



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-2017/70

**Taiwan eID Applet EAC with AA on ID-one
V8.1 - Standard LDS Platform on NXP
P6021M VB and on ID-One Cosmo v8.1-N -
Large Platform on NXP P6022M VB
(version 03 00 00 00)**

Paris, le 14 février 2018

*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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.



Référence du rapport de certification

ANSSI-CC-2017/70

Nom du produit

**Taiwan eID Applet EAC with AA on ID-one V8.1 -
Standard LDS Platform on NXP P6021M VB and on ID-
One Cosmo v8.1-N - Large Platform on NXP P6022M VB**

Référence/version du produit

Version 03 00 00 00

Conformité à un profil de protection

BSI-CC-PP-0056-V2-2012, [PP EAC], version 1.3.0
Machine Readable Travel Document with ICAO Application

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL5 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

Chunghwa Telecom (CHT)

N°99 Dianyan Road – Yangmei Distric, Taiwan
Taoyuan City 32661, Taiwan

IDEMIA

(ex Oberthur Technologies)

420 rue d'Estienne d'Orves, 92700 Colombes,
France

NXP Semiconductors GmbH

Stresemannallee 101, 22539 Hamburg,
Allemagne

Commanditaire

IDEMIA

420 rue d'Estienne d'Orves, 92700 Colombes, France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA



SOG-IS



Ce certificat 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	7
1.1. PRESENTATION DU PRODUIT	7
1.2. DESCRIPTION DU PRODUIT	7
1.2.1. Introduction	7
1.2.2. Services de sécurité	7
1.2.3. Architecture	8
1.2.4. Identification du produit	8
1.2.5. Cycle de vie	8
1.2.6. Configuration évaluée	9
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION	10
2.2. TRAVAUX D’EVALUATION	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	10
2.4. ANALYSE DU GENERATEUR D’ALEAS	10
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D’USAGE	12
3.3. RECONNAISSANCE DU CERTIFICAT	13
3.3.1. Reconnaissance européenne (SOG-IS)	13
3.3.2. Reconnaissance internationale critères communs (CCRA)	13
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT [CCV3.1R4]	14
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	15
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	17



1. Le produit

1.1. Présentation du produit

Le produit évalué est « Taiwan eID Applet EAC with AA on ID-one V8.1 - Standard LDS Platform on NXP P6021M VB and on ID-One Cosmo v8.1-N - Large Platform on NXP P6022M VB, version 03 00 00 00 » développé par *IDEMIA* et *NXP SEMICONDUCTORS GMBH*.

Le produit certifié est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels, dans une *eCover* ou dans une *eDatapage*. Le produit final peut prendre différentes formes, de carte ou de module, avec et/ou sans contact.

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-EAC].

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 : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme « Active Authentication » ou « Chip Authentication » ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme « Supplemental Access Control » (PACE) ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « Secure Messaging », des données lues ;
- l'authentification forte (avec validation de la chaîne de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (« Extended Access Control ») préalablement à tout accès aux données biométriques.

1.2.3. Architecture

Le produit est constitué :

- des microcontrôleurs NXP P6021M VB ou NXP P6022M VB avec leur librairie cryptographique certifiés respectivement sous les références [CER-IC1] et [CER-IC2] ;
- de la plateforme Javacard fermée « ID-One Cosmo V8.1-N Standard LDS » certifiée sous la référence [CER-JC1], ou de la plateforme Javacard fermée « ID-One Cosmo V8.1-N Large » certifiée sous la référence [CER-JC2] ou de la plateforme Javacard fermée « ID-One Cosmo V8.1-N R2 Large » qui a fait l'objet d'une maintenance [MAI-01] ;
- de l'applet « Taiwan eID Applet EAC with AA, version 03 00 00 00 ».

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 la méthode indiquée dans [GUIDES], qui permet :

- la sélection de l'application ;
- la lecture de la version commerciale de l'application obtenue par la commande GET DATA 00 CA DF 66 00. La réponse attendue est DF 66 0A 20 28 42 FF **03 00 00 00 01 02**, où **03 00 00 00** correspond à la version commerciale et **01 02** correspond à la version interne de l'application Taiwan eID ;
- la lecture de la réponse attendue à la commande GET DATA avec le tag DF 67 qui est : DF 67 04 0A 00 09 0B ;
- l'identification de la plateforme et du composant tel que décrit dans les paragraphes 1.2.4 de [CER-JC1], de [CER-JC2] et du paragraphe 2 de [MAI-01].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

	Phase	Acteur	Couvert par
Etape 1	Développement	<i>IDEMIA</i>	ALC
	Développement	<i>CHUNGHWA TELECOM</i>	ALC
Etape 2	Développement	<i>NXP SEMICONDUCTORS</i>	ALC
Etape 3	Fabrication	<i>NXP SEMICONDUCTORS</i>	ALC
Point de livraison TOE			
Etape 4	<i>Packaging</i>	<i>IDEMIA</i>	AGD_PRE
Etape 5	Pré-Personnalisation	<i>IDEMIA</i>	AGD_PRE
Etape 6	Personnalisation	Personnalisateur	AGD_PRE
Etape 7	Utilisation opérationnelle	Utilisateur final	AGD_OPE

Le produit a été développé sur les sites suivants :

CHUNGHWA TELECOM – Taiwan N°99 Dianyuan Road – Yangmei Distric, Taiwan Taoyuan City 32661, Taiwan	IDEMIA – Manila 19F – Ayala Life FGU Center, 6811 Ayala Avenue, Makati City, Philippines
---	--



<p>IDEMIA – Colombes 420 rue d’Estienne d’Orves 92700 Colombes, France</p>	<p>IDEMIA – Pessac Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France</p>
---	--

Les sites de développement des composants et des plateformes sont couverts par les certificats [CER-IC1], [CER-IC2], [CER-JC1] et [CER-JC2].

1.2.6. Configuration évaluée

Le certificat porte sur le produit identifié au 1.2.4 configuré comme suit :

- l’*applet* « Taiwan eID Applet EAC with AA, version 03 00 00 00 » est instanciée et les plateformes, couvertes par *[CER-JC1] et [CER-JC2] et sa maintenance [MAI-01]*, sont fermées sans possibilité de charger et d’instancier d’autres *applets* (l’*applet* Taiwan eID peut, cependant, être instanciée plusieurs fois) ;
- les recommandations du guide [GUIDES] sont strictement appliquées durant la phase « Personnalisation » du cycle de vie, ainsi que dans la phase de pré-personnalisation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et 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 le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation des microcontrôleurs certifiés le 11 octobre 2016 au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_VAN.5 et ASE_TSS.2 conformes au profil de protection [PP0084] sous les références BSI-DSZ-CC-0955-V2-2016 et BSI-DSZ-CC-0973-V2-2016 (voir [CER_IC1] et [CER_IC2]), et des plateformes certifiées le 5 septembre 2017 au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 conformes au profil de protection [PP JCS-O] sous les références ANSSI-CC-2017/47 et ANSSI-CC-2017/49 (voir [CER-JC1] et [CER-JC2]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 8 janvier 2018, 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 le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction 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 (voir [CER-IC1] et [CER-IC2]).

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 « Taiwan eID Applet EAC with AA on ID-one V8.1 - Standard LDS Platform on NXP P6021M VB and on ID-One Cosmo v8.1-N - Large Platform on NXP P6022M VB, Version 03 00 00 00 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 augmenté des composants AVA_VAN.5 et ALC_DVS.2.

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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce 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 signataires², 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 La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

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

Annexe 1. Niveau d'évaluation du produit [CCv3.1R4]

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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis



Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - Security Target Pollux EAC and AA, référence : 110 8394, version 3.0, 28/11/2017, <i>OBERTHUR TECHNOLOGIES</i>. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Public Security Target Pollux EAC and AA, référence : 110 8498, <i>IDEMIA</i>.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - POLLUX – Evaluation Technical Report : ETR, référence : LETI.CESTI.POL.ETR.001 – v2.0 – 08/09/2017 ; - POLLUX – Evaluation Technical Report : ETR, référence : LETI.CESTI.POL.ETR.001 – v3.0 – 08/01/2018.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - POLLUX – Configuration List, référence : 220 1043, version 3, 28/11/2017, <i>OBERTHUR TECHNOLOGIES</i>.
[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"> - Guidance Document – PREparative Procedures, référence : 220 1038, version 4, 28/11/2017, <i>OBERTHUR TECHNOLOGIES</i>. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - Guidance Document – OPERational User Guidances, référence : 220 1039, version 3, 10/04/2017, <i>OBERTHUR TECHNOLOGIES</i>.
[PP EAC]	<p>Protection Profile – Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE, version 1.3.0, 20 janvier 2012. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0056-V2-2012 le 10 février 2012.</i></p>
[PP0084]	<p>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.</i></p>
[PP JCS-O]	<p>Profil de protection « Java Card System Open Configuration ». <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2010/03 le 25 juin 2010 et maintenu sous la référence ANSSI-CC-2010/03-M01 le 29 mai 2012.</i></p>
[CER-IC1]	<p>NXP Secure Smart Card Controller P6021y VB including IC dedicated software. <i>Certifié par le BSI sous la référence BSI-DSZ-CC-0955-V2-2016 le 11 octobre 2016.</i></p>



[CER-IC2]	NXP Secure Smart Card Controller P6022y VB including IC dedicated software. <i>Certifié par le BSI sous la référence BSI-DSZ-CC-0973-V2-2016 le 11 octobre 2016.</i>
[CER-JC1]	Plateforme ID-One Cosmo v8.1-N - Standard LDS, masquée sur le composant NXP P6021M VB. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2017/47 le 5 septembre 2017.</i>
[CER-JC2]	Plateforme ID-One Cosmo v8.1-N - Large, masquée sur le composant NXP P6022M VB. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2017/49 le 5 septembre 2017.</i>
[MAI-01]	Plateforme ID-One Cosmo v8.1-N – Large, masquée sur le composant NXP P6022M VB. <i>Délivrée par l'ANSSI sous la référence ANSSI-CC-2017/49-M01.</i>



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 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 : <ul style="list-style-type: none"> - 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 1.4, août 2015.
[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 .
[AIS 34]	Application Notes and Interpretation of the Scheme (AIS) – Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & CC v3.1) and EAL6 (CC v3.1), AIS34, version 3, 3 septembre 2009, BSI (Bundesamt für Sicherheit in der Informationstechnik).

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