



PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/24

Carte Multima Protect V1 : composant AT90SC9608RC masqué par l'application MONEO V1

(référence AT578A7K-AA)

Paris, le 15 septembre 2005.

*Le Directeur central de la sécurité des
systèmes d'information*

Henri Serres
[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 présumées 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 2005/24

**Carte Multima Protect V1 : composant
AT90SC9608RC masqué par l'application
MONEO V1
(référence AT578A7K-AA)**

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 EVALUE.....	6
1.1. IDENTIFICATION DU PRODUIT	6
1.2. DEVELOPPEURS	6
1.3. DESCRIPTION DU PRODUIT EVALUE.....	6
1.3.1. <i>Architecture</i>	6
1.3.2. <i>Cycle de vie</i>	7
1.3.3. <i>Périmètre et limites du produit évalué</i>	7
2. L'EVALUATION	9
2.1. CONTEXTE	9
2.2. REFERENTIELS D'EVALUATION	9
2.3. COMMANDITAIRE	9
2.4. CENTRE D'EVALUATION	9
2.5. RAPPORT TECHNIQUE D'EVALUATION	10
2.6. EVALUATION DE LA CIBLE DE SECURITE	10
2.7. EVALUATION DU PRODUIT.....	10
2.7.1. <i>Les tâches d'évaluation</i>	10
2.7.2. <i>L'évaluation de l'environnement de développement</i>	10
2.7.3. <i>L'évaluation de la conception du produit</i>	11
2.7.4. <i>L'évaluation des procédures de livraison et d'installation</i>	12
2.7.5. <i>L'évaluation de la documentation d'exploitation</i>	13
2.7.6. <i>L'évaluation des tests fonctionnels</i>	13
2.7.7. <i>L'évaluation des vulnérabilités</i>	14
2.7.8. <i>L'analyse de la résistance des mécanismes cryptographiques</i>	14
3. LA CERTIFICATION	15
3.1. CONCLUSIONS	15
3.2. RESTRICTIONS D'USAGE	15
ANNEXE 1. VISITE DU SITE DE DEVELOPPEMENT DE LA SOCIETE AXALTO A LOUVECIENNES.....	17
ANNEXE 2. NIVEAUX D'ASSURANCE PREDEFINIS EAL	18
ANNEXE 3. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	19
ANNEXE 4. REFERENCES LIEES A LA CERTIFICATION	20

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la « Carte Multima Protect V1 : composant AT90SC9608RC masqué par l'application MONEO V1 (référence AT578A7K-AA) » développée par les sociétés Axalto 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_21 développé par Axalto.

Le produit contient les application suivantes :

- une application débit/ crédit B0' ;
- une application débit/ crédit CB-EMV-DDA (soit Visa, soit M/Chip) ;
- une application porte-monnaie électronique Moneo ;
- une application fidélité (FID) basée sur Moneo.

Ce certificat porte sur l'application porte-monnaie électronique Moneo, il est associé aux certificats 2005/22 et 2005/23 qui portent respectivement sur l'application débit/crédit B0' et sur l'application débit/crédit CB-EMV-DDA.

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

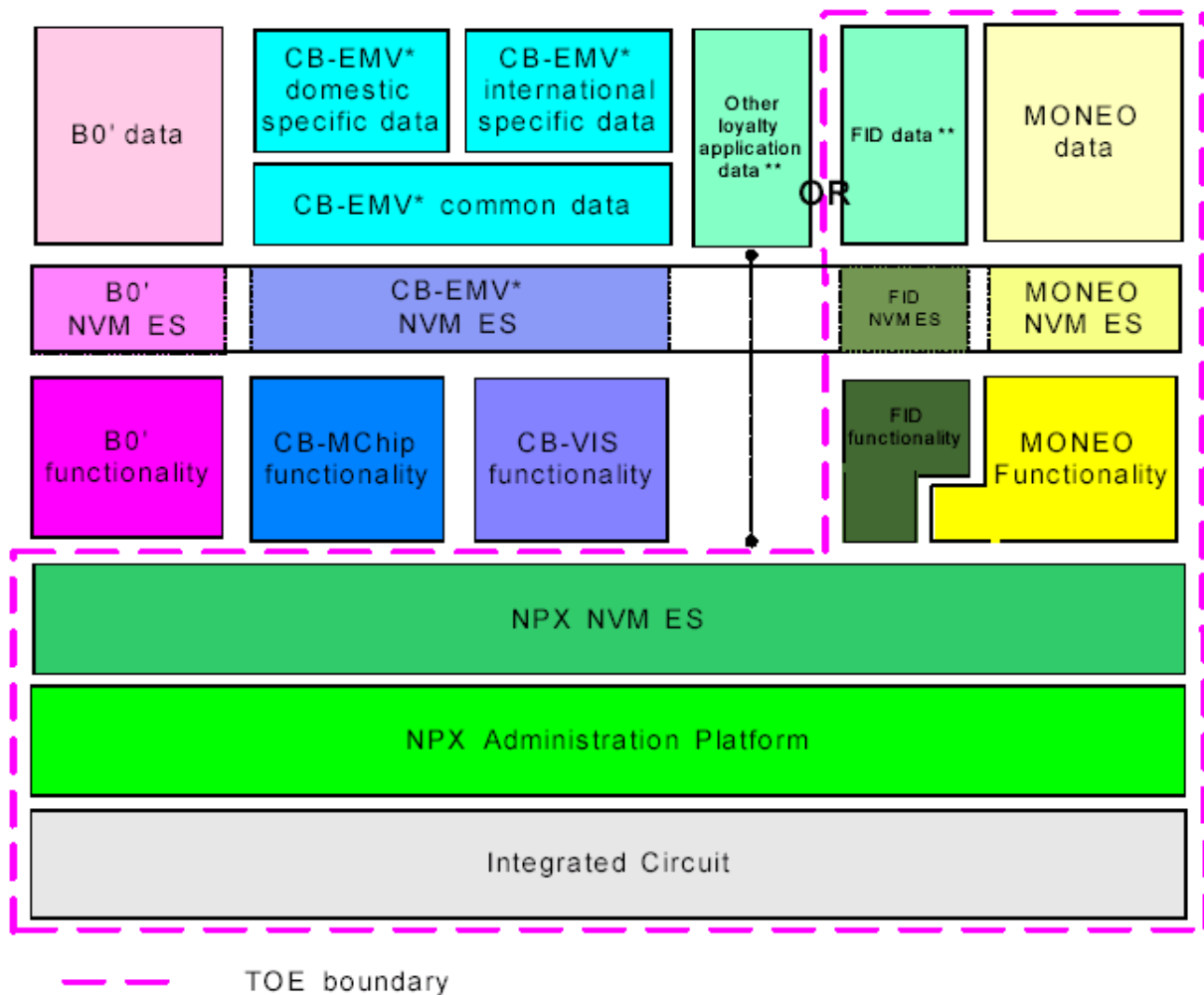


Figure 1 - Périmètre du produit évalué

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 MONEO V1 ;
- l'application FID ;
- la plate-forme d'administration NPX.

Ce rapport de certification présente les travaux d'évaluation relatifs à la partie Moneo 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 :

BO'	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	

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 produit évalué est dérivé de la carte Multima Classic (référence ST19XS08C/PIF) dont l'application MONEO V1 a été certifiée le 12 août 2003 sous la référence 2003/09 [2003/09].

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 4 mai 2004 au 8 août 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 EAL4¹ 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

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur les sites de :

¹ Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

- 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 lors de la visite du site d'Axalto à Louveciennes (cf Annexe 1). 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)
- Protected audit trail storage (FAU_STG.1)
- Enforced proof of origin (FCO_NRO.2)
- Enforced proof of receipt (FCO_NRR.2)
- 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)
- Basic data authentication (FDP_DAU.1)
- Export of user data without security attributes (FDP_ETC.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.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 authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Re-authenticating (FIA_UAU.6)
- 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)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- Function recovery (FPT_RCV.4)
- Replay detection (FPT_RPL.1)
- Non-bypassability of the TSP (FPT_RVM.1)
- 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'évaluations liés au composant d'assurance ADO_IGS.1 ont été considérés comme satisfaisants.

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 14 configurations évaluées.

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 [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Les fonctions NPX_SFIAubTOE, MONEO_FS1, MONEO_FS4 et MONEO_FS9 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 [INSTALL] [GUIDES] ; ces objectifs de sécurité concernent le système dans lequel sera utilisée l'application en phase finale d'utilisation (objectifs extraits de la cible de sécurité [ST § 4.2]). Dans le cadre de la présente évaluation, ces objectifs de sécurité sont issus du PP/0101 [PP/0101] (partie « Porte monnaie électronique ») et du PP/9911 [PP/9911] :

- la communication entre la carte et le terminal doit être sécurisée (en termes de protocole et de procédure) (OE.USE_DIAG) ;
- 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 (OE.SYSTEM) ;
- les appareils de chargement et d'acquisition ne doivent pas créer de valeur électronique, mais seulement distribuer aux parties autorisées le même montant de valeur électronique qu'ils reçoivent (OE.EV_DISTRIB) ;
- les appareils 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 (OE.LA_FAIL) ;
- l'application de l'appareil de chargement doit s'exécuter dans un domaine logique de sécurité disponible à cet effet, afin de prévenir les interférences et les altérations pouvant être provoquées par des agents frauduleux (OE.LA_DOMAIN) ;
- les appareils de chargement doivent enregistrer tous les événements et/ou données nécessaires, contribuant à une gestion efficace du système (OE.LA_RECORD) ;

- les appareils de chargement et d'acquisition doivent prévenir les accès et les opérations effectués par les utilisateurs sur des ressources sur lesquelles ils n'ont pas de permissions (OE.AUTH2) ;
- durant un chargement, l'appareil de chargement doit maintenir deux domaines de sécurité distincts : le domaine de transaction de débit, et le domaine de transaction de chargement du porte-monnaie électronique (OE.PSEUDO) ;
- les fournisseurs de porte-monnaies électroniques doivent s'assurer que la cible d'évaluation est délivrée et installée de manière à maintenir le niveau de sécurité (OE.INSTALL) ;
- les fournisseurs de porte-monnaies électroniques doivent s'assurer que la cible d'évaluation est gérée, administrée de manière à maintenir le niveau de sécurité (OE.MANAGE) ;
- les appareils d'acquisition doivent entrer dans un état sûr lors de défaillance durant d'une transaction de chargement, lors d'une transaction anormale ou bien lors du re-jeu d'une transaction, sans perte ou création de valeur électronique (OE.ACQ) ;
- les appareils d'acquisition doivent enregistrer tous les événements et/ou données nécessaires, contribuant à une gestion efficace du système (OE.A_RECORD) ;
- les fonctions de sécurité des appareils d'achat doivent prévenir toute modification des données de traçabilité de flux et des paramètres de l'appareil d'achat non autorisée, durant un transfert ou une mémorisation (OE.PD_INTEG_DATA) ;
- les fonctions de sécurité d'un appareil d'achat doivent prévenir toute entrée logique sur cet appareil faite par une personne, un équipement ou processus qui ne posséderait pas les droits d'accès suffisants, et prévenir les acteurs de contourner le modèle de flux de valeur électronique (OE.PD_LOGICAL) ;
- les fonctions de sécurité des appareils d'achat doivent assurer que les transactions re-jouées sont détectées et contrées (OE.PD_REPLAY) ;
- les fonctions de sécurité des appareils d'achat doivent assurer la poursuite correcte des opérations de ses fonctions de sécurité particulièrement durant une transaction anormale, comme par exemple une interruption de transaction (OE.PD_OPERATE).

Annexe 1. Visite du site de développement de la société Axalto à Louveciennes

Le site de développement de la société Axalto situé à Louveciennes, a fait l'objet d'une visite par l'évaluateur le 5 avril 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour la carte Multima Protect V1 (référence AT578A7K-AA).

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_AUT.1 et ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. 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 3. Références documentaires du produit évalué

[CONF]	Logiciel Multima Protect V1.0 ACM – Liste de configuration, référence LV-RD-13-ACM-04-3020, version D-01.00 du 05/04/2005.
[GUIDES]	- 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 1.02 du 01/02/2005. - Manuel de personnalisation - carte Multima Protect V1 - Application FID, référence LVRDMAN-04-3050, version 4.0 du 11/02/2005. - Manuel de personnalisation – carte Multima Protect V1 – Application MONEO, référence LVRDMAN-03-3027, version 1.2 du 17/02/2005.
[RTE]	- Rapport technique d'évaluation, référence LETI.CESTI.MYO.RTE.001, version 1.0 du 01/08/05. - Addendum au RTE, référence LETI.CESTI.MYO.RTE.002, version 1.0 du 08/08/05.
[ST]	Multima Protect V1 Software - Moneo part - Security Target, reference LV-RD-13-STT-03-3021, version 01.04 du 03/02/2005.
[Visite]	Rapport technique d'évaluation, chapitres 39 et 40, référence LETI.CESTI.MYO.RTE.001, version 1.0 du 01/08/05.
[2003/09]	Rapport de certification 2003/09 - Carte Multima Classic : composant ST19XS08C masqué par l'application Moneo V1 (référence ST19XS08/PIF du 12/08/03)
[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 4. 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

La reproduction de ce document sans altérations ni coupures est autorisée.