PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2007/05

Carte bancaire GemCB DDA : composant SLE66CX162PE masqué par les applications B4-B0' V3, CB-EMV, Moneo et Gemalto Fidelity (référence : MSI151_FILT009)

Paris, le 12 mars 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr

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

Référence du rapport de certification

2007/05

Nom du produit

Carte bancaire GemCB DDA : composant SLE66CX162PE masqué par les applications B4-B0' V3, CB-EMV, Moneo et Gemalto Fidelity

Référence/version du produit

référence : MSI151_FILT009

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2, AVA_VLA.4

Développeurs

Gemalto

La Vigie, Avenue du Jujubier, Z.I., Athélia IV, 13705 La Ciotat Cedex, France

Infineon Technologies AG

St.-Martin-Straße 76, 81609 München, Allemagne

Commanditaire

Gemalto

La Vigie, Avenue du Jujubier, Z.I., Athélia IV, 13705 La Ciotat Cedex, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 64, mél : m.dus@serma.com

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 bancaire GemCB DDA, constituée du composant SLE66CX162PE / m1531a24 développé par Infineon Technologies AG, et masqué par les applications B4-B0' V3, CB-EMV, Moneo et Gemalto Fidelity développé par Gemalto.
La référence du logiciel masqué en mémoire ROM est « MSI151 », et la référence du patch chargé en mémoire EEPROM est « FILT009 ».

Cette carte est destinée à être utilisée pour les opérations suivantes :
- opérations de débit/crédit selon les spécifications B4-B0' V3 (cf. [ST, §11.2]) ;
- opérations de débit/crédit selon les spécifications CB-EMV (cf. [ST, §11.2]), qui incluent, en plus des fonctions d'administration :
  - la personnalisation VSDC 1.4.0 CB ;
  - la personnalisation M/Chip Select 4 CB ;
- transactions de porte-monnaie électronique selon les spécifications Moneo, version 2.5.2 (cf. [ST, §11.2]) ;
- application de fidélité « Gemalto Fidelity ».

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité s'inspire du profil de protection [PP/9911] pour la carte en général et du profil de protection [PP/0101] pour l'application Moneo.

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 à l'aide de la commande « Get Data » qui doit renvoyer une série d'octets permettant d'identifier le produit. Les valeurs attendues des octets sont les suivantes :

	Label	Octet d'identification
Nom de famille	Full custom	A1
Nom de produit	GEMCB_DDA	0F
Version du logiciel de la carte	GEMCB_DDA	04
Version du programme	GEMCB_DDA	01
Identification du composant	SLE66PX162PE	BC
Version du patch EEPROM	FILT009	55

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- CB-EMV :
  - contrôle d'accès aux données,
  - audits des évènements de sécurité,
  - authentification de l'administrateur,
  - gestion des commandes,
  - calcul cryptographique et gestion des clés,
  - gestion du code PIN,
  - protection des données,
  - gestion de la sécurité de la carte,
  - chargement sécurisé des données secrètes,
  - génération de cryptogrammes des transactions,
- B0' :
  - certification des données,
  - gestion des pointeurs,
  - analyseur de commande,
  - calcul cryptographique (DES)
  - dispatcher de commande,
  - détection des erreurs de programmation de la mémoire EEPROM,
  - mécanismes de back-up,
  - contrôle d'intégrité,
  - présentation de clé/code,
  - gestion du cycle de vie et verrouillage des phases,
  - accès mémoire,
  - utilisation sécurisée des secrets,
  - gestion du statut de sécurité,
- Moneo :
  - gestion des limites de transaction,
  - contrôle d'accès,
  - authentification du terminal,
  - gestion des commandes,
  - calculs cryptographiques,
  - intégrité des données,
  - gestion des clés,
  - enregistrement des transactions,
  - authentification du porteur,
  - préservation d'un état sécurisé et back-up,
  - gestion des séquences d'exécution.

1.2.3. Architecture

Le produit est une carte à puce constituée :

- du composant SLE66CX162PE / m1531a24 développé par Infineon Technologies ;
- d'un logiciel MSI151, développé par Gemalto, masqué dans la mémoire ROM du composant ;
- d'un patch FILT009, développé par Gemalto, chargé dans la mémoire EEPROM du composant.

L'architecture du produit est résumée dans la figure suivante :

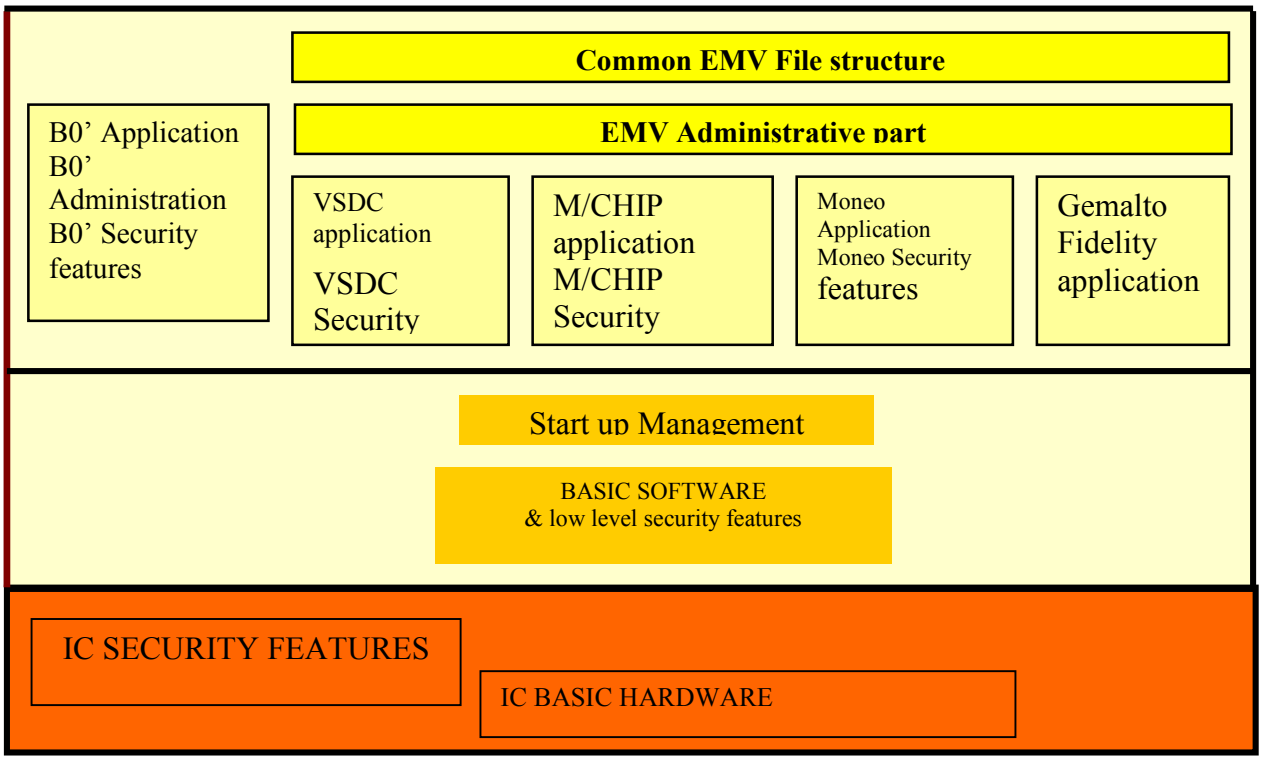

Figure 1 – Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

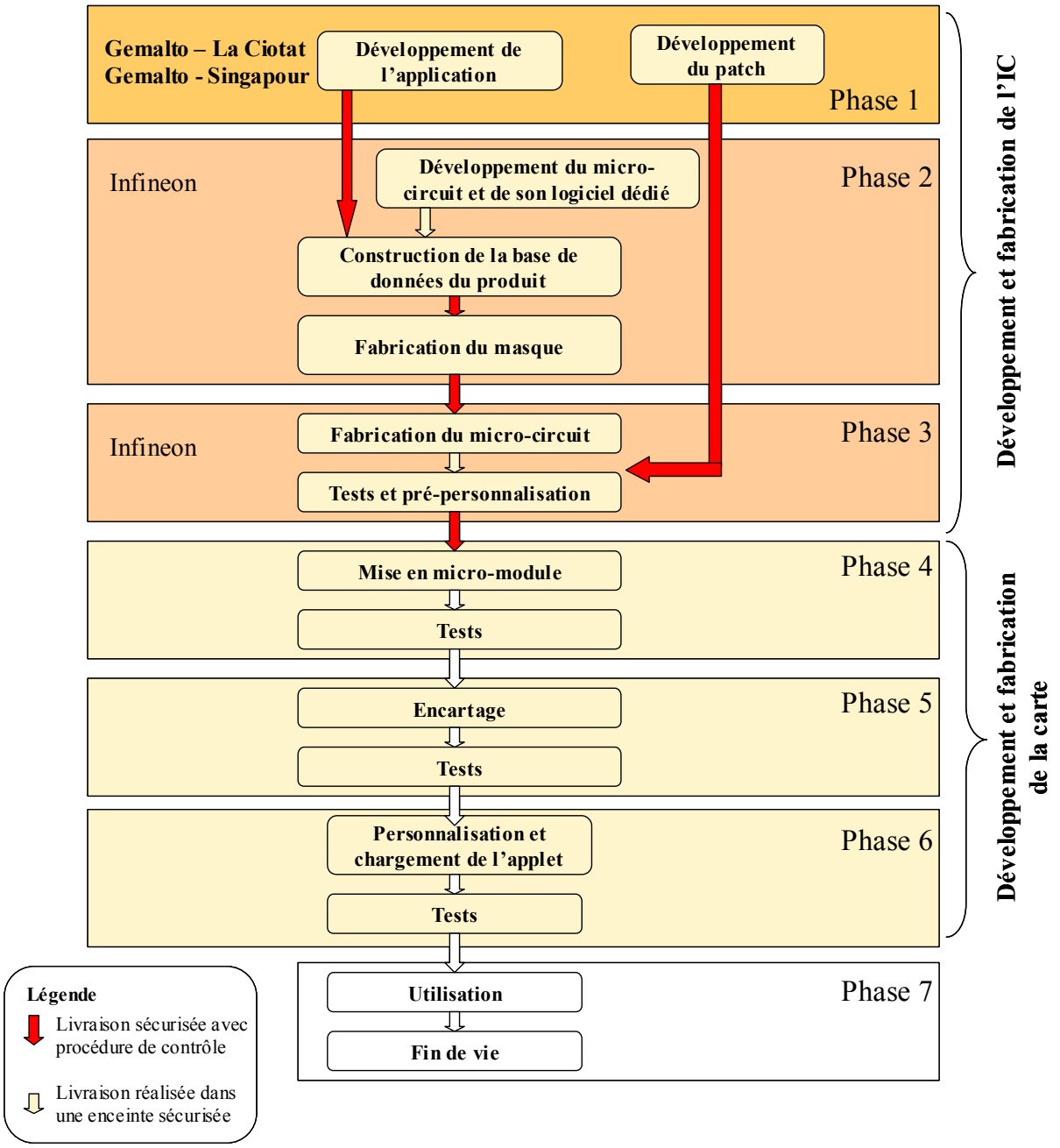

Figure 2 – Cycle de vie du produit

A noter : le patch FILT009 est chargé par le fabricant du micro-circuit, et le mécanisme de chargement de patch est ensuite verrouillé.

Le logiciel a été principalement développé sur le site de Gemalto à la Ciotat :

Gemalto

La Vigie, Avenue du Jujubier, Z.I.,
Athélia IV, BP 90
13702 La Ciotat Cedex, France

Une partie du développement du logiciel a été réalisée sur le site de Gemalto à Singapour :

Gemalto

12, Ayer Rajah Crescent,
Singapore 139941
Singapour

Le composant a été développé par Infineon Technologies :

Infineon Technologies AG

CCM MTH, Postfach 80 09 49
D-81609 München,
Allemagne

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les intervenants des phases 4 à 6 et comme utilisateurs ceux de la phase 7.

1.2.5. Configuration évaluée

Le produit comporte 4 applications (B0', EMV, Moneo et Gemalto Fidelity) qui peuvent être activées ou non. Le certificat porte sur les configurations suivantes :

- B0' et applications EMV (MCHIP ou VIS 1.4) ;
- B0', applications EMV et Gemalto Fidelity ;
- B0', applications EMV, Moneo ;
- B0', applications EMV, Moneo et Gemalto Fidelity ;
- applications EMV;
- applications EMV et Gemalto Fidelity ;
- applications EMV, Moneo ;
- applications EMV, Moneo et Gemalto Fidelity.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [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 et validées par la DCSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation a été réalisée en composition, 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 du microcontrôleur « SLE66CX162PE » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 11 novembre 2005 sous la référence BSI-DSZ-CC-0344-2005.

Le niveau de résistance du microcontrôleur a été confirmé le 11 octobre 2006 dans le cadre d'un processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 6 mars 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par 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 « Carte bancaire GemCB DDA : composant SLE66CX162PE masqué par les applications B4-B0' V3, CB-EMV, Moneo et Gemalto Fidelity (référence : MSI151_FILT009) » 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- la communication entre la carte et le terminal doit être sécurisée (en termes de protocole et de procédure) ;

Et pour l'application Moneo en particulier :

- le fournisseur de valeur doit garantir la valeur électronique dans l'ensemble du système. Les acteurs du système (y compris le porteur du porte-monnaie électronique) doivent appliquer la politique de sécurité du système, cette dernière devant être communiquée au porteur du porte-monnaie électronique par le fournisseur de valeur électronique ;
- les terminaux de chargement et de paiement ne doivent pas créer de valeur électronique, mais seulement distribuer aux parties autorisées le même montant de valeur électronique qu'ils reçoivent ;
- les terminaux de chargement doivent entrer dans un état sûr suite à une défaillance durant une transaction de chargement ou une transaction anormale, ou bien lors du re-jeu d'une transaction, sans perte ou création de valeur électronique ;
- un domaine de sécurité doit être disponible pour l'exécution de l'application du terminal de chargement, afin de prévenir les interférences et les altérations pouvant être provoquées par des agents frauduleux ;
- les terminaux de chargement doivent enregistrer tous les événements et/ou données nécessaires afin de contribuer à une gestion efficace du système ;
- les terminaux de chargement et de paiement doivent empêcher les utilisateurs d'accéder à des ressources et opérations pour lesquelles ils n'ont pas d'autorisation ;
- durant un chargement, le terminal doit maintenir deux domaines de sécurité distincts et séparés : le domaine de transaction de débit, et le domaine de transaction de chargement du porte-monnaie électronique ;

- les fournisseurs de porte-monnaie électronique doivent s'assurer que le porte-monnaie est délivré et installé de manière à maintenir le niveau de sécurité visé ;
- les fournisseurs de porte-monnaie électronique doivent s'assurer que le porte-monnaie est géré, administré et utilisé de manière à maintenir le niveau de sécurité visé ;
- le terminal de paiement doit garantir la confidentialité et l'intégrité des données sensibles qu'il manipule.

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
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level 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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annexe 2. Références documentaires du produit évalué

[ST]	Security Target - GemCB DDA, Référence : ASE01A10297A version 08 Gemalto
[RTE]	ESTEREL Project – Evaluation Technical Report, Référence : ESTEREL_ETR_V1.1 Serma Technologies
[CONF]	- STD configuration check list for EMV DDA on SLE66CX162PE, Référence : CFK06R10589_security version 04, Gemalto - Card Project configuration check for GemCB DDA, Référence : SCK01A10297A version A07, Gemalto - Configuration check Mchip part GemCB DDA, Référence : SCK02A10297A version A04, Gemalto - Configuration check Visa part GemCB DDA, Référence : SCK03A10297A version A02 Gemalto - Card project configuration check GemCB DDA B0' part, Référence : SCK04A10297A version A01, Gemalto - Configuration check Administrative part for GemCB DDA, Référence : SCK05A10297A version A06, Gemalto - Configuration check for GemCB DDA Moneo part, Référence : SCK06A10297A version A01, Gemalto - Configuration check product configuration for GemCB DDA, Référence : SCK07A10297A version A02 Gemalto
[GUIDES]	Guide d'installation et d'administration et d'utilisation du produit : - Chip Pre-initialization Specification GemCB_DDA (with corrective filter loading), Référence : CPS01A10297B version A01 Gemalto - Card Initialization Specification GemCB_DDA (corrective filter loaded in CIS), Référence : CIS01A10297B version A05 Gemalto - Personalization specification GemCB_DDA mask, Référence : PER01A10297B version A04 Gemalto

	- AGD-Guidance document GemCB DDA, Référence : AGD01A10297A version 01, Gemalto
[PP/0101]	Protection Profile Intersector Electronic Purse and Purchase Device (version without Last Purchase Cancellation), Version 1.3 March 2001. C*ertifié sous la référence PP/0101 le 12/03/0.*
[PP/9911]	Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. *Certifié sous la référence PP/9911.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié sous la référence BSI-PP-0002-2001.*

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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.