PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2007/09

Carte Moneo avec et sans contact : Composant AT90SC6408RFT masqué par l'application Moneo (référence : MONEOSC/AT58848E/1.0.1)

Paris, le 23 avril 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-2007/09

Nom du produit

Carte Moneo avec et sans contact : Composant AT90SC6408RFT masqué par l'application Moneo

Référence/version du produit

MONEOSC/AT58848E/1.0.1

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

Développeurs

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

Billettique Monétique Services

25, rue de Ponthieu, 75008 Paris, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@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 Moneo avec et sans contact, constituée du composant AT90SC6408RFT rev. E développé par ATMEL Secure Products Division, et masqué par l'application Moneo développée par Sagem Défense Sécurité. Le produit embarque également des applications de transport (CALYPSO), de fidélité (ANB) et de management de la carte (AIP), mais ces applications dites « propriétaires » ne font pas partie du périmètre d'évaluation.
Cette carte est destinée à être utilisée pour effectuer des transactions de porte-monnaie électronique selon les spécifications Moneo, version 2.5.2 (cf. [ST, §1.1])

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 (cf. [PP0101]).
Elle est de plus conforme aux profils de protection PP/9911 et PP/9806 (cf. [PP9911] et [PP9806]).

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 Moneo avec et sans contact ;
- Référence du produit : MONEOSC/AT58848E/1.0.1 ;
- Référence fondeur : AT58848-D-BA ;
- Référence du logiciel : OFFICIEL_MONEOSC_AT6408_1_0_1 ;
- Référence du composant : AT90SC6408RFT, référence AT58848 révision E.

Ces informations peuvent être vérifiées au travers de la réponse de la carte à l'initialisation (ATR) ou de la commande « Get data ». Les octets d'identification sont disponibles dans le guide « Documentation 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 :

- gestion du cycle de vie du produit ;
- initialisation du produit ;
- détection et réaction aux attaques ;
- intégrité des données et du code exécutable ;
- auto-tests des services de sécurité ;

- gestion des applications ;
- mécanismes transactionnels ;
- contrôle d'accès aux mémoires ;
- authentification du porteur ;
- authentification du service ;
- journaux d'événements ;
- calculs cryptographiques ;
- gestion des clés ;
- authentification des transactions.

1.2.3. Architecture

Le produit est constitué des éléments suivants :

- composant AT90SC6408RFT, référence AT58848 révision E ;
- logiciel embarqué MONEOSC, référence : MONEOSC/AT58848E/1.0.1, comprenant : un système d'exploitation doublé d'un gestionnaire d'applications, de l'application Moneo, et des applications de transport (CALYPSO), de fidélité (ANB) et de management de la carte (AIP). L'application de management de la carte est invalidée en phase d'utilisation, et les applications dites « propriétaires » (CALYPSO, ANB) ne font pas partie du périmètre d'évaluation.

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

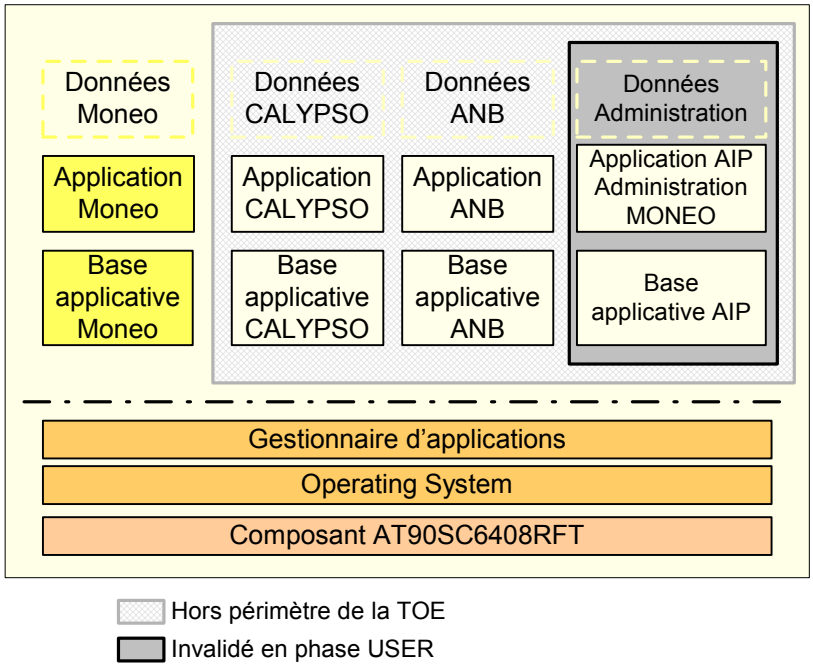

Figure 1 – Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

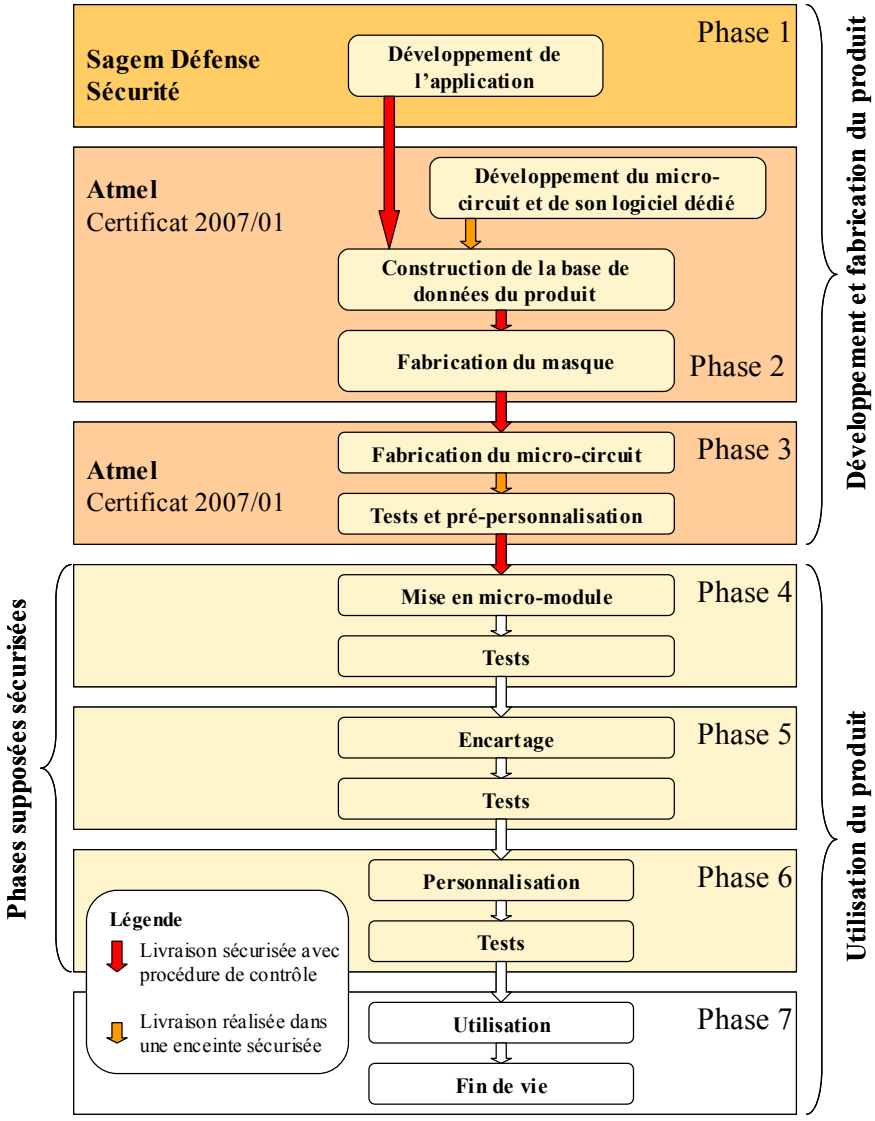

Figure 2 – Cycle de vie du produit

Le logiciel embarqué a été développé sur le site suivant :

Sagem Sécurité Défense

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

1.2.5. Configuration évaluée

Le produit comporte 3 applications finales (Moneo, Calypso, ANB) qui peuvent être activées ou non en phase d'utilisation. Le certificat porte sur les 2 configurations suivantes :

- Moneo et ANB ;
- Moneo, ANB et Calypso.

Ces configurations sont identifiables au travers des octets de réponse à l'initialisation (ATR).

Les applications ANB et Calypso sont dites en dehors du périmètre d'évaluation dans la mesure où aucune donnée associée n'est identifiée dans la cible de sécurité comme étant à protéger par le produit. Leur présence a néanmoins été prise en compte lors de l'évaluation, notamment dans le cadre de la recherche de vulnérabilité.

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, 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 AT90SC6408RFT rev. E au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP9806]. Ce microcontrôleur a été certifié le 15 janvier 2007 sous la référence 2007/01.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 12 avril 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 Moneo avec et sans contact : Composant AT90SC6408RFT masqué par l'application Moneo (référence : MONEOSC/AT58848E/1.0.1) » 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 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 du 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 du porte-monnaie électronique doivent s'assurer que le porte-monnaie est géré, administré et utilisé de manière à maintenir le niveau de sécurité visé ;
- les terminaux de paiement 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 ;
- les terminaux de paiement doivent enregistrer les évènements et les données nécessaires afin de participer à une gestion efficace de la sécurité.

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 MONEO avec et sans contact, Référence : SK-0000037230 version 1.5 Sagem Défense Sécurité
[RTE]	- Evaluation Technical Report Moneo Contact / Contactless on AT90SC6408RFT Microcontroler (MONEOSC/AT58848E/1.0.1), Référence : PEACOCK_ETR_V1.0 Serma Technologies - Addendum to Evaluation Technical Report - Moneo Contact / Contactless on AT90SC6408RFT Microcontroler (MONEOSC/AT58848E/1.0.1), Référence : PEACOCK_ETR_add_V1.0 Serma Technologies
[CONF]	Projet Moneo sans contact - Fiche de Version du Logiciel OFFICIEL_MONEOSC_AT6408_1_0_1, Référence : SK 0000053296-03 - 26 février 2007 Sagem Défense Sécurité
[GUIDES]	Guide du produit : - Documentation d'installation, de génération et de démarrage, Référence : SK 0000057306 indice 1.2, Sagem Défense Sécurité - Spécification d'administration de la carte Moneo sans contact, Référence : SK 0000036770 indice 1.4, Sagem Défense Sécurité - Electronic Purse Moneo card specification PME, Référence : DSI9A, version 2.5.2 - December 2001 + PDA 22032002 Billettique Monétique Services - Electronic PURSE Moneo Contactless CARD Specification PME, Référence : DSI9_WIFI, version 1.1.1 - January 2006, Billettique Monétique Services - No Banking Application, Version 2.0 DSI20 Billettique Monétique Services
[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. C*ertifié 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.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.