PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

SERVICE CENTRAL 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 99/03

Porte-monnaie électronique MONEO

Carte porteur (ST19SF16B RCL version B303)

et module de sécurité PSAM commerçant (ST19SF16B RCL version C103)

Septembre 1999

Ce document constitue le rapport de certification du produit "Porte-monnaie électronique MONEO carte porteur (ST19SF16B RCL version B303) et module de sécurité PSAM commerçant (ST19SF16B RCL version C103)".

Ce rapport de certification est disponible sur le site internet du Service Central de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.scssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

SCSSI
Centre de Certification de la Sécurité des Technologies de l'Information
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

mèl : ssi20@calva.net

Ce document est folioté de 1 à 40 et certificat.

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

CERTIFICAT 99/03

Porte-monnaie électronique MONEO

carte porteur (ST19SF16B RCL version B303)
et module de sécurité PSAM commerçant (ST19SF16B RCL version C103)

Développeurs : IBM Deutschland Gmbh ; STMicroelectronics SA

EAL1 augmenté

conforme au profil de protection PP/9908

Commanditaire :

Société Européenne de Monnaie Électronique

Le 29 septembre 1999,

Le Commanditaire :
le Directeur général de la S.E.M.E.
M. P. Fersztand

L'organisme de certification :
Le chef du Service central de la sécurité
des systèmes d'information

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 2.0 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 0.6.

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
SCSSI
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit constitué de la carte porteur ST19SF16B RCL (version B303) et du module de sécurité PSAM commerçant ST19SF16B RCL (version C103).

2 Les fonctionnalités évaluées sont consignées en annexe A du présent rapport.

3 Le niveau d'assurance atteint est le niveau EAL 1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités effectuée de manière indépendante" tel que décrits dans la partie 3 des critères communs [4].

4 Ce produit 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, version 1.2 de février 1999 [6]. Ce profil de protection a été déposé conjointement par la Société Financière du Porte-Monnaie Électronique (SFPMEI) et le GIE Cartes Bancaires CB (certificat PP/9908 [7]).

5 La carte porteur et le module de sécurité commerçant sont les éléments clés du porte-monnaie électronique MONEO, tel qu'il est exploité par la Société Européenne de Monnaie Électronique (SEME). Ce système sera expérimenté dans l'agglomération de Tours au cours du dernier trimestre 1999.

Chapitre 2

Résumé

2.1 Description de la cible d'évaluation

6 La cible d'évaluation est celle du couple "carte porteur porte-monnaie électronique ST19SF16B RCL (version B303) et module de sécurité PSAM commerçant ST19SF16B RCL (version C103) destiné à être inséré dans l'équipement d'acceptation du commerçant".

2.2 Résumé des caractéristiques de sécurité

2.2.1 Menaces

7 Les principales menaces identifiées dans la cible de sécurité [8] peuvent être résumées comme suit :

- blanchiment d'argent,
- usurpation d'identité de l'un des acteurs du système,
- création frauduleuse de valeur électronique,
- perte de valeur électronique.

8 L'objectif de sécurité principal du système de porte-monnaie électronique étant celui de la conservation du flux de valeur électronique, les biens à protéger au sein de la cible d'évaluation sont définis comme étant la valeur électronique, les paramètres d'administration du porte-monnaie électronique et de l'équipement d'acceptation du commerçant ainsi que les données de traçabilité. Ces biens doivent être protégés en intégrité.

2.2.2 Politiques de sécurité organisationnelles et hypothèses

9 L'annexe A donne les principales caractéristiques de sécurité telles qu'elles sont décrites dans la cible de sécurité [8], en particulier les politiques de sécurité organisationnelles ainsi que les hypothèses d'utilisation du produit.

2.2.3 Exigences fonctionnelles de sécurité

10 Les principales fonctionnalités de sécurité du produit décrites dans la cible de sécurité [8] sont les suivantes :

- authentification du porte-monnaie électronique et de l'équipement d'acceptation du commerçant,

- authentification des acteurs,

- contrôle d'accès (valeur électronique et contrôle de flux),

- preuves d'origine et de réception des transactions (chargement, achat, collecte),

- protection des fonctions de sécurité : notification et résistance aux attaques physiques, détection de rejeu, préservation d'état sûr, recouvrement des fonctions, séparation de domaines.

2.2.4 Exigences d'assurance

11 Les exigences d'assurance spécifiées dans la cible de sécurité [8] sont celles du niveau d'évaluation EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités effectuée de manière indépendante".

2.3 Acteurs dans l'évaluation

12 Le commanditaire de l'évaluation est la Société Européenne de Monnaie Électronique (S.E.M.E.) :

SEME
29 rue de Berri
F-75008 PARIS.

13 La cible d'évaluation a été développée par les sociétés :

- IBM Allemagne pour le développement des logiciels,

  IBM Deutschland Gmbh
  Smartcard solutions
  Schoenaicher Str. 220
  D- 71032 Boeblingen.

- STMicroelectronics a également participé au développement de la cible d'évaluation en tant que développeur et fabricant du composant microélectronique ST19SF16 :

  STMicroelectronics SA
  ZI de Rousset BP2
  F- 13106 Rousset Cedex.

2.4 Contexte de l'évaluation

14 L'évaluation a été menée conformément aux critères communs ([1] à [4]) et à la méthodologie définie dans le manuel CEM [5].

15 L’évaluation s’est déroulée simultanément au développement du produit.

16 L’évaluation a été conduite par les centres d’évaluation de la sécurité des technologies de l'information du CNET de Caen et de Serma Technologies :

- Centre National d’Études des Télécommunications CNET Caen
  42, rue des Coutures
  BP 6243
  F-14066 Caen Cedex.

- Serma Technologies
  30, avenue Gustavel Eiffel
  F- 33608 Pessac Cedex.

2.5 Conclusions de l'évaluation

17 Le produit soumis à évaluation dont la cible de sécurité [8] est partiellement reprise dans l’annexe A du présent rapport, satisfait aux exigences du niveau d’évaluation EAL1 augmenté du composant d’assurance AVA_VLA.2 “Analyse de vulnérabilités effectuée de manière indépendante” et est conforme aux exigences du profil de protection PP/9908 [6].

18 La recherche de vulnérabilités exploitables au cours de l’évaluation a été définie par la quantité d’informations disponibles pour le niveau EAL1 et par la compétence, l’opportunité et les ressources correspondant à un potentiel d’attaques tel qu’il est spécifié par le composant d’assurance AVA_VLA.2.

19 Les vulnérabilités connues du commanditaire de l’évaluation ont été toutes communiquées aux évaluateurs et au certificateur conformément au critère [AVA_VLA.2.4E].

20 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

Identification de la cible d'évaluation

3.1 Objet

21 La cible d'évaluation est le couple "carte porteur porte-monnaie électronique ST19SF16B RCL (version B303)" et "module de sécurité PSAM commerçant ST19SF16B RCL (version C103)" destinée à être inséré dans l'équipement d'acceptation du commerçant, suivant un modèle d'échanges entre les différents acteurs du système porte-monnaie électronique de MONEO.

22 Le porte-monnaie électronique MONEO est constitué du micro-circuit électronique ST19SF16B RCL inséré dans une carte porteur de format carte de crédit. Le micro-circuit électronique contient le système d'exploitation de la carte ainsi que l'application porte-monnaie électronique MONEO. Une deuxième application bancaire (application B4/B0' V2 conforme aux spécifications du GIE Cartes Bancaires CB) est disponible sur la version B303 de la carte. Ce rapport de certification exclut l'évaluation de cette deuxième application.

23 Le module de sécurité PSAM commerçant est constitué du micro-circuit électronique ST19SF16B RCL. Le micro-circuit électronique contient le système d'exploitation du module de sécurité PSAM ainsi que l'application porte-monnaie électronique MONEO en configuration C103.

24 Les phases d'encartage et de personnalisation des deux éléments de la cible d'évaluation sont hors du champ de l'évaluation.

3.2 Historique du développement

25 La partie logicielle de la cible d'évaluation a été préalablement développée au sein de la division "Smartcard solutions" de IBM Deutschland Gmbh. Le porte-monnaie électronique MONEO s'appuie sur les spécifications du système Geldkarte allemand. Les spécificités du système français ont été définies par la SEME.

26 Le composant ST19SF16 a été développé et testé par STMicroelectronics sur le site de Rousset. La production des micro-circuits est effectuée sur les sites d'Agrate (Italie) et Rousset (France).

3.3 Description du matériel

27 Le micro-circuit électronique ST19SF16 est un micro contrôleur de la famille des composants ST19SFXY. Il dispose d'une unité centrale de 8 bits associée à une mémoire de travail de 960 octets (RAM), d'une mémoire de programme de 32 Koctets (ROM), et d'une mémoire de données de 16Koctets (EEPROM).

28 Il dispose de différents mécanismes de sécurité participant à la réalisation des fonctions dédiées à la sécurité pour lesquelles l'évaluation a été demandée.

3.4 Description du logiciel

29 La cible d’évaluation est constituée des logiciels suivants :

- le système d’exploitation de la carte, masqué durant la phase de fabrication du produit,
- le logiciel d’application MONEO.

30 La configuration exacte de la cible d’évaluation est décrite en annexe B.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

31 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [8] qui est la référence pour l'évaluation.

32 Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Politique de sécurité

33 Le porte-monnaie électronique MONEO a vocation à être utilisé pour des paiements de petits montants. Lors d'un chargement du porte-monnaie électronique, l'émetteur de valeur électronique émet de la valeur électronique contre un paiement du porteur (transaction de chargement). Lors d'un paiement, le porte-monnaie électronique est débité de la valeur électronique correspondant au paiement (transaction d'achat). L'équipement d'acceptation du commerçant est crédité du montant correspondant. L'émetteur de valeur électronique la rachète ensuite au commerçant puis la détruit (transaction de remise). Le commerçant est crédité du montant correspondant. De plus, le système met en oeuvre une transaction dite de "réserve" qui s'apparente à une opération de chargement "off-line" pré-autorisée par l'émetteur de valeur électronique.

34 Le couple "porte-monnaie électronique et module de sécurité PSAM commerçant" s'incrit ainsi dans un circuit fermé de la valeur électronique appelé "ronde fermée de la valeur électronique" qui s'accompagne d'un circuit parallèle de flux financiers de sens inverse.

35 La politique de sécurité de la cible d'évaluation est fondée sur la conservation du flux de valeur électronique ainsi que sur l'authentification préalable des acteurs intervenant dans les différents échanges. Pour chaque type de transaction (chargement, achat, remise), la valeur électronique créditée doit toujours être égale à la valeur débitée. Dans ce modèle d'échanges, il ne doit pas y avoir de création ou de perte de valeur électronique ; seul l'émetteur de valeur électronique peut en créer ou en détruire.

36 Pour tout chargement, le porte-monnaie électronique doit s'être préalablement authentifié auprès du terminal de l'agent de chargement. Par ailleurs, le chargement du porte-monnaie électronique est limité à une valeur maximale.

37 Pour tout achat, le porte-monnaie électronique ainsi que l'équipement d'acceptation du commerçant à travers le module de sécurité doivent s'être préalablement authentifiés.

38 Pour toute remise, l'équipement d'acceptation du commerçant (module de sécurité) et l'équipement acquéreur doivent s'être préalablement authentifiés.

4.3 Menaces

39 Les menaces effectivement couvertes par le produit sont décrites dans le chapitre 3 de la cible de sécurité [8]. Elles sont reprises en annexe A.2.

4.4 Hypothèses d'utilisation et d'environnement

40 La cible d'évaluation doit être utilisée et administrée conformément aux exigences spécifiées dans la documentation d'utilisation et d'administration.

41 Les hypothèses d'utilisation et d'environnement du produit sont consignées dans le chapitre 3 de la cible de sécurité [8]. Celles-ci sont reprises en annexe A.

4.5 Architecture du produit

42 L'architecture du produit est normalement décrite dans les documents de conception générale et détaillée exigibles pour les composants d'assurance ADV_HLD et ADV_LLD.

43 Le niveau d'évaluation EAL1 considéré n'inclut pas l'évaluation de l'architecture du produit.

4.6 Description de la documentation

44 La documentation disponible pour l'évaluation est décrite en annexe B du présent rapport de certification.

4.7 Tests de la cible d'évaluation

45 Plusieurs types de tests ont été passés sur la carte porteur ainsi que sur le module de sécurité PSAM commerçant.

46 Les évaluateurs ont effectué un ensemble de tests sur le produit afin de vérifier par échantillonnage la conformité des fonctions de sécurité aux spécifications de sécurité. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL1.

47 De plus, dans le cadre du composant d'assurance AVA_VLA.2, les évaluateurs ont effectué de manière indépendante un ensemble de tests de pénétration sur le produit afin d'estimer l'efficacité des fonctions de sécurité offertes par le produit. Ces tests de pénétration sont adaptés à la nature du produit soumis à évaluation ainsi qu'à son environnement.

4.8 Configuration évaluée

48 La configuration exacte de la cible d’évaluation est décrite en annexe B.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

49 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [9].

5.2 Résultats de l'évaluation de la cible de sécurité

50 La cible de sécurité répond aux exigences de la classe ASE, telle que définie dans la partie 3 des critères communs [4].

5.2.1 ASE_DES Description de la TOE

51 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

52 La cible d'évaluation (TOE) est le couple "carte porteur porte-monnaie électronique ST19SF16BRCL (version B303) et module de sécurité PSAM commerçant ST19SF16B RCL (version C103)".

53 La description de la cible d'évaluation est précisée au chapitre 3 du présent rapport de certification.

5.2.2 ASE_ENV Environnement de sécurité

54 Les critères d'évaluation sont définis par les sections ASE_ENV.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

55 Les hypothèses d'utilisation et d'environnement du produit, les menaces auxquelles doit faire face le produit ainsi que les politiques de sécurité organisationnelles sont décrites dans la cible de sécurité [8]. Ces caractéristiques de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.3 ASE_INT Introduction de la ST

56 Les critères d'évaluation sont définis par les sections ASE_INT.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

57 L'introduction de la cible de sécurité [8] précise l'identification du produit et contient une vue d'ensemble de la cible de sécurité, ainsi qu'une annonce de conformité aux critères communs.

5.2.4 ASE_OBJ Objectifs de sécurité

58 Les critères d'évaluation sont définis par les sections ASE_OBJ.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

59 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrites dans la cible de sécurité [8]. Ces objectifs de sécurité sont repris en annexe A du présent rapport de certification.

5.2.5 ASE_PPC Annonce de conformité à un PP

60 Les critères d'évaluation sont définis par les sections ASE_PPC.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

61 L'évaluateur confirme l'annonce de conformité au profil de protection intitulé "Intersector Electronic Purse and Purchase Device (version for pilot schemes only)" référencé PP/9908 [6]. La cible de sécurité [8] constitue donc une instantiation correcte du profil de protection.

5.2.6 ASE_REQ Exigences de sécurité des TI

62 Les critères d'évaluation sont définis par les sections ASE_REQ.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

63 Les exigences de sécurité des TI fonctionnelles ou d'assurance sont décrites dans la cible de sécurité [8]. Ces exigences de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.7 ASE_SRE Exigences de sécurité des TI déclarées explicitement

64 Les critères d'évaluation sont définis par les sections ASE_SRE.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

65 La cible de sécurité [8] ne contient pas d'exigences de sécurité des TI déclarées explicitement et ne faisant donc pas référence à la partie 2 des critères communs [2].

5.2.8 ASE_TSS.1 Spécifications de haut niveau de la TOE

66 Les critères d'évaluation sont définis par les sections ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

67 La cible de sécurité [8] contient un résumé des spécifications des fonctions de sécurité du produit ainsi que les mesures d'assurance prises pour satisfaire les exigences d'assurance. L'évaluateur s'est assuré que ces fonctions de sécurité sont une représentation correcte des exigences fonctionnelles de sécurité et que les mesures d'assurance prises couvrent les exigences du niveau EAL1 augmenté.

5.3 Résultats de l'évaluation du produit

68 Le produit répond aux exigences des critères communs pour le niveau EAL1 augmenté du composant AVA_VLA.2 "Analyse de vulnérabilités effectuée de manière indépendante".

5.3.1 ADV_FSP.1 : Spécifications fonctionnelles informelles

69 Les critères d'évaluation sont définis par les sections ADV_FSP.1.iE de la classe ADV, telle que définie dans la partie 3 des critères communs [4].

70 Le développeur a fourni la documentation spécifiant les fonctions de sécurité du produit. Les interfaces externes sont également décrites.

71 L'évaluateur a examiné ces spécifications et montré pour le niveau considéré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

5.3.2 ADV_RCR.1 : Démonstration de correspondance informelle

72 Les critères d'évaluation sont définis par la section ADV_RCR.1.1E de la classe ADV, telle que spécifiée dans la partie 3 des critères communs [4].

73 Le développeur a fourni une documentation indiquant la correspondance entre les fonctions de sécurité telles qu'elles sont définies dans les spécifications (ADV_FSP) et la cible de sécurité (ASE_TSS).

74 Deux représentations des fonctions de sécurité ont donc été analysées par l'évaluateur ; celui-ci s'est assuré que les spécifications fonctionnelles (ADV_FSP) correspondent à une image complète et cohérente des fonctions de sécurité décrites dans la cible de sécurité [8] (ASE_TSS).

5.3.3 ACM_CAP.1 : Numéros de version

75 Les critères d'évaluation sont définis par la section ACM_CAP.1.1E de la classe ACM, telle que spécifiée dans la partie 3 des critères communs [4].

76 Le produit évalué porte la référence ST19SF16B RCL version B303 pour la carte porteur, et version C103 pour le module de sécurité PSAM commerçant, telle que définie dans l'annexe B du présent rapport.

77 L'évaluateur s'est également assuré de l'absence d'incohérence dans la documentation fournie.

5.3.4 ADO_IGS.1 : Procédures d'installation, de génération et de démarrage

78 Les critères d'évaluation sont définis par les sections ADO_IGS.1.iE de la classe ADO, telle que spécifiée dans la partie 3 des critères communs [4].

79 Les procédures d'installation, de génération et de démarrage du produit concernent principalement les phases de fabrication, d'encartage et de personnalisation du produit.

80 Elles définissent les exigences de sécurité que doivent satisfaire le fondeur, le masqueur, l'encarteur et le personnalisateur. En particulier, une procédure de livraison sûre du code exécutable à charger dans la mémoire EEPROM des composants a été définie.

81 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures conduisent à une configuration sûre du produit.

5.3.5 AGD_ADM.1 : Guide de l'administrateur

82 Les critères d'évaluation sont définis par la section AGD_ADM.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des critères communs [4].

83 L'administration du produit correspond à la phase de personnalisation de la carte porteur d'une part et du module de sécurité PSAM commerçant d'autre part. Les spécifications de personnalisation du produit ont été fournies.

84 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures permettent une administration sûre du produit.

5.3.6 AGD_USR.1 : Guide de l'utilisateur

85 Les critères d'évaluation sont définis par la section AGD_USR.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des critères communs [4].

86 La documentation utilisateur est constituée des spécifications d'interface du produit pour la carte porteur et le module de sécurité PSAM commerçant. Cette documentation s'accompagne également d'un ensemble de recommandations d'utilisation des fonctions de sécurité décrites dans les contrats d'exploitation du produit (contrat porteur et contrat commerçant). Une notice détaillée d'utilisation du produit à l'égard du porteur a également été fournie.

87 L'évaluateur s'est assuré que cette documentation correspondait à une utilisation sûre du produit.

5.3.7 ATE_IND.1 Tests effectués de manière indépendante - conformité

88 Les critères d'évaluation sont définis par les sections ATE_IND.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des critères communs [4].

89 Les évaluateurs ont effectué un ensemble de tests sur la carte porteur ainsi que sur le module de sécurité PSAM commerçant afin de vérifier par échantillonnage la conformité des fonctions de sécurité aux exigences fonctionnelles de sécurité.

90 Ces tests ont porté sur les logiciels embarqués et également sur le composant. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL1.

5.3.8 AVA_VLA.2 : Analyse de vulnérabilités effectuée de manière indépendante

91 Les critères d'évaluation sont définis par les sections AVA_VLA.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des critères communs [4].

92 L'évaluateur a réalisé des tests de pénétration de manière indépendante, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit (carte porteur et module de sécurité PSAM commerçant) résiste aux attaques correspondant à un potentiel de l'attaquant tel que défini par le composant AVA_VLA.2. Ces tests de pénétration ont porté sur les logiciels embarqués ainsi que sur le composant. Les attaques de nature évidente, incluant donc celles du domaine public, ont été également prises en compte dans cette analyse.

5.3.9 Verdicts

93 Pour tous les aspects des critères communs identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 6

Recommandations d’utilisation

94 Le produit “porte-monnaie électronique MONEO carte porteur ST19SF16B RCL (version B303) et module de sécurité PSAM commerçant ST19SF16B RCL (version C103)” est soumis aux recommandations d’utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

95 Le produit doit être utilisé conformément à l’environnement d’utilisation prévu dans la cible de sécurité [8].

96 Les processus d’encartage et de personnalisation sont des étapes critiques destinées à configurer le produit de manière sûre.

97 Les processus d’encartage et de personnalisation doivent être strictement définis et contrôlés ; des mesures de sécurité doivent être appliquées au cours de ces phases afin de pouvoir garantir l’intégrité et la confidentialité des biens à protéger du produit (codes et clés secrètes).

Chapitre 7

Certification

7.1 Objet

98 Le produit dont les caractéristiques de sécurité sont définies dans la cible de sécurité [8], satisfait aux exigences du niveau d'évaluation **EAL1 augmenté** du composant d'assurance **AVA_VLA.2** "Analyse de vulnérabilités effectuée de manière indépendante".

99 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL1 et **par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaques tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.**

7.2 Portée de la certification

100 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.

101 Le certificat ne s'applique qu'à la version évaluée du produit, telle qu'elle est définie en annexe B de ce rapport.

102 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Caractéristiques de sécurité

103 Les caractéritiques de sécurité évaluées sont décrites dans la cible de sécurité [8] qui est la référence pour l'évaluation.

104 La cible de sécurité étant rédigée en langue anglaise, les paragraphes ci-après sont une traduction française des politiques de sécurité organisationnelles, des hypothèses, des menaces ainsi que des objectifs et des exigences de sécurité.

A.1 Politiques de sécurité organisationnelles

OSP.DEB_BEF_CRED	Un débit précéde toujours un crédit lors d'une transaction.
OSP.AGGREG	Si l'équipement d'acceptation est capable de cumuler plusieurs montants de valeur électronique, le résultat global doit correspondre à une valeur équivalente à la somme de toutes les transactions individuelles.
OSP.PH_BEHAV	Le porte-monnaie électronique doit être traité de la même manière qu'un véritable porte-monnaie et ne doit pas être de ce fait prêté à des personnes non autorisées.
OSP.A_LA_TRUSTED	L'acquéreur et l'agent de chargement sont des agents autorisés par l'émetteur de valeur électronique.
OSP.EV_INDIC	Il doit exister un moyen pour indiquer au porteur le montant des transactions.
OSP.INTENT_TRANS	Chaque transaction électronique doit être une action intentionnelle du porteur. Une procédure doit être définie par le fournisseur du porte-monnaie électronique afin de permettre au porteur d'accepter ou de refuser les transactions.
OSP.IEP_ID	Le porte-monnaie électronique doit avoir une identification unique dans le système.
OSP.IEP_PD	L'équipement d'acceptation du commerçant doit avoir une identification unique pour l'acquéreur.
OSP.LINK_SP_PD	Le commerçant doit être associé à son équipement d'acceptation (son compte bancaire doit être crédité une seule fois par remise).
OSP.SP_A_CLT	Le commerçant ne peut être collecté que par sa banque acquéreur.
OSP.LOAD	Au cours d'un chargement, le porte-monnaie électronique est capable de cumuler plusieurs montants de valeur électronique, le résultat global doit être équivalent à la somme des montants individuels.
OSP.ROLE	La cible d'évaluation doit administrer des rôles de sécurité et ces rôles doivent être indépendants.

A.2 Menaces

A.2.1 Blanchiment d'argent

T.LAUND_MON	Blanchiment d'argent afin de cacher les sources réelles des transactions.

A.2.2 Usurpation d'identité

T.USP_LA_LD	Usurpation de l'identité de l'agent de chargement : chargement d'un porte-monnaie électronique avec de la fausse valeur électronique.
T.USP_IEP_LD	Usurpation de l'identité d'un porte-monnaie électronique : chargement de vraie valeur électronique dans un faux porte-monnaie.
T.USP_PP_EVP_PCH	Usurpation de l'identité du fournisseur de porte-monnaie ainsi que de l'émetteur de valeur électronique : paiement par un faux porte-monnaie électronique contenant de la fausse valeur électronique.
T.USP_PP_PCH_IEP	Usurpation de l'identité du fournisseur de porte-monnaie : paiement par un faux porte-monnaie électronique contenant de la vraie valeur électronique.
T.USP_PP_PCH_PD	Usurpation de l'identité du fournisseur de porte-monnaie : paiement par un porte-monnaie électronique contenant de la vraie valeur électronique avec un équipement d'acceptation frauduleux.
T.USP_PP_EVP_CLT	Usurpation de l'identité du fournisseur de porte-monnaie ainsi que de l'émetteur de valeur électronique : remise de fausse valeur électronique à l'acquéreur par un équipement d'acceptation frauduleux.
T.USP_A_CLT	Usurpation de l'identité de l'acquéreur : remise de valeur électronique dans un équipement acquéreur frauduleux.

A.2.3 Rejeu

T.RPLY_LD	Rejeu d'un chargement.
T.RPLY_PCH_C	Rejeu d'un paiement conduisant à une création de valeur électronique.
T.RPLY_PCH_L	Rejeu d'un paiement conduisant à une perte de valeur électronique.
T.RPLY_CLT	Rejeu d'une remise.

A.2.4 Défaillances

T.FAIL_PCH	Défaillances durant une transaction de paiement.
T.FAIL_CLT	Défaillances durant une transaction de remise.
T.FAIL_LD	Défaillances durant une transaction de chargement.

A.2.5 Contre-façon

T.FORG_LD_C	Contre-façon d'une transaction de chargement conduisant à une création de valeur électronique.
T.FORG_LD_L	Contre-façon d'une transaction de chargement conduisant à une perte de valeur électronique.
T.FORG_PCH_C	Contre-façon d'une transaction de paiement conduisant à une création de valeur électronique.
T.FORG_PCH_L	Contre-façon d'une transaction de paiement conduisant à une perte de valeur électronique.
T.FORG_CLT_C	Contre-façon d'une transaction de remise conduisant à une création de valeur électronique.
T.FORG_CLT_L	Contre-façon d'une transaction de remise conduisant à une perte de valeur électronique.

A.2.6 Répudiation

T.REP_LD	Répudiation illicite d'une transaction de chargement.
T.REP_PCH	Répudiation illicite d'une transaction de paiement par le porteur.
T.REP_CLT	Répudiation illicite d'une transaction de remise.
T.REP_PCH2	Répudiation illicite d'une transaction de paiement par le commerçant.

A.2.7 Perte d'intégrité

T.INTEG_EV	Modification non autorisée de valeur électronique.
T.INTEG_TD	Modification non autorisée des données de traçabilité.
T.INTEG_PARA1	Modification non autorisée des paramètres du porte-monnaie électronique.
T.INTEG_PARA2	Modification non autorisée des paramètres de l'équipement d'acceptation.

A.3 Hypothèses sur l'environnement

A.AD	L'équipement acquéreur préserve un état sûr lorqu'une erreur survient au cours d'une transaction de remise, ou en cas de transactions illicites.
A.LA	L'équipement de chargement préserve un état sûr lorqu'une erreur survient au cours d'une transaction de chargement, ou en cas de transactions illicites.
A. INDEP	Les fonctions de chargement et de paiement sont des applications indépendantes : un commerçant peut être également un agent de chargement mais dans ce cas l'application doit maintenir la séparation des deux domaines.

A.4 Objectifs pour la cible d'évaluation

O.EV	La TSF doit offrir les moyens pour éviter la création ou la perte de valeur électronique.
O.INTEG_DATA	La TSF doit offrir les moyens pour éviter la modification non autorisée des données de traçabilité ainsi que des paramètres du porte-monnaie électronique et de l'équipement d'acceptation.
O.LOGICAL	La TSF doit prévenir contre l'accès non autorisé à la cible d'évaluation et contre le contournement du modèle de flux de valeur électronique.
O.AUTH	La TSF doit assurer l'authentification de la cible d'évaluation vis-à-vis des équipements de chargement ou acquéreurs.
O.ACCESS	La TSF doit assurer le contrôle des données utilisateurs aux seuls utilisateurs autorisés.
O.OPERATE	La TSF doit assurer la continuité de la sécurité en cas de rupture de transactions.
O.REPLAY	La TSF doit assurer que les transactions illicites (rejeu) sont détectées et contrées.
O.TAMPER	La TSF doit se prémunir contre les attaques physiques.
O.RECORD	La TSF doit enregistrer les données de traçabilité.
O.LIMIT	Le montant de valeur électronique stockée dans le porte-monnaie électronique doit être limitée.
O.DOMAIN	La TSF doit maintenir une séparation des domaines entre l'application porte-monnaie électronique et d'autres applications.

A.5 Objectifs pour l'environnement

O.SYSTEM	L'émetteur de valeur électronique doit garantir la valeur électronique dans le système sur la base d'une politique de sécurité.
O.EV_DISTRIB	Les équipements de chargement et acquéreur ne doivent pas créer de valeur électronique.
O.LA_FAIL	L'équipement de chargement doit préserver un état sûr en cas d'erreurs de transactions, ou de transactions illicites.
O.LA_DOMAIN	Un domaine de sécurité propre doit être mis en place pour l'équipement de chargement.
O.LA_RECORD	L'équipement de chargement doit enregistrer les événements de sécurité nécessaires à l'exploitation du système.
O.AUTH2	Les équipements de chargement et acquéreurs doivent mettre en place une politique d'authentification de leurs utilisateurs.
O.PSEUDO	Au cours d'un chargement, l'équipement de chargement doit maintenir une séparation des domaines entre d'une part la transaction de débit et d'autre part la transaction de chargement du porte-monnaie électronique.
O. INSTALL	Le fournisseur de porte-monnaie électronique doit s'assurer que la cible d'évaluation est livrée et installée de manière sûre.
O. MANAGE	Le fournisseur de porte-monnaie électronique doit s'assurer que la cible d'évaluation est administrée de manière sûre.
O.ACQ	L'équipement acquéreur doit préserver un état sûr en cas d'erreurs de transactions, ou de transactions illicites.
O.A_RECORD	L'équipement acquéreur doit enregistrer les événements de sécurité nécessaires à l'exploitation du système.

A.6 Exigences fonctionnelles de sécurité

Audit de Sécurité	FAU_GEN.1	Génération de données d'audit.
	FAU_SAR.1	Revue d'audit.
	FAU_STG.1	Stockage protégé de traces d'audit.
Communication	FCO_NRO.2	Preuve systématique de l'origine.
	FCO_NRR.2	Preuve systématique de la réception.
Cryptographie	FCS_COP.1	Opération cryptographique.
Protection des données utilisateur	FDP_ACC.2	Contrôle d'accès complet.
	FDP_ACF.1	Contrôle d'accès basé sur les attributs de sécurité.
	FDP_DAU.1	Authentification de données élémentaire.
	FDP_ETC.1	Exportation de données de l'utilisateur sans attributs.
	FDP_IFC.1	Contrôle de flux d'information partiel.
	FDP_IFF.1	Attributs de sécurité simple.
	FDP_ITC.1	Importation de données de l'utilisateur sans attributs.
	FDP_SDI.1	Contrôle de l'intégrité des données stockées.
Identification et authentification	FIA_UID.1	Timing de l'identification.
	FIA_UAU.1	Timing de l'authentification.
	FIA_UAU.3	Authenfication infalsifiable.
	FIA_UAU.4	Mécanismes d'authentification.
	FIA_UAU.6	Réauthentification.
Protection des fonctions de sécurité	FPT_FLS.1	Défaillance avec préservation d'un état sûr.
	FPT_PHP.2	Notification d'une attaque physique.
	FPT_PHP.3	Résistance à une attaque physique.
	FPT_RCV.4	Reprise de fonction.
	FPT_RPL.1	Détection de rejeu.
	FPT_RVM.1	Capacité de la TSP à ne pas être court-circuitée.
	FPT_SEP.1	Séparation des domaines de la TSF.

A.7 Exigences d'assurance

Cible de sécurité	ASE	Évaluation de la cible de sécurité.
EAL1	ACM_CAP.1	Numéros de version.
	ADO_IGS.1	Procédures d'installation, de génération et de démarrage.
	ADV_FSP.1	Spécifications fonctionnelles informelles.
	ADV_RCR.1	Démonstration de correspondance informelle.
	AGD_ADM.1	Guide de l'administrateur.
	AGD_USR.1	Guide de l'utilisateur.
	ATE_IND.1	Tests effectués de manière indépendante - conformité.
Augmentation	AVA_VLA.2	Analyse de vulnérabilités effectuée de manière indépendante.

Annexe B

Configuration de la cible d'évaluation

105 La cible d'évaluation est constituée des microcircuits destinés à être insérés respectivement dans la carte porteur et le module de sécurité PSAM commerçant du système de porte-monnaie électronique MONEO.

106 Elle est référencée de la manière suivante :

Cible d'évaluation	Composant	Version de masque ROM logiciel	Version d'application MONEO
Carte porteur	ST19SF16B RCL	V2.5	B303[a]
Module de sécurité PSAM commerçant	ST19SF16B RCL	V2.5	C103[b]

a. Cette configuration comprend la personnalisation du produit en carte mixte incluant l'application moneo et l'application bancaire B0' (hors évaluation dans le cadre de ce certificat).
b. Cette configuration comprend la personnalisation du produit conforme aux spécifications de module de sécurité PSAM commerçant.

107 La documentation disponible pour le produit est la suivante :

- Documentation d'administration du produit : Procedures of mask configuration version 1.10,
- Documentation d'utilisation du produit : DSI version 1.5, documents d'exploitation (contrats porteur, notice d'utilisation).

Annexe C

Glossaire

C.1 Abréviations

CC	(Common Criteria) - Critères Communs, l'intitulé utilisé historiquement pour la présente norme à la place de l'intitulé officiel de l'ISO 15408: "Critères d'évaluation de la sécurité des technologies de l'information"
EAL	(Evaluation Assurance Level) - Niveau d'assurance de l'évaluation
PP	(Protection Profile) - Profil de protection
SF	(Security Function) - Fonction de sécurité
SFP	(Security Function Policy) - Politique d'une fonction de sécurité
ST	(Security Target) - Cible de sécurité
TI	(IT : Information Technology) - Technologie de l'Information
TOE	(Target of Evaluation) - Cible d'évaluation
TSF	(TOE Security Functions) - Ensemble des fonctions de sécurité de la TOE

C.2 Glossaire

Acquéreur	Agent autorisé de l'émetteur de valeur électronique qui est responsable de la collecte de valeur électronique auprès des équipements d'acceptation des commerçants.
Affectation	La spécification d'un paramètre identifié dans un composant.
Agent de chargement	Agent autorisé de l'émetteur de valeur électronique qui est responsable du chargement des porte-monnaie électroniques par de la valeur électronique créée préalablement par l'émetteur de valeur électronique.
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 les contre-mesures d'une TOE.
Cible d'évaluation (TOE)	Un produit ou un système TI et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité (ST)	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Classe	Un groupement de familles qui partagent un thème commun.
Composant	Le plus petit ensemble sélectionnable d'éléments qui peut être inclus dans un PP, une ST ou un paquet.
Émetteur de valeur électronique	L'émetteur de valeur électronique garantit la valeur électronique dans le système. Dans ce but, l'émetteur de valeur électronique crée la valeur électronique et la diffuse en échange de fonds, la collecte et la détruit en retour.
Équipement acquéreur	Afin de pouvoir collecter l'ensemble des transactions de valeur électronique, l'acquéreur dispose d'un ou plusieurs équipements acquéreurs.

Équipement d'acceptation	Équipement physiquement installé chez le commerçant utilisé pour accepter les paiements lors d'une transaction de paiement par porte-monnaie électronique. Dans le cadre de la cible d'évaluation, cet équipement contient un module de sécurité PSAM.
Évaluation	Estimation d'un PP, d'une ST ou d'une TOE par rapport à des critères définis.
Fournisseur du porte-monnaie électronique	Le fournisseur de porte-monnaie électronique est responsable de la sécurité du système de porte-monnaie (ici la SEME). Il est également responsable de l'administration des porte-monnaie électroniques et des équipements d'acceptation.
Fonction de sécurité	Une partie ou des parties de la TOE sur lesquelles on s'appuie pour appliquer un sous-ensemble étroitement imbriqué de règles tirées de la TSP.
Informel	Qui est exprimé à l'aide d'un langage naturel.
Itération	L'utilisation multiple d'un composant avec des opérations différentes.
MONEO	Nom du porte-monnaie électronique émis par les banques membres de la SEME.
Niveau d'assurance de l'évaluation	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.
Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Produit	Un ensemble de logiciels, microprogrammes ou matériels TI 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 TOE, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

PSAM	Module sécuritaire contenu dans la carte installée à l'intérieur des équipements d'acceptation des commerçants.
Raffinement	L'addition de détails à un composant.
Sélection	La spécification d'une ou de plusieurs entités à partir d'une liste au sein d'un composant.
Utilisateur	Toute entité (utilisateur humain ou entité TI externe) hors de la TOE qui interagit avec elle.
Valeur électronique	Contre-partie des fonds reçus par l'émetteur de valeur électronique ; elle est définie par l'identité de l'émetteur de valeur électronique, le montant et la devise.

Annexe D

Références

[1] [CC-1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIB-98-026, version 2.0 May 1998.

[2] [CC-2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIB-98-027, version 2.0 May 1998.

[3] [CC-2B] Common Criteria for Information Technology Security Evaluation Part 2 annexes CCIB-98-027A, version 2.0 May 1998.

[4] [CC-3] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIB-98-028, version 2.0 May 1998.

[5] [CEM] Common Methodology for Information Technology Security Evaluation CEM-99/008 version 0.6.

[6] Profil de protection PP/9908, Intersector Electronic Purse and Purchase Device, version for pilots scheme only, version 1.2 février 1999.

[7] Certificat PP/9908, avril 1999.

[8] Cible de sécurité “MONEO Security Target Part 1/2 Electronic purse and SAM” référencée PMEIGK/ADM/SEME/MDS-6P version 2.0, septembre 1999.

[9] Rapport technique d’évaluation, FT.CNET.3C.GLM.RE001, document non public.