PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale 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 2002/04

Gem CB-B0'/EMV :

Composant P8WE6004 V0D masqué par l'application MPH021
(référence : P8WE6004 V0D/C017D)

Avril 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

CERTIFICAT 2002/04

Gem CB-B0'/EMV :

Composant P8WE6004 V0D masqué par l'application MPH021
(référence : P8WE6004 V0D/C017D)
Développeurs : Philips Semiconductors, Gemplus

Critères Communs
EAL4 Augmenté

conforme au profil de protection PP/9911

Commanditaire : Gemplus
Centre d'évaluation : Serma Technologies

Le 22 avril 2002,

Le Directeur central de la sécurité
des systèmes d'information
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, Direction centrale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Chapitre 1

Résumé

1.1 Objet

1 Ce document est le rapport de certification du produit Gem CB B0'/EMV. Ce rapport doit être accompagné de la cible de sécurité du produit [ST].

2 Ce produit est une carte à microprocesseur P8WE6004 V0D sur laquelle est masquée le logiciel MPH021 incluant les applications bancaires B0' et EMV conformément aux recommandations du GIE Cartes Bancaires ; la référence du produit est P8WE6004 V0D/C017D. Le produit est conforme aux exigences du profil de protection PP/9911 «Smart Card Integrated Circuit with Embedded Software v2.0» [PP9911].

3 Le certificat de ce produit s'appuie sur le certificat du micro-circuit «Philips P8WE6004 V0D Secure 8-bit Smart Card Controler» émis par le BSI le 8 mars 2002 sous la référence : BSI-DSZ-CC-0170-2002 [BSI]. Ce certificat atteste que le micro-circuit P8WE6004 V0D atteint le niveau EAL 5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 et qu'il est conforme au profil de protection PP/9806 «Smartcard Integrated Circuit Protection Profile v2.0» [PP9806]. La validité de ce certificat est reconnue par le schéma français en vertu de l'accord de reconnaissance du SOG-IS [SOG-IS].

4 Les développeurs de la cible d'évaluation sont :

- pour le micro-circuit (P8WE6004 V0D) :

  - Philips Semiconductors GmbH
    Stresemannallee 101
    22529 Hamburg
    Allemagne ;

- pour le masque (MPH021) :

  - Gemplus
    Parc d'activités de Gémenos
    13881 Gémenos Cedex
    France.

5 L'évaluation a été menée conformément aux Critères Communs [CC] et à la méthodologie définie dans le manuel CEM [CEM].

6 Le niveau atteint par cette évaluation est le niveau d'assurance EAL 4 augmenté des composants ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4, conformément à la

partie 3 des Critères Communs [CC]. Le niveau de résistance des fonctions probabilistiques et permutationnelles est élevé (SOF-high).

1.2 Contexte de l'évaluation

7 L'évaluation s'est déroulée consécutivement au développement du produit d'avril 2001 à février 2002.

8 Le micro-circuit étant certifié par le schéma allemand, les travaux effectués dans le cadre de cet évaluation ont porté sur l'évaluation du masque et sur son intégration sûre dans le micro-circuit.

9 Le commanditaire de l'évaluation est Gemplus :

- Gemplus
  Parc d'activités de Gémenos
  13881 Gémenos Cedex
  France.

10 L'évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information de Serma Technologies :

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

Chapitre 2

Description de la cible d'évaluation

2.1 Périmètre de la cible d'évaluation

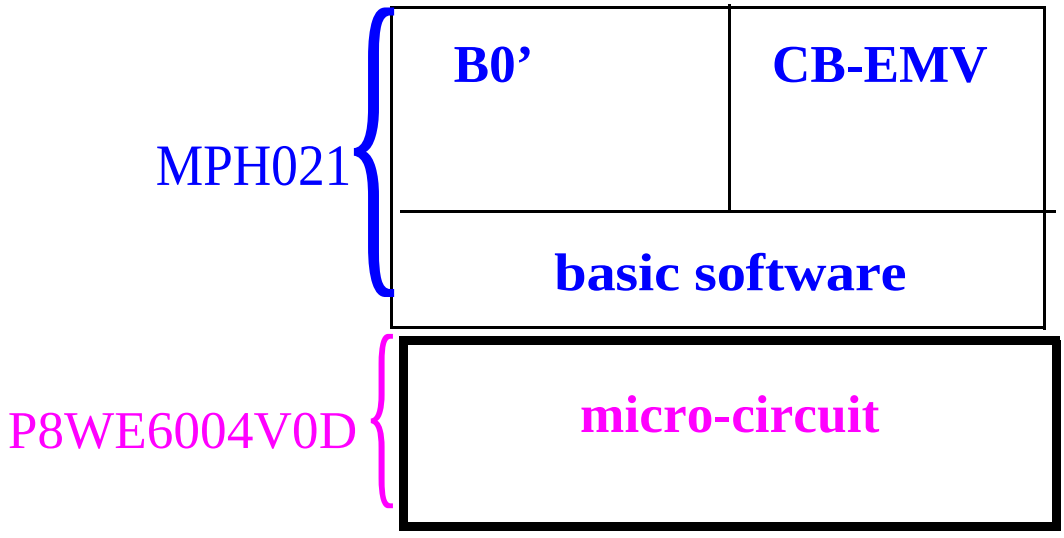
11 La cible d'évaluation est le produit Gem CB-B0'/EMV.

12 Ce produit se décompose en une partie matérielle :

- le micro-circuit P8WE6004V0D certifié EAL 5 augmenté et conforme au profil de protection PP/9806 [PP9806] ;

13 et une partie logicielle masquée sur le micro-circuit :

- le logiciel MPH021 qui contient les applications B0' et CB-EMV ainsi que la partie applicative (basic software) qui permet de communiquer avec le micro-circuit et de sélectionner les applications. Les applications sont conformes au cahier des charges CB-B0'/EMV V0.4 qui se réfère à EMV 3.1.1., VIS 1.3.2. et B4-B0' V3.



2.2 Cycle de vie

14 Le produit suit le cycle de vie d'une carte à puce tel qu'il est décrit dans les profils de protection PP/9806 [PP9806] et PP/9911 [PP9911].

Phase 1 : le développement des applications logicielles qui sont masquées sur le circuit a été examinée au cours de cette évaluation.

Phases 2 et 3 : ces phases qui correspondent au développement et à la fabrication du micro-circuit ont été examinées au cours de l'évaluation du micro-circuit par T-Systems et a fait l'objet du certificat BSI-DSZ-CC-0170-2002.

Phase 4 et 5 : ces phases correspondent à la mise en micro-module et l'encartage des composants.

Phase 6 : cette phase sert à la personnalisation des cartes. Lors de cette phase, le personnalisateur peut décider d'activer les deux applications ou seulement une seule des deux.

Phase 7 : la phase d'utilisation du produit par le porteur.

15 Les phases 1 à 3 correspondent au développement et à la fabrication de la cible d'évaluation, les phases 4 à 7 à son utilisation.

16 Le produit a été évalué tel qu'il sort de la phase 3, il appartient ensuite à l'utilisateur de personnaliser le produit (phase 6) pour le faire fonctionner avec les deux applications B0' et EMV, avec seulement l'application B0' ou avec seulement l'application EMV.

2.3 Fonctions de sécurité évaluées

17 Les fonctions de sécurité évaluées sont les suivantes :

- Fonctions assurées par le micro-circuit :
  - Génération de nombres aléatoires,
  - Calcul cryptographique du triple DES,
  - Contrôle des conditions correctes d'opération,
  - Protection physique du composant et des mémoires ;
- Fonctions communes à B0' et à EMV :
  - Gestion du RESET et des opérations de démarrage,
  - Vérification de l'intégrité du code en ROM ;
- Fonctions propres à B0' :
  - Vérification de la cohérence et de la validité des pointeurs,
  - Analyse de la cohérence des paramètres de commande,
  - Calcul cryptographique du triple DES,
  - Initialisation de B0',
  - Gestion de la mémoire EEPROM,
  - Gestion des clés et PIN,
  - Gestion du cycle de vie de B0',
  - Gestion des accès à la mémoire ;

- Fonctions propres à EMV :

  - Gestion des accès aux données utilisateur,
  - Gestion des authentifications mutuelles,
  - Gestion de la mémoire EEPROM,
  - Calcul cryptographique du DES et du MAC,
  - Gestion des clés cryptographiques,
  - Gestion du cycle de vie et de la configuration d'EMV,
  - Gestion du PIN et de l'authentification de l'utilisateur,
  - Génération de nombre aléatoire,
  - Gestion des attributs de sécurité.

2.4 Documentation

18 Le produit doit être accompagné de ses guides d'utilisation.

19 Ces guides s'adressent aux utilisateurs et aux administrateurs afin de permettre une utilisation sûre du produit ; ils sont décrits dans la fourniture d'évaluation «AGD - Guidance documents» [GUIDE].

20 Les guides administrateur décrivent les opérations qui garantissent une utilisation sûre du produit :

  - lors des livraisons du produit entre la phase 4 jusqu'à la phase 6
  - par le card manufacturer en phase 4 ;
  - par l'encarteur en phase 5, spécialement en ce qui concerne l'initialisation de la carte ;
  - par le personnalisateur en phase 6, spécialement en ce qui concerne l'initialisation de chacune des applications ;
  - par l'émetteur de la carte en phase 7.

21 Le guide utilisateur explique comment l'utilisateur (phase 7) doit utiliser la carte spécialement en ce qui concerne le code PIN.

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

22 Le produit a été évalué au niveau EAL 4 augmenté des composants ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4.

23 Ces critères d'évaluation ont été appliqués au composant masqué en s'appuyant sur les résultats de l'évaluation du micro-circuit certifié au niveau EAL 5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4

Classes d'Assurance	**Composants d'Assurance**
Cible de sécurité	Introduction de la ST (ASE_INT.1) Description de la TOE (ASE_DES.1) Environnement de sécurité (ASE_ENV.1) Objectifs de sécurité (ASE_OBJ.1) Annonce de conformité à un PP (ASE_PPC.1) Exigences de sécurité des TI (ASE_REQ.1) Exigences de sécurité des TI explicitement énoncées (ASE_SRE.1) Spécifications globales de la TOE (ASE_TSS.1)
Gestion de configuration	Automatisation partielle de la CM (ACM.AUT.1) Aide à la génération et procédures de réception (ACM_CAP.4) Couverture du suivi des problèmes par la CM Livraison et exploitation (ACM_SCP.2)
Livraison et exploitation	Détection de modifications (ADO_DEL.2) Procédures d'installation, de génération et de démarrage (ADO_IGS.1)
Développement	Définition exhaustive des interfaces externes (ADV_FSP.2) Conception de haut niveau - identification des sous-systèmes dédiés à la sécurité (ADV_HLD.2) **Implémentation de la TSF (ADV_IMP.2)** Conception de bas niveau descriptive (ADV_LLD.1) Démonstration de correspondance informelle (ADV_RCR.1) Modèle informel de politique de sécurité de la TOE (ADV_SPM.1)

Classes d'Assurance	Composants d'Assurance
Guides	Guide de l'administrateur (AGD_ADM.1) Guide de l'utilisateur (AGD_USR.1)
Support au cycle de vie	**Caractère suffisant des mesures de sécurité (ALC_DVS.2)** Modèle de cycle de vie défini par le développeur (ALC_LCD.1) Outils de développement bien définis (ALC_TAT.1)
Tests	Analyse de la couverture (ATE_COV.2) Tests : conception de haut niveau (ATE_DPT.1) Tests fonctionnels (ATE_FUN.1) Tests indépendants - échantillonnage (ATE_IND.2)
Estimation des vulnérabilités	Validation de l'analyse (AVA_MSU.2) Évaluation de la résistance des fonctions de sécurité de la TOE (AVA_SOF.1) **Résistance élevée (AVA_VLA.4)**

24 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.

25 Les travaux d'évaluation menés sont décrits dans le Rapport Technique d'Evaluation [RTE].

26 Dans le cadre des travaux d'évaluation, un audit organisationnel a été réalisé sur le site de développement de l'application MPH021 à Gémenos ; cet audit a permis de s'assurer de l'application de mesures de sécurité suffisantes pour protéger les données sensibles utilisées.

27 La résistance des fonctions utilisant un mécanisme de type probabilistique ou permutationnel a été évalué par l'évaluateur. Elle répond au niveau élevé (SOF-high) déclaré dans la cible de sécurité [ST].

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeur

28 Le développeur a effectué une campagne de test complète pour les deux applications pour vérifier la conformité avec les spécifications de Cartes Bancaires (CB) et de VISA.

29 Les tests sur le micro-circuit ont été fait par Philips.

3.2.2 Tests évaluateur

30 L'évaluateur a également mené une analyse de vulnérabilités, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élevé (composant AVA_VLA.4) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation suivants :

- la cible d'évaluation doit empêcher la manipulation des données sécuritaires,
- la cible d'évaluation ne doit pas pouvoir être clonée,
- la cible d'évaluation doit assurer la continuité d'opération de ses fonctions de sécurité,
- la cible d'évaluation doit s'assurer que les mécanismes de sécurité logiciels sont protégés contre la divulgation non-autorisée,
- la cible d'évaluation doit s'assurer que les informations sensibles en mémoires sont protégées contre la divulgation non-autorisée,
- la cible d'évaluation doit s'assurer que les informations sensibles en mémoires sont protégées contre la modification non-autorisée et la corruption,
- la cible d'évaluation doit contribuer à la non répudiation d'une transaction CB-EMV faite par un utilisateur autorisé,
- la cible d'évaluation doit fournir les moyens d'être authentifiée par des systèmes techniques distants pendant les phases 4 à 6 de sa fabrication.

Chapitre 4

Certification

4.1 Verdict

31 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL 4 augmenté des composants ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4, conformément à la partie 3 des Critères Communs [CC] :

- ADV_IMP.2 "Implémentation de la TSF",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",
- AVA_VLA.4 "Résistance élevée".

32 De plus, la cible d'évaluation est conforme au profil de protection «Smart Card Integrated Circuit with Embedded Software v2.0» [PP9911].

4.2 Recommandations

33 La cible d'évaluation "Gem CB-B0'/EMV : composant P8WE6004 V0D masqué par l'application MPH021 (référence : P8WE6004 V0D/C017D)" est soumise aux recommandations d'utilisation exprimées ci-dessous :

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

b) L'utilisation du produit doit être faite conformément aux guides d'administration et d'utilisation du produit [GUIDE].

4.3 Certification

34 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.

35 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 2. La certification de toute version ultérieure nécessitera au préalable une re-évaluation 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	Addition d'un ou de plusieurs composants d'assurance de la partie 3 des CC à une échelle prédéfinie d'assurance ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou par son environnement.
Cible d'évaluation	Produit ou système et documentation associée pour (administrateur et utilisateur) qui est l'objet d'une évaluation.
Cible de sécurité	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)	Paquet de composants d'assurance extraits de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	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	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

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- Part 1 : Introduction and general model, august 1999, version 2.1, réf : CCIMB-99-031 ;
- Part 2 : Security functional requirements, august 1999, version 2.1, réf : CCIMB-99-032 ;
- Part 3 : Security assurance requirements, august 1999, version 2.1, réf : CCIMB-99-033.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

[ST] "KASHMIR Security Target", version 0.5, réf : GEMPLUS-KASHMIR-ST.01, février 2002 (*document non public*).
cible de sécurité publique: référence :Gem CB-B0'/EMV Security Target, version publique.

[RTE] "Evaluation Technical Report, Serma Technologies", réf : ETR_KASHMIRv1.0, mars 2002 (*document non public*).

[GUIDE] "AGD - Guidance documents CB-B0'/EMV", Gemplus, version 0.3, réf : GEMPLUS-KASHMIR-AGD.01, février 2002.

[PP9806] "Smartcard Integrated Circuit, Version 2.0", septembre 1998, enregistré au catalogue des profils de protection certifiés sous la référence PP/9806.

[PP9911] "Smartcard Integrated Circuit with Embedded Software", version 2.0, juin 1999, enregistré au catalogue des profils de protection certifiés sous la référence PP/9911

[BSI] “Certification Report BSI-DSZ-CC-0170-2002 for Philips Smart Card Controller P8WE6004 V0D from Philips Semiconductors Gmbh Business Unit Identification”, Bundersamt für Sicherheit in der Informationtechnik, 8 mars 2002.

[SOG-IS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, version 2.0, April 1999, Management Commitee of Agreement Group.

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau Certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr