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

Ce document constitue le rapport de certification du produit “Applet Oberthur B4-B0’ V3 version 1.0 pour Multos 4”.

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 :

Ce documentestfolioté de 1 à 24 etcertificat.

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Applet Oberthur B4-B0’ V3 version 1.0 pour Multos 4”.

2 Le niveau d’assurance atteint est le niveau EAL4 augmenté des composants d’assurance suivants tels que décrits dans la partie 3 des Critères Communs [CC-3] :

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

3 La cible d’évaluation est l’application B4-B0’ V3 développée par Oberthur Card Systems destinée à être installée sur une carte à puce équipée du système d’exploitation Multos 4. Cette carte est destinée à être utilisée pour les opérations de retraits et de paiements dans le système "CB".

4 La version précédente de l’application ayant été certifiée précédemment [2000_05], la présente évaluation ne constitue qu’une ré-évaluation du produit focalisée sur les modifications apportées au produit et à son environnement de développement.

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

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

6 Elle s'est déroulée consécutivement au développement du produit de novembre 2000 à mars 2001.

7 La version précédente du produit ayant été certifiée précédément [2000_05], la présente évaluation n'est qu'une ré-évaluation du produit focalisée sur les modifications fonctionnelles et de l'environnement de développement de la cible d'évaluation.

8 Le commanditaire de l'évaluation est le Crédit Mutuel (ci-après "le commanditaire") :

- Crédit Mutuel
  34 rue du Wacken
  67000 Strasbourg
  France

9 La cible d'évaluation a été développée par la société Oberthur Card Systems (ci-après "le développeur") :

- Oberthur Card Systems
  25 rue Auguste Blanche
  92800 Puteaux
  France

10 L'évaluation a été conduite par le centre d'évaluation CEACI (ci-après "l'évaluateur") :

- CEACI
  18 avenue Edouard Belin
  31401 Toulouse Cedex
  France

2.2 Description de la cible d'évaluation

11 La cible d'évaluation est le produit "Applet Oberthur B4-B0' V3 version 1.0 pour Multos 4".

12 Cette application développée par Oberthur Card Systems doit être installée sur une carte à puce équipée du système d'exploitation Multos 4. Cette carte peut ensuite être utilisée pour des opérations de retraits ou de paiements dans le système "CB".

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

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

2.3 Conclusions de l'évaluation

14 Le produit soumis à évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance suivants tels que décrits dans la partie 3 des Critères Communs [CC-3]. :

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

15 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL4 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

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 La cible d'évaluation est l'application Oberthur B4-B0' V3 version 1.0 développée par Oberthur Card Systems destinée à être installée sur une carte à puce équipée du système d'exploitation Multos 4. Cette carte peut être ensuite utilisée pour les opérations de retraits et de paiements dans le système "CB".

3.2 Historique du développement

18 L'application B4-B0' V3 est basée sur les applets Oberthur B0' v1.0 et Routeur v1.0 précédément évaluées et certifiées [2000_05].

19 Depuis l'évaluation de la version précédente du produit, le site de développement d'Oberthur Card Systems a également été transferé de Gentilly vers Puteaux.

3.3 Description des matériels

20 Aucun matériel ne fait partie de la cible d'évaluation.

3.4 Description des logiciels

21 La cible d'évaluation consiste en une applet développée en langage MAL (Multos Assembler Language) pouvant être installée sur le système d'exploitation pour cartes à puce Multos 4.

3.5 Description de la documentation

22 La documentation d'utilisation et d'administration de l'applet Oberthur B4-B0' V3 certifiée est la suivante :

- Contrat porteur émis par les banques à destination des porteurs de cartes bancaires "CB" [USR],
- Manuels émis par le GIE Cartes Bancaires à destination des personnalisateurs et des émetteurs de cartes [ADM].

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

23 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

24 Les résultats de l'évaluation sont conditionnés par le respect des hypothèses sur l'utilisation et l'environnement d'utilisation de la cible d'évaluation suivantes :

- les procédures mises en place pour les différentes livraisons sont suffisantes pour garantir la confidentialité et l'intégrité des éléments transmis. Le personnel effectuant le transport est supposé de confiance ;
- le chargement et l'effacement de l'application évaluée sont effectuées dans un environnement sûr et par des personnes de confiance ;
- la plate-forme Multos fournit des mécanismes de sécurité permettant de protéger le code et des données de la cible d'évaluation contre la modification ou la divulgation par une autre application ou par le système d'exploitation ;
- la plate-forme Multos fournit des mécanismes de sécurité garantissant le chargement et l'effacement sûr des applications.

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

4.3 Menaces

26 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, vol ou modification d'informations ou d'éléments de la cible d'évaluation pendant son développement ;
- chargement non autorisé ou modification du code et des données de la cible d'évaluation lors de son chargement sur la plate-forme Multos ;
- personnalisation non autorisée ou divulgation, vol ou modification d'informations lors de la personnalisation ;
- utilisation non autorisée des services de la cible d'évaluation ;
- divulgation ou modification du code ou des données sensibles de la cible d'évaluation pendant son exploitation par :
  - des actions externes (commandes, I/O),

  - des actions internes (applications, système d'exploitation),
  - une utilisation dans des conditions anormales de fonctionnement ;
- répudiation des transactions ;
- répudiation de la personnalisation par un émetteur ;
- effacement non autorisé ou non-sûr de la cible d'évaluation.

4.4 Politiques de sécurité organisationnelles

27 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 :

- Pour pouvoir être utilisée dans le système "CB", la carte sur laquelle est installée la cible d'évaluation doit respecter les recommandations du GIE Cartes Bancaires pour la personnalisation des cartes et leur utilisation.

4.5 Fonctions de sécurité évaluées

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

- Contrôle d'accès aux informations stockées en mémoire (en lecture, en écriture et en effacement) en fonction de la phase de vie de l'application B0', de l'utilisateur et de la zone mémoire visée ;
- Irreversibilité du cycle de vie de l'application B0',
- Traçabilité des opérations (écritures en mémoire, authentifications),
- Authentification des utilisateurs et administrateurs,
- Authentification de l'application utilisée,
- Authentification des transactions,
- Réaction aux conditions anormales de fonctionnement des applications.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

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

5.2 Principaux résultats de l'évaluation

30 Le produit répond aux exigences des Critères Communs pour le niveau EAL4 augmenté des composants d'assurance suivants tels que décrit dans la partie 3 des Critères Communs [CC-3]. :

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

31 La version précédente de l'application ayant été certifiée précédement [2000_05], la présente évaluation ne constitue qu'une ré-évaluation du produit focalisée sur les modifications apportées au produit et à son environnement de développement.

32 Seules les tâches d'évaluation associées aux modifications apportées ont été refaites par l'évaluateur. Pour les autres tâches, les verdicts de l'évaluation précédente ont été conservés.

5.2.1 ASE : Evaluation de la cible de sécurité

33 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].

34 La nouvelle version de la cible de sécurité [ST] a été ré-évaluée. Seules des modifications mineures ont été nécessaires pour répondre aux exigences de la classe ASE. Ces modifications ont été regroupées dans un erratum associé à la cible de sécurité [ST].

35 Aucune conformité à un profil de protection n'est annoncée.

5.2.2 ADV_FSP.2 : Définition exhaustive des interfaces externes

36 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 [CC-3].

37 Certaines interfaces externes ayant été modifiées, l'évaluateur a ré-évalué les spécifications fonctionnelles, incluant la description des interfaces externes, fournies par le développeur.

38 L'évaluateur a examiné ces spécifications et montré pour le niveau considéré qu'elles représentent une description complète et homogène des fonctions de sécurité à évaluer.

5.2.3 ADV_SPM.1 : Modèle informel de politique de sécurité de la TOE

39 Les critères d'évaluation sont définis par les sections ADV_SPM.1.1E de la classe ADV, telle que définie dans la partie 3 des Critères Communs [CC-3].

40 Le modèle informel de la politique de sécurité de la TOE n'ayant pas été modifié, les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.4 ADV_HLD.2 : Conception de haut niveau - Identification des sous-systèmes dédiés à la sécurité

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

42 Le développeur a fourni une nouvelle conception de haut niveau de la cible d'évaluation.

43 L'évaluateur s'est assuré que cette nouvelle conception de haut niveau est toujours une instanciation correcte et complète des exigences fonctionnelles de sécurité de la cible de sécurité.

5.2.5 ADV_LLD.1 : Conception de bas niveau descriptive

44 Les critères d'évaluation sont définis par les sections ADV_LLD.1.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [CC-3].

45 Le développeur a fourni une nouvelle conception de bas niveau de la cible d'évaluation.

46 L'évaluateur s'est assuré que cette nouvelle conception de bas niveau est toujours une instantiation correcte et complète des exigences fonctionnelles de sécurité de la cible de sécurité.

5.2.6 ADV_IMP.2 : Implémentation de la TSF

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

48 Le développeur a fourni l'intégralité du nouveau code source de l'application.

49 Une analyse détaillée du code source a été de nouveau effectuée par les évaluateurs afin, d'une part, de vérifier que ces éléments de réalisation constituent une

représentation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation, et d'autre part, de rechercher des vulnérabilités potentielles.

5.2.7 ADV_RCR.1 : Démonstration de correspondance informelle

50 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].

51 Le développeur a fourni une documentation qui indique les correspondances entre les différents niveaux de représentation des fonctions de sécurité de la cible d'évaluation.

52 L'évaluateur a donc pu s'assurer de la conformité des spécifications fonctionnelles de sécurité à travers la conception de haut niveau, la conception de bas niveau ainsi que l'implémentation.

5.2.8 ACM_AUT.1 : Automatisation partielle de la CM

53 Les critères d'évaluation sont définis par la section ACM_AUT.1.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

54 Oberthur Card Systems utilisant le même système de gestion de configuration depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.9 ACM_CAP.4 : Aide à la génération et procédures de réception

55 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 [CC-3].

56 Oberthur Card Systems utilisant le même système de gestion de configuration depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

57 Seule une nouvelle liste de configuration a été fournie à l'évaluateur.

5.2.10 ACM_SCP.2 : Couverture du suivi des problèmes par la CM

58 Les critères d'évaluation sont définis par la section ACM_SCP.2.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

59 Oberthur Card Systems utilisant le même système de gestion de configuration depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.11 ADO_DEL.2 : Détection de modification

60 Les critères d'évaluation sont définis par la section ADO_DEL.2.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

61 Les procédures de livraison n'ayant pas été modifiées chez Oberthur Card Systems, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

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

62 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].

63 La fusion des applications B0' et Routeur ayant entraînée la modification des procédures de génération et d'installation, les nouvelles procédures ont été ré-évaluées.

64 L'évaluateur s'est assuré de l'absence d'incohérence dans ces procédures.

5.2.13 AGD_ADM.1 : Guide de l'administrateur

65 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].

66 Le guide d'administration [ADM] fourni par le GIE Cartes Bancaires n'ayant pas été modifiés depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.14 AGD_USR.1 : Guide de l'utilisateur

67 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].

68 Le guide d'utilisation [USR] fourni par le GIE Cartes Bancaires n'ayant pas été modifiés depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.15 ALC_DVS.2 : Caractère suffisant des mesures de sécurité

69 Les critères d'évaluation sont définis par la section ALC_DVS.2.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

70 En raison du changement de site de développement, l'évaluateur a ré-évalué la sécurité de l'environnement de développement d'Oberthur Card Systems à Puteaux.

71 Les procédures physiques, organisationnelles, techniques et liées au personnel mises en place assurent un niveau de protection suffisant de la cible d'évaluation, de ses constituants ainsi que de sa documentation. La visite du site de développement a permis de vérifier l'application de ces procédures.

5.2.16 ALC_LCD.1 : Modèle de cycle de vie défini par le développeur

72 Les critères d'évaluation sont définis par la section ALC_LCD.1.1E de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

73 Le modèle de cycle de vie de l'application fourni par le développeur n'ayant pas été modifié depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.17 ALC_TAT.1 : Outils de développement bien définis

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

75 Les outils de développement utilisé n'ayant pas été modifiés depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.18 ATE_FUN.1 : Tests fonctionnels

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

77 Le plan de test n'ayant pas été modifié depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

78 Seuls les résultats des tests passés sur le nouveau produit ont été fournis. Ces résultats ont été utilisés par l'évaluateur dans le cadre des tests fonctionnels indépendants menés.

5.2.19 ATE_COV.2 : Analyse de la couverture

79 Les critères d'évaluation sont définis par la section ATE_COV.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

80 L'analyse de couverture des tests n'ayant pas été modifiée depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.20 ATE_DPT.1 : Tests : conception de haut-niveau

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

82 L'analyse fournie par le développeur n'ayant pas été modifiée depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.21 ATE_IND.2 : Tests indépendants - échantillonnage

83 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 [CC-3].

84 Une partie des tests fonctionnels du développeur a été ré-exécutée pour vérifier les résultats obtenus par le développeur. Les tests fonctionnels ont été menés sur la plate-forme contituée des élements suivants :

- applet Oberthur B4-B0' V3,
- système d'exploitation Multos 4 version 1N' (sans AMD) développé par Keycorp,
- micro-circuit Infineon SLE66CX160M.

85 Des tests complémentaires développés par l'évaluateur ont également été effectués pour s'assurer que les fonctions de sécurité fonctionnent conformément à leurs spécifications.

5.2.22 AVA_MSU.2 : Validation de l'analyse

86 Les critères d'évaluation sont définis par la section AVA_MSU.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

87 L'analyse fournie par le développeur n'ayant pas été modifiée depuis l'évaluation précédente, les travaux d'évaluation associés n'ont pas été refaits et les verdicts "réussite" de l'évaluation précédente ont été conservés.

5.2.23 AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE

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

89 Le développeur a fourni une nouvelle analyse de la résistance des fonctions de sécurité du produit utilisant des mécanismes permutationnels ou probabilistiques. L'évaluateur a analysé cette documentation et mené une analyse indépendante pour confirmer le niveau visé (résistance élevée SOF-high).

90 L'organisme de certification a confirmé ce niveau pour les mécanismes cryptographiques sous réserve des recommandations énoncées au chapitre 6 de ce rapport.

5.2.24 AVA_VLA.4 : Résistance élevée

91 Les critères d'évaluation sont définis par les sections AVA_VLA.4.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

92 Le développeur a fourni une nouvelle analyse des vulnérabilités potentielles du produit. L'évaluateur a examiné cette fourniture et réalisé sa propre analyse de vulnérabilités de manière indépendante.

93 L'évaluateur a réalisé des tests de pénétration, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit résiste aux attaques de niveau élevé tel que défini par le composant AVA_VLA.4 "Résistance élevée".

94 Les tests réalisés ont porté uniquement sur l'applet B4-B0' V3. Les tests des éventuelles vulnérabilités liées à son fonctionnement sur une carte Multos 4 ne font pas partie de la présente évaluation.

5.2.25 Verdicts

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

Chapitre 6

Recommandations d'utilisation

96 La cible d'évaluation "Applet Oberthur B4-B0' V3 version 1.0 pour Multos 4" 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) Le chargement et l'effacement de l'application évaluée doivent être impérativement effectués dans un environnement sûr et par des personnes autorisées et de confiance.

c) La plate-forme Multos 4 sur laquelle seront chargées les applications doit impérativement fournir les fonctionnalités suivantes :

- chargement et effacement sécurisés d'applets,
- protection du code et des données de la cible d'évaluation contre la modification ou la divulgation par une autre application ou par le système d'exploitation,

d) La gestion des outils et des clés de personnalisation de la carte doit impérativement être effectuée dans un environnement sûr et par des personnes autorisées et de confiance.

Chapitre 7

Certification

7.1 Objet

97 Le produit soumis à évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance suivants tels que décrits dans la partie 3 des Critères Communs [CC-3]. :

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

98 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL4 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

7.2 Portée de la certification

99 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.

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

101 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

[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 "KEVIN Security Target - Spécifications fonctionnelles détaillées", réf. SRS 05651100SRS, version 1-AB, 5 décembre 2000 (diffusion contrôlée) ;
- Erratum, réf. FQR 1101146, version 1, 3 janvier 2001.

[RTE] Rapport technique d'évaluation, réf. KEV_RTE version 1.0L, 30 mars 2001 (diffusion contrôlée).

[2000_05] Rapport de Certification 2000_05 "Applications Oberthur B0' v1.0 et Routeur v1.0 conçues pour Multos v4.02", Schéma français d'évaluation et de certification, novembre 2000.

[USR] Documentation d'utilisation, réf. DET/DS/CBGEN4, version 1.0 (diffusion contrôlée).

[ADM] Documentation d'administration, réf. DET/DS/CBGEN6, version 1.0 (diffusion contrôlée).