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 2001/13

Système d'Exploitation
VOP 2.0.1 / Java Card 2.1.1 JPH33V2 version 1
installé sur le micro-circuit PHILIPS P8WE5033

Juin 2001

Ce document constitue le rapport de certification du produit “Système d’Exploitation VOP 2.0.1 / Java Card 2.1.1 JPH33V2 version 1 installé sur le micro-circuit PHILIPS P8WE5033”.

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
DCSSI
Centre de Certification
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: certification.dcssi@sgdn.pm.gouv.fr

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 2001/13

Système d'Exploitation
VOP 2.0.1 / Javacard 2.1.1 JPH33V2 version 1
installé sur le micro-circuit PHILIPS P8WE5033

Développeurs : Oberthur Card Systems, Philips Semiconducteurs

EAL1 Augmenté

Commanditaire : Oberthur Card Systems

Le 7 juin 2001,

Le Commanditaire :
Le Directeur R&D d'Oberthur Card Systems

Eric ALZAÏ

L'Organisme de certification :
Le Directeur chargé 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
DCSSI
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Système d’Exploitation VOP 2.0.1 / Javacard 2.1.1 JPH33V2 version 1 installé sur micro-circuit PHILIPS P8WE5033”.

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 [CC-3].

3 La cible d’évaluation est le système d’exploitation multi-application JPH33V2 développé par Oberthur Card Systems installé sur le micro-circuit P8WE5033 développé par Philips Semiconducteurs. Cette plate-forme est conçue pour accueillir des applications pour cartes à puce programmées en Java Card. Cette plate-forme se veut conforme aux spécifications Java Card 2.1.1 de Sun Microsystems [JC] et Open Plateform 2.0.1 de Visa International [OP].

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

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

5 Elle s'est déroulée consécutivement au développement du produit de septembre 2000 à avril 2001.

6 Le commanditaire de l'évaluation (ci-après "le commanditaire") et développeur du système d'exploitation (ci-après "le développeur") est Oberthur Card Systems :

- Oberthur Card Systems
  12bis, rue des Pavillons
  BP 133
  F - 92804 Puteaux.

7 Le développeur et fabricant du micro-circuit est Philips :

- Philips Semiconducteurs
  7/9, rue du Mont Valérien
  BP 317
  F - 92156 Suresnes.

8 L'évaluation a été conduite par le centre d'évaluation de la sécurité des technologies de l'information de Serma Technologies (ci-après "CESTI") :

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

2.2 Description de la cible d'évaluation

9 La cible d'évaluation est le système d'exploitation JPH33V2 développé par Oberthur Card Systems, installé sur le micro-circuit Philips P8WE5033.

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

- Séparation entre les applets ;

- Contrôle d'accès aux données (mécanisme d'authentification) ;

- Vérification d'intégrité des données sensibles ;

- Mécanismes transactionnels de mise à jour de l'EEPROM ;

- Interfaces assurant la confidentialité des biens des applications :

  - opérations cryptographiques (DES, RSA),
  - génération de clés RSA,
  - génération de nombres aléatoires.

2.3 Conclusions de l'évaluation

11 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 tels que décrit dans la partie 3 des Critères Communs [CC-3].

12 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.

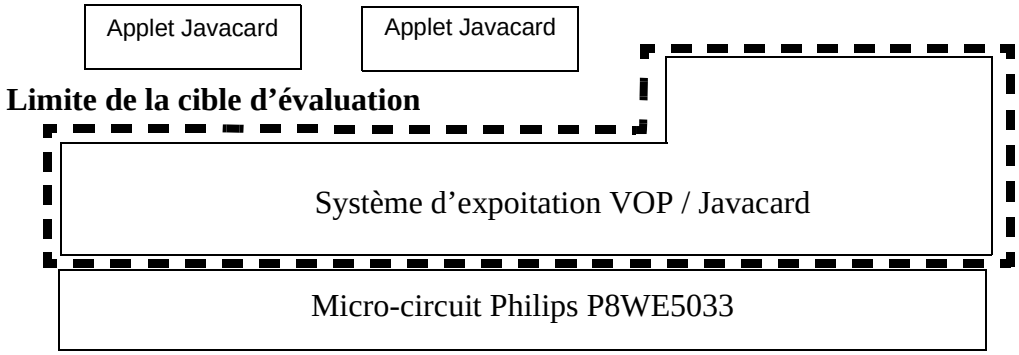
13 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

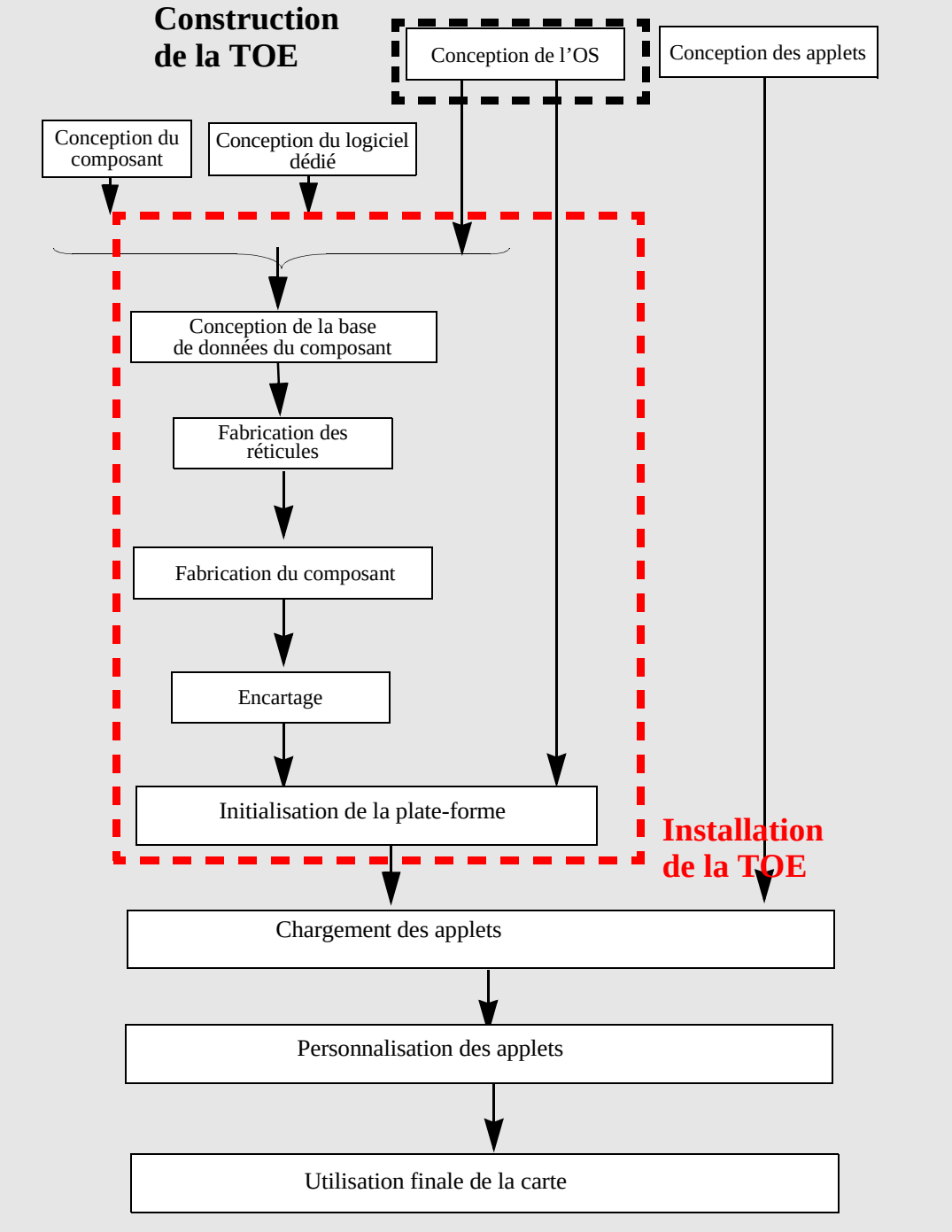
Identification de la cible d'évaluation

3.1 Objet

14 La cible d'évaluation est le système d'exploitation JPH33V2 développé par Oberthur Card Systems. Pour cette évaluation, ce système d'exploitation est installé sur le micro-circuit Philips P8WE5033.



3.2 Cycle de vie de la cible d'évaluation



3.3 Historique du développement

15 Le système d'exploitation a été développé par Oberthur Card Systems conformément aux spécifications Open Platform et Java Card publiées par Visa et Sun (respectivement [OP] et [JC]).

3.4 Description des matériels

16 Le système d'exploitation évalué est installé sur le micro-circuit Philips P8WE5033, qui ne fait pas partie de la cible d'évaluation et qui a les caractéristiques suivantes :

- architecture 8 bits,
- microcontrôleur 80C51,
- 96 Ko de ROM,
- 2 Ko de RAM étendue,
- 32 Ko d'EEPROM.

3.5 Description des logiciels

17 La cible d'évaluation est composée des logiciels suivants :

- BIOS (interface entre le composant matériel et le composant logique),
- Machine virtuelle conforme à Java Card 2.1.1,
- Interfaces d'application (API) conformes à Javacard 2.1.1,
- Application Open Platform OP2.0 configuration 1a (Card Manager, API OPSystem),
- Application résidente native (répartiteur de commande).

3.6 Description de la documentation

18 La documentation d'exploitation de la cible d'évaluation est la suivante :

- guide d'utilisation d'Oberthur Card Systems [GUIDE],
- guides Java Card [JC],
- guides Open Platform [OP] et [VOP].

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

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

4.2 Hypothèses

20 La cible d'évaluation doit être utilisée dans un environnement qui satisfasse aux hypothèses énoncées dans la cible de sécurité.

21 Ces hypothèses couvrent les aspects suivants :

- la protection des mémoires du circuit intégré,
- le développement de la cible d'évaluation,
- la livraison de la cible d'évaluation entre les différentes phases de son cycle de vie,
- la production et le développement du circuit intégré,
- la gestion des clés cryptographiques en dehors de la cible d'évaluation,
- le protocole de communication avec le terminal.

22 Le détail de ces hypothèses est disponible dans la cible de sécurité [ST].

4.3 Menaces

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

- le bytecode et les objets des applets,
- les PIN et les clés,
- les données d'authentification,
- les attributs de sécurité.

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

- divulgation ou modification non autorisée des biens de la cible d'évaluation,
- utilisation interdite d'applet,
- usurpation d'identité pour accéder à un objet partagé Java,
- modification non-autorisée de la mémoire.

4.4 Politiques de sécurité organisationnelles

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

- les interfaces de la cible d'évaluation doivent respecter les API Java Card ;
- la cible d'évaluation doit fournir les services qui permettent aux applets d'implémenter des mécanismes de sécurité.

4.5 Fonctions de sécurité évaluées

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

- notification et exécution des exceptions,
- utilisation des mécanismes de sécurité en fonction des commandes du Card Manager utilisées,
- isolation des contextes des applets,
- maintien des privilèges du contexte du Card Manager,
- gestion des points d'entrée du contexte d'exécution,
- gestion du buffer apdu,
- authentification mutuelle de l'administrateur et de la cible d'évaluation en phase d'utilisation,
- utilisation d'un MAC dans les échanges apdu,
- chiffrement par un algorithme DES des données confidentielles,
- comparaison sécurisée des données confidentielles en RAM et EEPROM, confidentialité des données résiduelles,
- atomicité des opérations d'écriture en EEPROM,
- fonctionnement correct du compteur de ratification,
- intégrité des clés lors de leur chargement ou de leur création,
- génération de nombres aléatoires et de clés de session,
- service cryptographique proposé aux applets,
- gestion des jeux de clés,
- vérification du cycle de vie de la carte et de la mémoire.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

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

5.2 Principaux résultats de l'évaluation

28 Le produit répond aux exigences des Critères Communs pour le niveau EAL1 augmenté du composant AVA_VLA.2 décrites dans la partie 3 des Critères Communs [CC-3].

5.2.1 ASE : Evaluation de la cible de sécurité

29 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 [CC-3].

30 La cible d'évaluation est le produit "Système d'Exploitation VOP 2.0.1 / Javacard 2.1.1 JPH33V2 version 1 installé sur le micro-circuit Philips P8WE5033".

31 La cible de sécurité [ST] fournie par le développeur décrit de manière suffisamment claire la cible d'évaluation, l'environnement supposé d'exploitation ainsi que les fonctions de sécurité évaluées.

5.2.2 ACM_CAP.1 : Numéro de version

32 Les critères d'évaluation sont définis par la section ACM_CAP.1.iE de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

33 La cible d'évaluation est référencée (JPH33V2 version 1) et identifiée par un nom de produit «GalactIC». La référence de masquage donnée par Philips est P8WE5033/00502.

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

34 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 [CC-3].

35 Les procédures de démarrage du produit correspondent à la pré-initialisation du système d'exploitation avec l'installation du Card Manager.

5.2.4 ADV_FSP.1 : Définition exhaustive des interfaces externes

36 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 [CC-3].

37 L'évaluateur a 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.

5.2.5 ADV_RCR.1 : Démonstration de correspondance informelle

38 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 [CC-3].

39 L'évaluateur s'est assuré de la correspondance entre les différentes représentations des fonctions de sécurité de la cible d'évaluation.

5.2.6 AGD_ADM.1 : Guide de l'administrateur

40 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 [CC-3].

41 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).

42 L'évaluateur s'est assuré que la documentation disponible permet une administration sûre du produit.

5.2.7 AGD_USR.1 : Guide de l'utilisateur

43 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 [CC-3].

44 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 guides de programmation de Sun Microsystems [JC] et Visa International [OP] et [VOP].

45 La documentation d'utilisation inclut également les recommandations de sécurité de programmation fournies par Oberthur Card Systems aux développeurs d'applets pour la plate-forme GalacticIC [GUIDE].

46 L'évaluateur s'est assuré que la documentation disponible permet une utilisation sûre du produit.

5.2.8 ATE_IND.1 : Tests indépendants - conformité

47 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 [CC-3].

48 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 a été testé.

5.2.9 AVA_VLA.2 : Analyse de vulnérabilité indépendante

49 Les critères d'évaluation sont définis par les sections AVA_VLA.2.iE de la classe AVA, telles que spécifiées dans la partie 3 des Critères Communs [CC-3].

50 L'évaluateur a réalisé des tests de pénétration indépendants, basés sur son analyse de vulnérabilité 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.

5.2.10 Verdicts

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

Chapitre 6

Recommandations d'utilisation

52 La cible d'évaluation "Système d'Exploitation VOP 2.0.1 / Javacard 2.1.1 JPH33V2 version 1 installé sur le micro-circuit Philips P8WE5033" 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 [ST].

b) Les règles du guide de programmation [GUIDE] pour les applets qui seront installées sur la plate-forme doivent être impérativement respectées.

c) Les applets qui seront chargées sur la plate-forme doivent passer par un «converter» et un «verifier» permettant de valider la correction de la sémantique et du format du bytecode généré.

Chapitre 7

Certification

7.1 Objet

53 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 tel que décrit dans la partie 3 des Critères Communs [CC-3].

54 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

55 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.

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

57 La certification de toute version ultérieure nécessitera au préalable une ré-évaluation en fonction des modifications apportées.

Annexe A

Glossaire et abréviations

apdu	«application protocol data unit» format des données échangées entre la carte à puce et le terminal.
API	«application programmer interface» interface de programmation entre les applications.
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.
Java Card	Sous ensemble du langage de programmation Java appliqué aux systèmes embarqués, spécialement aux cartes à puces.
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.
EEPROM	«Electrically Erasable Programmable ROM» ROM programmable effaçable électriquement.
ROM	«Read Only Memory» Mémoire morte.
RAM	«Random Access Memory» Mémoire vive.
PIN	«Personal Identification Number» Numéro personnel d'identification

Annexe B

Références

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

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

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

[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.

[ST] Cible de sécurité LEO Security Target, ref. FQR 110 963 version publique 2P et version à diffusion contrôllée 2.0, Oberthur Card Systems

[RTE] Rapport technique d'évaluation RTE_LEO_V1.0, Serma Technologies (diffusion contrôlée).

[GUIDE] GalactIC Operating system reference guide 2.1 V2, Oberthur Card Systems.

[OP] Open Platform Card Specification V2.0.1, décembre 1999, Visa International.

[VOP] Visa Open Platform Circuit Card Implementation Specification, mars 1999, Visa International (new specifications, octobre 2000).

[JC] Java Card 2.1.1 : Application Programming Interfaces, JCRE, Virtual Machine Specifications, mai 2000, Sun Microsystems.