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 2000/02

Plate-forme Javacard/VOP GemXpresso 211
(microcircuit Philips P8WE5032/MPH02)

Mai 2000

Ce document constitue le rapport de certification du produit "Plate-forme Javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02)".

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 2000/02

Plate-forme Javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02)

Développeurs :
Philips Semiconductors ; Gemplus

EAL1 augmenté

Commanditaires :

Groupement Carte Bleue
Gemplus

Le 17 mai 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 2.0 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
SGDN/SCSSI
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

Chapitre 1

Introduction

1 Ce document représente le rapport de certification de la plate-forme multi-applications GemXpresso 211 constituée du microcircuit Philips P8WE5032 et de son logiciel embarqué 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 [4].

3 Cette évaluation, partie du projet Vocable mené par le Groupement Carte Bleue et Visa International, a pour objectif d'étudier la sécurité offerte par 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 est conforme aux spécifications Javacard 2.1 de Sun Microsystems [8] et VOP de Visa International [9 et 10] à l'exception de la fonctionnalité d'effacement d'applet qui n'est pas disponible pour le produit certifié.

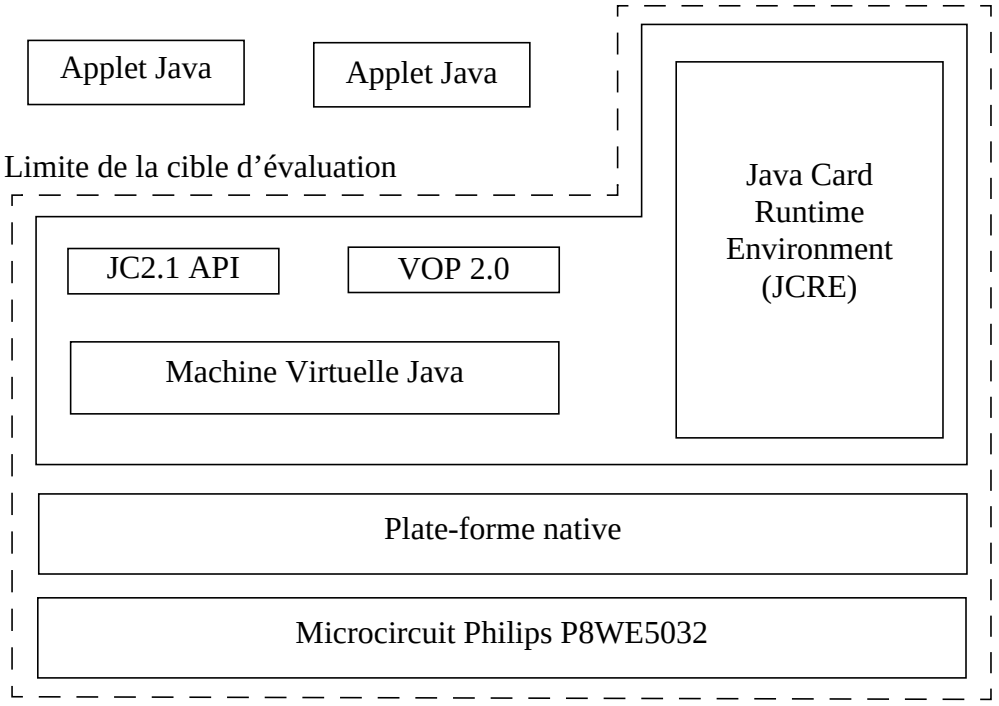
Chapitre 2

Résumé

2.1 Description de la cible d'évaluation

4 La cible d'évaluation est la plate-forme multi-applications GemXpresso 211 constituée du microcircuit Philips P8WE5032 (référence de masquage MPH02) et de son logiciel embarqué développé par Gempus.

5 La cible d'évaluation est composée des éléments suivants :



2.2 Résumé des caractéristiques de sécurité

2.2.1 Menaces

6 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,

- modification ou divulgation d'informations sensibles lors de l'utilisation de la plate-forme.

2.2.2 Politiques de sécurité organisationnelles

7 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 et des fonctionnalités de la plate-forme aux spécifications Javacard [8] et VOP [9 et 10].

2.2.3 Hypothèses

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

- les applets qui seront chargées sur la plate-forme doivent être développées et utilisées de manière sûre,
- des outils sûrs de conversion et de vérification des applets doivent être utilisés avant le chargement des applets sur la carte,
- les clés doivent être conservées de manière sûre par les différents utilisateurs (porteurs, émetteurs) de la carte en phase d'exploitation,
- le système (terminaux, protocoles) doit garantir la sécurité des données traitées,
- la carte doit être émise dans un délai maximal de 3 ans.

2.2.4 Exigences fonctionnelles de sécurité

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

- protection de la plate-forme et de ses fonctions de sécurité (résistance aux attaques physiques, séparation des domaines, auto-test),
- protection des données utilisateurs (contrôle d'accès, intégrité),
- détection d'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.

2.2.5 Exigences d'assurance

10 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 indépendante".

2.3 Acteurs dans l'évaluation

11 Les commanditaires de l'évaluation sont le Groupement Carte Bleue, et son sous-traitant Trusted Logic, et Gemplus :

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

TRUSTED LOGIC
5, Rue du Baillage
F-78000 Versailles
France

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

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

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

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

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

  PHILIPS Semiconductors
  Röhen und Halbleiterwerke
  D-22502 Hamburg
  Allemagne.

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 entre janvier et mars 2000 et a été menée consécutivement au développement du produit.

15 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

16 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”.

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

18 Les vulnérabilités connues des commanditaires de l’évaluation ont été toutes communiquées à l’évaluateur et au certificateur conformément au critère [AVA_VLA.2.4E].

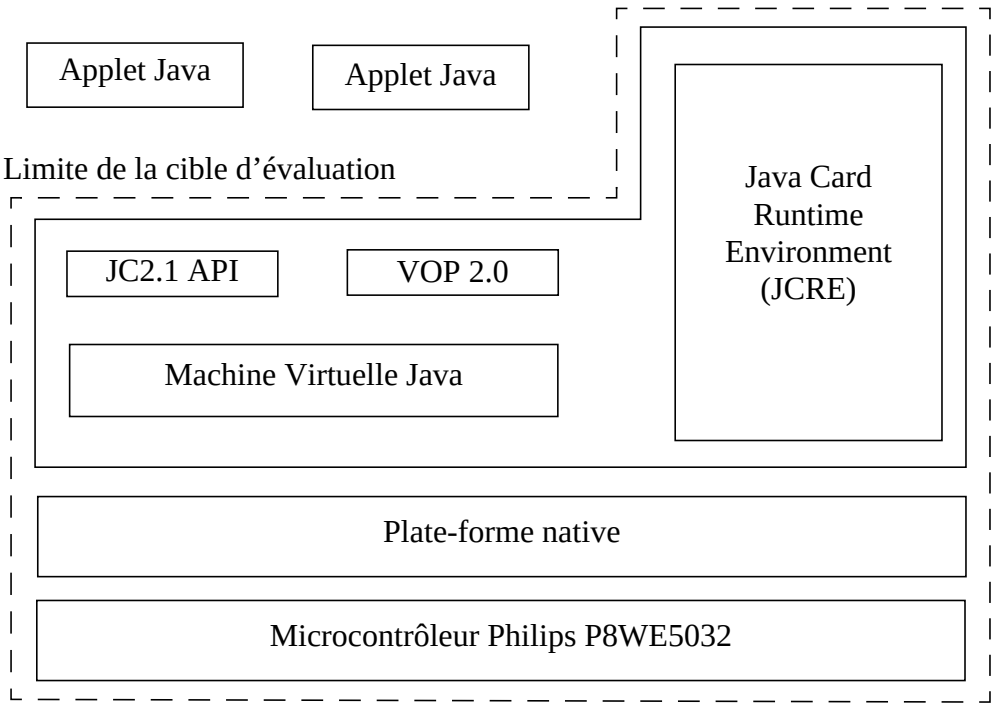
19 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

Identification de la cible d'évaluation

3.1 Objet

20 La cible d'évaluation est la plate-forme multi-applications GemXpresso 211 composée du microcircuit Philips P8WE5032 (référence de masquage MPH02) et de son logiciel embarqué développé par Gemplus :

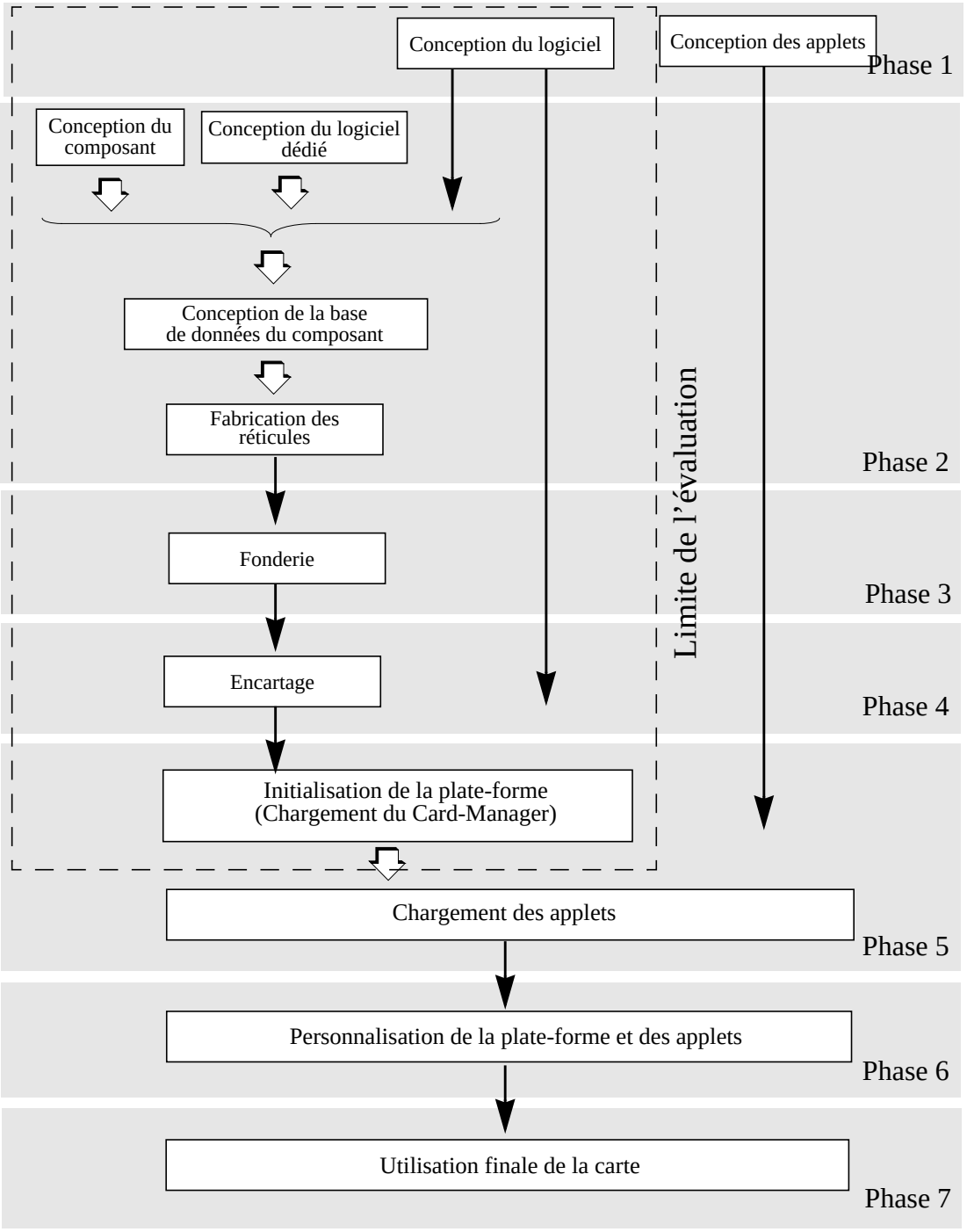


21 La carte soumise à évaluation ne supporte pas l'effacement d'applets (partiel ou total).

22 La vérification du code généré par les outils de développement des applets est hors du périmètre d'évaluation.

23 La configuration exacte de la cible d'évaluation est décrite en annexe A.

3.2 Cycle de vie de la cible d'évaluation



3.3 Description du matériel

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

25 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

26 Le logiciel embarqué développé par Gemplus est constitué des éléments suivants :

- le logiciel masqué sur le composant (phases 2 et 3),
- le Card Manager chargé en phase 5a,

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

27 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [6] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Politique de sécurité

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

29 Ces spécifications sont intégralement respectées pour le produit certifié à l'exception de la fonction d'effacement d'applets.

4.3 Menaces

30 Les menaces effectivement couvertes par le produit sont décrites dans le chapitre 3 de la cible de sécurité [6].

31 Ces menaces portent sur les points suivants :

- duplication fonctionnelle de la carte,
- divulgation non autorisée des biens de la plate-forme,
- vol ou utilisation non autorisée des biens de la plate-forme,
- modification non autorisée des biens de la plate-forme,
- modification ou divulgation des biens de la plate-forme lors des livraisons vers le fondeur, l'encarteur, le personnalisateur ou le développeur d'applets.

4.4 Hypothèses d'utilisation et d'environnement

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

33 Les hypothèses d'utilisation et d'environnement du produit sont consignées dans le chapitre 3 de la cible de sécurité [6].

34 Ces hypothèses portent sur les points suivants :

- les applets qui seront chargées sur la plate-forme doivent être développées et utilisées de manière sûre,
- des outils sûrs de conversion et de vérification doivent être utilisés avant le chargement des applets sur la carte,
- les procédures utilisées lors des livraisons doivent garantir la sécurité des données livrées,
- les clés doivent être conservées de manière sûre par les différents utilisateurs (porteurs, émetteurs) de la carte en phase d'exploitation,
- le système (terminaux, protocoles) doit garantir la sécurité des données traitées,
- la carte doit être émise dans un délai maximal de 3 ans.

4.5 Architecture du produit

35 Le détail de l'architecture du produit n'étant pas fourni à l'évaluateur pour les évaluations de niveau EAL1, les seules informations disponibles sont celles présentes dans la cible de sécurité [6].

4.6 Description de la documentation

36 La documentation disponible est référencée en annexe A du présent rapport de certification.

4.7 Tests de la cible d'évaluation

37 L'évaluateur a effectué des tests sur le produit afin de vérifier la conformité des fonctions de sécurité par rapport aux spécifications de sécurité. La procédure d'échantillonnage des fonctions testées a été jugée conforme aux exigences du niveau d'évaluation EAL1.

38 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. Ils permettent de s'assurer que le produit évalué resiste aux attaques correspondant à un potentiel d'attaque élémentaire tel que défini par le composant AVA_VLA.2.

4.8 Configuration évaluée

39 La configuration exacte de la cible d’évaluation est décrite en annexe A.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

40 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

41 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

42 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].

43 La cible d'évaluation (TOE) est la carte "Plate-forme Javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02)".

44 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

45 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].

46 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].

5.2.3 ASE_INT.1 : Introduction de la ST

47 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].

48 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

49 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].

50 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrites dans la cible de sécurité [6].

5.2.5 ASE_PPC.1 : Annonce de conformité à un PP

51 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].

52 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

53 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].

54 Les exigences de sécurité fonctionnelles ou d'assurance de la cible d'évaluation sont décrites dans la cible de sécurité [6].

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

55 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].

56 La cible de sécurité [6] 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

57 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].

58 La cible de sécurité [6] contient les spécifications globales 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

59 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

60 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].

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

62 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

63 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].

64 Le développeur a fourni une documentation indiquant la correspondance entre les fonctions de sécurité telles qu'elles sont définies dans les spécifications fonctionnelles (ADV_FSP) et la cible de sécurité (ASE_TSS). L'évaluateur s'est assuré que les spécifications fonctionnelles correspondent à une image complète et cohérente des fonctions de sécurité décrites dans la cible de sécurité.

5.3.3 ACM_CAP.1 : Numéros de version

65 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].

66 Le produit évalué est la plate-forme Gemplus GemXpresso 211 constituée du microcircuit Philips P8WE5032 (référence de masquage MPH02) et du logiciel embarqué développé par Gemplus. Le détail des numéros de version est disponible à l'annexe A.

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

67 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].

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

5.3.5 AGD_ADM.1 : Guide de l'administrateur

69 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].

70 La documentation d'administration contient les informations relatives aux commandes d'administration (initialisation du Card Manager, chargement d'applets) de la plate-forme.

5.3.6 AGD_USR.1 : Guide de l'utilisateur

71 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].

72 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 [8] et VOP de Visa [9 et 10].

73 La documentation d'utilisation inclut également les recommandations de programmation de Gemplus à l'intention des développeurs d'applets pour la plate-forme GemXpresso 211 [11].

5.3.7 ATE_IND.1 Tests indépendants - conformité

74 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].

75 L'évaluateur a effectué des tests sur le produit afin de vérifier la conformité des fonctions de sécurité par rapport aux spécifications de sécurité. La procédure d'échantillonnage des fonctions testées a été jugée conforme aux exigences du niveau d'évaluation EAL1.

5.3.8 AVA_VLA.2 : Analyse de vulnérabilités indépendante

76 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].

77 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. Ces tests de pénétration ont porté 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

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

Chapitre 6

Recommandations d'utilisation

79 Le produit "Plate-forme Javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02)" 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],

- Les règles du guide de programmation [11] pour les applets installées sur la plate-forme GemXpresso 211 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

80 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 indépendante".

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

7.2 Portée de la certification

82 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.

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

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

Annexe A

Configuration de la cible d'évaluation

85 La cible d'évaluation est la plate-forme multi-applications GemXpresso 211 composée du microcircuit Philips P8WE5032 (référence de masquage MPH02) et de son logiciel embarqué développé par Gemplus.

86 Elle est constituée des éléments suivants :

Composant	Version
JC2.1 VM	1.1
JC2.1 API	1.1
VOP 2.0	1.1
JCRE	1.0
Plate-forme native	1.1
Microcircuit Philips	P8WE5032 (référence de masquage MPH02)

87 L'état du Card Manager est INITIALIZED tel que défini dans la cible de sécurité [6].

88 La documentation disponible pour le produit est la suivante :

- Java Card 2.1 / VOP Platform, 08/09/99, Gemplus (diffusion limitée).
- 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 ;

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.
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.
Encarteur	Industriel insérant un composant masqué dans un support plastique au format d'une carte.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Fondeur	Industriel fabriquant des microcircuits.
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 A

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] Cible de sécurité, référence: MUSE-ST.990009 (document public).

[7] Rapport technique d'évaluation (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] Java Card 2.1 / VOP Platform, 08/09/99, Gemplus (document à diffusion limitée)