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 2001/03

Applications Oberthur B0' v1.0.1 et GemClub v1.3

chargées sur la plate-forme Javacard/VOP GemXpresso 211 V2

Janvier 2001

Ce document constitue le rapport de certification du produit “Applications Oberthur B0’ v1.0.1 et GemClub v1.3 chargées sur la plate-forme Javacard/VOP GemXpresso 211 V2”.

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 :

Secrétariat général de la défense nationale
SCSSI
Centre de Certification de la Sécurité des Technologies de l’Information
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: ssi20@calva.net

Ce document est folioté de 1 à 22 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

CERTIFICAT 2001/03

Applications Oberthur B0' v1.0.1 et GemClub v1.3

chargées sur la plate-forme Javacard/VOP GemXpresso 211 V2

Développeurs : Oberthur Card Systems, Gemplus, Trusted Logic

EAL1 Augmenté

Commanditaire : Groupement Carte Bleue

Le 9 février 2001,

Le Commanditaire :
L'Administrateur du Groupement Carte Bleue

M. Gérard NEBOUY

L'Organisme de certification :
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 :
Secrétariat général de la défense nationale
SCSSI
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

IT Security Certified

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification des applications Oberthur B0' v1.0.1 et GemClub v1.3 chargées sur la plate-forme Javacard/VOP GemXpresso 211 V2.

2 Le niveau d'assurance atteint est le niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

3 La cible d'évaluation est constituée des applications Oberthur B0' v1.0.1 et GemClub v1.3. Pour l'évaluation, ces deux applications sont installées sur la plate-forme GemXpresso 211 V2 développée par Gemplus et précédemment certifiée [8] au même niveau d'assurance.

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 avec d'autres applications sur une seule et unique carte.

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 Elle s'est déroulée consécutivement au développement du produit en décembre 2000 et janvier 2001.

6 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

TRUSTED LOGIC
5 Rue du Baillage
F-78000 Versailles

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

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

  OBERTHUR CARD SYSTEMS
  25 rue Auguste Blanche
  BP 133
  F-92800 Puteaux

- Gemplus et Trusted Logic pour le développement de l'application GemClub :

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

  TRUSTED LOGIC
  5 Rue du Baillage
  F-78000 Versailles

8 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

2.2 Description de la cible d'évaluation

9 La cible d'évaluation est constituée des applications Oberthur B0' v1.0.1 et GemClub v1.3.

10 L'application Oberthur B0' est une application de débit/crédit destinée à être utilisée dans le système "Cartes Bancaires" et programmée en java.

11 L'application GemClub est une application de fidélité. Elle est en fait constituée des trois applets suivantes :

- GemClub Applet v1.3 développée par Gemplus en java,
- GemClub Proxy v1.0 développée par Trusted Logic en java,
- Reader Interface v1.0 développée par Trusted Logic également en java.

12 Pour l'évaluation, ces applications sont installées sur la plate-forme GemXpresso 211 V2 développée par Gemplus et précédemment certifiée [8] au niveau d'assurance EAL1 augmenté. La plate-forme GemXpresso 211 V2 est hors du périmètre de la présente évaluation.

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

- Isolation de l'application B0',
- Contrôle d'accès aux informations de l'application B0' stockées en mémoire,
- Irréversibilité des phases de vie de l'application B0',
- Traçabilité des opérations sur l'application B0',
- Authentification des utilisateurs et administrateurs de l'application B0',
- Authentification des données utilisées par l'application B0',
- Réaction aux conditions anormales de fonctionnement de l'application B0'.

2.3 Conclusions de l'évaluation

14 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" défini dans la partie 3 des Critères Communs [3].

15 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.

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

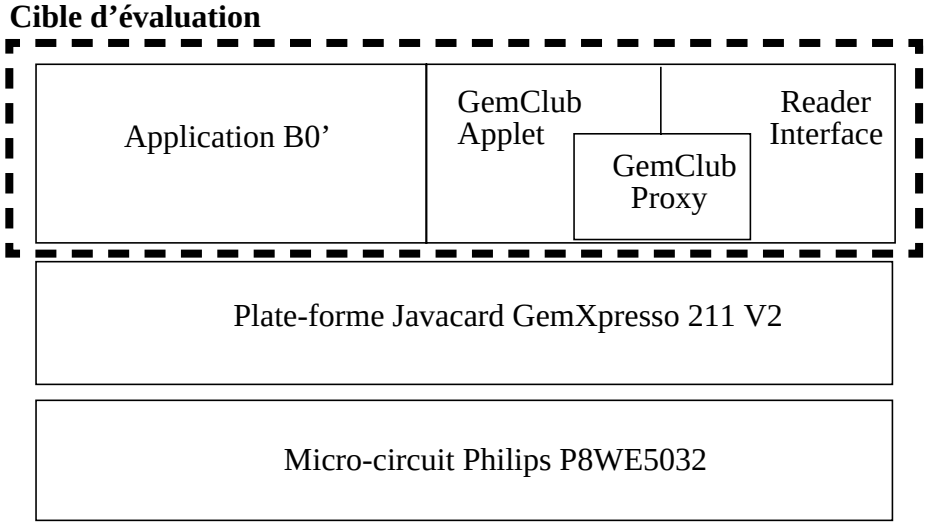
3.1 Objet

17 Les applications évaluées sont destinées à cohabiter sur une unique carte à puce.

18 L'application Oberthur B0' v1.0.1 sera utilisée pour les opérations de paiement et de retrait comme toute autre carte du système Cartes Bancaires.

19 L'application GemClub, constituée des applets GemClub Applet v1.3, GemClub Proxy v1.0 et Reader Interface v1.0, est destinée à être utilisée pour des applications diverses de fidélité.

20 Pour l'évaluation, ces applications sont installées sur la plate-forme GemXpresso 211 V2 développée par Gemplus et précédemment certifiée [8]. La plate-forme est hors du périmètre de la présente évaluation.



21 La version précédente de l'application Oberthur B0' avait été certifiée avec la version précédente de la plate-forme GemXpresso 211 [7]. La ré-évaluation de ces deux éléments s'est déroulée en deux phases : premièrement la ré-évaluation de la plate-forme GemXpresso 211 V2 ayant abouti au certificat 2000/06 et, dans un deuxième temps la ré-évaluation de l'application Oberthur B0', objet du présent rapport de certification.

3.2 Historique du développement

22 L'application Oberthur B0' v1.0.1 est développée par Oberthur Card Systems.

23 L'application GemClub v1.3 est développée par Gemplus et Trusted Logic pour le groupement Carte Bleue.

24 Ces deux applications sont destinées à être chargées sur une plate-forme multi-applicative de type Javacard.

3.3 Description des matériels

25 La cible d'évaluation ne comprend pas d'élément matériel.

3.4 Description des logiciels

26 La cible d'évaluation est uniquement composée des logiciels suivants :

a) Oberthur B0' v1.0.1 conforme aux spécifications B4/B0' V2 du GIE Cartes Bancaires,

b) GemClub Applet v1.3,

c) GemClub Proxy v1.0,

d) Reader Interface v1.0.

3.5 Description de la documentation

27 La documentation disponible est constituée essentiellement des documents émis par le GIE Cartes Bancaires pour l'utilisation des cartes de type B0'.

28 Les documents disponibles sont les suivants :

- Documentation d'utilisation v1.0, réf. CBX4 du 6/06/99 et Documentation d'administration v1.0, réf. CBX6 du 26/06/99 pour l'application B0' ;

- GemClub Core Reference Manual v1.0, mars 2000 pour l'application GemClub.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

29 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.

30 Dans le cadre de cette évaluation, l'application GemClub ne met pas en oeuvre de fonction de sécurité. Les seuls biens à protéger sont les biens de l'application de B0'.

4.2 Hypothèses

31 La cible d'évaluation doit être utilisée dans un environnement qui satisfait aux hypothèses énoncées dans la cible de sécurité [5].

32 Ces hypothèses couvrent les aspects suivants :

- utilisation d'outils sûrs de conversion et de vérification des applets avant leur chargement sur la carte,
- gestion sûre des clés et des codes porteurs (PIN) par les porteurs et émetteurs des cartes,
- procédures de livraison sûre des cartes en phase d'exploitation.

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

4.3 Menaces

34 Les biens à protéger au sein de la cible d'évaluation sont les suivants :

- les données sensibles utilisées par l'application B0' et que celle-ci doit protéger,
- les applets elles-même qui doivent être protégées par la plate-forme sur laquelle elles sont installées.

35 Les menaces couvertes par la cible d'évaluation ou par son environnement sont celles définies dans la cible de sécurité [5]. Elles peuvent être résumées comme suit :

- menaces sur la carte complète (manque d'étanchéité entre les applets, modification du code des applets,...),
- divulgation ou modification des biens de l'application B0',

- répudiation des transactions de B0',
- menaces liées au cycle de vie de B0',
- divulgation ou modification des applets lors de leur livraison au responsable du chargement sur la carte.

4.4 Politiques de sécurité organisationnelles

36 Les politiques de sécurité organisationnelles que doit respecter la cible d'évaluation et son environnement sont celles définies dans la cible de sécurité [5]. Elles peuvent être résumées comme suit :

- respect des règles d'usage du GIE Cartes Bancaires à destination des utilisateurs et personnalisation de cartes bancaires B0',
- respect des règles de programmation Java Card 2.1 et issue de l'évaluation de la plate-forme GemXpresso 211 V2,
- utilisation de terminaux et de protocoles sûrs de communication avec la carte,
- mise en place de procédures empêchant le chargement d'applets non autorisées.

4.5 Fonctions de sécurité évaluées

37 La liste des fonctions de sécurité évaluées est disponible dans la cible de sécurité [5]. Ces fonctions de sécurité peuvent être résumées comme suit :

- Isolation de l'application B0',
- Contrôle d'accès aux informations de l'application B0' stockées en mémoire,
- Irréversibilité des phases de vie de l'application B0',
- Traçabilité des opérations sur l'application B0',
- Authentification des utilisateurs et administrateurs de l'application B0',
- Authentification des données utilisées par l'application B0',
- Réaction aux conditions anormales de fonctionnement de l'application B0'.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

38 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [6].

5.2 Principaux résultats de l'évaluation

39 Le produit répond aux exigences des Critères Communs pour le niveau EAL1 augmenté du composant AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrits dans la partie 3 des Critères Communs [3].

40 Les modifications de l'application B0' précédemment certifiée [7] n'ayant pas d'impact sur les fonctions de sécurité, une partie des travaux d'évaluation n'a pas été de nouveau réalisée.

5.2.1 ASE : Evaluation de la cible de sécurité

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

42 La cible de sécurité [5] rassemble l'ensemble des caractéristiques de sécurité de la cible d'évaluation. Ces caractéristiques sont résumées au chapitre 4 du présent rapport de certification.

43 La cible de sécurité contient un résumé des spécifications des fonctions de sécurité du produit ainsi que les mesures d'assurance prises pour satisfaire les exigences d'assurance du niveau EAL1 augmenté.

5.2.2 ADV_FSP.1 : Spécifications fonctionnelles informelles

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

45 Les modifications apportées à l'application Oberthur B0' n'ayant pas d'impact sur les fonctions de sécurité à évaluer, les spécifications fonctionnelles utilisées pour le certificat 99/07 ont pu être intégralement reprises.

46 Les tâches d'évaluation réalisées et les verdicts correspondant restent donc valables.

5.2.3 ADV_RCR.1 : Démonstration de correspondance informelle

47 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].

48 La correspondance entre les fonctions de sécurité identifiées dans la cible de sécurité [5] et les spécifications fonctionnelles est assurée par la reprise intégrale des fonctions dans les spécifications.

5.2.4 ACM_CAP.1 : Numéros de version

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

50 La cible d'évaluation est uniquement composée des éléments suivants :

- applet Oberthur B0' v1.0.1,
- applet GemClub Applet v1.3,
- applet GemClub Proxy v1.0,
- applet Reader Interface v1.0.

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

51 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].

52 Les procédures d'installation, de génération et de démarrage de la cible d'évaluation portent sur les phases de chargement et de personnalisation des applets sur la plate-forme GemXpresso 211 V2.

53 Les tâches d'évaluation réalisées dans le cadre du certificat 99/07 et les verdicts correspondants restent valables.

5.2.6 AGD_ADM.1 : Guide de l'administrateur

54 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].

55 Les administrateurs déclarés de la cible d'évaluation sont les émetteurs des cartes et leurs délégataires. Les documents d'administration sont constitués des guides du GIE Cartes Bancaires pour l'administration de l'application B0'.

56 Les tâches d'évaluation réalisées dans le cadre du certificat 99/07 et les verdicts correspondants restent valables.

5.2.7 AGD_USR.1 : Guide de l'utilisateur

57 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].

58 Les utilisateurs déclarés de la cible d'évaluation sont les porteurs de cartes bancaires. Les documents d'utilisation sont constitués des guides du GIE Cartes Bancaires pour l'utilisation des cartes B0'.

59 Les tâches d'évaluation réalisées dans le cadre du certificat 99/07 et les verdicts correspondants restent valables.

5.2.8 ATE_IND.1 : Tests Indépendants - Conformité

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

61 Même si les modifications de l'application Oberthur B0' n'ont pas d'impact sur les fonctions de sécurité à évaluer, l'intégralité des tests fonctionnels réalisés pour le certificat a été rejouée pour s'assurer du fonctionnement correct de la cible d'évaluation.

5.2.9 AVA_VLA.2 : Analyse de vulnérabilités indépendante

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

63 Les modifications de l'application Oberthur B0' n'ayant pas d'impact sur les fonctions de sécurité à évaluer, l'analyse de vulnérabilités réalisée par l'évaluateur pour le certificat 99/07 reste valable.

64 Toutefois, l'évaluateur a réalisé de nouveau une partie des tests de pénétration pour s'assurer qu'aucune vulnérabilité exploitable n'existe pour un niveau d'attaque élémentaire.

5.2.10 Verdicts

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

Chapitre 6

Certification

Recommandations d'utilisation

66 La cible d'évaluation "applications Oberthur B0' v1.0.1 et GemClub v1.3 chargées sur la plate-forme Javacard/VOP GemXpresso 211 V2" est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

a) Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [5],

b) le chargement, l'installation et l'effacement des applets doivent être réalisés dans un environnement sûr et par du personnel de confiance,

c) 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 porteur (PIN) qui lui est fourni avec sa carte.

Chapitre 7

Certification

7.1 Objet

67 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

68 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

69 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.

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

71 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.
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	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.
Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Produit	Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

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] Méthodologie commune l'évaluation de la sécurité des technologies de l'information Partie 2 : Méthodologie d'évaluation CEM-99/045, version 1.0 Août 1999.

[5] Cible de sécurité, réf. VOCA/ASTRE2/ST v1.0, 30 janvier 2001.

[6] Rapport Technique d'Évaluation, réf. RTE_ASTRE2 v1.0 (diffusion contrôlée).

[7] Rapport de Certification 99/07 "Plate-forme Javacard/VOP GemXpresso 211 (micro-circuit Philips P8WE5032/MPH02) avec applets Oberthur B0' v0.32 et Visa VSDC v1.08", niveau EAL1 augmenté, décembre 1999.

[8] Rapport de Certification 2000/06 "Plate-forme Javacard/VOP GemXpresso 211 V2 (Composant masqué Philips P8WE5032/MPH04, Card Manager A000000018434D)", niveau EAL1 augmenté, octobre 2000.