Q.2020 Liste de configuration, référence PX2051286, version v1r4 du 12 novembre 2020.
[GUIDES]	Guide d'installation du produit : - Zed! Q.2020 Guide d'installation FR, référence PX2011233, version 1. Guide d'administration du produit : - Manuel des politiques Q.2020 FR, référence PX2011213, version 1 ; - Mise en œuvre de la signature des politiques FR, référence PX13C133r3, version 1. Guide d'utilisation du produit : - Zed! Q.2020 Guide d'utilisation des conteneurs chiffrés FR, référence PX2011230r2 ; - Zed! Limited Edition Q.2020 Guide FR, référence PX2011235.

ANNEXE C. 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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.