PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2007/13

Carte EMV PRO Y: composant Atmel AT90SC9618RCT rév. D, masqué par le logiciel EMV PRO Y : application Monéo porteur (référence : EMVDDA/AT58823D/4.0.1)

Paris, le 8 juin 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

Référence du rapport de certification

DCSSI-2007/13

Nom du produit

Carte EMV PRO Y: composant Atmel AT90SC9618RCT rév. D, masqué par le logiciel EMV PRO Y : application Monéo porteur (référence : EMVDDA/AT58823D/4.0.1)

Référence/version du produit

EMVDDA/AT58823D/4.0.1

Conformité à un profil de protection

PP/9806 et PP/9911

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

Développeur(s)

Sagem Défense Sécurité

Avenue du Gros Chêne,
95610 Eragny sur Oise,
France

Atmel

Maxwell Building - Scottish Enterprise technology Park, East Kilbride G75 0QR
Ecosse, Royaume-Uni.

Commanditaire

Sagem Défense Sécurité

Avenue du Gros Chêne,
95610 Eragny sur Oise,
France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

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 EMV PRO Y: composant Atmel AT90SC9618RCT rév. D, masqué par le logiciel EMV PRO Y : application Monéo porteur » développée par Sagem Défense Sécurité.

Le produit embarque d'autres applications. Trois de ces applications ont été évaluées conjointement et certifiées sous les références indiquées :

- une application Administration (DCSSI-2007/10),
- une application bancaire B0' (DCSSI-2007/11),
- une application bancaire EMV (DCSSI-2007/12),

Les autres applications également embarquées n'ont pas été évaluées. Leur présence a néanmoins été prise en compte lors de l'évaluation, notamment dans le cadre de la recherche de vulnérabilité.

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/0101 [PP0101].
Elle est conforme aux profils de protection [PP/9911] et [PP/9806].

La TOE permet dans l'environnement de l'utilisateur final, d'effectuer les actions suivantes :

- le chargement d'EV ;
- le paiement de proximité.

Le chargement de valeurs électroniques est réalisé par le "EV provider" qui crédite la carte de la valeur demandée par le porteur.

Le paiement de proximité est réalisé par le "Service Provider" qui transfert des valeurs de la carte du porteur vers le "Purchase Device".

Les différents acteurs du système Monéo sont présentés dans la cible de sécurité [ST].

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 : Carte EMV PRO Y : Application B0' ;
- Référence du produit : EMVDDA/AT58823D/4.0.1 ;
- Référence du logiciel : OFFICIEL_EMVDDA_9618_4_0_1 ;
- Référence du composant : ATMEL - AT90SC9618RCT, révision D.

Ces informations peuvent être vérifiées au travers de la réponse de la carte à l'initialisation (ATR). Les octets d'identification sont disponibles dans le guide « Document d'installation, de génération et de démarrage » (cf. [GUIDES]) pour vérification.

1.2.2. Services de sécurité

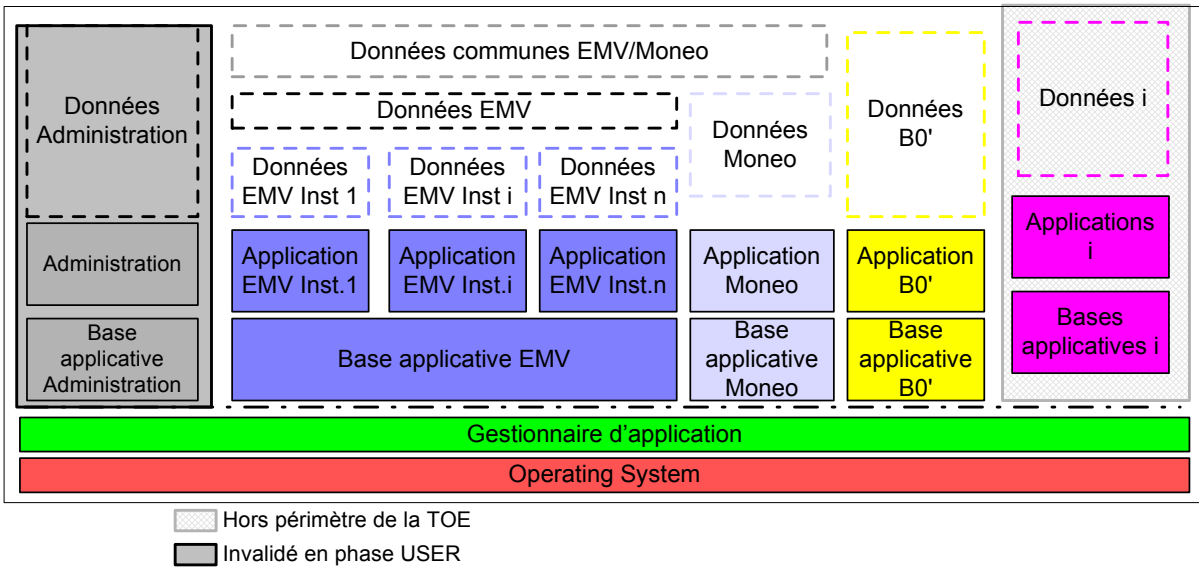
Les principaux services de sécurité fournis par le produit sont :
- La transaction Monéo Load ;
- La transaction Monéo Unload ;
- La transaction Monéo Quickload ;
- La transaction Monéo Débit ;
- La transaction Monéo de Débit incrémental ;
- La transaction Monéo de Débit incrémental France Télécom ;
- La mise à jour des clés ;
- L'authentification du porteur.

1.2.3. Architecture

Le produit est constitué d'un circuit intégré (AT90SC9618RCT révision D, d'ATMEL) avec le code exécutable chargé en mémoire ROM et les données et patch éventuel chargés en mémoire l'EEPROM.

Le logiciel embarqué en mémoire ROM est composé :
- d'un système d'exploitation qui réalise, entre-autre, l'interface avec les fonctionnalités du composant,
- d'un gestionnaire d'application qui réalise l'interface entre les applications et les services du système d'exploitation,
- des applications elles-mêmes.

Chaque application est constituée :
- d'une base applicative chargée en mémoire ROM qui est le code exécutable de l'application,
- d'un logiciel application qui constitue le contexte de travail de l'application,
- de données spécifiques chargées en EEPROM qui constituent toutes les données dont a besoin l'application.



Le périmètre d'évaluation pour l'application Monéo est composé de :

- le composant Atmel AT90SC9618RCT, révision D ;
- l'operating system (OS),
- le gestionnaire d'application (GA),
- l'application Monéo porteur (base applicative, l'application et les données).

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

Phase	Description	Autorité
Phase 1	Développement du logiciel embarqué de la carte à puce	**Sagem Défense Sécurité** est responsable du développement du logiciel intégré à la carte à puce et de la spécification des exigences de pré-personnalisation du circuit intégré.
Phase 2	Développement du circuit intégré (CI)	**Atmel** conçoit le CI, développe le logiciel dédié du CI et transmet les informations, le logiciel et les outils au logiciel embarqué du développeur (**Sagem Défense Sécurité**), par des procédures de vérification et de livraison sécurisées. A partir du circuit intégré, du logiciel dédié et du logiciel embarqué, il construit la base de données du circuit intégré de la carte à puce, indispensable à la réalisation du masque du circuit intégré.
Phase 3	Fabrication et test du circuit intégré	**Atmel** est responsable de la production du circuit intégré, qui se déroule en trois étapes principales : fabrication, test et pré-personnalisation fondeur du circuit intégré.
Phase 4	Encapsulation et test du circuit intégré	Le **constructeur de conditionnement du circuit intégré** est responsable du conditionnement

		(encapsulation) et du test du circuit intégré.
Phase 5	Finition du produit Carte à puce	Le **constructeur de la carte à puce** est responsable de la finition et du test de la carte à puce.
Phase 6	Personnalisation de la carte à puce	Le **personnalisateur** est responsable de la personnalisation de la carte à puce et des derniers tests.
Phase 7	Exploitation de la carte à puce	L'**émetteur de carte à puce** est responsable de la livraison du produit à l'**utilisateur final**, ainsi que de la fin du cycle de vie.

Le produit a été développé sur le site suivant :

Sagem Défense Sécurité

Etablissement R&D d'Eragny - Avenue du gros Chêne
95610 Eragny sur Oise,
France

Le composant a été développé par ATMEL Secure Products Division :

ATMEL Secure Products Division
Maxwell Building
Scottish Enterprise technology Park
East Kilbride, G75 0QR
Ecosse, Royaume-Uni

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC], 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, 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 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 du microcontrôleur sécurisé Atmel AT90SC9618RCT rév. D au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP/9806]. Ce microcontrôleur a été certifié le 14 décembre 2006 sous la référence 2006/26.

L'évaluation s'appuie sur les résultats d'évaluation du produit Carte EMV PRO Y: composant Atmel AT90SC9618RCT rév. D, masqué par le logiciel : application Administration réf. EMVDDA/AT58823D/4.0.1 évalué et certifié conjointement sous la référence 2007/10.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 3 mai 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

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 EMV PRO Y: composant Atmel AT90SC9618RCT rév. D, masqué par le logiciel EMV PRO Y : application Monéo porteur » 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 :

- Des protocoles et procédures de communication sécurisés doivent être utilisés entre la carte à puce et le terminal.
- Le fournisseur de valeur électronique (Electronic Value Provider) doit garantir la valeur électronique dans le système de porte-monnaie électronique (PME) sur la base des règles de sécurité du système. Les acteurs du système dont le porteur du porte-monnaie électronique doivent appliquer les règles de sécurité du système. Le fournisseur de valeur électronique doit communiquer au porteur les règles qui régissent l'utilisation du porte-monnaie électronique.
- Le terminal de paiement doit avoir au moins le même niveau de sécurité que le porte-monnaie électronique.
- Les terminaux de chargement (LD) et d'acquisition (AD) ne doivent pas créer de valeur électronique : ils doivent distribuer aux parties autorisées le même montant de valeur électronique qu'ils ont reçu.
- Le terminal de chargement doit entrer dans un état sécurisé en cas de défaillance au cours de transactions de chargement ou au cours de transactions anormales, de transactions rejouées ou falsifiées, sans qu'il n'y ait perte ou création de valeur électronique.
- Un domaine de sécurité doit être disponible pour l'utilisation du terminal de chargement, afin de le protéger des interférences et des attaques issues d'agents ne faisant pas partie des agents de confiance.
- Le terminal de chargement doit enregistrer les évènements et les données nécessaires pour s'assurer que des informations existent afin de participer à une gestion efficace de la sécurité

- Les terminaux de chargement et d'acquisition doivent empêcher les utilisateurs d'avoir accès à des ressources et d'y effectuer des opérations pour lesquelles ils ne possèdent pas de permission.
- Au cours d'un chargement, le terminal de chargement doit maintenir deux domaines séparés : d'une part le domaine de transaction de débit et, d'autre part, le domaine de chargement du porte-monnaie électronique.
- Le fournisseur du porte-monnaie électronique doit assurer que le porte-monnaie électronique est livré et installé de sorte que le niveau de sécurité visé soit préservé.
- Le fournisseur du porte-monnaie électronique doit assurer que le porte-monnaie électronique est géré, administré et fonctionne de sorte que le niveau de sécurité visé soit préservé.
- Le terminal d'acquisition doit entrer dans un état sécurisé en cas de défaillance au cours de transactions, au cours de transactions anormales, de transactions rejouées ou falsifiées, sans qu'il n'y ait perte ou création de valeur électronique.
- La version du patch chargée en EEPROM doit être vérifiée conformément au guide d'installation.

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]	Cible de sécurité EMV/DDA - MONEO : Application Monéo, Référence : ERA U32 CIS 008/03 indice U du 15/03/07.
[RTE]	Rapport technique d'évaluation : Référence : LETI.CESTI.BAA.RTE.002 - v1.1 - 02/05/07
[CONF]	Projet EMV PRO Y Fiche de Version du Logiciel OFFICIEL_EMVDDA_9618_4_0_1, du 19/03/07, Référence : SK 0000053174-01 version 1.5
[GUIDES]	Guide d'installation du produit : - Document d'installation, de génération et de démarrage, Référence : SK-0000057308-01 Version J du 18/12/06, Guide d'utilisation et d'administration du produit : - Guide d'administration en phase user, Référence : ERA U32 DR 215/03 Version D du 16/01/07, - Spécifications d'administration, Référence : ERA U32 DR 025/03 Version V du 26/03/07, - Spécifications d'initialisation, Référence : ERA U32 DR 180/03 Version J du 26/03/07, - Spécifications fonctionnelles carte EMV PRO Y, Référence :ERA U32 DR 040 03 Version L du 08/02/07, - Spécifications de personnalisation, Référence : ERA U32 DR 179/03 Version S du 26/03/07.
[PP/9911]	Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. *Certifié par la DCSSI sous la référence PP/9911.*
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certifié par la DCSSI sous la référence PP/9806.*
[PP/0101]	Protection Profile Intersector Electronic Purse and Purchase Device (version without Last Purchase Cancellation), Version 1.3 March 2001. *Certifié par la DCSSI sous la référence PP/0101.*

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.