Schéma Français

de la Sécurité des Technologies de l’Information

Ce document constitue le rapport de certification du produit “Plate-forme Palmera Protect V2.0 JavaCard (composant masqué SLE66CX320P/SB62)”.

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 Latour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr

La reproduction de tout ou partie de ce document, sans altérations ni coupures, est autorisée.

Tous les noms des produits ou des services de ce document sont des marques déposées de leur propriétaire respectif.

Ce document est folioté de 1 à 26 et certificat.

PREMIER MINISTRE

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

CERTIFICAT 2001/06

Plate-forme Palmera Protect V2.0 JavaCard

(composant masqué SLE66CX320P/SB62)

Développeur : Infineon Technologies AG, SchlumbergerSema

EAL1 Augmenté

Commanditaire : SchlumbergerSema

Le 3 août 2001,

Le Commanditaire :
Le Président Cartes SchlumbergerSema

Jorgen RASMUSSEN

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

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Plate-forme Palmera Protect V2.0 JavaCard (composant masqué SLE66CX320P/SB62)”.

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 [CC-3].

3 La cible d’évaluation est la plate-forme multi-applications Palmera Protect V2.0 constituée du micro-circuit Infineon SLE66CX320P et de son système d’exploitation développé par SchlumbergerSema. Cette plate-forme est conçue pour accueillir tout type d’applications pour cartes à puce programmées en JavaCard (langage Java restreint).

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 simultanément au développement du produit de septembre 2000 à mars 2001.

6 Le commanditaire de l'évaluation est la société Schlumberger (ci-après "le commanditaire") :

- SchlumbergerSema
  50, avenue Jean Jaurès
  BP 620-12
  92542 Montrouge Cedex
  France

7 Les développeurs de la cible d'évaluation sont les sociétés suivantes :

- SchlumbergerSema pour le système d'exploitation :

  SchlumbergerSema
  284, avenue de la Pomme de Pin
  St Cyr en Val
  BP 6021
  45060 Orléans Cedex 2
  France

- Infineon Technologies AG pour le micro-circuit :

  Infineon Technologies AG
  Postfach 80 17 60
  81617 München
  Allemagne

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

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

2.2 Description de la cible d'évaluation

9 La cible d'évaluation est la plate-forme multi-applications Palmera Protect V2.0 constituée du micro-circuit Infineon SLE66CX320P et de son système d'exploitation développé par SchlumbergerSema. Cette plate-forme est conçue pour accueillir tout type d'applications pour cartes à puce programmées en JavaCard (langage Java restreint).

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

a) Fonctionnalités JavaCard [JC21] :

- Protection physique du micro-circuit,
- Détection des perturbations environnementales,
- Dissimulation des calculs effectués par le micro-circuit,
- Contrôle d'accès aux mémoires,
- Auto-test au démarrage du micro-circuit,
- Fonctions cryptographiques,
- Gestion des commandes reçues,
- Contrôle d'accès aux objets gérés par la plate-forme,
- Gestion des exceptions,
- Interpréteur sûr de bytecode,
- Atomicité des traitements.

b) Fonctionnalités OP [OP] :

- Gestion de la carte,
- Gestion des droits d'accès,
- Enregistrement des états successifs de la plate-forme,
- Gestion des clés cryptographiques,
- Gestion du code porteur (PIN),
- Gestion du cycle de vie de la plate-forme,
- Gestion de l'état des applets,
- Authentification des utilisateurs et des administrateurs de la plate-forme.

2.3 Conclusions de l'évaluation

11 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 [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.

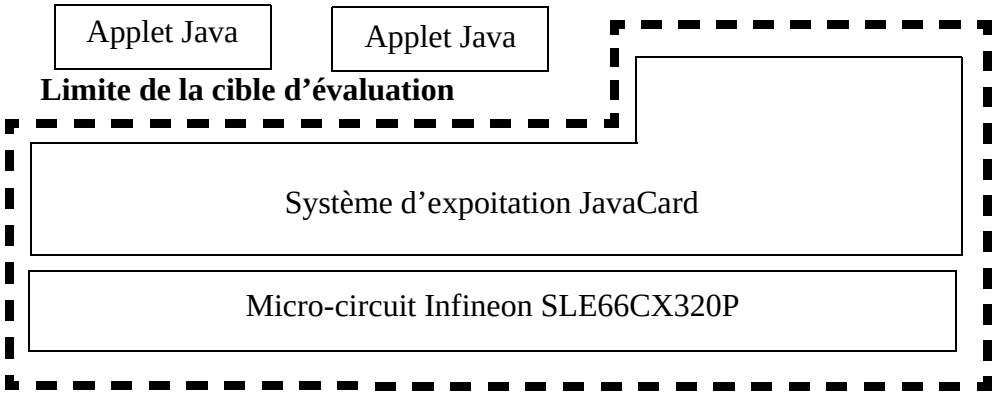
13 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

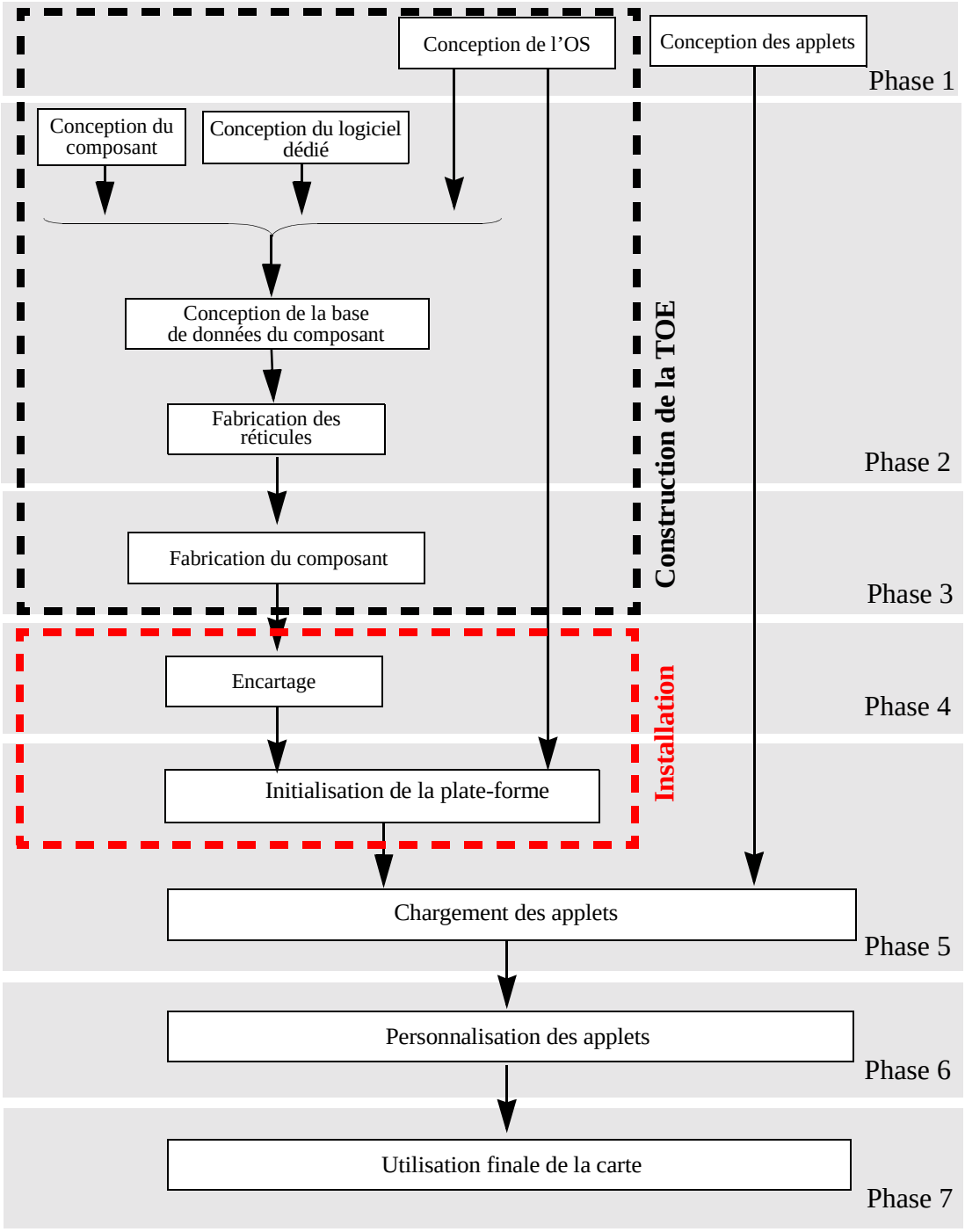
Identification de la cible d'évaluation

3.1 Objet

14 La cible d'évaluation est la plate-forme multi-applications Palmera Protect V2.0 constituée du micro-circuit Infineon SLE66CX320P (référence de masquage SB62) et de son système d'exploitation développé par SchlumbergerSema.



3.2 Cycle de vie de la cible d'évaluation



3.3 Description du matériel

15 Le micro-circuit utilisé est le composant SLE66CX320P développé et fabriqué par Infineon Technologies AG.

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

3.4 Description du logiciel

17 Le système d'exploitation est développé par SchlumbergerSema sur le site d'Orléans pour être ensuite masqué sur le micro-circuit (référence de masquage SB62).

18 Dans le contexte de l'évaluation, l'état du système d'exploitation est INITIALIZED tel qu'il est défini dans les spécifications OP [OP] et VOP [VOP].

3.5 Description de la documentation

19 La documentation d'utilisation de la plate-forme Palmera Protect V2.0 est la suivante :

- guide de programmation Schlumberger [USM],
- guide API Javacard [JCAPI],
- guide de programmation Visa [ADG].

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

20 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

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

22 Ces hypothèses couvrent les aspects suivants :

- la gestion hors de la plate-forme des éléments secrets (clés cryptographiques, PIN) est suffisante pour garantir leur confidentialité,
- l'intégrité et la confidentialité des éléments sensibles traités par le système (terminaux, protocoles) sont garanties,
- les procédures de stockage et de livraison des cartes garantissent la sécurité des données sensibles,
- les applets respectent les recommandations de programmation de SchlumbergerSema [USM],
- les applets sont développées dans un environnement sûr,
- un convertisseur et un vérificateur sont utilisés avant le chargement des applets.

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

4.3 Menaces

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

a) Durant les phases de contruction de la plate-forme :

- les informations et outils utilisés pour le développement du micro-circuit et du système d'exploitation,
- les différentes représentations de la plate-forme lors de sa construction (réticules, wafers, échantillons).

b) Durant les phases d'exploitation de la plate-forme :

- la plate-forme elle-même,

- la conception du micro-circuit,
- le code du système d'exploitation,
- les données du système d'exploitation,
- le code des applets chargées sur la plate-forme,
- les données de ces applets.

25 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 :

- clonage fonctionnel de la plate-forme,
- divulgation ou modification des informations de conception du micro-circuit et du système d'exploitation,
- divulgation des informations et des outils de test du micro-circuit et du système d'exploitation,
- vol de plate-forme ou d'échantillons durant les phases de construction,
- divulgation ou modification des données de la plate-forme,
- modification non autorisée du comportement des fonctions de sécurité,
- chargement non autorisé d'applets ou d'autres programmes,
- manque d'isolation entre les applets chargées.

4.4 Politiques de sécurité organisationnelles

26 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 :

- la plate-forme doit respecter les spécifications JavaCard 2.1 [JC21] et VOP 2.0 [VOP],
- la plate-forme doit pouvoir être identifiée de manière unique,
- la plate-forme doit fournir des services cryptographiques conformes aux normes en vigueur.

4.5 Fonctions de sécurité évaluées

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

a) Fonctionalités JavaCard [JC21] :

- Protection physique du micro-circuit,
- Détection des perturbations environnementales,
- Dissimulation des calculs effectués par le micro-circuit,
- Contrôle d'accès aux mémoires,
- Auto-test au démarrage du micro-circuit,
- Fonctions cryptographiques,
- Gestion des commandes reçues,
- Contrôle d'accès aux objets gérés par la plate-forme,

- Gestion des exceptions,
- Interpréteur sûr de bytecode,
- Atomicité des traitements.

b) Fonctionalités OP [OP] :

- Gestion de la carte,
- Gestion des droits d'accès,
- Enregistrement des états successifs de la plate-forme,
- Gestion des clés cryptographiques,
- Gestion du code porteur (PIN),
- Gestion du cycle de vie de la plate-forme,
- Gestion de l'état des applets,
- Authentification des utilisateurs et des administrateurs de la plate-forme.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

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

5.2 Principaux résultats de l'évaluation

29 Le produit répond aux exigences des Critères Communs pour le niveau d'assurance EAL 1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante".

5.2.1 ASE : Evaluation de la cible de sécurité

30 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].

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

5.2.2 ADV_FSP.1 : Spécifications fonctionnelles informelles

32 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].

33 Le développeur a fourni la documentation spécifiant les fonctions de sécurité du produit ainsi que leurs interfaces externes. Les interfaces externes sont ici les méthodes JavaCard décrites dans les spécifications JavaCard [JC21].

34 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.

5.2.3 ADV_RCR.1 : Démonstration de correspondance informelle

35 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].

36 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.

5.2.4 ACM_CAP.1 : Numéros de version

37 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 [CC-3].

38 La cible d'évaluation est la plate-forme multi-applications Palmera Protect V2.0 constituée du micro-circuit Infineon SLE66CX320P (référence de masquage SB62) et de son système d'exploitation développé par SchlumbergerSema.

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

39 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].

40 Les procédures d'installation et de génération du produit portent sur les phases d'initialisation et de personnalisation de la plate-forme.

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

42 L'évaluateur s'est assuré que ces procédures permettent d'installer la cible d'évaluation dans un état sûr.

5.2.6 AGD_ADM.1 : Guide de l'administrateur

43 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].

44 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).

45 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

46 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].

47 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 [JCAPI] et Visa International [ADG].

48 La documentation d'utilisation inclut également les recommandations de sécurité de programmation fournies par SchlumbergerSema aux développeurs d'applets pour la plate-forme Palmera Protect V2.0 [USM].

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

5.2.8 ATE_IND.1 Tests indépendants - conformité

50 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].

51 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 a été testée.

5.2.9 AVA_VLA.2 : Analyse de vulnérabilités indépendante

52 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 [CC-3].

53 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.

54 Ces tests de pénétration ont porté sur le système d'exploitation ainsi que sur le micro-circuit.

5.2.10 Verdicts

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

Chapitre 6

Recommandations d'utilisation

56 Le produit "Plate-forme Palmera Protect V2.0 JavaCard (composant masqué SLE66CX320P/SB62)" 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 [ST] ;

- Les règles du guide de programmation [USM] pour les applets installées sur la plate-forme Palmera Protect V2.0 doivent être impérativement respectées ;

- Les applets visant à être installées sur la plate-forme doivent impérativement être vérifiées avant leur installation en utilisant un outil de vérification («verifier») fiable.

Chapitre 7

Certification

7.1 Objet

57 Le produit soumis à évaluation satisfait aux exigences du 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 [CC-3].

58 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

59 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.

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

61 La certification de toute version ultérieure nécessitera au préalable une ré-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	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.

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 «Security Target : MERAPI v1.2», réf. MRD07SBG003007 (diffusion libre).

[RTE] Rapport technique d'évaluation, réf. ETR_MERAPI2_V1.0 (diffusion contrôlée).

[USM] Applet Programming Guide, réf. ORDUSM003002 version 1.0, SchlumbergerSema.

[JC21] Java Card 2.1 Virtual Machine Specification v1.1, juin 1999, Sun Microsystems.

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

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

[JCAPI] Java Card 2.1 Application Programming Interface, Sun Microsystems.

[ADG] Visa Open Platform - Card Applet Developer's Guide – mars 2000, Visa International.