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 2000/06

Plate-forme Javacard/VOP GemXpresso 211 V2
(Composant masqué Philips P8WE5032/MPH04,
Card Manager A000000018434D)

Octobre 2000

Ce document constitue le rapport de certification du produit "Plate-forme Javacard/VOP GemXpresso 211 V2 (Composant masqué Philips P8WE5032/MPH04, Card Manager A000000018434D".

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.

Mél: ssi20@calva.net

Ce document est folioté de 1 à 32 et certificat.

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

CERTIFICAT 2000/06

Plate-forme Javacard/VOP GemXpresso 211 V2
(Composant masqué Philips P8WE5032/MPH04, Card Manager A000000018434D)

Développeurs :
Gemplus, Philips Semiconductors

EAL1 augmenté

Commanditaires :
Groupement Carte Bleue
Gemplus

Le 20 octobre 2000,

Les Commanditaires :		L'Organisme de Certification :
L'Administrateur du Groupement Carte Bleue M. Gérard NEBOUY	Le Directeur de la Division Bancaire de Gemplus M. Sami BAGHDADI	Le Directeur Chargé de la Sécurité des Systèmes d'Information M. Henri SERRES

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

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

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

Organisme de Certification
SGDN/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 de la plate-forme multi-applications GemXpresso 211 V2 constituée du microcircuit Philips P8WE5032 et de son système d'exploitation développé par Gemplus.

2 Le niveau d'assurance atteint est le niveau EAL 1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

3 Cette évaluation a pour objectif l'étude de la plate-forme multi-applications Javacard développée par Gemplus conçue pour accueillir tout type d'applications pour cartes à puce programmées en Java. Cette plate-forme se veut conforme aux spécifications Javacard 2.1 de Sun Microsystems [7] et VOP de Visa International [8 et 9].

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

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

5 Une première évaluation, portant sur la version précédente de la plate-forme GemXpresso 211, a donné lieu à un rapport de certification (2000/02) pour le même niveau d'évaluation EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante".

6 Même si une fonction d'effacement des applets a été ajoutée pour la nouvelle plate-forme, l'évaluation consiste donc en une réévaluation.

7 Cette réévaluation s'est déroulée entre juillet et septembre 2000 et a été menée consécutivement au développement du produit.

2.2 Description de la cible d'évaluation

8 La cible d'évaluation est la plate-forme multi-applications GemXpresso 211 V2 constituée du microcircuit Philips P8WE5032 (référence de masquage MPH04) et de son système d'exploitation développé par Gemplus.

2.3 Résumé des fonctions de sécurité évaluées

2.3.1 Résumé des fonctions de sécurité

9 Le détail des fonctions de sécurité évaluées résumées ci-après est disponible dans la cible de sécurité [5] :

- Protection de la plate-forme et de ses fonctions de sécurité,
- Protection des données utilisateurs (contrôle d'accès, intégrité),
- Traitement des évènements liés à la sécurité,
- Identification et authentification des utilisateurs,
- Opérations cryptographiques et gestion des clés,
- Gestion des fonctions de sécurité et des données de la plate-forme.

2.3.2 Niveau d'évaluation

10 Le niveau d'évaluation visé identifié dans la cible de sécurité [5] est le niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante".

11 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 *élémentaire* tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

2.4 Acteurs dans l'évaluation

12 Les commanditaires de l'évaluation sont le Groupement Carte Bleue et Gemplus :

Groupement Carte Bleue
21, Boulevard de la Madeleine
F-75001 Paris
France

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

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

- Gemplus pour le développement du système d'exploitation :

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

- Philips Semiconductors en tant que développeur et fabricant du composant microélectronique :

  Philips Semiconductors
  Röhen und Halbleiterwerke
  D-22502 Hamburg
  Allemagne

14 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

15 Le produit soumis à évaluation satisfait aux exigences du niveau d’évaluation EAL1 augmenté du composant d’assurance AVA_VLA.2 “Analyse de vulnérabilités indépendante”.

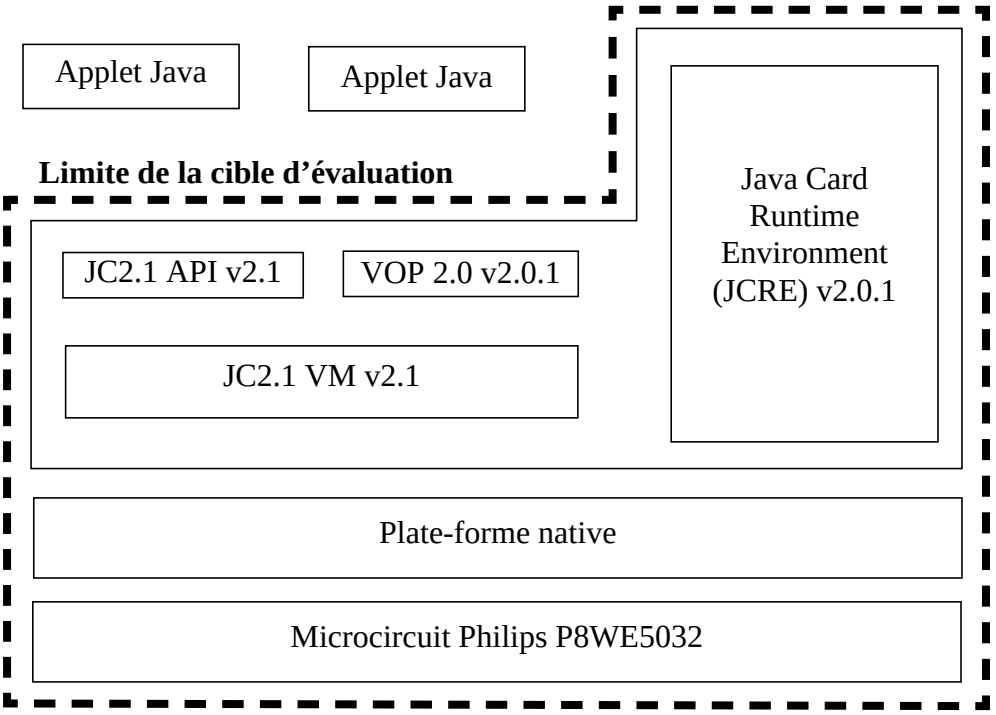
16 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

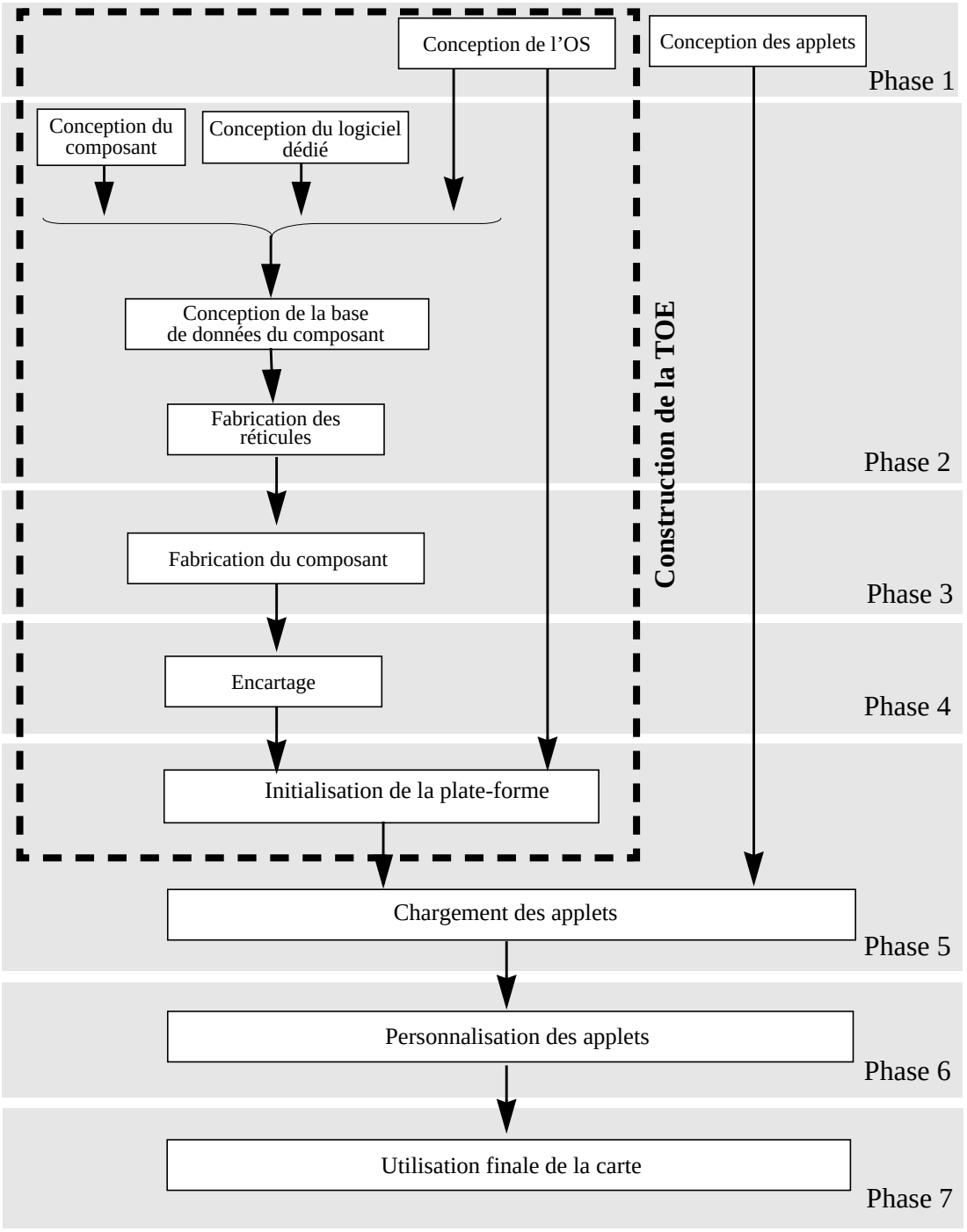
Identification de la cible d'évaluation

3.1 Architecture de la cible d'évaluation

17 La cible d'évaluation est la plate-forme multi-applications GemXpresso 211 composée du microcircuit Philips P8WE5032 (référence de masquage MPH04) et du système d'exploitation développé par Gemplus :



3.2 Cycle de vie de la cible d'évaluation



18 Le produit certifié est celui disponible après l'initialisation de la plate-forme (phase 5a).

19 Il n'existe aucune exigence fonctionnelle de sécurité particulière sur les systèmes utilisés dans la construction de la TOE (phases 1 à 5).

3.3 Description du matériel

20 Le microcircuit utilisé est le composant P8WE5032 développé et fabriqué par Philips Semiconductors.

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

22 Le support plastique ne fait pas partie de la cible d'évaluation.

3.4 Description du logiciel

23 Le système d'exploitation développé par Gemplus est constitué des deux éléments suivants :

- le logiciel fourni par Gemplus à Philips Semiconductors pour être directement masqué sur le composant (phases 2 et 3) : référence de masquage MPH04,
- le logiciel chargé sur le composant à l'initialisation de la plate-forme (phase 5a) : Card Manager AID=A000000018434D.

24 Dans le contexte de l'évaluation, l'état du système d'exploitation (Card Manager) est INITIALIZED tel qu'il est défini dans les spécifications OP et VOP de Visa International [8 et 9].

3.5 Description de la documentation

25 La documentation d'utilisation de la plate-forme GemXpresso 211 V2 certifiée est la suivante :

- Java Card 2.1 / VOP 2.0 Platform, 11/09/99, Gemplus (diffusion contrôlée) ;
- VISA Open Platform Specification v2.0, 19/04/99, Visa International ;
- VISA Open Platform Card Implementation Specification Draft, 08/03/99, Visa International ;
- VISA Open Platform Card Conformance Test Plan v2.0, 04/99, Visa International ;
- Javacard 2.1 Virtual Machine Specification v1.1, 07/06/99, Sun Microsystems ;
- Javacard 2.1 API Specification v1.1, 07/06/99, Sun Microsystems ;

- Javacard 2.1 Runtime Environment Specification v1.1, 07/06/99, Sun Microsystems.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

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

4.2 Politique de sécurité

27 Visa International et Sun Microsystems définissent un ensemble de politiques d'utilisation et d'implémentation pour les plate-formes multi-applications destinées à accueillir des applets développées en Java (Javacard [7], VOP [8 et 9]).

28 La cible d'évaluation est conforme à ces politiques de sécurité.

4.3 Menaces

29 Les menaces couvertes par la cible d'évaluation ou par les mesures prises dans son environnement sont les suivantes :

- duplication fonctionnelle du système d'exploitation (clonage),
- divulgation ou modification non autorisée des données sensibles du système d'exploitation lors de son développement ou de son exploitation,
- utilisation non autorisée des fonctions du système d'exploitation,
- accès non autorisé aux données d'une applet par une autre applet,
- divulgation ou modification des données sensibles du système d'exploitation lors des livraisons vers le fondeur, l'encarteur, le personnalisateur ou le développeur d'applets.

30 Le détail de ces menaces est disponible dans la cible de sécurité [5].

4.4 Hypothèses d'utilisation et d'environnement

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

32 Les résultats de l'évaluation sont conditionnés par le respect des hypothèses sur l'utilisation et l'environnement d'utilisation de la cible d'évaluation suivantes :

- l'implémentation des applets qui seront chargées sur la plate-forme respectent les recommandations sécuritaires de Gemplus [10],
- des outils sûrs de conversion et de vérification agréés par Sun Microsystems sont utilisés avant le chargement des applets sur la carte,
- les procédures de stockage et de livraison des cartes garantissent la sécurité des données sensibles,
- les clés sont conservées de manière sûre par les différents utilisateurs (porteurs, émetteurs) de la carte en phase d'exploitation,
- le système (terminaux, protocoles) garantit la sécurité des données traitées,
- la plate-forme est émise pour une durée maximale de 3 ans.

33 Le détail de ces hypothèses est disponible dans la cible de sécurité [5].

4.5 Fonctions de sécurité évaluées

34 Les fonctions de sécurité évaluées sont les suivantes :

4.5.1 Protection de la plate-forme et de ses fonctions de sécurité :

- Installation et effacement sûrs des applets,
- Isolation des applets,
- Observation impossible des opérations de comparaison,
- Test automatique du composant, de l'intégrité de la ROM et des paramètres d'état de la carte à chaque démarrage.

4.5.2 Protection des données utilisateurs (contrôle d'accès, intégrité) :

- Gestion des mémoires du composant,
- Contrôle d'accès aux objets Java,
- Intégrité du PIN, des clés, de l'état du système d'exploitation et de leurs paramètres,
- Compteurs de ratification lors de l'accès au PIN.

4.5.3 Traitement des évènements liés à la sécurité :

- Audit des évènements liés à la sécurité (problème d'intégrité des données d'authentification, fonctionnement hors des conditions normales de températures ou d'alimentation,...),
- Réaction face aux évènements détectés.

4.5.4 Identification et authentification des utilisateurs :

- Authentification des utilisateurs et administrateurs.

4.5.5 Opérations cryptographiques et gestion des clés :

- Fonctions cryptographiques,
- Gestion du PIN, des clés cryptographiques.

4.5.6 Gestion des fonctions de sécurité et des données de la plate-forme :

- Gestion des objets Java stockés en EEPROM et en RAM,
- Traitement des commandes envoyées par les utilisateurs à la carte,
- Gestion des paramètres de sécurité du système d'exploitation,
- Gestion des états du système d'exploitation et des applets.

35 Le détail de ces fonctions est disponible dans la cible de sécurité [5].

4.6 Tests de la cible d'évaluation

36 L'évaluateur a effectué des tests sur le produit afin de vérifier la conformité des fonctions de sécurité par rapport aux spécifications de sécurité. Conformément aux exigences du niveau EAL1, seule une partie de ces fonctions de sécurité ont été testées.

37 De plus, l'évaluateur a effectué de manière indépendante un ensemble de tests de pénétration sur le produit afin d'estimer l'efficacité des fonctions de sécurité. Ces tests de pénétration sont adaptés à la nature du produit soumis à évaluation ainsi qu'à son environnement d'exploitation supposé. Ils permettent de s'assurer que le produit évalué résiste aux attaques correspondant à un potentiel d'attaque *élémentaire* tel que défini par le composant AVA_VLA.2.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

38 Une première évaluation, portant sur la version précédente de la plate-forme GemXpresso 211, a donné lieu à un rapport de certification (2000/02) pour le même niveau d'évaluation EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante".

39 Même si la fonction d'effacement des applets a été ajoutée pour la nouvelle version de la plate-forme, l'évaluation consiste donc en une réévaluation. L'évaluateur a utilisé dans la mesure du possible les résultats d'évaluation du projet précédent consignés dans le rapport technique d'évaluation associé au certificat 2000/02 [11].

40 Les résultats de cette réévaluation sont exposés dans un nouveau rapport technique d'évaluation [6].

5.2 Résultats de l'évaluation de la cible de sécurité

41 La cible de sécurité répond aux exigences de la classe ASE, telle que définie dans la partie 3 des Critères Communs [3].

42 En raison de la modification de la cible d'évaluation (ajout de la fonction de sécurité d'effacement des applets, modification de la fonction d'authentification des administrateurs), une nouvelle évaluation de la cible de sécurité a eu lieu.

5.2.1 ASE_DES.1 : Description de la TOE

43 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 [3].

44 La cible d'évaluation est la plate-forme multi-applications GemXpresso 211 V2 composée du microcircuit Philips P8WE5032 (référence de masquage MPH04) et de son logiciel embarqué développé par Gemplus.

45 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

46 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 [3].

47 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 [5].

5.2.3 ASE_INT.1 : Introduction de la ST

48 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 [3].

49 L'introduction de la cible de sécurité [5] 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

50 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 [3].

51 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrites dans la cible de sécurité [5].

5.2.5 ASE_PPC.1 : Annonce de conformité à un PP

52 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 [3].

53 La cible de sécurité [5] ne revendique pas de conformité à un profil de protection.

5.2.6 ASE_REQ.1 : Exigences de sécurité des TI

54 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 [3].

55 Les exigences de sécurité fonctionnelles ou d'assurance de la cible d'évaluation sont décrites dans la cible de sécurité [5].

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

56 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 [3].

57 La cible de sécurité [5] ne contenant pas d'exigence de sécurité spécifiée explicitement, cette tâche n'est pas applicable.

5.2.8 ASE_TSS.1.1 : Spécifications globales de la TOE

58 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 [3].

59 La cible de sécurité [5] contient les spécifications globales des fonctions de sécurité du produit ainsi que les mesures d'assurance prises pour satisfaire les exigences d'assurance de la TOE. L'évaluateur s'est assuré que ces fonctions de sécurité sont une représentation correcte des exigences fonctionnelles de sécurité de la TOE et que les mesures d'assurance prises couvrent les exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante".

5.3 Résultats de l'évaluation du produit

60 Le produit répond aux exigences des Critères Communs pour le niveau EAL1 augmenté du composant AVA_VLA.2 "Analyse de vulnérabilités indépendante".

5.3.1 ADV_FSP.1 : Spécifications fonctionnelles informelles

61 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 [3].

62 Le développeur a fourni une nouvelle documentation uniquement pour les fonctions de sécurité du produit ajoutées ou modifiées depuis l'évaluation initiale. Les interfaces externes y sont également décrites.

63 L'évaluateur a de nouveau examiné l'ensemble des spécifications et montré pour le niveau d'évaluation 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

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

65 Le développeur n'a fourni qu'un complément de documentation indiquant la correspondance entre la nouvelle fonction de sécurité d'effacement des applets telle qu'elle est définie dans les spécifications fonctionnelles (ADV_FSP) et la cible de sécurité (ASE_TSS). L'évaluateur s'est assuré de cette correspondance.

5.3.3 ACM_CAP.1 : Numéros de version

66 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 [3].

67 La cible d'évaluation est la plate-forme multi-applications GemXpresso 211 V2 composée du microcircuit Philips P8WE5032 (référence de masquage MPH04) et de son logiciel embarqué développé par Gemplus.

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

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

69 Les procédures d'installation et de génération du produit portent sur les phases de chargement et d'initialisation du Card Manager de la plate-forme.

70 Les procédures de démarrage du produit portent sur la réponse au "reset" de la carte.

71 Les procédures d'initialisation de la plate-forme ayant été modifiées, l'évaluateur les a de nouveau évaluées.

5.3.5 AGD_ADM.1 : Guide de l'administrateur

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

73 La documentation d'administration contient les informations relatives aux commandes d'administration de la plate-forme (chargement, effacement d'applets, prépersonnalisation de la plate-forme).

74 L'évaluateur s'est assuré que l'ajout ou la modification des fonctions de sécurité ont correctement été prises en compte dans la documentation et qu'elle ne remettent pas en cause l'administration sûre du produit.

5.3.6 AGD_USR.1 : Guide de l'utilisateur

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

76 La documentation d'utilisation contient les informations relatives à la mise en oeuvre des fonctions de sécurité de la cible d'évaluation accessibles aux développeurs d'applets, sous forme de pointeurs précis vers les spécifications Javacard de Sun [7] et VOP de Visa [8 et 9].

77 La documentation d'utilisation inclut également les recommandations de sécurité de programmation fournies par Gemplus aux développeurs d'applets pour la plate-forme GemXpresso 211 V2 [10].

78 Comme pour la documentation d'administration, l'évaluateur s'est assuré que l'ajout ou la modification des fonctions de sécurité ont correctement été prises en compte dans la documentation et qu'elle ne remettent pas en cause l'utilisation sûre du produit.

5.3.7 ATE_IND.1 Tests indépendants - conformité

79 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 [3].

80 L'évaluateur a effectué des tests sur le produit afin de vérifier la conformité des fonctions de sécurité par rapport aux spécifications de sécurité. Conformément aux exigences du niveau EAL1, seul un échantillon représentatif de ces fonctions de sécurité ont été testées.

81 La nouvelle fonction de sécurité d'effacement des applets a été testée. Pour les autres fonctions, des tests fonctionnels de non-régression ont été réalisés suivant la même méthode d'échantillonnage que pour l'évaluation précédente.

5.3.8 AVA_VLA.2 : Analyse de vulnérabilités indépendante

82 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 [3].

83 L'évaluateur a réalisé des tests de pénétration indépendants, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit résiste aux attaques correspondant à un potentiel de l'attaquant *élémentaire* tel que défini par le composant AVA_VLA.2.

84 De nouveaux tests de pénétration ont été mis en oeuvre pour analyser la nouvelle fonction de sécurité d'effacement des applets. Pour les autres fonctions, une partie des tests de pénétration de l'évaluation précédente ont été de nouveau réalisés.

5.3.9 Verdicts

85 Pour tous les aspects des Critères Communs identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 6

Recommandations d'utilisation

86 Le produit "Plate-forme Javacard/VOP GemXpresso 211 V2" 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 [5],

- Les règles du guide de programmation [10] pour les applets installées sur la plate-forme GemXpresso 211 V2 doivent être impérativement respectées.

  Les règles à respecter sont notamment les suivantes :

  - ne pas inclure de composant *export*,
  - ne pas utiliser d'objets partagés (composant *shared*),
  - ne pas définir de champs ou de méthodes en *public static*,
  - ne faire qu'une instance par applet,
  - ne pas étendre les classes de l'API Java Card portant sur l'intégrité des données (composant *expand*),
  - utiliser les données *transient* à bon escient.

- Les développeurs d'applets doivent utiliser des outils de génération et de vérification du code des applets, agréés par Sun Microsystems.

- L'établissement d'un lien sécurisé entre le développeur d'applets et l'entité responsable du chargement des applets est nécessaire.

Chapitre 7

Certification

7.1 Objet

87 Le produit dont les caractéristiques de sécurité sont définies dans la cible de sécurité [5], satisfait aux exigences du niveau d'évaluation EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante".

88 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 *élémentaire* tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

7.2 Portée de la certification

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

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

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

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Card Manager	Élément du système d'exploitation responsable de la gestion des applets et du cycle de vie de la plate-forme.
Chargeur	Industriel responsable du chargement des applets sur une plate-forme multi-applications.
Cible d'évaluation (TOE)	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité (ST)	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Logiciel embarqué	Logiciel présent sur une puce.
Masque	Ensemble d'instructions organisées, reconnaissables et exécutables par le processeur d'un microcircuit électronique.
Niveau d'assurance de l'évaluation	Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des 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 de la carte.
Produit	Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection (PP)	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

Références

[1] [CC-1] Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information Partie 1: Introduction et modèle général CCIB-99-031, version 2.1 Août 1999.

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

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

[4] [CEM] Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0 August 1999.

[5] Cible de sécurité, référence: MUSE2-ST.000609 version 2.2 (document public).

[6] Rapport technique d'évaluation RTE_MUSE2 v1.0, Serma Technologies (diffusion contrôlée).

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

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

[9] Visa Open Platform Card Implementation Specification, mars 1999, Visa International.

[10] Java Card 2.1 / VOP 2.0 Platform, 11/09/99, Gemplus (diffusion contrôlée).

[11] Rapport technique d'évaluation RTE_MUSE v1.0, Serma Technologies (diffusion contrôlée).