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 2001/05

Carte mixte MONEO/CB :

application porte-monnaie électronique MONEO et application bancaire B4/B0' V3 (référence ST19SF16CC/RCQ version B312/B023)

et Module de sécurité SAM commerçant

(référence ST19SF16CC/RCQ version C112)

Avril 2001

Ce document constitue le rapport de certification du produit “Carte mixte MONEO/CB : application porte-monnaie électronique MONEO et application bancaire B4/B0’ V3 (référence ST19SF16CC/RCQ version B312/B023) et Module de sécurité SAM commerçant (référence ST19SF16CC/RCQ version C112)”.

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
DCSSI
Centre de Certification de la Sécurité des Technologies de l’Information
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: certification.dcssi@sgdn.pm.gouv.fr

Ce document est folioté de 1 à 30 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

CERTIFICAT 2001/05

Carte mixte MONEO/CB :

application porte-monnaie électronique MONEO et application bancaire B4/B0' V3 (référence ST19SF16CC/RCQ version B312/B023)

et Module de sécurité SAM commerçant

(référence ST19SF16CC/RCQ version C112)

Développeurs : IBM, STMicroelectronics SA

EAL4 augmenté

Commanditaire : BMS

Le 27 avril 2001,

Le Commanditaire :
Le Directeur de BMS
Pierre FERSZTAND

L'Organisme de certification :
Le Directeur chargé 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 Latour-Maubourg
75700 PARIS 07 SP.

IT Security Certified

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Carte mixte MONEO/CB : application porte-monnaie électronique MONEO et application bancaire B4/B0’ V3 (référence ST19SF16CC/RCQ version B312/B023) et Module de sécurité SAM commerçant (référence ST19SF16CC/RCQ version C112)”. La cible d’évaluation est donc constituée du composant ST19SF16CC masqué par le logiciel IBM version 2.6.

2 Le niveau d’assurance atteint est le niveau EAL4 augmenté des composants d’assurance ADV_IMP.2 “Implémentation de la TSF”, ALC_DVS.2 “Caractère suffisant des mesures de sécurité” et AVA_VLA.4 “Résistance élevée” tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

3 Ce produit est conforme aux profils de protection “Smartcard Integrated Circuit” et “Smartcard Integrated Circuit with Embedded Software” enregistrés auprès de la DCSSI dans le catalogue des profils de protection certifiés respectivement sous les références PP/9806 [7] et PP/9911 [8].

4 De plus, ce produit est basé sur le profil de protection "Intersector Electronic Purse and Purchase Device" enregistré auprès de la DCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9909 [9]. Il ne peut cependant pas s’y réclamer conforme car il n’implémente pas, entre autres, les fonctionnalités d’annulation de la dernière transaction et de mise à jour des paramètres du porte-monnaie électronique.

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

5 L'évaluation a été menée conformément aux Critères Communs ([1] à [3]) et à la méthodologie définie dans le manuel CEM [4].

6 Elle s'est déroulée consécutivement au développement du produit de février 2000 à février 2001.

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

- IBM pour le développement du masque (ci-après le "masqueur")

  IBM Deutschland Entwicklung GmbH
  Schönaicher Str. 220
  D-71032 Böblingen,

- STMicroelectronics SA pour le développement et la fabrication du microcircuit (ci-après le "fondeur")

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

8 Le commanditaire de l'évaluation est la société Billettique Monétique Services (BMS) :

- BMS
  25, rue de Ponthieu
  F-75008 Paris.

9 Le GIE Cartes Bancaires "CB" et la Société Financière du Porte-Monnaie Electronique Interbancaire (SFPMEI) ont également participé à cette évaluation en tant qu'observateurs :

- GIE Cartes Bancaires "CB"
  31, rue de Berri
  F-75008 Paris,

- SFPMEI
  4, avenue Bertie Albrecht
  F-75008 Paris.

10 L'évaluation a été conduite par les centres d'évaluation de la sécurité des technologies de l'information (ci-après "CESTI") :

- CEA/LETI pour l'évaluation des applications et la réalisation des travaux de composition

  CEA/LETI
  17, rue des Martyrs
  F-38054 Grenoble Cedex 9,

- SERMA Technologies pour l'évaluation du microcircuit électronique

  SERMA Technologies
  30, avenue Gustave Eiffel
  F-33608 Pessac Cedex.

11 Le présent rapport de certification se focalise sur les travaux d'évaluation réalisés par le CESTI du CEA/LETI (ci-après l'"évaluateur"). En effet, les résultats de l'évaluation du microcircuit par le CESTI de SERMA Technologies sont traités dans le rapport de certification 2001/04 [10] et ne sont pas repris dans le présent rapport.

2.2 Description de la cible d'évaluation

12 La cible d'évaluation est le produit "Carte mixte MONEO/CB : application porte-monnaie électronique MONEO et application bancaire B4/B0' V3 (référence ST19SF16CC/RCQ version B312/B023) et Module de sécurité SAM commerçant (référence ST19SF16CC/RCQ version C112)".

13 Ce produit est conforme aux profils de protection "Smartcard Integrated Circuit" et "Smartcard Integrated Circuit with Embedded Software" enregistrés auprès de la DCSSI dans le catalogue des profils de protection certifiés respectivement sous les références PP/9806 [7] et PP/9911 [8].

14 De plus, ce produit est basé sur le profil de protection "Intersector Electronic Purse and Purchase Device" enregistré auprès de la DCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9909 [9]. Il ne peut cependant pas s'y réclamer conforme car il n'implémente pas les fonctionnalités d'annulation de la dernière transaction et de mise à jour des paramètres du porte-monnaie électronique.

15 Le détail des fonctions de sécurité évaluées est disponible dans la cible de sécurité [5].

16 Pour l'application MONEO, elles se résument comme suit :

- authentification de la carte mixte MONEO/CB et du module de sécurité commerçant,
- authentification des acteurs,

- contrôle d'accès,
- 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.

17 Pour l'application B4/B0' V3, elles se résument comme suit :

- intégrité des informations de la mémoire,
- authentification des utilisateurs et des administrateurs du produit,
- contrôle d'accès (zones mémoire),
- irréversibilité des phases,
- imputabilité et audit (identité du blocage carte, identité de l'écriture d'un mot).
- protection des fonctions de sécurité : résistance aux attaques physiques, préservation d'état sûr, séparation de domaines.

2.3 Conclusions de l'évaluation

18 Le produit soumis à évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et AVA_VLA.4 "Résistance élevée" tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

19 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL4 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

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 la Carte mixte MONEO/CB : application porte-monnaie électronique MONEO et application bancaire B4/B0' V3 (référence ST19SF16CC/RCQ version B312/B023) et le Module de sécurité SAM commerçant (référence ST19SF16CC/RCQ version C112).

22 La carte mixte MONEO/CB est une carte porteur de format carte de crédit. Le microcircuit contient le système d'exploitation de la carte ainsi que l'application porte-monnaie électronique MONEO en configuration B312 et l'application bancaire B4/B0' V3 en configuration B023 conforme aux spécifications du GIE Cartes Bancaires "CB".

23 Le module de sécurité SAM commerçant est destiné 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. Le microcircuit électronique contient le système d'exploitation du module de sécurité ainsi que l'application porte-monnaie électronique MONEO en configuration C112.

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. L'application porte-monnaie électronique MONEO s'appuie sur les spécifications du système Geldkarte allemand. Les spécificités du système français ont été définies par BMS. L'application bancaire B4/B0' V3 s'appuie sur les spécifications du GIE Cartes Bancaires "CB".

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

3.3 Description du matériel

27 Le microcircuit électronique ST19SF16 est un microcontrôleur de la famille des composants ST19SFxx. 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 16 Koctets (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 du logiciel IBM version 2.6 développé par IBM Deutschland GmbH qui comprend les éléments suivants :

- un système d'exploitation,
- deux applications, MONEO et B4/B0' V3 ; pour le module de sécurité commerçant, l'application B0' est également présente mais inutilisable.

30 Le système d'exploitation et les applications sont masqués en ROM pendant la phase de fabrication du circuit intégré. La mémoire EEPROM contient les données applicatives.

31 La mémoire EEPROM peut également comprendre des données de fidélisation pour une éventuelle mise en œuvre de ce type d'application (ces données sont uniquement présentes dans la carte mixte MONEO/CB).

3.5 Description de la documentation

32 La documentation d'exploitation de la cible d'évaluation est la suivante :

- guide d'administration pour l'application MONEO [11] et pour l'application B4/B0' V3 [12] ;
- guide d'utilisation pour l'application MONEO [13] et pour l'application B4/B0' V3 [14].

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

33 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [5] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Hypothèses

34 La cible d'évaluation doit être utilisée dans un environnement qui satisfait aux hypothèses énoncées dans les profils de protection [8] et [9], et à une hypothèse complémentaire spécifique à l'application B4/B0' V3.

35 Les hypothèses énoncées dans le profil de protection [8] couvrent les aspects suivants :

- livraison de la cible d'évaluation entre les différentes étapes de son cycle de vie,
- utilisation de la cible d'évaluation pendant les phases de production (phases d'encartage et de personnalisation),
- protection des données sensibles de la cible d'évaluation échangées avec les équipements avec lesquels elle dialogue (terminaux, …).

36 Les hypothèses énoncées dans le profil de protection [9] couvrent les aspects suivants :

- capacité pour les équipements avec lesquels la cible d'évaluation dialogue d'entrer dans un état sûr lorsqu'une anomalie se produit pendant une transaction,
- indépendance des fonctionnalités de chargement et de paiement lorsque qu'un même équipement met en œuvre ces deux fonctionnalités.

37 L'hypothèse complémentaire énoncée dans la cible de sécurité [5] et spécifique à l'application B4/B0' V3 couvre l'aspect suivant :

- capacité pour les équipements avec lesquels la cible d'évaluation dialogue d'entrer dans un état sûr lorsqu'une anomalie se produit pendant une transaction.

38 Le détail de ces hypothèses est disponible dans les profils de protection [8] et [9] et dans la cible de sécurité [5].

4.3 Menaces

39 Les menaces couvertes par la cible d'évaluation ou par son environnement sont celles définies par les profils de protection [8] et [9]. Des menaces spécifiques à l'application B4/B0' V3 ont été introduites dans la cible de sécurité [5].

40 Les biens à protéger sont les spécifications, la conception, les outils de développement et la technologie des logiciels, les logiciels embarqués ainsi que les données applicatives de la carte ou du module de sécurité.

41 Les principales menaces portent sur :

- la divulgation et la modification non autorisées des biens de la cible d'évaluation,
- le blanchiment d'argent,
- l'usurpation d'identité de l'un des acteurs du système,
- la création frauduleuse de valeur électronique,
- la perte de valeur électronique.

42 Le détail de ces menaces est disponible dans les profils de protection [8] et [9] et dans la cible de sécurité [5].

4.4 Politiques de sécurité organisationnelles

43 Le profil de protection [8] ne définit pas de politique de sécurité organisationnelle. Le profil de protection [9] définit des politiques pour l'application MONEO et des politiques de sécurité complémentaires spécifiques à l'application B4/B0' V3 sont définies dans la cible de sécurité [5].

44 Les politiques de sécurité organisationnelles expriment essentiellement des contraintes sur le mode d'exploitation du système porte-monnaie électronique et du système bancaire français.

45 Le détail de ces politiques de sécurité organisationnelles est disponible dans le profil de protection [9] et dans la cible de sécurité [5].

4.5 Fonctions de sécurité évaluées

46 Les fonctions de sécurité évaluées sont décrites ci-dessous. Le détail de ces fonctions est disponible dans la cible de sécurité [5].

47 Ces fonctions sont découpées en deux catégories : les fonctions liées à l'application MONEO d'une part et les fonctions liées à l'application B4/B0' V3 d'autre part.

4.5.1 Fonctions liées à l'application MONEO

48 Les fonctions liées à l'application MONEO sont les suivantes :

- authentification du module de sécurité commerçant par la carte mixte MONEO/CB,
- authentification de la carte mixte MONEO/CB par le module de sécurité commerçant,
- authentification de la carte mixte MONEO/CB par l'équipement de chargement,
- authentification du module de sécurité commerçant par l'équipement de collecte,
- authentification du porteur de la carte mixte MONEO/CB lors d'une opération de chargement rapide,
- intégrité des données collectées,
- audit des transactions (paiement et chargement),
- limitation du montant des transactions (chargement, paiement, chargement rapide) et du nombre de transactions (chargement rapide),
- accès libre en lecture pour le porteur du montant de valeur électronique contenu dans la carte mixte MONEO/CB,
- activation ou désactivation libre de l'application MONEO de la carte mixte MONEO/CB par le porteur,
- protection contre le rejeu : une transaction doit faire intervenir au moins une donnée d'authentification différente par rapport aux transactions précédentes,
- contrôle d'accès aux données utilisateurs,
- retour à un état sûr en cas d'interruption d'une transaction,
- notification et réaction en cas de détection de fonctionnement anormal de l'application MONEO ou d'attaques physiques.

4.5.2 Fonctions liées à l'application B4/B0' V3

49 Les fonctions liées à l'application B4/B0' V3 sont les suivantes :

- intégrité des données contenues dans les différentes mémoires du microcircuit,
- authentification des différents utilisateurs de la carte mixte MONEO/CB (encarteur, personnalisateur, émetteur et porteur),
- authentification de l'application B4/B0' V3,
- certification des transactions,
- inhibition du mode test et irréversibilité des phases de vie,
- cloisonnement des zones mémoires et contrôle d'accès aux mémoires (en phase d'utilisation, en cas de blocage ou d'invalidation de l'application B4/ B0' V3),
- imputabilité et audit des opérations sur la carte,
- notification et réaction en cas de fonctionnement anormal de l'application B4/B0' V3 ou d'attaques physiques,
- réinitialisation globale des ressources de l'application au démarrage d'une session et réinitialisation partielle des ressources entre deux opérations d'une même session.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

50 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [6] produit par le CESTI du CEA/LETI.

51 Les résultats de l'évaluation du microcircuit par le CESTI de SERMA Technologies sont traités dans le rapport de certification 2001/04 [10] et ne sont pas repris dans le présent rapport.

5.2 Principaux résultats de l'évaluation

52 Le produit répond aux exigences des Critères Communs pour le niveau EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et AVA_VLA.4 "Résistance élevée" tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

5.2.1 ASE : Evaluation de la cible de sécurité

53 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE, ASE_ENV.1.iE, ASE_INT.1.iE, ASE_OBJ.1.iE, ASE_PPC.1.iE, ASE_REQ.1.iE, ASE_SRE.1.iE et ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des Critères Communs [3].

54 La cible d'évaluation est la Carte mixte MONEO/CB : application porte-monnaie électronique MONEO et application bancaire B4/B0' V3 (référence ST19SF16CC/ RCQ version B312/B023) et le Module de sécurité SAM commerçant (référence ST19SF16CC/RCQ version C112).

55 Les travaux d'évaluation de la cible de sécurité ont pu être facilités du fait de sa conformité à des profils de protection [8] et [9] certifiés.

5.2.2 ACM_AUT.1 : Automatisation partielle de la gestion de configuration

56 Les critères d'évaluation sont définis par la section ACM_AUT.1.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

57 Le masqueur a fourni la documentation du système de gestion de configuration utilisé pour le développement du logiciel.

58 Le système est fondé sur une gestion automatique de la configuration à travers un outil de gestion de configuration permettant de s'assurer que seuls les changements autorisés sur le produit sont possibles.

59 L'évaluateur a analysé la documentation et vérifié au cours de l'audit du site de développement l'utilisation effective de l'outil de gestion de configuration, en accord avec les procédures décrites.

5.2.3 ACM_CAP.4 : Aide à la génération et procédures de réception

60 Les critères d'évaluation sont définis par la section ACM_CAP.4.iE de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

61 Le masqueur a fourni la documentation du système de gestion de configuration.

62 Ce système impose un contrôle des objets produits au cours du développement chez le masqueur. Des procédures permettent de prendre en compte dans le système de gestion de configuration les objets composant la cible d'évaluation (procédure de réception).

63 L'évaluateur a vérifié au cours de l'audit du site de développement que les procédures décrites étaient effectivement appliquées.

5.2.4 ACM_SCP.2 : Couverture du suivi des problèmes par la gestion de configuration

64 Les critères d'évaluation sont définis par la section ACM_SCP.2.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

65 Le système de gestion de configuration appliquée par le masqueur couvre la cible d'évaluation ainsi que l'ensemble de sa documentation (documentation de conception et éléments de réalisation, documentation de test, documentation d'utilisation et d'administration, outils de développement) ; il couvre également toute erreur de sécurité du produit qui pourrait être découverte.

5.2.5 ADO_DEL.2 : Détection de modifications

66 Les critères d'évaluation sont définis par la section ADO_DEL.2.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [3].

67 Le masqueur a fourni les procédures de livraison de la cible d'évaluation au fondeur et des tables d'initialisation au commanditaire. Ces procédures ont été vérifiées au cours de l'audit du site de développement.

68 Dans le cadre des travaux de composition et conformément à une recommandation exprimée dans le rapport de certification du microcircuit, l'évaluateur a réalisé un audit partiel du site d'encartage de Oberthur à Vitré afin de vérifier que les mesures de sécurité mises en œuvre garantissent l'intégrité et la confidentialité de la cible d'évaluation tant que celle-ci est en mode ISSUER.

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

69 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 [3].

70 Les procédures d'installation, de génération et de démarrage pour ce type de cible d'évaluation se limitent à la procédure de mise sous tension.

71 L'évaluateur a vérifié que l'ATR renvoyé par la carte à la mise sous tension était conforme à l'ATR décrit dans la documentation fournie par le masqueur, et ce pour chacune des configurations de la cible d'évaluation (carte mixte MONEO/CB et module de sécurité commerçant).

5.2.7 ADV_FSP.2 : Définition exhaustive des interfaces externes

72 Les critères d'évaluation sont définis par les sections ADV_FSP.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

73 Le masqueur a fourni la documentation spécifiant les fonctions de sécurité du produit et leurs interfaces externes.

74 L'évaluateur a examiné ces spécifications et montré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

5.2.8 ADV_HLD.2 : Conception de haut niveau - identification des sous-systèmes dédiés à la sécurité

75 Les critères d'évaluation sont définis par les sections ADV_HLD.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

76 Le masqueur a fourni la conception de haut niveau de la cible d'évaluation.

77 Cette conception présente la structure générale du produit en terme de sept sous-systèmes. L'évaluateur s'est assuré que cette conception de haut niveau est une instanciation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

5.2.9 ADV_IMP.2 : Implémentation de la TSF

78 Les critères d'évaluation sont définis par les sections ADV_IMP.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

79 Le masqueur a fourni l'intégralité du code source de la cible d'évaluation.

80 L'évaluateur s'est assuré que le code source est une instanciation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

81 De plus, l'évaluateur a vérifié que les exigences définies dans le guide d'utilisation du composant fourni par le fondeur [15] sont prises en compte lors du

développement du logiciel. Dans le cas de non respect de certaines exigences, l'évaluateur s'est assuré de l'absence de vulnérabilités exploitables.

5.2.10 ADV_LLD.1 : Conception de bas niveau descriptive

82 Les critères d'évaluation sont définis par les sections ADV_LLD.1.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

83 Le masqueur a fourni la conception de bas niveau de la cible d'évaluation.

84 Cette conception décompose chaque sous-système en modules. Ces modules ainsi que leurs interfaces sont décrits. L'évaluateur s'est assuré que cette conception de bas niveau est une instanciation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

5.2.11 ADV_RCR.1 : Démonstration de correspondance informelle

85 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 [3].

86 Le masqueur a fourni une documentation qui indique les correspondances entre les différents niveaux de représentation des fonctions de sécurité de la cible d'évaluation.

87 L'évaluateur a donc pu s'assurer que les exigences de sécurité fonctionnelles exprimées dans la cible de sécurité sont correctement et complètement implémentées à travers les spécifications fonctionnelles, la conception de haut niveau, la conception de bas niveau et l'implémentation de la cible d'évaluation.

5.2.12 ADV_SPM.1 : Modèle informel de politique de sécurité de la TOE

88 Les critères d'évaluation sont définis par les sections ADV_SPM.1.1E de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

89 Le masqueur a fourni un modèle informel de politique de sécurité de la cible d'évaluation. Les politiques suivantes sont couvertes par le modèle :

- la politique de contrôle d'accès aux fichiers ;
- la politique de contrôle de flux lors des transactions (application MONEO uniquement).

90 L'évaluateur a examiné ce modèle. Il a montré qu'il fournit une description claire et homogène des règles et caractéristiques des politiques de sécurité, que cette description correspond à la description des fonctions de sécurité dans les spécifications fonctionnelles.

5.2.13 AGD_ADM.1 : Guide de l'administrateur

91 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 [3].

92 Le masqueur a fourni la documentation d'administration des fonctions de sécurité du produit [11] et [12]. Ces guides d'administration sont à l'usage des encarteurs et personnalisateurs (y compris les émetteurs de cartes).

93 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.

5.2.14 AGD_USR.1 : Guide de l'utilisateur

94 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 [3].

95 BMS a fourni la documentation d'utilisation des fonctions de sécurité du produit pour l'application MONEO [13] et le GIE Cartes Bancaires "CB" a fourni la documentation d'utilisation des fonctions de sécurité du produit pour l'application B4/B0' V3 [14].

96 Le guide d'utilisation pour l'application MONEO [13] concerne le porteur pour la carte mixte MONEO/CB et le commerçant pour le module de sécurité, ainsi que les terminaux avec lesquels la cible d'évaluation dialogue.

97 Le guide d'utilisation pour l'application B4/B0' V3 [14] concerne les porteurs de la carte mixte MONEO/CB et l'émetteur de la carte.

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

5.2.15 ALC_DVS.2 : Caractère suffisant des mesures de sécurité

99 Les critères d'évaluation sont définis par la section ALC_DVS.2.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

100 L'évaluateur a analysé la sécurité des locaux dans lesquels a eu lieu le développement de la cible d'évaluation. Ces locaux, qui appartiennent à IBM, sont situés dans une zone sécurisée dédiée du laboratoire IBM à Böblingen en Allemagne.

101 Des procédures physiques, organisationnelles, techniques, liées au personnel assurent la protection en intégrité et en confidentialité de la cible d'évaluation, de ses constituants ainsi que de sa documentation. Un audit du site de Böblingen a permis de vérifier l'application de ces procédures.

102 L'évaluateur a également analysé la sécurité des locaux du commanditaire s'attachant à vérifier que des procédures adéquates sont mises en œuvre afin de garantir l'intégrité, la confidentialité et la traçabilité des informations sensibles liées à la cible d'évaluation que BMS héberge.

5.2.16 ALC_LCD.1 : Modèle de cycle de vie défini par le développeur

103 Les critères d'évaluation sont définis par la section ALC_LCD.1.1E de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

104 Le masqueur n'a pas fourni de modèle de cycle de vie de la cible d'évaluation, cependant l'ensemble de la documentation produite dans le cadre de l'évaluation a permis de caractériser un modèle de développement mis en œuvre par IBM.

105 L'évaluateur s'est assuré que les mesures mises en œuvre sont adéquates et que les phases de développement et de maintenance de la cible d'évaluation sont correctement gérées.

5.2.17 ALC_TAT.1 : Outils de développement bien définis

106 Les critères d'évaluation sont définis par la section ALC_TAT.1.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

107 Le masqueur a fourni la documentation relative aux outils de développement de la cible d'évaluation. Le développement de la cible d'évaluation est réalisé à l'aide d'un logiciel commercial (2500 AD Software Inc).

108 Le logiciel est masqué sur un composant issu de la famille ST19SFxx, le masqueur a donc utilisé le manuel de programmation fourni par le fondeur, qui décrit le jeu d'instructions du composant ainsi que les différents modes d'adressage.

109 L'évaluateur a vérifié que les outils de développement utilisés sont bien définis.

5.2.18 ATE_COV.2 : Analyse de la couverture

110 Les critères d'évaluation sont définis par la section ATE_COV.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

111 Le masqueur a fourni une analyse de la documentation de test justifiant la couverture de la spécification des fonctions de sécurité par des tests.

112 L'évaluateur a vérifié que pour chaque aspect des fonctions de sécurité, le masqueur a défini au minimum un test.

5.2.19 ATE_DPT.1 : Tests : conception de haut niveau

113 Les critères d'évaluation sont définis par la section ATE_DPT.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

114 Le masqueur a fourni une analyse de la documentation de test justifiant la réalisation de tests fonctionnels pour les sous-systèmes identifiés dans la conception de haut niveau de la cible d'évaluation.

115 L'évaluateur a examiné cette documentation et s'est assuré de sa cohérence.

5.2.20 ATE_FUN.1 : Tests fonctionnels

116 Les critères d'évaluation sont définis par la section ATE_FUN.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

117 Le masqueur a fourni une documentation de test détaillée pour chacun des tests ; cette documentation décrit le plan des tests, l'objectif des tests, les procédures de tests à réaliser ainsi que les résultats des tests.

118 L'évaluateur s'est assuré de la complétude de cette documentation.

5.2.21 ATE_IND.2 : Tests indépendants - échantillonnage

119 Les critères d'évaluation sont définis par les sections ATE_IND.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

120 L'évaluateur a effectué un ensemble de tests sur la cible d'évaluation. Il a procédé à un échantillonnage des programmes de test du masqueur. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL4.

121 Des tests complémentaires ont également été effectués par l'évaluateur pour démontrer que les fonctions de sécurité fonctionnent conformément à leurs spécifications.

5.2.22 AVA_MSU.2 : Validation de l'analyse

122 Les critères d'évaluation sont définis par la section AVA_MSU.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

123 BMS et le GIE Cartes Bancaires "CB" ont fourni respectivement une analyse des guides d'exploitation de la cible d'évaluation pour chacune des applications. L'objectif de cette analyse est de garantir que des éléments trompeurs, déraisonnables ou contradictoires sont absents de ces guides et que des procédures sûres pour tous les modes d'exploitation de la cible d'évaluation ont été définies.

124 L'évaluateur s'est assuré de la complétude de cette analyse et a confirmé que l'utilisation des guides conduit à une utilisation et une configuration sûres de la cible d'évaluation.

5.2.23 AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE

125 Les critères d'évaluation sont définis par la section AVA_SOF.1.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

126 Le masqueur a fourni une analyse de la résistance des fonctions de sécurité de la cible d'évaluation.

127 L’évaluateur a analysé cette documentation et mené des analyses complémentaires. La cotation indépendante faite par l’évaluateur est en accord avec l’analyse du masqueur.

128 La résistance des fonctions de sécurité est considérée comme élevée (SOF-high).

5.2.24 AVA_VLA.4 : Résistance élevée

129 Les critères d’évaluation sont définis par les sections AVA_VLA.4.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

130 Le masqueur et le GIE Cartes Bancaires “CB” ont fourni une analyse des vulnérabilités potentielles du produit. L’ évaluateur a examiné ces fournitures et réalisé sa propre analyse de vulnérabilités indépendante.

131 Les tests de pénétration ont été conduits en deux étapes :

- l’évaluateur a mené des tests sur la cible d’évaluation dans son environnement d’exploitation normal,
- puis l’évaluateur a réalisé des tests intrusifs et en environnement perturbé sur la cible d’évaluation.

132 L’objectif de ces tests de pénétration est de vérifier que la cible d’évaluation résiste aux attaques correspondant à un potentiel élevé de l’attaquant tel que défini par le composant AVA_VLA.4 “Résistance élevée”.

5.2.25 Verdicts

133 Pour tous les aspects des critères communs identifiés ci-dessus, un avis “réussite” a été émis.

Chapitre 6

Recommandations d'utilisation

134 Le produit "Carte mixte MONEO/CB : application porte-monnaie électronique MONEO et application bancaire B4/B0' V3 (référence ST19SF16CC/RCQ version B312/B023) et Module de sécurité SAM commerçant (référence ST19SF16CC/ RCQ version C112)" est soumis aux recommandations d'utilisation exprimées ci-dessous.

- le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [5] ;

- le produit doit être utilisé et administré conformément aux guides d'utilisation [11] et [12] et d'administration [13] et [14].

135 Le respect de ces recommandations conditionne la validité du certificat.

Chapitre 7

Certification

7.1 Objet

136 Le produit soumis à évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité" et AVA_VLA.4 "Résistance élevée" tels que décrits dans la partie 3 des Critères Communs [3]. Par ailleurs, la résistance des fonctions de sécurité est cotée élevée (SOF-high).

137 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL4 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

7.2 Portée de la certification

138 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.

139 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 3.

140 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 des Critères Communs 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.
Emetteur	Banque ou organisme émetteur de la carte mixte MONEO/CB.
Encarteur	Industriel insérant le composant masqué dans un support plastique, en forme de carte.
Evaluation	Estimation d'un profil de protection ou d'une cible d'évaluation par rapport à des critères définis.
Logiciel embarqué	Logiciel présent sur une puce.
Masque	Ensemble d'instructions organisées, reconnaissables et exécutables par le processeur d'un microcircuit électronique.
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 Critères Communs.
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.
Personnalisateur	Industriel inscrivant dans la mémoire de données du composant masqué les données spécifiques à une application.

Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Porteur	Utilisateur final de la carte mixte MONEO/CB.
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.

Acronymes

ATR	Answer To Reset
CM	Configuration Management
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable and Programmable Read Only Memory
RAM	Random Access Memory
ROM	Read Only Memory
SAM	Security Access Module
SOF	Strength of Function
TOE	Target of Evaluation
TSF	TOE Security Functions

Annexe B

Références

[1] [CC-1] 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.

[2] [CC-2] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.

[3] [CC-3] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 3 : Exigences d'assurance de sécurité CCIMB-99-033, version 2.1 Août 1999.

[4] [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.

[5] Cible de sécurité "Moneo Security Target ", version 03.01 du 31 janvier 2001 (diffusion contrôlée).

[6] Rapport technique d'évaluation référencé LETI.CESTI.SETI.RE.001, version 1.1 du 21 février 2001 (diffusion contrôlée).

[7] Profil de protection "Smartcard Integrated Circuit", version 2.0 de septembre 1998, enregistré sous la référence PP/9806 (document public).

[8] Profil de protection "Smartcard Integrated Circuit with Embedded Software", version 2.0 de juin 1999, enregistré sous la référence PP/9911 (document public).

[9] Profil de protection "Intersector Electronic Purse and Purchase Device", version 1.2 de février 1999, enregistré sous la référence PP/9909 (document public).

[10] Rapport de certification 2001/04 "Plate-forme ST19 (technologie 0.6µ) : Micro-circuit ST19SF16CCxyz" de mars 2001 (document public).

[11] Guide d'administration MONEO "Moneo - Administration Documentation", référencé IBM BB-MONEO_AGD_ADM.1-01, version 1.0 du 10 août 2000.

[12] Guide d'administration B4/B0' V3 "Evaluation de la sécurité du composant masqué B4/B0' V3, Documentation d'administration", référencé GIE CB DET/DS/CBGEN6, version 1.0 de septembre 2000.

[13] Guide d'utilisation MONEO "Porte-monnaie électronique interbancaire, Guide d'utilisation du produit PME MONEO", référencé SEME AGD_USR.1 PartIV, version 1.0 du 19 juin 2000.

[14] Guide d'utilisation B4/B0' V3 "Evaluation de la sécurité du composant masqué B4/B0' V3, Documentation d'utilisation", référencé GIE CB DET/DS/CBGEN4, version 1.0 de septembre 2000.

[15] Guide d'utilisation du composant "ST19 Security application manual" référencé APM.19.SECU/0006V1.2 (diffusion contrôlée).