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-2017/28

ID-One ePass IDL Full EACv2 in EAC with PACE MRTD configuration on Infineon SLE77CLFX2400P and SLE77CLFX2407P

Paris, le 11 mai 2017

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

Guillaume POUPARD
[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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2017/28

Nom du produit

ID-One ePass IDL Full EACv2 in EAC with PACE MRTD configuration on Infineon SLE77CLFX2400P and SLE77CLFX2407P

Référence/version du produit

code SAAAAR : 084194

Conformité à un profil de protection

Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE [PP_EACwPACE]

Version 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02

Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP_PACE]

Version 1.01, BSI-CC-PP-0068-V2-2011-MA-01

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2 et AVA_VAN.5

Développeur(s)

Oberthur Technologies
420 rue d'Estienne d'Orves,
CS 40008, 92705 Colombes, France

Infineon Technologies AG
Am Campeon 1-12, 885579 Neubiberg,
Allemagne

Commanditaire

Oberthur Technologies
420 rue d'Estienne d'Orves, CS 40008, 92705 Colombes, France

Centre d'évaluation

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

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 la carte à puce « ID-One ePass IDL Full EACv2 in EAC with PACE MRTD configuration on Infineon SLECLFX2400P and SLE77CLFX2407P », pouvant être utilisée en mode contact ou sans contact. Le produit est développé par *OBERTHUR TECHNOLOGIES* et *INFINEON TECHNOLOGIES AG*.

Le produit implémente les fonctions de document de voyage électronique conformément (1) aux spécifications de l'organisation de l'aviation civile internationale (ICAO), et (2) préconisations de la Commission Européenne pour les passeports européens biométriques (Décision d'exécution C(2013) 6181) et titres de séjour européens biométriques (Décision d'exécution C(2013) 6178). Ce produit permet à l'aide d'un système d'inspection, la vérification de l'authenticité du document de voyage et l'identification de son porteur lors du contrôle aux frontières.

La cible d'évaluation est composée de l'application ID-One ePass Full EAC v2 MRTD, en configuration [EACwPACE] (*Extended Access Control with Password Authenticated Connection Establishment*) avec AA (*Active Authentication*) qui réalise les fonctions de document électronique de voyage.

Mutatis mutandis, ce produit peut aussi être utilisé en tant que permis de conduire conforme à l'ISO/IEC 18013 ou ISO/IEC TR 19446 utilisant les mécanismes (1) PACE, (2) AA et (3) EAC. En effet les deux applications (document de voyage et permis de conduire) partagent les mêmes mécanismes et structures de données. Ainsi, ce document reste applicable dans le cas où le produit est utilisé en tant que permis de conduire.

Ce microcontrôleur et son logiciel embarqué peuvent être intégrés sous forme de module ou d'*inlay*. Le produit final peut être un passeport, un permis de conduire, une carte plastique, etc.

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 strictement conforme au profil de protection [PP_EACwPACE].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- la protection, en intégrité et en confidentialité, des données lues à l'aide du mécanisme de *Secure Messaging* ;

- l'authentification du microcontrôleur par le mécanisme optionnel *Active Authentication* (AA) ;
- le mécanisme *Extended Access Control* (EAC) d'authentification forte entre le microcontrôleur et le système d'inspection préalable à tout accès aux données biométriques, permettant l'établissement d'un canal sécurisé fort (*secure messaging*) ;
- Le mécanisme *Password Authenticated Connection Establishment* (PACE) pour (1) l'authentification entre le microcontrôleur et le système d'inspection, et (2) l'établissement d'un canal sécurisé fort (*secure messaging*).

Il existe en plus, une fonction optionnelle hors périmètre de cette évaluation, *Digital Blurred Image* permettant de rendre la photo illisible après une phase d'activation du document, éventuellement réalisable à distance.

1.2.3. Architecture

Le produit est une carte à puce qui est constitué :

- d'un microcontrôleur SLE77CLFX2400P ou SLE77CLFX2407P développé par *INFINEON TECHNOLOGIES* ;
- d'un module « BIOS » qui fournit les fonctionnalités pour la gestion des accès vers la couche applicative. Il fournit également les fonctions de gestion des exceptions et de communication ;
- d'une librairie cryptographique qui fournit à la couche applicative, les fonctions de sécurité cryptographique ;
- d'un module *Secure Messaging* qui fournit les fonctionnalités pour protéger en intégrité, authenticité et confidentialité les données permettant ainsi de disposer d'un moyen de communication sécurisée durant les phases de fabrication, de personnalisation et d'utilisation opérationnelle ;
- de *Resident Application* (RA), un jeu de commandes complet qui permet la gestion de la carte dans sa phase opérationnelle ;
- de l'*Application Creation Engine* (ACRE), un jeu de commandes complet utilisé pour pré-personnaliser la carte et ses applications ;
- de l'application *Machine Readable Travel Document* (MRTD), un jeu de commandes complet qui permet la gestion des données MRTD durant la phase opérationnelle ;
- et d'un *boot* qui est en charge de gérer le démarrage des applications MRTD, RA et ACRE.

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 des *CPLC Data* suivants :

- *IC fabricator* : 0x4830 ;
- *IC type* : 0x7734 (SLE77CLFX2400P) ou 0x7767 (SLE77CLFX2407P) ;
- *Operating System identifier* : 0x8231 ;
- *Operating System release date* : 0x7012 ;
- *Operating release level* : 0x303D.
- *SAAAAR code* : 0x084194FF (l'octet de poids faible 0xFF est *RFU*[1]).

[1] Réservé pour un usage futur.

Ces valeurs peuvent être vérifiées en utilisant la commande GETDATA avec le *tag* 9F7F comme indiqué dans [GUIDES].

Durant les phases de pré-personnalisation et de personnalisation, les commandes « WRITE LOCK » et « READ LOCK » [GUIDES] sont disponibles pour activer ou désactiver une configuration (BAC, EAC, PACE, etc.), ou pour consulter la(es) configuration(s) activée(s) de la TOE.
A noter que ces commandes ne sont plus disponibles en phase d'utilisation (phase 4 du [PP_EACwPACE] et [PP_PACE], *step* 7 du [PP0035] du cycle de vie).

1.2.5. Cycle de vie

Les deux cycles de vie du produit sont décrits au chapitre 2.2.3 de la cible de sécurité [ST].

Les microcontrôleurs SLE77CLFX240xP, nom commercial des M7794 A12 and G12 ont été développés et fabriqués par *INFINEON TECHNOLOGIES*. Les sites de développement et de fabrication des microcontrôleurs sont détaillés dans le rapport de certification [CERT_IC].

Les produits sont développés sur les sites suivants :

OBERTHUR TECHNOLOGIES **– Site de Colombes**
420 rue d'Estienne d'Orves
92700 Colombes
France

OBERTHUR TECHNOLOGIES **– Site de Pessac**
Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

OBERTHUR CARD SYSTEMS SCIENCE AND TECHNOLOGY **- Site de Shenzhen**
4F, Great wall technology building
No 2, KeFa Rd
Science and Technology park, Nanshan district
Shenzhen, 518057
P. R. of CHINA

OBERTHUR TECHNOLOGIES **– Site de Vitré**
Avenue d'Helmstedt
BP 90308
35503 Vitré Cedex
France

Les « administrateurs du produit » sont les nations ou organisations émettrices des documents. Les « utilisateurs du produit » sont les détenteurs des documents et les systèmes d'inspection pendant la phase d'utilisation.

1.2.6. Configuration évaluée

Le certificat porte sur la configuration incluant :

- le mécanisme EAC (*Extended Access Control*) - incluant entre autre le mécanisme CA (*Chip Authentication*) - enrichi par rapport au [PP_EACwPACE] avec la fonctionnalité d'exigence d'un niveau minimum de *secure messaging* préalablement configuré pour accéder aux données biométriques sensibles (iris, empreinte biométrique), afin de garantir un niveau de confidentialité adéquate ;
- le mécanisme PACE (*Password Authenticated Connection Establishment*) ;
- le mécanisme AA (*Active Authentication*) qui est optionnel et éventuellement désactivé ;
- les phases de pré-personnalisation et de personnalisation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans les microcontrôleurs déjà certifiés par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation des microcontrôleurs « M7794 A12 et G12 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP0035]. Ces microcontrôleurs ont été certifiés, le 12 juin 2015 sous la référence « BSI-DSZ-CC-0964-2015 ». Le niveau de résistance de ces microcontrôleurs a été confirmé le 7 avril 2017 [CERT_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 avril 2017, 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 [RGS] si les documents [GUIDES] sont respectés. 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.5 visé.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI ([RTE]). 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.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur [CERT_IC].
Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas 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.5 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 « ID-One ePass IDL Full EACv2 in EAC with PACE MRTD configuration on Infineon SLE77CLFX2400P and SLE77CLFX2407P », code SAAAAR : 084194 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur 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, 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, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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 EAL2 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, la Pologne, 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, le Qatar, 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 5+	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	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Semiformal modular 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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
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	3	Testing: modular 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	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ID-One ePass IDL Full EACv2 in EAC with PACE MRTD configuration – Security Target, référence FQR110 8176, version 4 en date du 20 février 2017, *OBERTHUR*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ID-One ePass IDL Full EACv2 in EAC MRTD configuration – Security Target Lite, référence FQR110 8336, version 2 en date de février 2017, *OBERTHUR*.
[RTE]	Rapport technique d'évaluation : Evaluation Technical Report, référence ASTERION_ETR_v1.2, version 1.2 en date du 21 avril 2017, *SERMA SAFETY & SECURITY*.
[ANA-CRY]	Cryptographic Mechanisms Evaluation Report, référence ASTERION_MRTD_cryptography_v1.1 / 1.1, version 1.1 daté du 17 mars 2017, *SERMA SAFETY & SECURITY*.
[CONF]	Liste de configuration du produit : - Configuration List, référence FQR 110 8173, version 3 en date du 12 avril 2017, *OBERTHUR*.
[GUIDES]	- ePass ICAO essential Perso Guide, référence FQR 110 7226, version 6 datée du 9 janvier 2017, *OBERTHUR* ; - ePass ICAO essential OPErational user Guide, référence FRQ 110 8250, version 2 datée du 18 octobre 2016, *OBERTHUR* ; - Recommendations for crypto assessment compatibility, référence FRQ 110 8357, version 1 datée du 3 février 2017, *OBERTHUR*.
[PP_EACwPACE]	Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Application Control with PACE, version 1.3.2, 5 décembre 2012. Certifié et maintenu par le BSI *(Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.
[PP_PACE]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.01, 22 juillet 2014. Certifié et maintenu par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-CC-PP-0068-V2-2011-MA-01.
[PP0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-PP-0035-2007.

[CERT_IC]	Infineon Technologies Security Controller M7794 A12 and G12 with optional RSA2048/4096 v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software. Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* le 7 avril 2017 sous la référence BSI-DSZ-CC-0964-V2-2017.

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[CC RA]	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.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.