PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

DIRECTION CENTRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

Rapport de certification 2001/20

Porte-monnaie électronique MODEUS :
carte porteur MODEUS card v1.1
(référence : ST16RF58/RSE+)
et module de sécurité commerçant SAM TC/C v1.1
(référence : ST19SF16FF/RVN)

Décembre 2001

PREMIER MINISTRE

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

CERTIFICAT 2001/20

Porte-monnaie éléctronique MODEUS : carte porteur MODEUS card v1.1

(référence : ST16RF58/RSE+)

et module de sécurité commerçant SAM TC/C v1.1

(référence : ST19SF16FF/RVN)

Développeurs : ASK, CP8, STMicroelectronics

EAL1 Augmenté

conforme au profil de protection PP/9908

Commanditaire : BMS (Modeus)

Le 5 décembre2001,

Le Commanditaire :
Le Directeur Général de BMS

Pierre Fersztand

L'Organisme de certification :
Le Directeur central de la sécurité des systèmes d'information
Henri Serres

Ce produit a été évalué par un centre d'évaluation de la sécurité des TI conformément aux Critères Communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée du produit dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de certification :
Secrétariat Général de la Défense Nationale
DCSSI
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

Chapitre 1

Résumé

1.1 Objet

1 Ce document représente le rapport de certification de la carte porteur MODEUS card v1.1 et du module de sécurité commerçant SAM TC/C v1.1. Ces deux éléments font partie du système de porte-monnaie électronique MODEUS.

2 La cible d'évaluation est composée des deux micro-circuits avec leurs logiciels embarqués. Ces composants sont destinés à être intégrés dans des supports plastiques pour constituer, pour l'un, la carte porteur en mode sans contact pour le porte-monnaie électronique MODEUS et, pour l'autre, le module de sécurité en mode contact inséré dans le terminal du commerçant.

3 Les développeurs de la cible d'évaluation sont :

- STMicroelectronics pour les deux micro-circuits :
  STMicroelectronics
  ZI de Rousset - BP2
  13106 Rousset Cedex
  France.

- ASK pour l'application porte-monnaie électronique de la carte porteur :
  ASK
  15, traverse des Brucs
  06560 Sophia Antipolis
  France.

- CP8 pour l'application du module de sécurité commerçant :
  CP8
  36-38, route de la Princesse
  78431 Louveciennes cedex
  France.

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

5 Le niveau d'assurance atteint est le niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [CC].

6 L'évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information CESTI LETI :

- CESTI LETI
  17, rue des Martyrs
  38054 Grenoble cedex 9
  France.

1.2 Contexte de l'évaluation

7 L'évaluation s'est déroulée consécutivement au développement du produit de mai 2000 à juillet 2001.

8 La cible d'évaluation est conforme au profil de protection "Intersector Electronic Purse and Purchase Device (version for pilot schemes only)" enregistré auprès du SCSSI sous la référence PP/9908 [PP/9908].

9 Le commanditaire de l'évaluation est BMS :

- BMS (MODEUS)
  25, rue de Pontieu
  75008 Paris
  France.

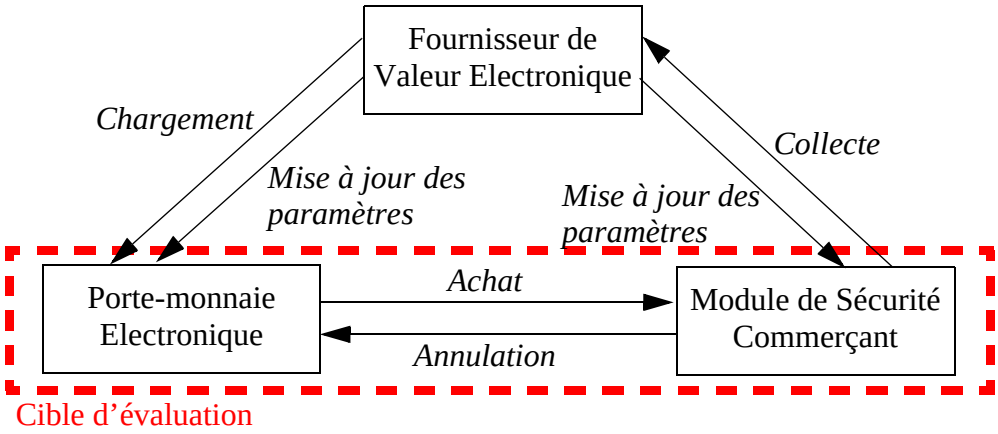
Chapitre 2

Description de la cible d'évaluation

2.1 Périmètre de la cible d'évaluation

10 La cible d'évaluation est constituée des deux élément suivants :

- le composant masqué ST16RF58/RSE+ utilisé dans la carte porteur MODEUS card v1.1 ;
- le composant masqué ST19SF16FF/RVN utilisé dans le module de sécurité commerçant SAM TC/C v1.1.



2.2 Cycle de vie

11 Le cycle de vie de ces deux cartes se décompose de la manière suivante :

- Développement des masques,
- Phase de fabrication pendant laquelle le logiciel embarqué est masqué sur le composant,
- Encartage,
- Phase de pré-personnalisation pendant laquelle des informations spécifiques (complément de code, architecture mémoire, numéro de série, clé de fabrication) sont insérées dans la carte,
- Phase opérationnelle pendant laquelle la carte est utilisée.

2.3 Fonctions de sécurité évaluées

12 Les fonctions de sécurité évaluées sont les suivantes :

- Contrôle d'accès,
- Authentification de données externes,
- Authentification de données internes,
- Certification des transactions,
- Intégrité des données internes,
- Détection d'une utilisation anormale,
- Enregistrement des dernières opérations,
- Détection du rejeu de transactions.

2.4 Documentation disponible

13 La documentation disponible décrit les procédures d'utilisation de la carte porteur [GUIDE_PORTEUR], du module de sécurité commerçant [GUIDE_COMMERCANT] et du terminal de paiement [GUIDE_TPME].

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

14 Le niveau visé pour la cible d'évaluation est EAL1 augmenté du composant AVA_VLA.2 «Analyse de vulnérabilités indépendante» :

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	Introduction de la ST (ASE_INT.1) Description de la TOE (ASE_DES.1) Environnement de sécurité (ASE_ENV.1) Objectifs de sécurité (ASE_OBJ.1) Annonce de conformité à un PP (ASE_PPC.1) Exigences de sécurité des TI (ASE_REQ.1) Exigences de sécurité des TI explicitement énoncées (ASE_SRE.1) Spécifications globales de la TOE (ASE_TSS.1)
Gestion de configuration	Numéros de version (ACM_CAP.1)
Livraison et exploitation	Procédures d'installation, de génération et de démarrage (ADO_IGS.1)
Développement	Spécifications fonctionnelles informelles (ADV_FSP.1) Démonstration de correspondance informelle (ADV_RCR.1)
Guides	Guide de l'administrateur (AGD_ADM.1) Guide de l'utilisateur (AGD_USR.1)
Tests	Tests indépendants - conformité (ATE_IND.1)
Estimation des vulnérabilités	Analyse de vulnérabilités indépendante (AVA_VLA.2)

15 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.

16 Le détail des travaux d'évaluation menés est disponible dans le Rapport Technique d'Evaluation [RTE].

17 Les travaux d'évaluation ont été menés à la fois sur le composant masqué utilisé dans la carte porteur et sur celui utilisé dans le module commerçant.

18 Conformément au niveau visé, les seules informations de conception qui ont été fournies à l'évaluateur sont les spécifications fonctionnelles des fonctions de sécurité.

19 Les procédures d'installation, de génération et de démarrage (composant ADO_IGS.1) évaluées sont les procédures de réponse au Reset de l'application.

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeur

20 Conformément au niveau d'évaluation visé, le développeur n'a pas eu à fournir sa stratégie de tests fonctionnels.

3.2.2 Tests évaluateur

21 L'évaluateur a effectué des tests indépendants pour déterminer par échantillonnage que les fonctions de sécurité de la cible d'évaluation se comportent comme spécifiées.

22 L'évaluateur a également mené une analyse de vulnérabilités, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élémentaire (composant AVA_VLA.2) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation suivants :

- Empêcher la création ou la perte de valeur électronique,
- Empêcher la modification non-autorisée des données ou paramètres pendant les transferts ou le stockage,
- Empêcher l'accès à la cible d'évaluation par des acteurs qui veulent outrepasser le modèle de flux de la valeur électronique,
- Permettre l'authentification de la cible de sécurité auprès des appareils de chargement et d'acquisition,
- S'assurer que les données d'utilisations ne sont accessibles que par les personnes autorisées,
- Assurer la continuité de service des fonctions de sécurité,
- Empêcher le rejeu de transactions,
- Prévenir les attaques physiques,
- Enregistrer les données de flux,
- Limiter le montant de valeur électronique,
- Assurer le cloisonnement avec d'autres applications.

Chapitre 4

Certification

4.1 Verdict

23 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [CC].

4.2 Recommandations

24 La cible d'évaluation "Porte-monnaie électronique MODEUS : carte porteur MODEUS card v1.1 (référence : ST16RF58/RSE+) et module de sécurité commerçant SAM TC/C v1.1 (référence : ST19SF16FF/RVN)" est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

a) Le fournisseur de valeur électronique doit garantir la sécurité de la valeur dans le système porte-monnaie électronique sur la base de la politique de sécurité du système ;

b) Les équipements de chargement et de collecte ne doivent pas permettre de créer ou de perdre de la valeur électronique de manière illicite ;

c) Les évènements et données sensibles doivent être enregistrés dans le système ;

d) Des domaines de sécurités doivent être maintenus pendant les transactions dans le système ;

e) L'émetteur des cartes porteurs et des modules commerçant doit garantir la sécurité des produits lors de leur livraison et installation puis lors de leur utilisation.

4.3 Certification

25 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

26 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 2. La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

Références

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- Partie 1 : Introduction et modèle général CCIMB-99-031, version 2.1 Août 1999.
- Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.
- Partie 3 : Exigences d'assurance de sécurité CCIMB-99-033, version 2.1 Août 1999.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Partie 2 : Méthodologie d'évaluation CEM-99/045, version 1.0 Août 1999.

[PP/9908] Profil de Protection PP/9908 «Intersector Electronic Purse and Purchase Device (Version for Pilot Schemes Only) Version 1.2», Société Financière du PMEI - GIE Cartes Bancaires, fév. 1999.

[ST] - Intersector Electronic Purse, PME MODEUS V1.1, MONPAR security target, réf : MOD1-STV1.1 - 1.04 du 13 décembre 2000 (diffusion contrôlée)

[RTE] Rapport Technique d'Evaluation, réf : LETI.CESTI.MON.RTE.001, version 1.0 du 23 juillet 2001 (diffusion contrôlée).

[GUIDE_PORTEUR] Conditions générales de fonctionnement de la carte MODEUS dans le cadre des expérimentations, contrat applicable au système v1, MODEUS.

[GUIDE_COMMERCANT] Contrat d'adhésion au système de paiement par carte MODEUS dans le cadre des expérimentations (contrat d'acceptation), contract applicable au système v1, MODEUS.

[GUIDE_TPME] Manuel d'utilisation du TPME MODEUS (Terminal de Paiement en Monnaie Electronique) Mode à contact, version du 1er septembre 2000, MODEUS et Manuel d'utilisation du TPME MODEUS (Terminal de Paiement en Monnaie Electronique) Mode sans contact, version du 17 avril 2000, MODEUS

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification 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 07 SP

certification.dcssi@sgdn.pm.gouv.fr