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 99/04

Application bancaire B4/B0' V2
de la carte mixte MONEO/CB
(référence : ST19SF16B RCL version B303/B002)

Septembre 1999

Ce document constitue le rapport de certification du produit "application bancaire B4/B0’ V2 de la carte mixte MONEO/CB (référence ST19SF16B RCL version B303/B002)".

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 99/04

Application bancaire B4/B0' V2
de la carte mixte MONEO/CB

(référence : ST19SF16B RCL version B303/B002)

Développeurs : IBM Deutschland Gmbh ; STMicroelectronics SA

EAL1 augmenté

Commanditaire :

Société Européenne de Monnaie Électronique

Le septembre 1999,

Le Commanditaire :
la S.E.M.E.

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 bancaire ST19SF16B RCL (version B303/B002).

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 La carte porteur ST19SF16B RCL est une carte mixte contenant l'application bancaire B4/B0' V2, objet du présent rapport de certification, et l'application porte-monnaie électronique MONEO certifiée au niveau EAL1 augmenté tel que décrit dans le rapport de certification 99/03 [6].

Chapitre 2

Résumé

2.1 Description de la cible d'évaluation

5 La cible d'évaluation est l'application bancaire B4/B0' V2 de la carte mixte MONEO/CB référencée ST19SF16B RCL version B303/B002.

2.2 Résumé des caractéristiques de sécurité

2.2.1 Menaces

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

- divulgation des éléments secrets de l'application (code et clés),
- usurpation d'identité de l'un des acteurs du système,
- clonage de l'application,
- perte d'intégrité des biens à protéger de l'application.

2.2.2 Politiques de sécurité organisationnelles et hypothèses

7 L'annexe A donne les principales caractéristiques de sécurité telles qu'elles sont décrites dans la cible de sécurité [7], en particulier les politiques de sécurité organisationnelles ainsi que les hypothèses d'utilisation du produit.

2.2.3 Exigences fonctionnelles de sécurité

8 Les principales fonctionnalités de sécurité du produit décrites dans la cible de sécurité [7] sont les suivantes :

- 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.

2.2.4 Exigences d'assurance

9 Les exigences d'assurance spécifiées dans la cible de sécurité [7] 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

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

SEME
29 rue de Berri
F-75008 PARIS.

11 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.

12 Le Groupement des Cartes Bancaires CB a également participé à l'évaluation :

GIE CB
31 rue de Berri
F-75008 PARIS.

2.4 Contexte de l'évaluation

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

14 L'évaluation s'est déroulée simultanément au développement du produit.

15 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

16 Le produit soumis à évaluation dont la cible de sécurité [7] 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”.

17 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.

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

19 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

20 La cible d'évaluation est l'application bancaire B4/B0' V2 de la carte mixte MONEO/CB référencée ST19SF16B RCL version B303/B002.

21 Le micro-circuit électronique ST19SF16B RCL est destiné à être 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 bancaire B4/B0' V2 et l'application porte-monnaie électronique MONEO qui a également fait l'objet d'une évaluation et est certifiée au niveau EAL1 augmenté (certificat 99/03 [6]).

22 Les phases d'encartage et de personnalisation de la cible d'évaluation sont hors du champ de l'évaluation.

3.2 Historique du développement

23 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 bancaire B4/B0' V2 s'appuie les spécifications du GIE Cartes Bancaires CB.

24 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

25 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).

26 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

27 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 bancaire B4/B0' V2, installé en mémoire EEPROM.

28 La configuration exacte de la cible d'évaluation est décrite en annexe B.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

29 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [7] qui est la référence pour l'évaluation.

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

4.2 Politique de sécurité

31 La carte bancaire "CB" est distribuée au porteur qui l'utilise pour des prestations bancaires nécessitant le composant masqué telles que le paiement de proximité (transaction monétaire effectuée par le porteur chez un commerçant en sa présence au moyen de la carte bancaire "CB" et du terminal de paiement électronique du commerçant), ou le télépaiement (transaction monétaire effectuée à distance par le porteur au moyen de la carte bancaire "CB" et d'un équipement télématique).

32 Le produit permet d'assurer :

- la confidentialité des données sensibles contenues dans la mémoire des données (codes et clés secrètes),
- la confidentialité du logiciel d'application,
- l'authentification des différents utilisateurs du produit.

33 Le produit garantit qu'à l'issue de la phase de fabrication du produit, l'accès aux données de l'application bancaire sera uniquement contrôlé par le logiciel d'application.

34 Le produit met en oeuvre, suivant les différentes phases de vie de la carte, des fonctions d'authentification et de contrôle d'accès vis-à-vis de ses utilisateurs et administrateurs ainsi que des fonctions d'authentification de la carte et des transactions bancaires.

35 Le produit permet de garantir la pérennité des données des mémoires.

36 Une fonction d'hyperviseur de sécurité détecte des conditions de fonctionnement ou d'environnement anormales et génère toute action adéquate pour garantir la sécurité du produit.

37 Le produit met également en oeuvre des fonctions d'imputation (limité à l'enregistrement de l'identité de l'utilisateur à l'origine du blocage de la carte et à l'enregistrement de l'identité de l'utilisateur à l'origine de l'écriture d'un mot dans

les zones réservées en écriture de la mémoire utilisateur du composant masqué) et d'audit (lecture simple de ces enregistrements).

4.3 Menaces

38 Les menaces effectivement couvertes par le produit sont décrites dans le chapitre 3 de la cible de sécurité [7]. Elles sont reprises en annexe A.2.

4.4 Hypothèses d'utilisation et d'environnement

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

40 Les hypothèses d'utilisation et d'environnement du produit sont consignées dans le chapitre 3 de la cible de sécurité [7]. Celles-ci sont reprises en annexe A.

4.5 Architecture du produit

41 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.

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

4.6 Description de la documentation

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

4.7 Tests de la cible d'évaluation

44 Plusieurs types de tests ont été passés sur la cible d'évaluation.

45 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.

46 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

47 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

48 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [8].

5.2 Résultats de l'évaluation de la cible de sécurité

49 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

50 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].

51 La cible d'évaluation (TOE) est l'application bancaire B4/B0' V2 de la carte mixte MONEO/CB référencée ST19SF16B RCL version B303/B002.

52 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

53 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].

54 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 [7]. Ces caractéristiques de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.3 ASE_INT Introduction de la ST

55 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].

56 L'introduction de la cible de sécurité [7] 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

57 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].

58 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrites dans la cible de sécurité [7]. 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

59 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].

60 La cible de sécurité ne précise aucune annonce de conformité à un profil de protection.

5.2.6 ASE_REQ Exigences de sécurité des TI

61 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].

62 Les exigences de sécurité des TI fonctionnelles ou d'assurance sont décrites dans la cible de sécurité [7]. 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

63 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].

64 La cible de sécurité [7] 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

65 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].

66 La cible de sécurité [7] contient un résumé des spécifications des fonctions de sécurité du produit ainsi que des 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 couvrent les exigences du niveau d'évaluation EAL1 augmenté.

5.3 Résultats de l'évaluation du produit

67 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

68 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].

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

70 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

71 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].

72 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).

73 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 [7] (ASE_TSS).

5.3.3 ACM_CAP.1 : Numéros de version

74 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].

75 Le produit évalué porte la référence ST19SF16B RCL version B303/B002, telle qu'elle est définie dans l'annexe B du présent rapport.

76 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

77 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].

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

79 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.

80 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

81 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].

82 Les administrateurs successifs du produit sont :

- le fondeur, au cours de la phase de fabrication et de tests,
- l'encarteur, au cours de la phase d'encartage,
- le personnalisateur, au cours de la phase de personnalisation,
- le GIE Cartes Bancaires "CB", au cours de la phase d'utilisation.

83 La phase principale de l'administration du produit correspond à la phase de personnalisation de la carte porteur. Les spécifications de personnalisation du produit ont été fournies.

84 L'évaluateur s'est assuré de l'absence d'incohérence dans la documentation d'administration 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 Au cours de la phase d'utilisation, les utilisateurs du produit sont :

- l'émetteur (la banque),
- le délégataire de l'émetteur (un prestataire de services),
- le porteur (client de la banque et détenteur de la carte bancaire "CB").

87 La documentation utilisateur est constituée des spécifications externes du produit (jeu de commandes B4/B0' V2) ainsi que d'une documentation d'utilisation. Celle-ci s'accompagne d'un ensemble de recommandations d'utilisation des fonctions de sécurité décrites dans les contrats d'exploitation du produit (contrat porteur et contrat d'acceptation).

88 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

89 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].

90 Les évaluateurs ont effectué un ensemble de tests sur la carte afin de vérifier par échantillonnage la conformité des fonctions de sécurité aux exigences fonctionnelles de sécurité.

91 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

92 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].

93 L'évaluateur a réalisé des tests de pénétration de manière indépendante, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit 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

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

Chapitre 6

Recommandations d'utilisation

95 Le produit "application bancaire B4/B0' V2 de la carte mixte MONEO/CB référencée ST19SF16B RCL (version B303/B002)" est soumis aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

96 Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [7].

6.1 Personnalisation du produit

97 Le processus de personnalisation est une étape critique destinée à configurer le produit de manière sûre.

98 La personnalisation doit être strictement définie et contrôlée ; des mesures de sécurité doivent être appliquées au cours de la personnalisation afin de pouvoir garantir l'intégrité et la confidentialité des données secrètes introduites dans le produit (codes et clés secrètes).

6.2 Mise en opposition de cartes

99 Le système utilisateur du produit doit permettre de détecter des cartes mises en opposition.

6.3 Contrôles de flux

100 Le volume des transactions monétaires qui peuvent être réalisées par une même carte pour une période donnée sans autorisation particulière doit être limité.

101 Le système utilisateur du produit doit réaliser d'autres contrôles lors d'une transaction bancaire qui font appel à un centre serveur d'autorisations de manière aléatoire ou en cas de dépassement d'un plafond.

Chapitre 7

Certification

7.1 Objet

102 Le produit dont les caractéristiques de sécurité sont définies dans la cible de sécurité [7], satisfait aux exigences du niveau d'évaluation **EAL1 augmenté** du composant d'assurance **AVA_VLA.2** "Analyse de vulnérabilités effectuée de manière indépendante".

103 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

104 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.

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

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

Annexe A

Caractéristiques de sécurité

107 Les caractéritiques de sécurité évaluées sont décrites dans la cible de sécurité [7] qui est la référence pour l'évaluation.

108 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.

1.1 Politiques de sécurité organisationnelles

OSP_CHECK_AV	La valeur d'authentification (V.A.) est une information chiffrée écrite dans la mémoire utilisateur du micro-circuit programmé lors de la personnalisation. Cette VA est constituée d'un ensemble de données d'identification pertinentes présentes dans la mémoire utilisateur. L'équipement d'acceptation du commerçant vérifie cette VA.
OSP_FLUX_CONT	Ce contrôle est effectué par l'équipement d'acceptation du commerçant qui permet de limiter le volume des transactions bancaires réalisées pour une carte, sans demande d'autorisation pendant une période donnée.
OSP_BLACK_LIST	C'est une liste d'opposition des cartes CB, mise à jour régulièrement par les institutions bancaires et envoyée aux équipements d'acceptation des commerçants.
OSP_SEC_CONV	Le Groupement des cartes bancaires "CB" établit avec les encarteurs et les personnalisateurs une convention de sécurité qui définit les exigences de sécurité pour l'obtention de l'agrément de sécurité de leurs sociétés.

1.2 Menaces

1.2.1 Divulgation de B0'

T.DIVULG_LOGIC	Divulgation de la partie logique de l'application B0'.
T.DIVULG_PERSO	Divulgation de l'identifiant de chaque autorité qualifiée pour personnaliser le composant.
T.DIVULG_USE	Divulgation de l'identifiant de chaque autorité qualifiée pour utiliser ou modifier les fonctions fournies par le composant masqué, à savoir celui de l'émetteur, celui du délégataire de l'émetteur et celui du porteur.
T.DIVULG_CRYPTO	Divulgation des identifiants utilisés pour la cryptographie.

1.2.2 Clonage de B0'

T.CLON_NOT_PERSO	Substitution du composant masqué ou de la partie logique de l'application B0' d'une carte bancaire CB non personnalisée, c'est-à-dire les conséquences de leur remplacement par un clone sur une carte CB personnalisée.
T.CLON_PERS	Substitution du composant masqué ou de la partie logique de l'application B0' d'une carte bancaire CB personnalisée, c'est-à-dire les conséquences de leur remplacement par un clone sur une carte CB personnalisée.

1.2.3 Usurpation de B0'

T.USPB0_PERS_A	Personnalisation de l'application B0' par des entités différentes de celles autoritées, à savoir l'encarteur puis le personnalisateur.
T.USPB0_USE_H	Utilisation des services de paiements de proximité et de télépaiement offerts par le système CB, au moyen d'une carte, par un utilisateur différent du porteur.
T.USPB0_PERS_S	Personnalisation des services de paiements de proximité et de télépaiement offerts par le système CB, au moyen d'une carte, par une entité différente de celle autorisée, à savoir l'émetteur ou son délégataire.
T.USPB0_USE_C	Utilisation des services de paiement de proximité et de télépaiement offerts par le système CB, au moyen d'une carte qui n'a pas été émise par un émetteur autorisé.

1.2.4 Modification de l'intégrité de B0'

T.INTEGR_ME8	Modification non autorisée des données confidentielles suivantes : - la partie logique de l'application B0', - l'identifiant de chaque autorité habilitée à personnaliser le composant masqué, à savoir celui de l'encarteur et celui du personnalisateur, - l'identifiant de chaque autorité habilitée à utiliser ou à modifier les services offerts par le micro-circuit programmé, à savoir celui de l'émetteur, celui du délégataire de l'émetteur et celui du porteur, - les identifiants utilisés pour la cryptographie.
T.INTEGR_USE	Modification non autorisée, au cours de la phase d'utilisation, des données de configuration et d'exploitation.
T.INTEGR_ME10	Modification non autorisée d'une quelconque donnée en phase d'invalidation.

1.3 Hypothèses sur l'environnement

A.TERM	Le terminal B0' doit être en mesure de préserver un état sûr du système lorsqu'une erreur surgit au cours d'une transaction de paiement.

1.4 Objectifs pour la cible d'évaluation

O.B0_AUTH	La TSF doit assurer l'authentification de la cible vis-à-vis de l'émetteur.
O.B0_TAMPER	La TSF doit assurer la prévention contre les attaques physique des parties de sécurité critiques de la TOE.
O.B0_ACCESS	La TSF doit assurer le contrôle d'accès des données utilisateur aux seuls utilisateurs autorisés.
O.B0_INTEG_DATA	La TSF doit éviter la modification non autorisée des données.
O.B0_OPERATE	La TSF doit assurer le fonctionnement continu correct de la TOE.

1.5 Objectifs pour l'environnement

O.B0_ELECTRO_MASKER	Les matériels utilisés dans le développement du micro-circuit électronique doivent être protégés.
O.B0_LOGIC_MASKER	Les éléments logiciels utilisés dans le développement des logiciels doivent être protégés.
O.B0_LOGIC_PRINT	Il doit être fourni à l'installateur de l'application B0' une méthode pour vérifier et contrôler l'intégrité et la version de l'application B0'.
O.B0_LOGIC_LIVRAISON	Les données de traçabilité doivent être enregistrées en vue de l'administration de sécurité.
O.B0_INSTALLATOR	Il doit exister une procédure qui protége les éléments logiciels au cours de la phase d'installation.
O.B0_EMBEDDER_DELIVER	Il doit exister une procédure qui garantit la livraison sûre entre le fabricant de micro-circuits et l'encarteur.
O.B0_PERSONALISER_DELIVER	Il doit exister une procédure qui garantit la livraison sûre entre l'encarteur et le personnalisateur.
O. B0_DEVICE	Au cours de la phase d'utilisation, les matériels et les méthodes associées doivent garantir l'intégrité et la confidentialité des données.

1.6 Exigences fonctionnelles de sécurité

Audit de Sécurité	FAU_GEN.1	Génération de données d'audit.
	FAU_SAA.1	Analyse de violation potentielle.
	FAU_SAR.1	Revue d'audit.
Communication	FCO_NRO.2	Preuve systématique de l'origine.
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_IFC.1	Contrôle de flux d'information partiel.
	FDP_IFF.1	Attributs de sécurité simple.
	FDP_RIP.1	Protection partielle des informations résiduelles.
	FDP_SDI.2	Contrôle de l'intégrité des données stockées et actions à entreprendre.
Identification et authentification	FIA_AFL.1	Gestion d'une défaillance de l'authentification.
	FIA_ATD.1	Définition des attributs d'un utilisateur.
	FIA_UAU.1	Timing de l'authentification.
	FIA_UID.1	Timing de l'identification.
Gestion	FMT_MOF.1	Gestion du comportement des fonctions de sécurité.
	FMT_MSA.1	Gestion des attributs de sécurité.
	FMT_MSA.2	Attributs de sécurité sûrs.
	FMT_MTD.1	Gestion des données de la TSF.
	FMT_SMR.1	Rôles de sécurité.
Protection des fonctions de sécurité	FPT_FLS.1	Défaillance avec préservation d'un état sûr.
	FPT_PHP.3	Résistance à une attaque physique.
	FPT_SEP.1	Séparation des domaines de la TSF.
	FPT_TST.1	Test de la TSF.

1.7 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

109 La cible d'évaluation est constituée du micro-circuit destiné à être inséré dans la carte porteur mixte MONEO/CB.

110 Elle est référencée de la manière suivante :

Composant	Version de masque ROM logiciel	Version d'application MONEO	Version d'application B4/B0' V2
ST19SF16B RCL	V2.5	B303[a]	B002[b]

a. Hors évaluation dans le cadre de ce rapport de certification,
b. Cette configuration comprend la personnalisation du produit en carte bancaire CB.

111 La documentation disponible pour le produit est la suivante :

- Documentation d'administration du produit, référencée CBGUI6 version 1,
- Documentation d'utilisation du produit, référencée CBGUI4 version 1.

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

Affectation	La spécification d'un paramètre identifié dans un composant.
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.
Blocage	État du composant masqué dans lequel les fonctionnalités du produit nécessitant une authentification préalable d'un utilisateur sont indisponibles. En phase de personnalisation, cet état est irréversible. En phase d'utilisation, le déblocage du composant masqué nécessite une authentification simultanée du porteur et de l'émetteur.
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.
Clone	Reproduction frauduleuse du produit.
Composant	Le plus petit ensemble sélectionnable d'éléments qui peut être inclus dans un PP, une ST ou un paquet.
Délégataire de l'émetteur	Délégué habilité par l'émetteur, responsable de l'ouverture des droits d'accès à des services.
Émetteur	Établissement bancaire français, membre du groupement des cartes bancaires "CB", responsable de la production de ses propres cartes.

Encartage	Insertion du composant masqué dans un support plastique, en forme de carte, incluant la phase d'assemblage en micromodules et la phase d'implantation du composant masqué sur son support plastique.
Encarteur	Industriel responsable du processus d'encartage.
Évaluation	Estimation d'un PP, d'une ST ou d'une TOE par rapport à des critères définis.
Fondeur	Fabricant du microcircuit électronique.
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.
Invalidation	Phase de fin de vie du composant masqué.
Itération	L'utilisation multiple d'un composant avec des opérations différentes.
Masqueur	Développeur de logiciels spécifiques embarqués sur microcircuits électroniques.
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.
Personnalisateur	Industriel responsable du processus de personnalisation.
Personnalisation	Inscription des informations d'identification, d'authentification, et de services bancaires dans le composant masqué, sur les pistes magnétiques et sur le support plastique afin d'associer chaque carte bancaire à son porteur.
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	Client d'une banque, utilisateur des services bancaires qui lui sont offerts par l'intermédiaire de la carte "CB".
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.
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.

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] Rapport de Certification 99/03 “Porte-monnaie électronique carte porteur (ST19SF16B RCL version B303) et module de sécurité PSAM commerçant (ST19SF16B RCL version C103)”, septembre 1999.

[7] Cible de sécurité “MONEO Security Target Part 2/2 B0’” référencée PMEIGK/ADM/SEME/MDS-6B version 3.0, septembre 1999.

[8] Rapport technique d’évaluation, FT.CNET.3C.GLM.RE002, document non public.