Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2011/05

Porte-monnaie électronique "Gemalto ECC CPU card sur plateforme GCX5.1 masquée (MPH098) sur le composant NXP P5CD081V1A"

Paris, le 13 AVR. 2011

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ 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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2011/05

Nom du produit

Porte-monnaie électronique "Gemalto ECC CPU card sur plateforme GCX5.1 masquée (MPH098) sur le composant NXP P5CD081V1A"

Référence/version du produit

CPU e-purse sur GCX5.1 MPH098 version 1.0

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Gemalto SA

6 rue de la Verrerie,
92197 Meudon, France

NXP Semiconductors GmbH

Stresemannallee 101,
D-22502 Hamburg, Germany

Commanditaire

Gemalto SA

6 rue de la Verrerie, 92197 Meudon, France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 37 78, mél : elisabeth.crochon@cea.fr

Accords de reconnaissance applicables

CCRA

SOG-IS

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

1.1. Présentation du produit

Le produit évalué est le Porte-monnaie électronique "Gemalto ECC CPU card sur plateforme GCX5.1 masquée (MPH098) sur le composant NXP P5CD081V1A", développé par Gemalto.

La TOE (*Target Of Evaluation* ou cible d'évaluation) est une carte à puce avec application de porte-monnaie électronique (*CPU e-purse*), sur plateforme Java Card fermée, avec interfaces contact et sans contact.
L'application de porte-monnaie électronique est adaptée aux paiements de faible valeur. Ses fonctionnalités sont identiques à celles d'un porte-monnaie traditionnel, à la différence que la monnaie fiduciaire est remplacée par de la monnaie électronique. Sa fonction première est de permettre à son propriétaire d'effectuer des paiements électroniques de façon simple, rapide et sécurisée.

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 du produit est identifiable par les éléments suivants :

- nom commercial : *ECC CPU card* ;
- référence du produit : *CPU e-purse on GCX5.1* ;
- référence du logiciel : *V1.0 on MPH098* ;
- référence du composant : NXP P5CD081 V1A.

Ces informations peuvent être vérifiées par la réponse de la carte à l'initialisation (ATR[1]) ainsi que par des données de traçabilités (CPLC[2]).

L'ATR doit être le suivant :

3B 6E 00 00	80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00 (protocole T0)
3B EE 00 00 81 31 80 42	80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00 xx[3] (protocole T1)

1 *Answer To Reset*
2 Card manager Production Life Cycle
3 xx: checksum byte calculated

Les données de traçabilité sont ainsi obtenues via :

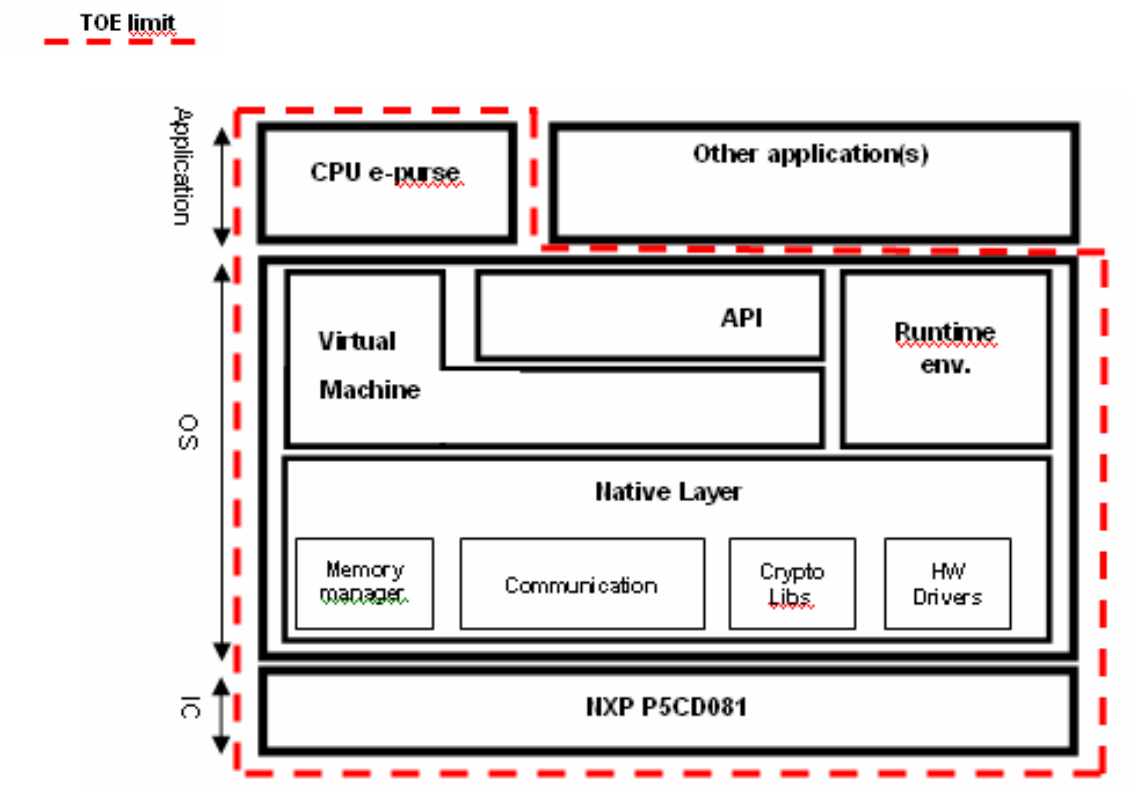
- un GET DATA de valeur **9F7FH** pour les données de traçabilité de la ROM, dont les 13 premiers octets doivent être **9F 7F 2A 40 70 51 44 19 81 01 04 01 00** avec :
  - rappel des données du GET DATA : **9F 7F** ;
  - information sur la taille de la réponse : **2A** ;
  - fabricant du composant : **40 70** (NXP) ;
  - type du composant : **51 44** (P5CD081) ;
  - identifiant du système d'exploitation : **19 81** (GEMALTO OS) ;
  - date de la version du système d'exploitation : **01 04** (14/04/2010) ;
  - version du système d'exploitation : **01 00** (1.0).
- un GET DATA de valeur **DF13H** pour la lecture de l'identification de l'applet (*CPUe-purse*), qui doit donner le résultat suivant :
  - rappel des données du GET DATA : **DF 13** ;
  - pour usage interne : **00** ;
  - version de l'applet : **10 00** (1.0.00) ;
  - identification de la date de la version de l'applet : **02 81** (07/10/2010).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité de la monnaie électronique (*EM-Electronic Money*) sur les opérations de chargement, de crédit et de débit ;
- la protection des biens sensibles en intégrité et en confidentialité, que ce soit en utilisation ou lorsqu'ils sont stockés ;
- l'authentification mutuelle avec le SAM ECC (*Easy Card Corporation Secure Access Module*) durant les opérations de chargement et de débit ;
- l'authentification mutuelle avec un système hôte durant les opérations de crédit ;
- l'invalidation (désactivation) de la carte via une commande *Write-lock*.

1.2.3. Architecture



Le produit est une carte à puce constituée :

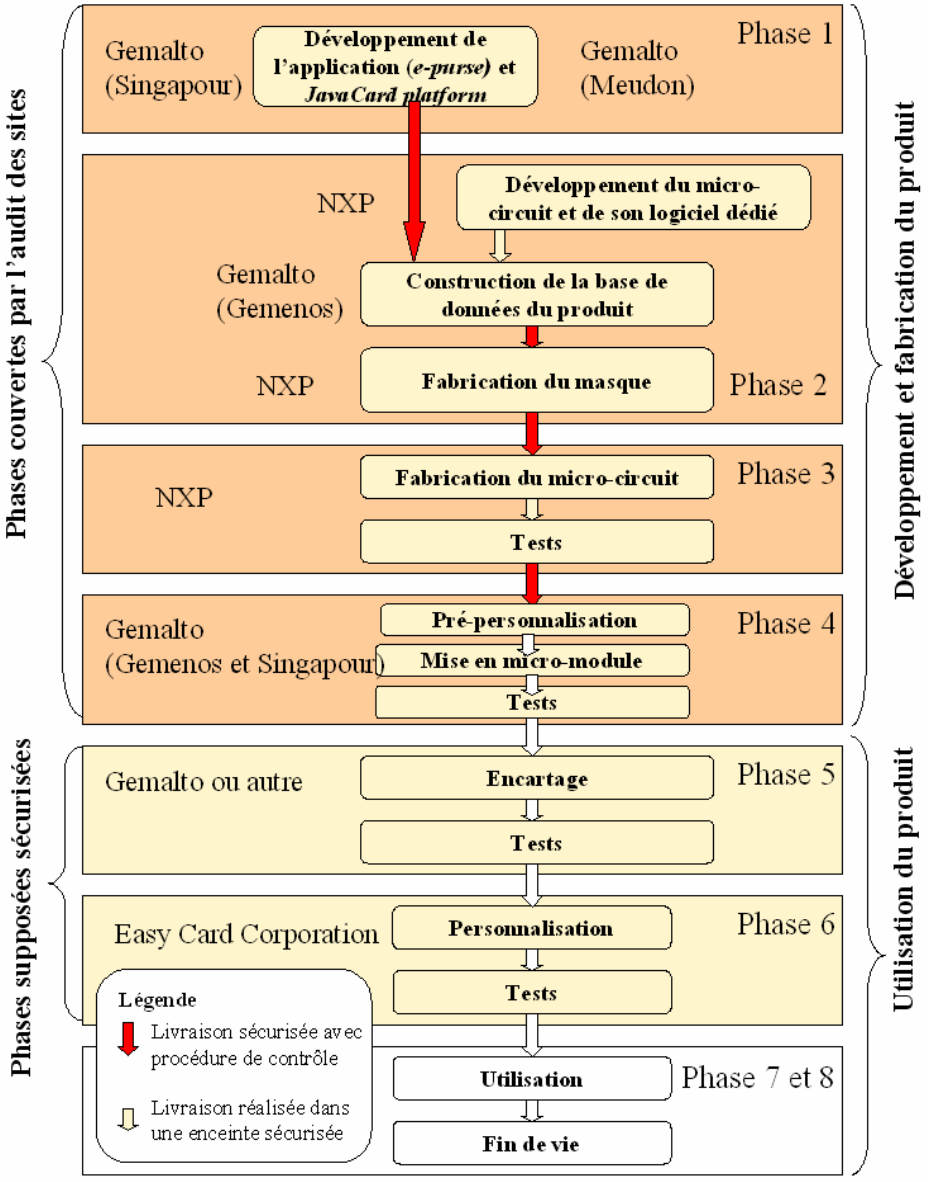
- de l'application « *CPU e-purse*» ;
- d'un système d'exploitation (*OS*) : GCX5.1 comportant :
  - une plateforme Java Card composée :
    - d'un environnement *runtime* ;
    - d'une machine virtuelle Java ;
    - d'API.
  - une partie native composée elle-même :
    - d'un gestionnaire de mémoire *Memory management* ;
    - d'un gestionnaire de communication *Communication management* ;
    - d'un gestionnaire de librairies cryptographiques et de librairies cryptographiques Cryptolibs.
- d'un composant NXP P5CD081V1A.

Les autres applets présentes sur la carte ne font pas partie de la cible d'évaluation (*TOE*) et sont donc en dehors du périmètre d'évaluation[1].

[1] applications : VSDC271, MchipPayPass, DualPSE.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Gemalto(La Ciotat) : hébergement des serveurs IT

Le produit a été développé sur les sites suivants :

GEMALTO Site de Meudon

6 rue de la Verrerie
91197 Meudon Cedex
France

GEMALTO Site de Singapour

12 Ayar Rajah Crescent
Singapour 139941
Singapour

GEMALTO Site de Gemenos

Avenue Pic de Bertagne
13881 Gémenos Cedex
France

NXP Semiconductors GmbH

Stresemannallee 101,
D-22502 Hamburg
Germany

Les transitions entre ces phases de développement conduisent à des transferts de biens sensibles immatériels (données de conception, code source) et matériels (échantillons de produit en cours de développement).

Dans le cadre de cette évaluation, la sécurité des processus de livraison cités ci-après a été évaluée au titre du composant ALC :

- livraison du logiciel dédié et guide au développeur de l'application (en amont de la phase 1) ;
- livraison du code du logiciel embarqué au fabricant du microcontrôleur (entre la phase 1 et la phase 2) ;
- livraison des données requises par le fabricant des masques (durant la phase 2) ;
- livraison des masques au fabricant du microcontrôleur (entre la phase 2 et la phase 3) ;
- livraison des microcontrôleurs à l'assembleur et à l'encarteur (entre les phases 3 et 4).

Les processus de livraison cités ci-après sont en dehors du périmètre de l'évaluation et leur sécurité n'a donc pas été évaluée :

- livraison des cartes au pré-personnalisateur (entre les phases 4 et 5) ;
- livraison des cartes pré-personnalisées au personnalisateur (entre les phases 5 et 6).

La sécurité de ces processus de livraison est couverte par des guides [GUIDES].

1.2.5. Configuration évaluée

Le certificat porte sur la configuration décrite au §1.2.1.

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 la méthode d'évaluation [CEM].
Pour les composants d'assurance qui ne sont pas couverts par la [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, le guide [CC AP] a été appliqué.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en appliquant le guide [COMP], qui permet de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a pris en compte les résultats de l'évaluation du microcontrôleur NXP « P5CD081 V1A et son logiciel dédié» au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_VAN.5 et ASE_TSS.2 conforme au profil de protection [PP]. Ce microcontrôleur a été certifié le 10 novembre 2009 sous la référence BSI-DSZ-CC-0555-2009 [CERTIF_IC].
Le niveau de résistance du microcontrôleur a été confirmé par le BSI le 17 décembre 2010 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 22/03/2011, 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] de l'ANSSI 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 utilisé par le produit final est celui proposé par le produit hôte et a été évalué dans le cadre de l'évaluation BSI-DSZ-CC-0555-2009 [CERTIF_IC].

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 « Porte-monnaie électronique "Gemalto ECC CPU card sur plateforme GCX5.1 masquée (MPH098) sur le composant NXP P5CD081V1A", version 1.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 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, 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. 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, l'Italie, 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 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 the 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_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	2	3	3	4	2	Testing: security enforcing modules
	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	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target for ECC CPU card, version 2.0, reference ROR20512_CCD_ASE_001 , 24th january 2011,* GEMALTO. - *Security Target lite for ECC CPU card, version 1.01, reference ROR20512_CCD_ASE_002, 7th april 2011,* GEMALTO.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (ETR), version 1.2, reference DRT/LETI/DCIS/CESTI/.FOR.4.044.G, 22th march 2011,* CEA LETI.
[CONF]	Liste de configuration du produit : - *TOE applet elements configuration, reference Items for applet.zip, 21st december 2010 ;* GEMALTO. - *TOE platform elements configuration, reference Items for GCX5.1.zip, 21st december 2010 ;* GEMALTO. - *TOE cryptolib elements configuration, version 1.1, reference LIB/ALC directory, 11th june 2010.* GEMALTO.
[CERTIF_IC]	Rapport de certification : *NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software, référence : BSI-DSZ-CC-0555-2009, 10 novembre 2009,* BSI.
[GUIDES]	- *AGD : Guidance Documents, version1.0, reference ROR20512_CCD_AGD_006, 22nd december 2010 ;* o *Personalization Specification – CPU Card, version A18, reference CPU_PS_ECC, 18th october 2010 ;* o *Pre-Personalization Specification, version A01, reference CPU_PPS_ECC, 29th april 2010 ;* o *Functional Specification, version A18, reference CPU_FS_ECC, 21st october 2010 ;* o *FSP : complete functionnal specification, version 1.0, reference ROR20512_CCD_ADV_FSP_002, 20th december 2010 ;* o *Software Requirement Specifications – GCX5.1 platform "EasyCard", version A06, reference ROR20855_005_SRS_GCX5, 17th september 2010 ;* o *Key Management Specification – CPU Card, version*

	A18, reference KMS_ECC, 19th october 2010. GEMALTO.
[PP]	Security IC Protection Profile, version 1.0, 23rd august 2007. Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-CC-0035-2007.

Annexe 3. Références liées à la certification

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>[CER/P/01]</td><td>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.</td></tr>
<tr><td>[CC]</td><td>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.</td></tr>
<tr><td>[CEM]</td><td>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,
July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.</td></tr>
<tr><td>[CC AP]</td><td>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.</td></tr>
<tr><td>[COMP]</td><td>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.</td></tr>
<tr><td>[CC RA]</td><td>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</td></tr>
<tr><td>[SOG-IS]</td><td>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</td></tr>
<tr><td>[REF-CRY]</td><td>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</td></tr>
<tr><td>[REF-KEY]</td><td>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</td></tr>
<tr><td>[REF-AUT]</td><td>Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr</td></tr>
</table>