Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/46

Carte Multima Protect V1.1 : composant AT90SC9608RC masqué par l'application B4 B0' V3

(référence AT578A7-O-AB)

Paris, le 21 décembre 2005.

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ Ti 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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/46

Carte Multima Protect V1.1 : composant AT90SC9608RC masqué par l'application B4 B0' V3 (référence AT578A7-O-AB)

Développeurs : Axalto, Atmel

Critères Communs version 2.2

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

Conforme au profil de protection PP/9911

Commanditaire : Axalto

Centre d'évaluation : CEA LETI

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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la « Carte Multima Protect V1.1 : composant AT90SC9608RC masqué par l'application B4 B0' V3 (référence AT578A7-O-AB) » développée par les sociétés Axalto et Atmel.

1.2. Développeurs

Le développeur du masque est :

Axalto

36-38, rue de la Princesse,
BP 45
78431 Louveciennes Cedex
France

Le développeur du micro-circuit est:

Atmel Smart card IC's Ltd

Maxwell Building
Scottish Enterprise Technology Park
Birniehill Roundabout
East Kilbride, G75 0QR
Ecosse, Royaume-Uni

1.3. Description du produit évalué

1.3.1. Architecture

Le produit est constitué d'un micro-circuit AT90SC9608RC révision I développé sur Atmel dans lequel est masqué le logiciel Multima P1_Ph1_28 développé par Axalto.
Le produit contient les application suivantes :

- une application débit/ crédit B0' ;
- une ou plusieurs application(s) débit/ crédit CB-EMV SDA/DDA (soit Visa, soit M/Chip) ;
- une application « loyalty » standard ;
- une application porte-monnaie électronique Moneo ;
- une application fidélité (FID) basée sur Moneo.

Ce certificat porte sur l'application débit/crédit B0', il est associé aux certificats 2005/47 et 2005/48 qui portent respectivement sur l'application débit/crédit CB-EMV SDA/DDA et sur l'application porte-monnaie électronique Moneo.

Le schéma suivant, issu de la cible de sécurité [ST], présente une vue logique du produit évalué :

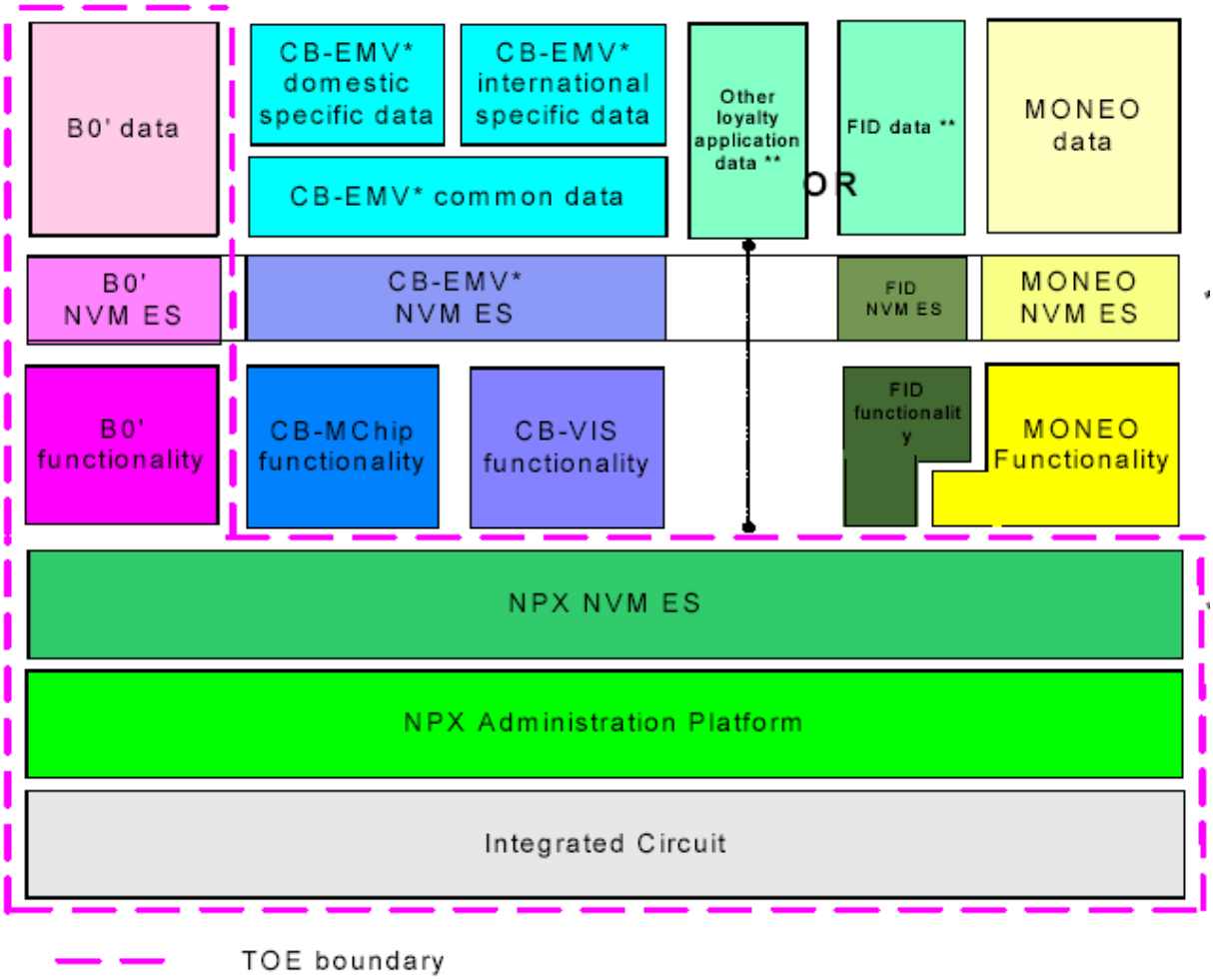

Figure 1 - Périmètre du produit évalué

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

Phase 1	Développement du masque
Phase 2	Développement du micro-circuit
Phase 3	Fabrication du composant masqué et tests
Phase 4	Encartage
Phase 5	Pré-personnalisation
Phase 6	Personnalisation
Phase 7	Utilisation

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend les éléments suivants :

- le micro-circuit AT90SC9608RC ;
- l'application B4 B0'V3 ;

- la plate-forme d'administration NPX

Ce rapport de certification présente les travaux d'évaluation relatifs à la partie B0' du produit, comme indiqué sur le schéma de la Figure 1. Les autres applications de la carte ne font donc pas partie du périmètre d'évaluation et sont considérées pour la présente évaluation comme appartenant à l'environnement du produit.
En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication (phase 3).
Le composant AT90SC9608RC a déjà été évalué et certifié (les résultats des travaux sont présentés dans le rapport de certification associé [2004/35]). L'évaluation de la partie relative au micro-circuit (phase 2 et 3) n'a donc pas été refaite, mais les résultats de l'évaluation précédente ont été pris en compte, conformément aux recommandations du guide pour la composition [COMP].

Le produit évalué existe dans les configurations suivantes :

B0'	Mastercard	Visa	Moneo	FID	Loyalty
x	x				
x	x		x		
x		x			
x		x	x		
x			x		
	x				
	x		x		
		x			
		x	x		
			x		
x	x		x		x
x		x	x		x
x			x	x	
			x	x	

2. L'évaluation

2.1. Contexte

L'évaluation a été effectuée selon le schéma de composition défini dans le document [COMP]. La composition consiste à réaliser l'évaluation d'un composant masqué en évaluant d'une part le micro-circuit, et d'autre part la partie logicielle en vérifiant qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur le micro-circuit.

Cette évaluation a été réalisée sur la base des résultats de l'évaluation du micro-circuit AT90SC9608RC rev. I au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4, conforme au profil de protection PP/9806 [PP/9806]. Ce micro-circuit a été certifié le 15 décembre 2004 sous la référence 2004/35. Le niveau de résistance du micro-circuit aux attaques a été confirmé le 9 septembre 2005 dans le cadre du processus de surveillance.

Le produit évalué est dérivé de la carte Multima Protect V1 (référence AT578A7K-AA) dont l'application B4 B0'V3 a été certifiée le 15 septembre 2005 sous la référence 2005/22 [2005/22]. Une partie des verdicts de la présente évaluation s'appuie donc sur les résultats des travaux menés lors de la précédente évaluation.

2.2. Référentiels d'évaluation

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

2.3. Commanditaire

Axalto

36-38, rue de la Princesse,
BP 45
78431 Louveciennes Cedex
France

2.4. Centre d'évaluation

CEA - LETI

17 rue des Martyrs
38054 Grenoble Cedex 9
France

Téléphone : +33 (0)4 38 78 40 87

Adresse électronique : alain.merle@cea.fr

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée du 15 septembre 2005 au 2 décembre 2005.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.6. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection PP/9911 [PP/9911].

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_VLA.4	Highly resistant

[1] Annexe 1 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur les sites de :

- Axalto à Louveciennes,
- Atmel à East Kilbride.

Les mesures de sécurité analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Des procédures de génération permettent par ailleurs de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures analysées a été effectuée dans le cadre de l'évaluation ayant conduit au certificat 2005/22. L'application des procédures sur le site d'Atmel à East Kilbride a été vérifiée dans le cadre de l'évaluation du micro-circuit.

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.7.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD), implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Audit data generation (FAU_GEN.1)
- Potential violation analysis (FAU_SAA.1)
- Audit review (FAU_SAR.1)
- Selective proof of origin (FCO_NRO.1)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)

- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Export of user data without security attributes (FDP_ETC.1)
- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failures handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Unforgeable authentification (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Timing of identification (FIA_UID.1)
- User-subject binding (FIA_USB.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TOE security functions data (FMT_MTD.1)
- Specification of management functions (FMT_SMF.1)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Resistance to physical attack (FPT_PHP.3)
- TSF domain separation (FPT_SEP.1)
- Inter-TSF data consistency (FPT_TDC.1)
- TSF testing (FPT_TST.1)

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.7.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre le développeur du masque (Axalto) et le fondeur (Atmel).

Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.

Aucune procédure spécifique de mise en œuvre du produit n'est nécessaire. Les travaux d'évaluation liés au composant d'assurance ADO_IGS.1 ont été considérés comme satisfaits.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.7.5. L'évaluation de la documentation d'exploitation

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.
L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.7.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.
L'évaluateur a réalisé ses tests fonctionnels indépendants sur des cartes configurées de manière à représenter l'ensemble des 8 configurations évaluées (voir le tableau page 8).

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.7.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Les fonctions B0_FS2, B0_FS3, B0_FS4 et B0_FS5 ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé **élevé (SOF-high)**.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests de pénétration.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau **élevé**.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour 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 résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [GUIDES] :

- la communication entre la carte et le terminal doit être sécurisée (en termes de protocole et de procédure),
- les méthodes et terminaux utilisés en phase d'utilisation doivent garantir l'intégrité et la confidentialité des données.

Annexe 1. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Classe ADO Livraison et opération	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Classe AGD Guides d'utilisation	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Classe ATE Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Classe AVA Estimation des vulnérabilités	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Annexe 2. Références documentaires du produit évalué

[CONF]	Multima Protect V1.1 - Références, référence LV-RD-13-REF-05-3040, version 01.01 du 24/11/2005.
[GUIDES]	- Spécifications techniques de la personnalisation du masque B4-B0' V3, référence DET/ES/SPE/2000-01, version 4.1 du 20/06/2000. - Spécifications techniques de la personnalisation du masque B4-B0' V3 Addendum n°1, référence DET/ES/SPE/2000-01, version 4.0.1 du 18/01/2001. - Spécifications techniques de la personnalisation du masque B4-B0' V3 Addendum n°2, référence DET/ES/SPE/2000-01, version 4.0ad2 du 18/06/2001. - Document d'administration B0, référence DET/DS/CBGEN6, version 1.0 du 01/09/2000. - Multima Protect V1 AGD-USR, référence LV-RD-13-USR-04-3006, version 1.01 du 04/02/2005. - AGD-ADM Multima Protect V1, référence LV-RD-13-ADM-04-3005, version 1.04 du 28/11/2005.
[RTE]	Rapport technique d'évaluation, référence LETI.CESTI.MYO2.RTE.001, version 1.0 du 01/12/05.
[ST]	Multima Protect V1 Software - B0' part - Security Target, reference LV-RD-13-STT-03-3029 révision 01.06 du 17/11/2005.
[2005/22]	Rapport de certification 2005/22 - Carte Multima Protect V1 : composant AT90SC9608RC masqué par l'application B4 B0' V3 (référence AT578A7K-AA).
[2004/35]	Rapport de certification du « Micro-circuit ATMEL AT90SC9608RC rev. I », référence 2004/35 du 15/12/2004.
[PP/9911]	« Smartcard integrated circuit with embedded software » v2.0 Issue June 1999.
[PP/9806]	« Smartcard integrated circuit Protection Profile version 2.0 »

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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[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 2.0, April 1999, Management Committee of Agreement Group.

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
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr