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 99/07

Plate-forme Javacard/VOP GemXpresso 211
(microcircuit Philips P8WE5032/MPH02)
avec applets Oberthur B0' v0.32 et Visa VSDC v1.08

Décembre 1999

Ce document constitue le rapport de certification du produit "Plate-forme Javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02) avec applets Oberthur B0' v0.32 et Visa VSDC v1.08".

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.

Ce document est folioté de 1 à 56 et certificat.

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

CERTIFICAT 99/07

Plate-forme Javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02) avec applets Oberthur B0' v0.32 et Visa VSDC v1.08

Développeurs :
Philips Semiconductors ; Gemplus ; Oberthur Card Systems ; Visa International

EAL1 augmenté

Commanditaire :
Groupement Carte Bleue

Le 31 décembre 1999,

Le Commanditaire :
L'Administrateur du
Groupement Carte Bleue
M. Gérard NEBOUY

L'organisme de certification :
Le chef du Service central de la sécurité des systèmes d'information
Le Général Jean-Louis DESVIGNES

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 contenant les applications de débit/crédit B0' d'Oberthur et VSDC de Visa. Ces deux applications, développées en Java, reposent sur la plate-forme GemXpresso 211 de Gemplus et le microcircuit Philips P8WE5032.

2 Les caractéristiques de sécurité 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 Cette évaluation, partie du projet Vocable mené par le Groupement Carte Bleue et Visa, a pour but d'étudier la coexistence des applications de débit/crédit de type B0' du GIE Cartes Bancaires et EMV de Visa International sur une seule et unique carte.

5 L'autre aspect innovant de ce projet concerne l'utilisation de la plate-forme VOP/ Javacard GemXpresso de Gemplus. Plate-forme multi-applicative, elle a été conçue pour accueillir tout type d'application pour cartes à puce programmée en Java. Cette plate-forme est conforme aux spécifications Javacard 2.1 de Sun Microsystems [8]et OP 2.0 de Visa International [9] à l'exception de la fonctionnalité de chargement de toute nouvelle applet qui est bloquée pour le produit certifié.

Chapitre 2

Résumé

2.1 Description de la cible d'évaluation

6 La cible d'évaluation est la carte destinée à être utilisée pour toute opération de débit/crédit conformément aux normes B0' du GIE Cartes Bancaires [11] et EMV de Visa International [12].

7 Les applications B0' et VSDC, développées en Java, reposent sur la plate-forme GemXpresso 211 de Gemplus et sur le microcircuit Philips P8WE5032.

8 Les composants de la cible d'évaluation sont les suivants :

Composant	Version
Applet Oberthur B0'	0.32
Applet Visa VSDC	1.08
Plate-forme Gemplus GemXpresso	211
Microcircuit Philips	P8WE5032/MPH02

2.2 Résumé des caractéristiques de sécurité

2.2.1 Préambule

9 Dans le cadre de cette évaluation, l'applet VSDC ne met pas en oeuvre de fonction de sécurité. Les biens de VSDC ne sont protégés que par des fonctions de sécurité de la plate-forme et par les mesures de sécurité prises lors du développement et de l'exploitation de la carte.

2.2.2 Menaces

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

- duplication fonctionnelle non autorisée de la carte,
- modification ou divulgation d'informations sensibles lors du développement de la plate-forme et des applets,

- modification ou divulgation d'informations sensibles lors de l'utilisation de la carte,

- chargement de nouvelles applets en phase d'utilisation.

2.2.3 Politiques de sécurité organisationnelles

11 Les principales politiques de sécurité organisationnelles identifiées dans la cible de sécurité [6] peuvent être résumées comme suit :

- Pour des raisons d'interopérabilité, Carte Bleue et ses banques exigent la conformité de l'implémentation de la plate-forme et des applets aux spécifications Javacard 2.1 de Sun [8] et VOP 2.0 de Visa [10].

2.2.4 Hypothèses

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

- conservation sûre des clés par les différents utilisateurs (porteurs, émetteurs) de la carte en phase d'exploitation,

- utilisation d'outils sûrs de conversion et de vérification des applets avant leur chargement sur la carte,

- sécurité des terminaux et des protocoles utilisés par ceux-ci,

- limite de validité de la carte (3 ans).

2.2.5 Exigences fonctionnelles de sécurité

13 Les principales fonctionnalités de sécurité du produit décrites dans la cible de sécurité [6] sont les suivantes :

- authentification des différents utilisateurs de l'applet B0',

- contrôle d'accès mis en oeuvre par la plate-forme et par l'applet B0',

- séparation des domaines (mémoire, données) entre les applets,

- protection des fonctions de sécurité : notification et résistance aux attaques physiques, contrôle de l'intégrité et de la confidentialité des mémoires.

2.2.6 Exigences d'assurance

14 Les exigences d'assurance spécifiées dans la cible de sécurité [6] 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

15 Le commanditaire de l'évaluation est le Groupement Carte Bleue et son sous-traitant Trusted Logic :

Groupement CARTE BLEUE
21 Boulevard de la Madeleine
F-75001 Paris
France

TRUSTED LOGIC
5 Rue du Baillage
F-78000 Versailles
France

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

- Oberthur Card Systems pour le développement de l'applet B0' :

  OBERTHUR CARD SYSTEMS
  3-5 Avenue Galliéni
  F-94250 Gentilly
  France

- Visa International pour le développement de l'applet VSDC :

  VISA INTERNATIONAL
  14 Rue Auber
  F-75009 Paris
  France

- Gemplus pour le développement de la plate-forme GemXpresso :

  GEMPLUS
  Parc d'Activités de Gémenos
  B.P. 100
  F- 13881 Gémenos Cedex
  France

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

  PHILIPS Semiconductors
  Röhen und Halbleiterwerke
  D-22502 Hambourg
  Allemagne.

2.4 Contexte de l'évaluation

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

18 L'évaluation s'est déroulée entre le 15 septembre 1999 et le 26 novembre 1999 et a été menée consécutivement au développement du produit.

19 L'évaluation a été réalisée par le centre d'évaluation de la sécurité des technologies de l'information de Serma Technologies :

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

2.5 Conclusions de l'évaluation

20 Le produit soumis à évaluation dont la cible de sécurité [6] 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".

21 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'attaque tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

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

23 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

24 La cible d'évaluation est la carte destinée à être utilisée pour toute opération de débit/crédit conformément aux normes B0' du GIE Cartes Bancaires [11] et EMV de Visa International [12] en phase 7 du cycle de vie défini dans le schéma de la page suivante.

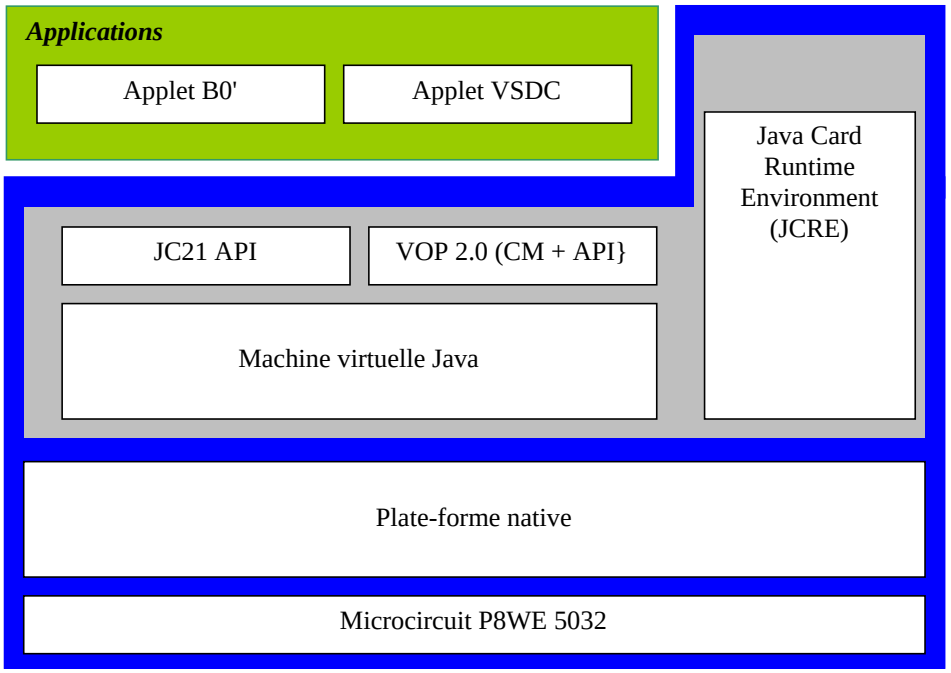
25 Cette carte est constituée du microcircuit électronique P8WE5032 inséré dans une carte porteur de format carte de crédit.

26 Le microcircuit électronique contient le système d'exploitation de la carte ainsi que le logiciel de Gemplus constituant la plate-forme GemXpresso 211.

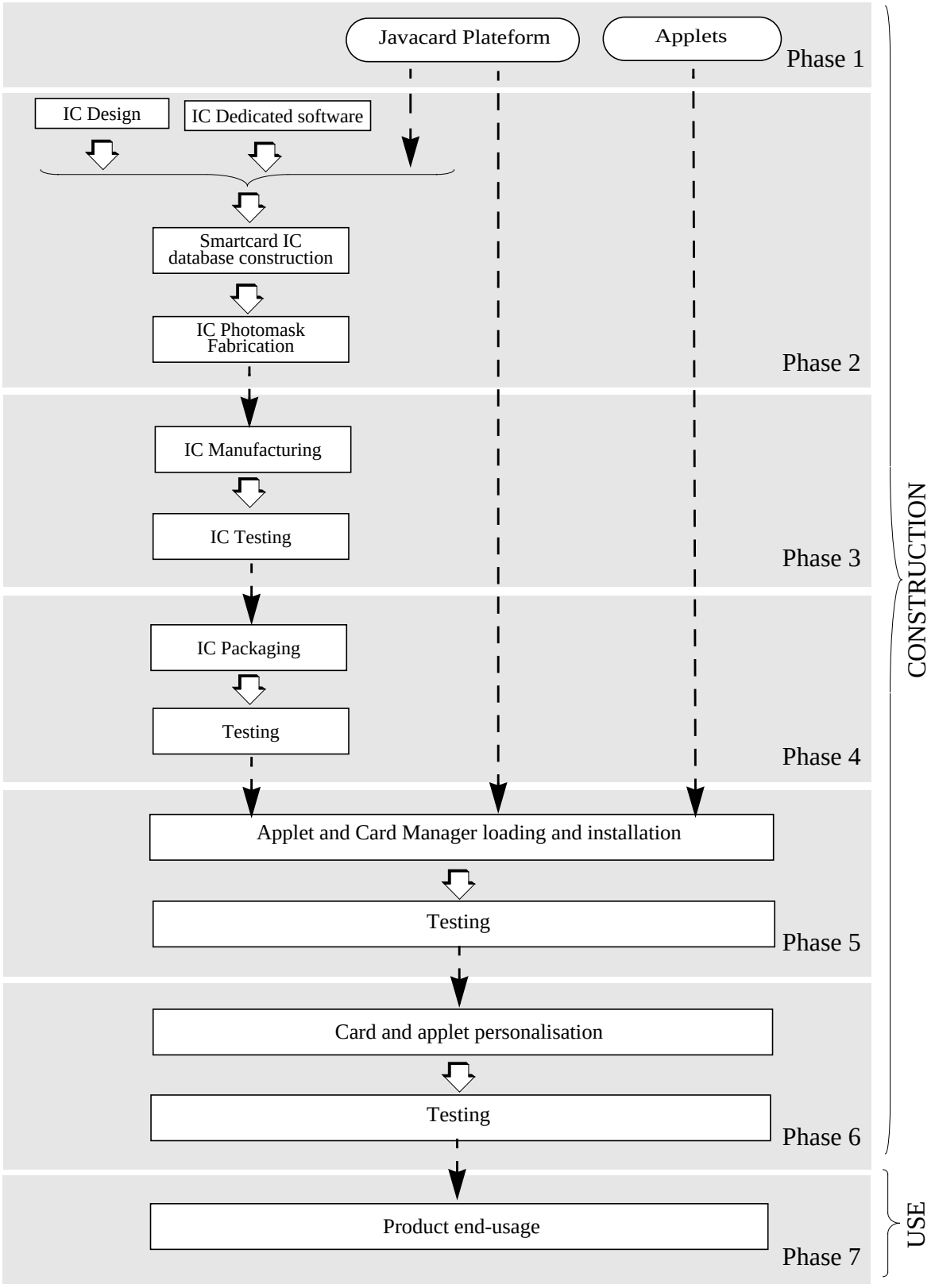
27 Deux applications de débit/crédit (l'applet Oberthur B0' et l'applet Visa VSDC) sont également chargées pour être utilisées en phase d'exploitation de la carte. Aucune autre applet ne peut être chargée sur ce produit certifié.

3.2 Description de l'architecture

28



3.3 Cycle de vie de la cible d'évaluation



3.4 Historique du développement

29 Le microcircuit P8WE5032 est développé et testé par Philips (phases 2 et 3).

30 La plate-forme GemXpresso est développée par Gemplus (phase 1). Cette plate-forme s'appuie sur les spécifications "Java Card Virtual Machine" de Sun Microsystems [8] et "Open Platform" de Visa [9]. Une partie de cette plate-forme, constituant le logiciel embarqué, est masquée en phase 2 et 3 alors que l'autre partie, le Card Manager, est chargé en phase 5.

31 L'applet B0' est développée par Oberthur (phase 1). Cette applet s'appuie sur les spécifications B4/B0' V2 du GIE Cartes Bancaires [11].

32 L'applet VSDC est développée par Visa (phase 1). Cette applet s'appuie sur les spécifications EMV de Visa International [12].

33 Ces deux applets sont chargées sur la plate-forme puis personnalisées par Gemplus en phases 5 et 6.

3.5 Description du matériel

34 Le microcircuit électronique utilisé est le composant P8WE5032 de Philips.

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

3.6 Description du logiciel

36 La cible d'évaluation est constituée des logiciels suivants :

- le logiciel embarqué masqué durant la phase de fabrication du produit (phases 2 et 3),
- le Card Manager chargé (phase 5),
- les applets B0' et VSDC chargées sur la plate-forme (phase 5).

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

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

38 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [6] qui est la référence pour l'évaluation.

39 Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques. Celles-ci sont reprises en détail en annexe A.

4.2 Politique de sécurité

40 La carte évaluée est utilisée pour toutes les opérations de débit/crédit définies par les normes B0' du GIE Cartes Bancaires [11] et EMV de Visa International [12].

41 Ces normes établissent des règles d'usage à destination des utilisateurs potentiels de la carte (émetteurs et porteurs) et définissent les mesures de sécurité nécessaires aux opérations de paiement et de retrait.

42 Visa International et Sun Microsystems définissent également un ensemble de règles d'utilisation et d'implémentation pour les plate-formes multi-applicatives à base de Java (Javacard [8], OP [9] et VOP [10]).

43 Ces spécifications sont intégralement respectées pour le produit certifié à l'exception de la fonction de téléchargement de nouvelles applets en phase d'utilisation de la carte (phase 7).

4.3 Menaces

44 Les menaces effectivement couvertes par le produit sont décrites dans le chapitre 3 de la cible de sécurité [6] et sont reprises en annexe A.

45 Ces menaces portent essentiellement sur les points suivants :

- duplication fonctionnelle de la carte,
- divulgation non autorisée des biens de la plate-forme et des applets,
- vol ou utilisation non autorisée des biens de la plate-forme et des applets,
- modification non autorisée des biens de la plate-forme et des applets,
- menaces sur la livraison des données du logiciel embarqué,

- menaces sur la livraison des données du Card Manager et des applets,
- divulgation et modification des biens de B0',
- répudiation des transactions de B0',
- Authentification des utilisateurs de B0',
- menaces liées au cycle de vie de B0'.

4.4 Hypothèses d'utilisation et d'environnement

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

47 Les hypothèses d'utilisation et d'environnement du produit sont consignées dans le chapitre 3 de la cible de sécurité [6] et sont reprises en annexe A.

48 Ces hypothèses portent essentiellement sur les points suivants :

- gestion sûre des clés et des PIN par les porteurs et émetteurs,
- utilisation d'outils sûrs de conversion et de vérification des applets avant leur chargement,
- la sécurité des terminaux et des protocoles utilisés par ceux-ci,
- l'émission de la carte dans un délai maximum de 3 ans.

4.5 Architecture du produit

49 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.

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

4.6 Description de la documentation

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

4.7 Tests de la cible d'évaluation

52 Plusieurs types de tests ont été passés sur la carte.

53 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.

54 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

55 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

56 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [7].

5.2 Résultats de l'évaluation de la cible de sécurité

57 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.1 : Description de la TOE

58 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].

59 La cible d'évaluation (TOE) est la carte "Plate-forme Javacard/VOP GemXpresso 211 (composant Philips P8WE5032/MPH02) avec applets Oberthur B0' v0.32 et Visa VSDC v1.08".

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

5.2.2 ASE_ENV.1 : Environnement de sécurité

61 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].

62 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 [6]. Ces caractéristiques de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.3 ASE_INT.1 : Introduction de la ST

63 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].

64 L'introduction de la cible de sécurité [6] 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.1 : Objectifs de sécurité

65 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].

66 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrites dans la cible de sécurité [6]. Ces objectifs de sécurité sont repris en annexe A du présent rapport de certification.

5.2.5 ASE_PPC.1 : Annonce de conformité à un PP

67 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].

68 La cible de sécurité [6] ne revendiquant pas de conformité à un profil de protection, cette tâche d'évaluation n'est pas applicable.

5.2.6 ASE_REQ.1 : Exigences de sécurité des TI

69 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].

70 Les exigences de sécurité des TI fonctionnelles ou d'assurance sont décrites dans la cible de sécurité [6]. Ces exigences de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.7 ASE_SRE.1 : Exigences de sécurité des TI déclarées explicitement

71 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].

72 La cible de sécurité [6] ne contient pas d'exigence 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.1.1 : Spécifications de haut niveau de la TOE

73 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].

74 La cible de sécurité [6] 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

75 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

76 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].

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

78 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

79 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].

80 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).

81 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 [6] (ASE_TSS).

5.3.3 ACM_CAP.1 : Numéros de version

82 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].

83 Le produit évalué est composé du composant Philips P8WE5032/MPH02, de la plate-forme Gemplus GemXpresso 211 et des applets Oberthur B0' v0.32 et Visa VSDC v1.08 tels que définis dans l'annexe B du présent rapport.

84 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

85 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].

86 Les procédures d'installation, de génération et de démarrage du produit portent sur les phases de chargement des applets et du Card Manager et de leur personnalisation.

87 Les procédures de livraison au chargeur garantissent l'intégrité et l'origine du code chargé. Pour l'applet B0' en particulier, des procédures de signature et de vérification sont définies par le GIE Cartes Bancaires.

88 Le chargement est réalisé en conformité avec les spécifications VOP de Visa International [10].

89 Les procédures de personnalisation des applets et de la plate-forme garantissent la confidentialité des données sensibles utilisées par le personnalisateur.

90 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

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 [4].

92 L'administration du produit se déroule en phase d'exploitation de la carte (phase 7). Les administrateurs déclarés du produit sont les émetteurs des cartes et leurs délégataires. Les applications disponibles par ces administrateurs sont le Card Manager et les applets B0' et VSDC.

93 Les documents d'administration sont constitués des guides du GIE Cartes Bancaires pour l'administration de B0', de Visa pour l'administration de VSDC et de Gemplus pour l'administration de la plate-forme.

94 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

95 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].

96 L'utilisation du produit se déroule en phase d'exploitation de la carte (phase 7). Les utilisateurs déclarés du produit sont les porteurs des cartes et les différents terminaux. Les applications disponibles par ces utilisateurs sont le Card Manager et les applets B0' et VSDC.

97 Les documents d'utilisation sont constitués des guides du GIE Cartes Bancaires pour l'utilisation de B0', de Visa pour l'utilisation de VSDC et de Gemplus pour l'utilisation de la plate-forme.

98 L'évaluateur s'est assuré que cette documentation décrivait correctement l'utilisation sûre du produit.

5.3.7 ATE_IND.1 Tests effectués de manière indépendante - conformité

99 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].

100 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.

101 Ces tests ont porté sur les applications chargées ainsi que sur les fonctions de sécurité de la plate-forme. 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

102 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].

103 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 *faible* tel que défini par le composant AVA_VLA.2. Ces tests de pénétration ont porté sur les applications chargées, sur la plate-forme javacard ainsi que sur le microcircuit. Les attaques de nature évidente, incluant donc celles du domaine public, ont été également prises en compte dans cette analyse.

5.3.9 Verdicts

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

Chapitre 6

Recommandations d'utilisation

105 Le produit "plate-forme javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02) avec applets Oberthur B0' v0.32 et Visa VSDC v1.08" est soumis aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

- Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [6],

- Le porteur doit utiliser sa carte conformément aux recommandations fournies par l'émetteur, sa banque. Il est notamment le seul responsable de la protection du code PIN qui lui est fourni avec sa carte.

Chapitre 7

Certification

7.1 Objet

106 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".

107 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 faible tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.**

7.2 Portée de la certification

108 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.

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

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

Annexe A

Caractéristiques de sécurité

111 Les caractéristiques de sécurité évaluées sont décrites dans la cible de sécurité [6] qui est la référence pour l'évaluation.

112 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

P.JCP_DEV	Pour des raisons d'interopérabilité, Carte Bleue et ses banques exigent la conformité de l'implémentation de la plate-forme javacard avec les spécifications VOP 2.0 [10] et javacard 2.1 [8].
P.APP_DEV	Pour des raisons d'interopérabilité et de sécurité, Carte Bleue et ses banques exigent que l'implémentation des applets - n'utilisent que des fonctions standard VOP et Javacard, - protègent suffisament les données sensibles, - utilisent des outils de développement approuvés tels qu'un converteur et un vérificateur d'applets.

A.2 Menaces

A.2.1 Duplication fonctionnelle

T.CLON	Duplication fonctionnelle (complète ou partielle) de la carte. (phases 1 à 7)

A.2.2 Divulgation non-autorisée des biens du composant

T.DIS_INFO	Divulgation des biens du fondeur (spécifications du composant, architecture, outils de développement) livrés au développeur du logiciel embarqué. (phase 1)
T.DIS_DESIGN	Divulgation de l'architecture du composant. (phases 2 à 7)
T.DIS_DSOFT	Divulgation du système d'exploitation du composant. (phases 2 à 7)
T.DIS_TEST	Divulgation des informations de test du composant. (phases 2 et 3)
T.DIS_TOOLS	Divulgation des outils de développement du composant. (phases 2 et 3)
T.DIS_PHOTOMASK	Divulgation des informations du photomasque utilisé pour construire le composant. (phases 2 et 3)

A.2.3 Divulgation non-autorisée des biens du logiciel embarqué

T.DIS_DEL	Divulgation des biens du développeur du logiciel embarqué (code source, clés de prépersonnalisation) livrés au fondeur. (phase 1)
T.DIS_ES1	Divulgation des biens à protéger (code source, spécifications, paramètres des fonctions de sécurité) chez le développeur du logiciel embarqué. (phase 1)
T.DIS_TEST_ES	Divulgation des informations et des programmes de test chez le développeur du logiciel embarqué. (phase 1)
T.DIS_ES2	Divulgation du logiciel embarqué et de ses données sensibles. (phases 2 à 7) Cette menace inclut la divulgation par l'intermédiaire d'une applet chargée.

A.2.4 Divulgation non-autorisée des biens des applets et du Card Manager

T.DIS_APP1	Divulgation des biens à protéger (code source, spécifications, paramètres des fonctions de sécurité) chez les développeurs d'applets. (phase 1)
T.DIS_TEST_APP	Divulgation des informations et des programmes de test chez les développeurs d'applets. (phase 1)
T.DIS_APP2	Divulgation des applications et de leurs données sensibles. (phases 5 à 7) Cette menace inclut la divulgation par l'intermédiaire d'une applet chargée.

A.2.5 Vol ou utilisation non-autorisée des biens du composant

T.T_SAMPLE	Vol ou utilisation non-autorisée d'échantillons de composants. (phases 2 et 3)
T.T_PHOTOMASK	Vol ou utilisation non-autorisée de photomasques. (phases 2 et 3)

A.2.6 Vol ou utilisation non-autorisée des biens du logiciel embarqué

T.T_DEL_JCP	Vol ou utilisation non-autorisée du logiciel embarqué et de ses données sensibles lors de la livraison au fondeur. (phase 1-2)
T.T_TOOL_JCP	Vol ou utilisation non-autorisée des outils de développement du logiciel embarqué. (phase 1)
T.T_SAMPLE2	Vol ou utilisation non-autorisée d'échantillons de composants masqués. (phase 1)
T.T_ES	Vol ou utilisation non-autorisée de composants masqués. (phases 4 à 7)

A.2.7 Vol ou utilisation non-autorisée des biens des applets et du Card Manager

T.T_DEL_APP	Vol ou utilisation non-autorisée des applets ou de leurs données sensibles lors de la livraison au chargeur. (phase 1-5)
T.T_TOOL_APP	Vol ou utilisation non-autorisée des outils de développement des applets. (phase 1)
T.T_CMD	Utilisation non-autorisée de commandes envoyées à la carte. (phases 4 à 7)
T.T_PRODUCT	Vol ou utilisation non-autorisée de cartes (phases 2 et 3)
T.IMPERSONATE	Une applet ne peut pas obtenir des accès non-autorisés en se faisant passer pour une autre. (phases 6 et 7)

A.2.8 Modification non-autorisée des biens du composant

T.MOD_DESIGN	Modification non-autorisée de l'architecture du composant. (phases 2 et 3)
T.MOD_PHOTOMASK	Modification non-autorisée des photomasques. (phases 2 et 3)
T.MOD_DSOFT	Modification non-autorisée du système d'exploitation du composant. (phases 2 et 3).

A.2.9 Modification non-autorisée des biens du logiciel embarqué

T.MOD_DEL_JCP	Modification non-autorisée du logiciel embarqué ou de ses données sensibles lors de la livraison au fondeur. (phase 1-2)
T.MOD_JCP	Modification non-autorisée du logiciel embarqué, de ses données sensibles ou des informations associées (spécifications techniques). (phase 1)
T.MOD_LOAD_JCP	Chargement non-autorisé du Card Manager. (phases 4 à 7)
T.MOD_EXE_JCP	Exécution non-autorisée du logiciel embarqué. (phases 4 à 7)

T.MOD_SHARE_JCP	Modification non-autorisée du comportement des programmes par interaction avec d'autres programmes. (phases 4 à 7)
T.MOD_SOFT_JCP	Modification non-autorisée du logiciel embarqué et de ses données. (phases 2 à 7) Cette menace inclut les modifications par des attaques internes (par une applet) ou externes.

A.2.10 Modification non-autorisée des biens des applets et du Card Manager

T_MOD_DEL_APP	Modification non-autorisée des applets ou de leurs données sensibles lors de la livraison au chargeur. (phase 1-5)
T.MOD_APP	Modification non-autorisée des applets, de leurs données sensibles ou des informations associées (spécifications techniques). (phase 1)
T.MOD_LOAD_APP	Chargement non-autorisé d'applications. (phases 4 à 7) Cette menace inclut le chargement d'applets autre que B0' et VSDC en phase 5 et le chargement de toute applet en phases 4, 6 et 7.
T.MOD_EXE_APP	Exécution non-autorisée des applets. (phases 4 à 7)
T.MOD_SHARE_APP	Modification non-autorisée du comportement des applets par interaction avec d'autres applets. (phases 4 à 7)
T.MOD_SOFT_APP	Modification non-autorisée des applets et de leurs données. (phases 5 à 7) Cette menace inclut les modifications par des attaques internes (par des applets) ou externes.

A.2.11 Menaces lors des livraisons des données du logiciel embarqué

T.DIS_DEL1	Divulgation du logiciel embarqué et de ses données lors des livraisons à l'encarteur, au chargeur et au personnalisateur. (phases 1-4,5,6)
T.DIS_DEL2	Divulgation du logiciel embarqué et de ses données livrées à l'encarteur, au chargeur et au personnalisateur. (phases 1-4,5,6)
T.MOD_DEL1	Modification non-autorisée du logiciel embarqué et de ses données lors des livraisons à l'encarteur, au chargeur et au personnalisateur. (phases 1-4,5,6)
T.MOD_DEL2	Modification non-autorisée du logiciel embarqué et de ses données livrées à l'encarteur, au chargeur et au personnalisateur. (phases 1-4,5,6)

A.2.12 Menaces lors des livraisons données des applets et du Card Manager

T.DIS_DEL3	Divulgation des applications et de leurs données lors des livraisons au chargeur et au personnalisateur. (phases 1-5,6)
T.DIS_DEL4	Divulgation des applications et de leurs données livrées au chargeur et au personnalisateur. (phases 1-5,6)
T.MOD_DEL3	Modification non-autorisée des applications et de leurs données lors des livraisons au chargeur et au personnalisateur. (phases 1-5,6)
T.MOD_DEL4	Modification non-autorisée des applications et de leurs données livrées au chargeur et au personnalisateur. (phases 1-5,6)

A.2.13 Divulgation ou modification des biens de B0'

T.EXT_INF_APP	Modification non-autorisée ou divulgation d'informations en phase d'exploitation de l'applet B0' par des actions externes (commandes).
T.INT_INF_APP	Modification non-autorisée, divulgation ou vol d'informations en phase active de l'applet B0' par des actions internes (commandes).
T.ENV_ACC	Utilisation de conditions anormales d'utilisation pour accéder à des données sensibles en phase d'utilisation.
T.ACC_DATA	Divulgation de données sensibles par des actions externes (commandes).

A.2.14 Répudiation des opérations de B0'

T.REP_TRANSAC	Répudiation d'une transaction par un porteur ou un commerçant.
T.REP_ISSUER	Répudiation de la personnalisation de B0' par un émetteur.

A.2.15 Authentification

T.AUTH_CH	Utilisation de B0’ par un porteur non-autorisé.
T.AUT_ISSUER	Utilisation de B0’ par un porteur autorisé mais avec une carte émise par un émetteur ou un délégataire non autorisé.

A.2.16 Cycle de vie de B0’

T.BLOCK_DATA	Accès non autorisé aux données protégées de l’applet B0’ quand celle-ci est en état bloquée.
T.STATE_APP	Modification non autorisée de l’état de l’applet B0’.
T.STATE_MOD	Modification de n’importe quelles données lorsque l’applet B0’ est passée en état invalidée.

A.3 Hypothèses sur l'environnement

A.3.1 Hypothèses sur les outils utilisés

A.CONVERTER	Le convertisseur doit correctement générer un code intermédiaire (bytecode) vérifiable.
A.VERIFIER	Le vérificateur de code intermédiaire (bytecode) doit s'assurer que les instructions utilisées sont correctes.

A.3.2 Hypothèses sur la gestion du code PIN et des clés

A.PIN_MGT	Le porteur est la seule personne à connaître son code PIN en clair.
A.KEY_MGT	L'émetteur et les serveurs d'administration des cartes doivent conserver des clés de la plate-forme et des applications à un haut niveau de confidentialité.

A.3.3 Hypothèses sur la phase d'exploitation

A.USE_DIAG	Des protocoles et des procédures sûrs doivent être utilisés entre la carte et un terminal.
A.USE_SYS	L'intégrité et la confidentialité des données sensibles conservées par le système (terminaux, communications,..) est assurée.
A.VALID_CARD	Les cartes doivent être émises dans une limite de 3 ans.

A.4 Objectifs de sécurité pour la cible d'évaluation

A.4.1 Objectifs de sécurité globaux

O.TAMPER_ES	La plate-forme doit être résistante aux attaques contre ses mécanismes de sécurité.
O.TAMPER	La carte doit être résistante aux attaques physiques contre ses mécanismes de sécurité.
O.CLON	Les fonctions de la carte doivent être protégées d'une duplication fonctionnelle.
O.OPERATE	La carte doit assurer un fonctionnement correct et continu des fonctions de sécurité.
O.FLAW	La carte ne doit pas contenir d'erreurs dans son architecture, son implémentation et son exploitation.
O.DIS_MECHANISM	La carte doit assurer que les mécanismes de sécurité du composant sont protégés contre la divulgation non-autorisée.
O.DIS_MECHANISM2	La carte doit assurer que les mécanismes de sécurité de la plate-forme sont protégés contre la divulgation non-autorisée.
O.DIS_MEMORY	La carte doit assurer que les informations sensibles conservées en mémoire sont protégées contre la divulgation non-autorisée.
O.MOD_MEMORY	La carte doit assurer que les informations sensibles conservées en mémoire sont protégées contre la modification non-autorisée.
O_FIREWALL	La plate-forme doit assurer l'étanchéité entre les applets.
O.APP_LOAD	Les applets ne peuvent être chargées sur la plate-forme qu'en phase 5b.

A.4.2 Objectifs de sécurité pour l'applet B0'

O.AUTH_PER	L'applet B0' doit authentifier le personnalisateur avant de lui donner accès à la mémoire de B0'.
O.AUTH_ISS	L'applet B0' doit authentifier l'émetteur avant de lui donner accès aux commandes et à la mémoire de B0' en phase d'utilisation.

O.AUTH_DEL_ISS	L'applet B0' doit authentifier l'émetteur délégué avant de lui donner accès aux commandes et à la mémoire de B0' en phase d'utilisation.
O.AUTH_CH	L'applet B0' doit authentifier le porteur avant de lui donner accès aux commandes et à la mémoire de B0' en phase d'utilisation.
O.AUTH_UBLK	L'applet B0' doit authentifier l'administrateur de déblocage avant de lui donner accès au déblocage de l'application.
O.NUMB_AUTH	L'applet doit limiter le nombre de tentatives d'authentification.
O.PROT_EXT	L'applet B0' doit être conçue pour assurer que son code et ses données ne peuvent pas être altérés ou accessibles par un moyen non-autorisé
O.PROT_DATA	L'applet doit assurer que les données sensibles (code PIN et clés) de chaque utilisateur sont protégées et conservées de manière sure.
O.DATA_CERT	L'applet doit pouvoir certifier l'autenticité des données qui peuvent être reprises dans les zones mémoire par chaque utilisateur.
O.ACCESS_RIGHTS	L'applet doit contrôler l'accès des différents groupes à leurs données sur la base de droits d'accès prédéfinis.
O.SAV_AUTH_ERR	L'applet doit enregistrer le type d'identité de l'utilisateur pour lequel une authentification échoue.
O.TRC_AUTHO	L'applet doit garder la trace de l'identité des autorités qui écrivent dans la mémoire.
O.ID_AUTHO	L'applet doit permettre à un utilisateur d'identifier l'autorité qui a écrit en mémoire.
O.STATE_BLOCKED	L'applet doit basculer en état bloquée après un nombre donné de tentative d'authentification. Le retour à un état normal est possible sur présentation d'une clé.
O.STATE_INV	L'applet doit basculer en état invalidée après toute erreur d'authentification pendant la phase de personnalisation ou sur demande. Cet état est définitif.
O.INV_MOD	L'applet doit interdire toute modification des données en état invalidée.

O.STATE_CTRL	L'applet doit contrôler les différents états de son cycle de vie. Tout retour dans un état précédent est interdit.
O.MEMORY	La mémoire utilisée doit être validée, cohérente et ne doit pas dépasser la taille de mémoire allouée.

A.5 Objectifs de sécurité pour l'environnement

A.5.1 Objectifs sur la phase 1

O.DEV_TOOLS	Le logiciel embarqué, le Card Manager et les applets doivent être développées d'une manière sûre.
O.DEV_DIS_ES	Les développeurs du logiciel embarqué, du Card Manager et des applets doivent utiliser des procédures pour contrôler le stockage et l'utilisation des documents et des outils de développement.
O.DEV_DIS	Le développeur du composant doit utiliser des procédures pour contrôler le stockage et l'utilisation des documents et des outils de développement.
O.SOFT_DLV	Le logiciel embarqué doit être livré au développeur du composant d'une manière sûre garantissant l'intégrité et la confidentialité du logiciel.
O.SOFT_MECH	Pour atteindre le niveau de sécurité exigé dans le PP/ 9806, la plate-forme doit utiliser les fonctionnalités de sécurité du composant décrites dans sa documentation.
O.INIT_ACS	Les données d'initialisation ne doivent être accessibles que par le personnel autorisé.
O.SAMPLE_ACS	Les échantillons ne doivent être accessibles que par le personnel autorisé.
O.USE_APPLET	Les données utilisateurs sont sous contrôle des applets.
O.DEV_APPLET	Les applets doivent être développées en respectant les règles de programmation Javacard 2.1 [8], VOP 2.0 [10] et celles fournies par Gemplus.

A.5.2 Objectifs sur la phase 2

O.SOFT_ACS	La plate-forme ne doit être accessible chez le développeur du composant que par le personnel autorisé.
O.DESIGN_ACS	Les spécifications et les autres informations sensibles du composant ne doivent être accessibles que par le personnel autorisé chez le développeur du composant.

O.DSOFT_ACS	Les spécifications et les autres informations sensibles du système d'exploitation du composant ne doivent être accessibles que par le personnel autorisé chez le développeur du composant.
O.MASK_FAB	Les procédures techniques, organisationnelles et physiques durant la fabrication du photomask doivent garantir l'intégrité et la confidentialité de la TOE.
O.MECH_ACS	Le détail des spécifications des mécanismes de sécurité hardware ne doit être accessible que par le personnel autorisé chez le développeur du composant.
O.TI_ACS	les informations techniques touchant à la sécurité ne doivent être accessibles que par le personnel autorisé chez le développeur du composant.

A.5.3 Objectifs sur la phase 3

O.TOE_PRT	Le processus de fabriquation doit garantir la protection de la TOE de tous types d'utilisation non autorisée tels que des attaques physiques ou des vols.
O.IC_DLV	Les procédures de livraison du fabriquant du composant doit garantir l'intégrité et la confidentialité de la TOE et de ses biens.

A.5.4 Objectifs sur les livraisons lors des phases 4 à 7

O.DLV_PROTECT	Des procédures doivent assurer la protection de la TOE et de ses informations durant la livraison.
O.DLV_AUDIT	Des procédures doivent assurer que des actions correctives sont prises en cas d'opération non sûres durant la livraison.
O.DLV_RESP	Des procédures doivent assurer que les personnes chargées des livraisons sont suffisament compétentes.

A.5.5 Objectifs sur les livraisons entre les phases 1 et 4,5,6

O.DLV_DATA	Les données du logiciel embarqué doivent être livrées du développeur de la plate-forme au fabriquant du composant d'une manière sûre.
O.DLV_APP	Le code des applets et du card manager doivent être livrés des développeurs au chargeur d'une manière sûre.

A.5.6 Objectifs sur les phases 4 à 7

O.ENCART_TEST	Des tests doivent être réalisés sur la plate-forme en phase 4.
O.LOAD_TEST	Des tests doivent être réalisés sur la TOE en phase 5.
O.PERSO_TEST	Des tests doivent être réalisés sur la TOE en phase 6.
O.USE_TEST	Des tests doivent être réalisés sur la TOE en phase 7.
O.USE_DIAG	Des protocoles de communication sûrs doivent être utilisés entre la carte et les terminaux.

O.USE_SYS	L'intégrité et la confidentialité des données stockées et traitées par le système (terminaux, communications,..) doit être garantie.
O.VALID_CARD	La carte doit être émise dans un délai maximal de 3 ans.

A.6 Exigences fonctionnelles de sécurité

Audit de Sécurité	FAU_ARP.1	Alarmes de sécurité.
	FAU_SAA.1	Analyse des violations potentielles.
	FAU_STG.1	Stockage protégé de traces d'audit.
Cryptographie	FCS_CKM.1	Génération de clés cryptographiques.
	FCS_CKM.3	Accès aux clés cryptographiques.
	FCS_CKM.4	Destruction des clés cryptographiques.
	FCS_COP.1	Opération cryptographique.
Protection des données utilisateur	FDP_ACC.1	Contrôle d'accès partiel.
	FDP_ACC.2	Contrôle d'accès complet.
	FDP_ACF.1	Contrôle d'accès basé sur les attributs de sécurité.
	FDP_DAU.2	Authentification de données avec garantie d'identité.
	FDP_ETC.1	Exportation de données de l'utilisateur sans attributs.
	FDP_ITC.1	Importation de données de l'utilisateur sans attributs.
	FDP_RIP.1	Protection partielle des informations résiduelles.
	FDP_RIP.2	Protection complète 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_UAU.3	Authenfication infalsifiable.
	FIA_UAU.4	Mécanismes d'authentification à usage unique.
	FIA_UAU.7	Authentification avec feed-back protégé.
	FIA_UID.1	Timing de l'identification.
	FIA_USB.1	Correspondance utilisateur-sujet.
Gestion de la sécurité	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_MSA.3	Initialisation statique d'attribut.
	FMT_MTD.1	Gestion des données de la TSF.
	FMT_MTD.2	Gestion des valeurs limites des données de la TSF.
	FMT_SMR.1	Rôles de sécurité.
	FMT_SMR.2	Restrictions sur les rôles de sécurité.
Protection de la vie privée	FPR_UNO.1	Non-observabilité.

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_TDC.1	Cohérence élémentaire des données de la TSF entre des TSF.
	FPT_TST.1	Test de la TSF.
Utilisation des ressources	FRU_RSA.1	Quotas maximum.

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

113 La cible d'évaluation est la carte destinée à être utilisée pour toute opération de débit/crédit conformément aux normes B0' du GIE Cartes Bancaires [11] et EMV de Visa International [12].

114 Elle est composée des éléments suivants :

Composant	Version
Applet Oberthur B0'	0.32
Applet Visa VSDC	1.08
Plate-forme Gemplus GemXpresso	211
Microcircuit Philips	P8WE5032/MPH02

115 La documentation disponible pour le produit est la suivante :

- Contrat porteur fourni par la banque émettrice de la carte,
- Java Card 2.1 Virtual Machine Specification de Sun Microsystems [8],
- Open Platform Card Specification [9] et Visa Open Platform Card Specification de Visa International [10].

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
OP	(Open Platform) - Spécifications des plate-formes multiapplicatives
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
VOP	(Visa Open Platform) - Spécifications des plate-formes multiapplicatives
VSDC	(ViSa Debit/Credit) - Application de débit/crédit développée par Visa International

C.2 Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par les contre-mesures d'une TOE.
Chargeur	Industriel responsable du chargement des applets sur une plate-forme multi-applicative.
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.
Emetteur	Banque ou organisme émetteur de la carte de débit/crédit.
Encarteur	Industriel insérant un composant masqué dans un support plastique au format d'une carte.
Evaluation	Estimation d'un PP, d'une ST ou d'une TOE par rapport à des critères définis.
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.
Fondeur	Industriel fabriquant des composants masqués.
Informel	Qui est exprimé à l'aide d'un langage naturel.
Itération	L'utilisation multiple d'un composant avec des opérations différentes.
Logiciel embarqué	Logiciel masqué sur une puce exécutant les opérations d'une application.

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 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 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 d'un carte de débit/crédit.
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.
Système d'exploitation du composant	Logiciel masqué sur une puce pilotant les méchanismes spécifiques du 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 1.0.

[6] Cible de sécurité référencée VOCA/PFG/VB/ST - Version 0.8, novembre 1999.

[7] Rapport technique d'évaluation, RTE_ASTRE v3.0 (document non public).

[8] Java Card 2.1 Virtual Machine Specification v1.1 - juin 1999, Sun Microsystems

[9] Open Platform Card Specification, v2.0 - avril 1999, Visa International

[10] Visa Open Platform Card Implementation Specification - mars 1999, Visa International

[11] Spécifications de Sécurité de l'Application B4-B0' V2 - janvier 1999, GIE Cartes Bancaires (document non public).

[12] EMV'96 Integrated Circuit Card Specification for Payment Systems v3.1.1 - mai 1998