



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-2012/76

**Application IAS Classic v3 sur plateforme Java
Card en configuration ouverte de la carte à
puce MultiApp ID V2.1
sur composant P5CC081V1A**

**Référence : IAS Classic V3 on MultiApp ID V2.1
Version : MPH117 avec filtre V2.2**

Paris, le 3 décembre 2012

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

[Original signé]

Patrick Pailloux



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.anssi@ssi.gouv.fr

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



Référence du rapport de certification

ANSSI-CC-2012/76

Nom du produit

Application IAS Classic v3 sur plateforme Java Card en configuration ouverte de la carte à puce MultiApp ID V2.1 sur composant P5CC081V1A

Référence/version du produit

Référence IAS Classic V3 on MultiApp ID V2.1, Version MPH117 avec filtre V2.2

Conformité à un profil de protection

**[BSI-PP-0005-2002], version v1.04
Protection Profile — Secure Signature-Creation Device Type 2,
[BSI-PP-0006-2002], version v1.05
Protection Profile — Secure Signature Creation Device Type 3**

Critères d'évaluation et version

CC version 3.1 révision 3

Niveau d'évaluation

**EAL4 Augmenté
ALC_DVS.2 et AVA_VAN.5**

Développeurs

GEMALTO
La Vigie Avenue du Jujubier, ZI Athélia IV
BP 90, 13702 La Ciotat, France

NXP
101 Stresemannallee, D-22502 Hambourg
Allemagne

Commanditaire

GEMALTO
La Vigie Avenue du Jujubier, ZI Athélia IV BP 90, 13702 La Ciotat, France

Centre d'évaluation

SERMA Technologies
30 Avenue Gustave Eiffel, 33608 Pessac, France

Accords de reconnaissance applicables



Le produit est reconnu au niveau EAL4.

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	6
1.1. PRÉSENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	9
1.2.5. <i>Configuration évaluée</i>	10
2. L'ÉVALUATION	11
2.1. RÉFÉRENTIELS D'ÉVALUATION	11
2.2. TRAVAUX D'ÉVALUATION	11
2.3. COTATION DES MÉCANISMES CRYPTOGRAPHIQUES SELON LES RÉFÉRENTIELS TECHNIQUES DE L'ANSSI	11
2.4. ANALYSE DU GÉNÉRATEUR D'ALÉAS.....	11
3. LA CERTIFICATION	12
3.1. CONCLUSION.....	12
3.2. RESTRICTIONS D'USAGE.....	12
3.3. RECONNAISSANCE DU CERTIFICAT	13
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	13
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	13
ANNEXE 1. NIVEAU D'ÉVALUATION DU PRODUIT.....	14
ANNEXE 2. RÉFÉRENCES DOCUMENTAIRES DU PRODUIT ÉVALUÉ	15
ANNEXE 3. RÉFÉRENCES LIÉES À LA CERTIFICATION	17

1. Le produit

1.1. Présentation du produit

Le produit évalué est l'application « IAS Classic v3 sur plateforme Java Card en configuration ouverte de la carte à puce MultiApp ID V2.1 sur composant P5CC081V1A », référence IAS Classic V3 on MultiApp ID V2.1, en version MPH117 avec filtre V2.2, développé par GEMALTO et NXP.

Le produit évalué est composé :

- de l'applet IAS Classic v3 qui permet à l'utilisateur de signer électroniquement des données ;
- de la plateforme ouverte JavaCard MultiApp version 2.1 qui permet de charger des applets, durant la phase opérationnelle. Cette plateforme est certifiée par ailleurs sous la référence [ANSSI-CC-2012/24].

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM et l'EEPROM du produit.

1.2. Description du produit

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 aux profils de protection [BSI-PP-0005-2002] et [BSI-PP-006-2002], adaptés à la version 3.1 des CC (ces PP ayant été rédigés selon la version 2.1 des CC).

1.2.1. 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 présents dans la réponse que donne le produit suite à la commande GET DATA (cf. [GUIDES]).

Sur les produits, la commande GET DATA pour le tag 01 03 doit donner une des réponses suivantes :

- B0 85 36 38 16 22 47 90 50 81 00
- B0 85 36 38 17 22 47 90 50 81 00



Cette réponse se décompose comme indiqué dans le tableau ci-dessous.

Nom de la famille	Java Card	B0h
Nom du système d'exploitation	MultiApp ID V2.1	85h
Numéro du masque	MPH117	36h
Nom du produit	Generic MPH117 product	38h
Configuration du produit	IAS XL personnalisée / non personnalisée	16h / 17h
Version du filtre	version 2.2	22h
Fabricant du microcontrôleur	NXP	47 90h
Version du microcontrôleur	P5CC081V1A	50 81h

1.2.2. Services de sécurité

Les services de sécurité évalués fournis par le produit sont :

- la confidentialité et de l'intégrité des clés cryptographiques et des données applicatives pendant l'exécution des opérations cryptographiques ;
- la confidentialité et de l'intégrité des données d'authentification et des données applicatives pendant l'exécution des opérations d'authentification ;
- l'isolation des applications entre contextes différents et la confidentialité et de l'intégrité des données applicatives entre les applications ;
- l'intégrité de l'exécution du code applicatif ;
- l'authentification du signataire par un code PIN ;
- la génération des données de création et de vérification de signature ;
- l'import et stockage des données de création de signature ;
- l'export des données de vérification de signature ;
- la création d'une signature électronique.

1.2.3. Architecture

Le produit, présenté figure 1, est constitué des éléments suivants :

- des fonctionnalités matérielles du composant (CPU, RAM, ROM, EEPROM, I/O, coprocesseurs cryptographiques) ;
- d'une partie native composée elle-même :
 - o d'un gestionnaire de mémoire *Memory Manager* ;
 - o d'un gestionnaire de communication *Communication* ;
 - o de bibliothèques cryptographiques *Crypto libs* ;
- d'un système Java Card (JCS : Java Card System) composée :
 - o d'un environnement *runtime* (JCRE) ;
 - o d'une machine virtuelle Java (VM) ;
 - o d'une interface de programmation (Java API) ;
 - o d'un gestionnaire d'applications (Card Manager) ;
- de l'application IAS Classic ;
- d'autres applications ne rentrant pas dans la cible de l'évaluation.

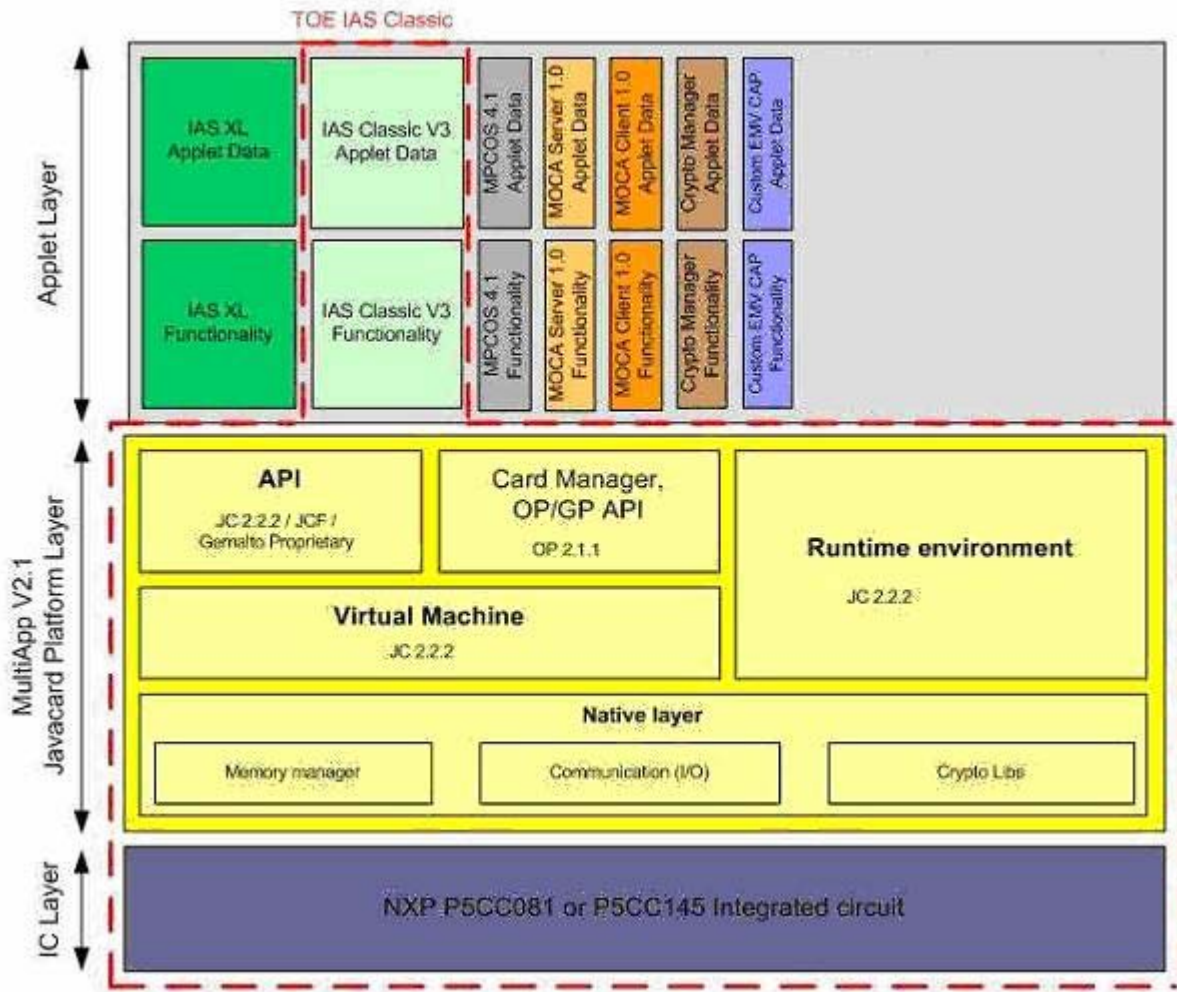


Figure 1 : Architecture



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

Le composant est fabriqué chez NXP. Il est ensuite envoyé sur le site de Gemalto où il est initialisé et pré-personnalisé. Le produit est ensuite verrouillé par une clé diversifiée et envoyé au personnalisateur.

Le produit a été développé sur les sites suivants :

Développement	Gemalto Meudon Gemalto La Ciotat Gemalto Gémenos
Fabrication du micro-module, initialisation et encartage	Gemalto Gémenos Gemalto Pte Ltd Singapore
Pré-personnalisation	Gemalto Gémenos Gemalto Pte Ltd Singapore Gemalto Vantaa

Gemalto

6 Rue de la verrerie
92190 Meudon
France

Gemalto

La Vigie Avenue du Jujubier, ZI Athélia IV BP 90
13702 La Ciotat
France

Gemalto

525 Avenue du Pic de Bertagne
13420 Gémenos
France

Gemalto Pte Ltd

Turvalaaksonkaari 2
12 Ayer Rajah Crescent, Singapore 139941
Singapore

Gemalto

Turvalaaksonkaari 2
FI-01741 Vantaa
Finlande

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification [BSI-DSZ-CC-0555-2009].

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le pré-personnalisateur, le personnalisateur et le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateur le porteur de la carte souhaitant utiliser les services de signature de l'applet.

1.2.5. Configuration évaluée

L'évaluateur a testé l'application IAS Classic v3 sur la plateforme Java Card masquée sur le composant P5CC081.

Les autres applets masquées sur le produit ont été analysées dans le cadre de cette évaluation au titre de l'environnement de la cible de sécurité. Elles sont conformes aux règles de développement imposées par la plateforme Java Card.

Le certificat porte sur l'application IAS Classic v3 sur la plate-forme ouverte Java Card, telle que présentée au paragraphe 1.2.1, et configurée conformément au guide de personnalisation (cf. [GUIDES]).



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

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 sur la plate-forme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software » au niveau EAL5 augmenté des composants ALC_DVS.2, ASE_TSS.2 et AVA_VAN.5, conforme au profil de protection [BSI-PP-0035-2007]. Ce microcontrôleur a été certifié le 10 novembre 2009 sous la référence [BSI-DSZ-CC-0555-2009]. Le niveau de résistance du microcontrôleur a été confirmé en octobre 2011 par le BSI.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 5 septembre 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 les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques 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 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit reprenant les résultats de la plateforme [ANSSI-CC-2012/24] dans le périmètre de l'évaluation et a été analysé par le centre d'évaluation. L'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN 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 « Application IAS Classic v3 sur plateforme Java Card en configuration ouverte de la carte à puce MultiApp ID V2.1 sur composant P5CC081V1A », référence IAS Classic V3 on MultiApp ID V2.1, version MPH117 avec filtre V2.2 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 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].



3.3. Reconnaissance du certificat

Ce certificat fait l'objet d'une reconnaissance internationale

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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. 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 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 4+	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	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic 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	4	Problem tracking 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	1	Well-defined development tools
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	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"> - MultiAppID V2.1Software - Security Target - IASClassic V3 part référence R0A21037_012_CCD_ASE-IASClassic_2, version v1.1 du 23 août 2012 éditée par GEMALTO. <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"> - IAS Classic V3 on MultiApp ID V2.1 – Security Target – Public version référence R0A21037_012_CCD_ASE - IASClassic, version v1.1 du 23 août 2012 éditée par GEMALTO.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report CALLISTO-IAS Project référence CALLISTO_ETR_IASClassic_v1.1, version v1.1 du 5 septembre 2012 édité par SERMA Technologies.
[CONF]	<p>Liste de configuration :</p> <ul style="list-style-type: none"> - MultiApp v2.1 platform / IAS Classic V3- Configuration list version du 19 octobre, édité par GEMALTO.
[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"> - MultiApp ID V2.1 Software AGD top-level document – IAS Classic V3 Application référence R0A21037_036_CC D_AGD-IASClassic, version v1.0 du 16 avril 2012 édité par GEMALTO. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - IAS Classic Applet V3 Reference Manual référence DOC116499E, du 23 octobre 2008 édité par GEMALTO.
[BSI-DSZ-CC-0555-2009]	<p>NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A,P5CD041V1A, P5CD021V1A and P5CD016V1Aeach with IC dedicated Software. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 10 novembre 2009 sous la référence BSI-DSZ-CC-0555-2009.</i></p>
[BSI-PP-0005-2002]	<p>Protection Profile - Protection Profile — Secure Signature-Creation Device Type 2, version v1.04 du 25 juillet 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002.</i></p>
[BSI-PP-0006-2002]	<p>Protection Profile - Protection Profile — Secure Signature Creation Device Type 3, version v1.05 du 25 juillet 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0006-2002.</i></p>



[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i>
[ANSSI-CC-2012/24]	Plateforme Java Card de la carte à puce MultiApp ID V2.1 masquée sur le composant P5CC081V1A. <i>Certifié par l'ANSSI le 29 juin 2012 sous la référence ANSSI-CC-2012/24.</i>



Annexe 3. Références liées à la certification

Décret 2002-535 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, 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 IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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]	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 (RGS_B_1), voir www.ssi.gouv.fr . Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir www.ssi.gouv.fr .