Schéma Français

PREMIER MINISTRE

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

CERTIFICAT 2001/07

Applet Mondex Purse 2 version 0203 pour Multos 4

Développeur : Mondex International

EAL4 Augmenté

Commanditaire : Crédit Mutuel

Le 24 avril 2001,

Le Commanditaire :
Le Directeur du Crédit Mutuel

M. Claude BRUN

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
DCSSI
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 du produit “Applet Mondex Purse 2 version 0203 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 Mondex Purse 2 développée par Mondex International destinée à être installée sur une carte à puce équipée du système d’exploitation Multos 4. Cette carte peut être ensuite utilisée comme porte-monnaie électronique dans le système Mondex.

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 pour se terminer en mars 2001.

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

- Crédit Mutuel
  34 rue du Wacken
  67000 Strasbourg
  France

7 La cible d'évaluation a été développée par la société Mondex International (ci-après "le développeur") :

- Mondex International Limited
  47-53 Cannon Street
  London EC4M 55Q
  Grande Bretagne

8 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

9 La cible d'évaluation est le produit "Applet Mondex Purse 2 version 0203 pour Multos 4".

10 Cette application développée par Mondex International doit être installée sur une carte à puce équipée du système d'exploitation Multos 4. Cette carte peut ensuite être utilisée comme porte-monnaie électronique dans le système Mondex.

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

- Contrôle des flux de valeur électronique (création interdite, transactions dans un unique domaine, transactions inter-devises),
- Enregistrement des transactions réussies ou interrompues,
- Gestion de l'état de l'application,
- Authentification mutuelle des porte-monnaie,
- Migration du système,
- Contrôle d'accès aux fonctionnalités de l'application.

2.3 Conclusions de l'évaluation

12 Le produit soumis à évaluation satisfait aux exigences du 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.

13 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.

14 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

15 La cible d'évaluation est l'application Mondex Purse 2 développée par Mondex International destinée à être installée sur une carte à puce équipée du système d'exploitation Multos 4. Cette carte peut être ensuite utilisée comme porte-monnaie électronique dans le système Mondex.

3.2 Historique du développement

16 L'application Mondex Purse 2 version 0203 pour Multos 4 a été développée en 1999 par Mondex International pour être utilisée dans leur système de porte-monnaie électronique.

17 Cette même applet avait été évaluée avec la plate-forme sur laquelle elle était installée au niveau EAL1+ en 1999. Cette évaluation s'est conclue par l'émission du certificat 9909 [9909].

3.3 Description des matériels

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

3.4 Description des logiciels

19 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

20 La documentation d'utilisation et d'administration de l'applet Mondex Purse 2 certifiée est la suivante :

- Guide sécuritaire à destination des émetteurs [ISSUER].

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

21 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

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

23 Ces hypothèses couvrent principalement les aspects suivants :

- les équipements de chargement ou de paiement restent dans un état sûr même en cas d'erreurs lors d'une transaction,
- la plate-forme (micro-circuit et système d'exploitation) sur laquelle est chargée l'applet est suffisamment résistante aux attaques physiques pour protéger les données et le code de l'applet,
- la plate-forme garantit l'étanchéité entre les données des différentes applets chargées sur la carte.

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

4.3 Menaces

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 :

- Blanchiment d'argent,
- Usurpation de l'identité des différents acteurs du système (émetteur de valeur électronique, porteur, commerçant, ...),
- Rejeu de transactions,
- Défaillance de l'application lors d'une transaction,
- Contre-façon de transactions,
- Fausse répudiation d'une transaction,
- Perte d'intégrité des données du porte-monnaie.

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 :

- Le porte-monnaie électronique doit être traité de la même manière qu'un véritable porte-monnaie avec des pièces et des billets de banque et ne doit pas être prêté, spécialement à des personnes non autorisées.
- Les acquéreurs (généralement les commerçants) et les agents de chargement des cartes sont des agents autorisés par l'émetteur de valeur électronique,
- Il doit exister un moyen pour indiquer au porteur le montant de valeur électronique des transactions,
- Chaque transaction électronique doit être une action intentionnelle du porteur,
- Le porte-monnaie électronique doit avoir une identification unique dans le système,
- L'équipement d'acceptation du commerçant doit avoir une identification unique pour l'équipement acquéreur,
- Le commerçant doit être associé à son équipement d'acceptation,
- Le commerçant ne peut être collecté que par sa banque acquéreur.
- La cible d'évaluation doit administrer des rôles de sécurité et ces rôles doivent être indépendants,
- Les enregistrements des transactions incomplètes doivent être sauvegardés régulièrement dans le système,
- Les licences représentent les mécanismes pour contrôler l'accès aux opérations réservées.

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 :

- Contrôle des flux de valeur électronique (création interdite, transactions dans un unique domaine, transactions inter-devises),
- Enregistrement des transactions réussies ou interrompues,
- Gestion de l'état de l'application,
- Authentification mutuelle des porte-monnaie,
- Migration du système,
- Contrôle d'accès aux fonctionnalités de l'application.

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 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.

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 suffisament claire la cible d'évaluation, l'environnement supposé d'exploitation ainsi que les fonctions de sécurité évaluées.

32 Aucune conformité à un profil de protection n'est annoncée même si la cible de sécurité s'inspire fortement du profil de protection PP/9909 [PP9909].

5.2.2 ADV_FSP.2 : Définition exhaustive des interfaces externes

33 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].

34 Le développeur a fourni la documentation spécifiant les fonctions de sécurité du produit et leurs interfaces externes.

35 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

36 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].

37 Le développeur a fourni un modèle informel de la politique de sécurité de la TOE.

38 L'évaluateur a examiné ce modèle et montré que toutes les fonctions de sécurité décrites dans les spécifications fonctionnelles constituent une représentation complète et homogène de ce modèle.

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

39 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].

40 Le développeur a fourni la conception de haut niveau de la cible d'évaluation.

41 Cette conception présente la structure générale du produit en terme de sous-systèmes. L'évaluateur s'est assuré que cette conception de haut niveau est une instanciation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

5.2.5 ADV_LLD.1 : Conception de bas niveau descriptive

42 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].

43 Le développeur a fourni la conception de bas niveau de la cible d'évaluation.

44 Cette conception décrit les modules constituant le produit et l'ensemble de leurs interfaces. L'évaluateur s'est assuré que cette conception de bas niveau est une instantiation correcte et complète des exigences fonctionnelles de sécurité de la cible d'évaluation.

5.2.6 ADV_IMP.2 : Implémentation de la TSF

45 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].

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

47 Une analyse détaillée du code source a été 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

48 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].

49 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.

50 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

51 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].

52 Le développeur a fourni la documentation du système de gestion de configuration utilisé pour le développement des applications chez Mondex International.

53 Le système est fondé sur une gestion automatique de la configuration à travers un outil de gestion de configuration permettant de s'assurer que seuls les changements autorisés sur le produit sont possibles.

54 L'évaluateur a analysé la documentation et vérifié au cours de l'audit du site de développement l'utilisation effective de cet outil en accord avec les procédures du développeur.

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 Ce système impose un contrôle des objets produits au cours du développement chez le développeur. Des procédures permettent de prendre en compte dans le système de gestion de configuration les objets composant la cible d'évaluation (procédure de réception). Des procédures gèrent également les révisions majeures et mineures de la cible d'évaluation.

57 Le système de gestion de configuration énumère ainsi tous les modules élémentaires à partir desquels la cible d'évaluation a été construite.

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 Le système de gestion de configuration utilisé par le développeur couvre le produit ainsi que l'ensemble de sa documentation ; il couvre également toute erreur de

sécurité qui pourrait être découverte ; il contrôle donc la documentation de conception du produit, la documentation de test du produit et les éléments de réalisation du produit (code source).

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 Le développeur a fourni les procédures de livraison de l'application au responsable de son chargement sur les cartes Multos 4. Leur application a été vérifiée au cours d'une visite sur le site de développement de Mondex International.

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 Les procédures d'installation, de génération et de démarrage du produit concernent le formatage de l'application Mondex Purse 2 et son chargement sur les cartes Multos 4.

64 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation.

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 développeur a fourni la documentation d'administration des fonctions de sécurité du produit [ISSUER]. Ces guides d'administration sont à usage :

- des responsables du chargement de l'application,
- des personnalisateurs de l'application.

67 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures permettent une administration sûre du produit.

5.2.14 AGD_USR.1 : Guide de l'utilisateur

68 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].

69 Le développeur a fourni le guide à destination des émetteurs [ISSUER] leur permettant de rédiger la documentation d'utilisation pour les porteurs de porte-monnaie Mondex.

70 L'évaluateur s'est assuré que cette documentation permet une utilisation sûre du produit.

5.2.15 ALC_DVS.2 : Caractère suffisant des mesures de sécurité

71 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].

72 L'évaluateur a analysé la sécurité de l'environnement de développement de Mondex International à Londres.

73 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

74 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].

75 Le développeur a fourni le modèle de cycle de vie des applications.

76 L'évaluateur a analysé ce modèle et s'est assuré de l'absence d'incohérences dans ce modèle.

5.2.17 ALC_TAT.1 : Outils de développement bien définis

77 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].

78 Le développeur a fourni la documentation relative aux outils de développement utilisés et notamment le langage MAL.

79 L'évaluateur a examiné cette documentation et s'est assuré de l'absence d'incohérences dans cette documentation. L'analyse de l'implémentation du produit (ADV_IMP.2) a également permis à l'évaluateur de confirmer la complétude de cette documentation.

5.2.18 ATE_FUN.1 : Tests fonctionnels

80 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].

81 Le développeur a fourni la documentation de tests du produit. Les tests fournis par le développeur correspondent à un ensemble de tests logiciels des fonctions de sécurité des applications.

82 Une documentation détaillée de tests a été fournie pour chacun des tests ; ces documentations décrivent le plan des tests, l'objectif des tests, les procédures de tests à réaliser ainsi que les résultats des tests.

83 L'évaluateur s'est assuré de la complétude de cette documentation.

5.2.19 ATE_COV.2 : Analyse de la couverture

84 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].

85 Le développeur a fourni une analyse de la documentation de tests justifiant la couverture de la totalité des fonctions de sécurité.

86 L'évaluateur a confirmé cette analyse.

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

87 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].

88 Le développeur a fourni une analyse de la documentation de tests justifiant la réalisation de tests fonctionnels pour les sous-systèmes identifiés dans la conception de haut-niveau des applications.

89 L'évaluateur a examiné cette documentation et s'est assuré de sa cohérence.

5.2.21 ATE_IND.2 : Tests indépendants - échantillonnage

90 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].

91 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 Mondex Purse 2 version 0203,
- système d'exploitation Multos 4 version 1N' + AMD 0010 (v001) développé par Keycorp,
- micro-circuit Infineon SLE66CX160M.

92 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

93 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].

94 Le développeur a fourni une analyse des guides d'installation, de génération, de démarrage, d'utilisation et d'administration de la cible d'évaluation. L'objectif de cette analyse est de garantir que des éléments trompeurs, déraisonnables ou contradictoires sont absents de ces guides et que les procédures sûres pour tous les modes d'exploitation ont été prises en compte.

95 L'évaluateur s'est assuré de la complétude de cette analyse et a appliqué de nouveau ces procédures afin de confirmer que le cible d'évaluation peut être configurée et utilisée de manière sûre en n'utilisant que les guides fournis.

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

96 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].

97 Le développeur a fourni une 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).

98 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

99 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].

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

101 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 définies par le composant AVA_VLA.4 "Résistance élevée".

102 Les tests réalisés ont porté uniquement sur l'applet Mondex Purse 2. Le test des éventuelles vulnérabilités liées à son fonctionnement sur une carte Multos 4 ne font pas partie de la présente évaluation.

5.2.25 Verdicts

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

Chapitre 6

Recommandations d'utilisation

104 La cible d'évaluation "Applet Mondex Purse 2 version 0203 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 des applications évaluées 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,

Chapitre 7

Certification

7.1 Objet

105 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.

106 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

107 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.

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

109 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 CCIB-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 CCIB-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 CCIB-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 "EAL4 Common Criteria Security Target for the Mondex Purse Application", réf. mxi-yoda-stg-001 version 2.0, 16 janvier 2001 (diffusion contrôlée).

[RTE] Rapport technique d'évaluation, réf. YO_RTE version 1.0L, 29 mars 2001 (diffusion contrôlée).

[ISSUER] Guide sécuritaire à destination des émetteurs "Mondex Purse 2.0/4 Guidelines for Card Issuers", réf. mxi-yoda-doc-005, version 1.1, 14 mars 2001 (diffusion contrôlée).

[9909] Rapport de Certification 9909, Schéma français d'évaluation et de certification, décembre 1999.

[PP9909] Profil de Protection PP/9909 "Intersector Electronic Purse and Purchase Device" version 1.2, février 1999.