PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

SERVICE CENTRAL 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 99/09

Porte-monnaie électronique "Mondex Purse 2"

version 0203

(composant SLE66CX160S, système d'exploitation MULTOS V4.1N)

Novembre 1999

Ce document constitue le rapport de certification du produit "Porte-monnaie électronique “Mondex Purse 2” version 0203 (composant SLE66CX160S ; système d’exploitation MULTOS V4.1N)".

Ce rapport de certification est disponible sur le site internet du Service Central de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.scssi.gouv.fr

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

SCSSI
Centre de Certification de la Sécurité des Technologies de l’Information
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

mèl : ssi20@calva.net

Ce document est folioté de 1 à 40 et certificat.

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

CERTIFICAT 99/09

Porte-monnaie électronique "Mondex Purse 2"

version 0203
(composant SLE66CX160S ; système d'exploitation MULTOS Version 4.1N)

Développeur : Mondex International

EAL1 augmenté

Commanditaire :
Crédit Mutuel

Le XX novembre 1999,

Le Commanditaire :
Crédit Mutuel
Le Directeur
M. Brun

L'organisme de certification :
Le chef du Service central de la sécurité
des systèmes d'information
Le général Jean-Louis Desvignes

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 2.0 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
SCSSI
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit constitué de la carte porte-monnaie électronique “Mondex Purse 2”, version 0203.

2 Les fonctionnalités évaluées sont consignées en annexe A du présent rapport.

3 Le niveau d’assurance atteint est le niveau EAL 1 augmenté du composant d’assurance AVA_VLA.2 “Analyse de vulnérabilités effectuée de manière indépendante” tel que décrits dans la partie 3 des critères communs [4].

Chapitre 2

Résumé

2.1 Description de la cible d'évaluation

4 La cible d'évaluation est le porte-monnaie électronique "Mondex purse 2". La particularité de ce produit est la possibilité de transférer de la valeur électronique d'un porte-monnaie vers un autre porte-monnaie.

2.2 Résumé des caractéristiques de sécurité

2.2.1 Menaces

5 Les principales menaces identifiées dans la cible de sécurité [6] peuvent être résumées comme suit :

- blanchiment d'argent,
- usurpation d'identité de l'un des acteurs du système,
- création frauduleuse de valeur électronique,
- perte de valeur électronique.

6 Les biens à protéger au sein de la cible d'évaluation sont définis comme étant la valeur électronique, les paramètres d'administration du porte-monnaie électronique ainsi que les messages de type "exception log". Ces biens doivent être protégés en intégrité.

2.2.2 Politiques de sécurité organisationnelles et hypothèses

7 L'annexe A donne les principales caractéristiques de sécurité telles qu'elles sont décrites dans la cible de sécurité [6], en particulier les politiques de sécurité organisationnelles ainsi que les hypothèses d'utilisation du produit.

2.2.3 Exigences fonctionnelles de sécurité

8 Les principales fonctionnalités de sécurité du produit décrites dans la cible de sécurité [6] sont les suivantes :

- authentification du porte-monnaie électronique,
- authentification des acteurs,
- contrôle d'accès (valeur électronique et contrôle de flux),

- preuves d'origine et de réception des transactions (chargement, achat, collecte),

- protection des fonctions de sécurité : notification et résistance aux attaques physiques, détection de rejeu, préservation d'état sûr, recouvrement des fonctions, séparation de domaines.

2.2.4 Exigences d'assurance

9 Les exigences d'assurance spécifiées dans la cible de sécurité [6] sont celles du niveau d'évaluation EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités effectuée de manière indépendante".

2.3 Acteurs dans l'évaluation

10 Le commanditaire de l'évaluation est le Crédit Mutuel :

Crédit Mutuel
34 rue du Wacken
F-67000 Strasbourg.

11 La cible d'évaluation a été développée par la société:

- Mondex International pour le développement des logiciels,

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

- Keycorp a participé au développement de la cible d'évaluation en tant que développeur du système d'exploitation MULTOS :

  Keycorp Australia

- Infineon a également participé au développement de la cible d'évaluation en tant que développeur et fabricant du composant micro-électronique SLE66CX160S :

  Infineon Technologies AG
  CC MTH
  PO Box 80 17 60
  D- 81617 Munich

2.4 Contexte de l'évaluation

12 L'évaluation a été menée conformément aux critères communs ([1] à [4]) et à la méthodologie définie dans le manuel CEM [5].

13 L'évaluation s'est déroulée simultanément au développement du produit.

14 L'évaluation a été conduite par le centre d'évaluation de la sécurité des technologies de l'information (CEACI) des sociétés SOREP-ERULEC et CNES :

- Centre d'Études et d'Analyses des Circuits Intégrés (CEACI)
  18 avenue Edouard Belin
  F-31441 Toulouse Cedex

2.5 Conclusions de l'évaluation

15 Le produit soumis à évaluation dont la cible de sécurité [6] est partiellement reprise dans l'annexe A du présent rapport, satisfait aux exigences du niveau d'évaluation EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités effectuée de manière indépendante".

16 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'attaques tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

17 Les vulnérabilités connues du commanditaire de l'évaluation ont été toutes communiquées aux évaluateurs et au certificateur conformément au critère [AVA_VLA.2.4E].

18 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

19 La cible d'évaluation est le produit "Mondex Purse 2" version 0203.

20 Le porte-monnaie électronique "Mondex Purse 2" est constitué du micro-circuit électronique SLE66CX160S, destiné à être inséré dans une carte porteur de format carte de crédit. Le micro-circuit électronique contient le système d'exploitation de la carte (MULTOS V4.1N) ainsi que l'application porte-monnaie électronique Mondex, applet du système d'exploitation. D'autres applications peuvent être chargées sur le produit. Ce rapport de certification exclut une telle configuration.

21 Les phases d'encartage et de personnalisation de la cible d'évaluation sont hors du champ de l'évaluation.

3.2 Historique du développement

22 Le système d'exploitation MULTOS (Multi-Application Operating System) a été développée par la société Keycorp en Australie.

23 Le composant SLE66CX160S a été développé et testé par la société Infineon sur le site de Munich. La production des micro-circuits est effectuée en Allemagne.

3.3 Description du matériel

24 Le micro-circuit électronique SLE66CX160S est un micro contrôleur de la famille des composants SLE66. Il dispose d'une unité centrale de 8 bits associée à une mémoire de travail de 1 koctets (RAM), d'une mémoire de programme de 32 Koctets (ROM), et d'une mémoire de données de 16Koctets (EEPROM).

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

3.4 Description du logiciel

26 La cible d'évaluation est constituée des logiciels suivants :

- le système d'exploitation MULTOS, masqué durant la phase de fabrication du produit,

- l'application "Mondex Purse 2", applet chargée durant la production du micro-circuit.

27 La configuration exacte de la cible d'évaluation est décrite en annexe B.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

28 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [6] qui est la référence pour l'évaluation.

29 Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Politique de sécurité

30 L'objectif du porte-monnaie électronique Mondex est de fournir une solution alternative de type électronique à l'usage de la monnaie fiduciaire (pièces de monnaie et de billets de banque).

31 La valeur électronique est d'abord créée par l'émetteur de valeur électronique appelée dans le système Mondex "Originator". Cette valeur est ensuite distribuée à travers un mécanisme d'échanges entre porte-monnaie électroniques.

32 Les porte-monnaie électroniques peuvent donc, dans ce système, distribuer de la valeur électronique pour acheter ou recevoir de la valeur électronique. Les paiements peuvent être effectués vers des banques ou en provenance de banques, entre consommateurs et commerçants ou directement entre porteurs. Dans tous ces cas, la valeur électronique peut être transférée vers tout autre porte-monnaie électronique ; toutefois, certains porte-monnaie électroniques ne peuvent dialoguer qu'à l'intérieur d'un groupe de porte-monnaie prédéfinis appelé "classe".

33 La politique de sécurité de la cible d'évaluation est fondée sur la conservation du flux de valeur électronique ainsi que sur l'authentification préalable des acteurs intervenant dans les différents échanges. Pour chaque type de transaction, la valeur électronique créditée doit toujours être égale à la valeur débitée. Dans ce modèle d'échanges, il ne doit pas y avoir de création ou de perte de valeur électronique ; seul l'émetteur de valeur électronique (Originator) peut en créer ou en détruire.

4.3 Menaces

34 Les menaces effectivement couvertes par le produit sont décrites dans le chapitre 3 de la cible de sécurité [6]. Elles sont reprises en annexe A.2.

4.4 Hypothèses d'utilisation et d'environnement

35 La cible d'évaluation doit être utilisée et administrée conformément aux exigences spécifiées dans la documentation d'utilisation et d'administration.

36 Les hypothèses d'utilisation et d'environnement du produit sont consignées dans le chapitre 3 de la cible de sécurité [6]. Celles-ci sont reprises en annexe A.

4.5 Architecture du produit

37 L'architecture du produit est normalement décrite dans les documents de conception générale et détaillée exigibles pour les composants d'assurance ADV_HLD et ADV_LLD.

38 Le niveau d'évaluation EAL1 considéré n'inclut pas l'évaluation de l'architecture du produit.

4.6 Description de la documentation

39 La documentation disponible pour l'évaluation est décrite en annexe B du présent rapport de certification.

4.7 Tests de la cible d'évaluation

40 Plusieurs types de tests ont été passés sur la carte porte-monnaie électronique "Mondex purse 2".

41 Les évaluateurs ont effectué un ensemble de tests sur le produit afin de vérifier par échantillonnage la conformité des fonctions de sécurité aux spécifications de sécurité. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL1.

42 De plus, dans le cadre du composant d'assurance AVA_VLA.2, les évaluateurs ont effectué de manière indépendante un ensemble de tests de pénétration sur le produit afin d'estimer l'efficacité des fonctions de sécurité offertes par le produit. Ces tests de pénétration sont adaptés à la nature du produit soumis à évaluation ainsi qu'à son environnement.

4.8 Configuration évaluée

43 La configuration exacte de la cible d'évaluation est décrite en annexe B.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

44 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [8].

5.2 Résultats de l'évaluation de la cible de sécurité

45 La cible de sécurité répond aux exigences de la classe ASE, telle que définie dans la partie 3 des critères communs [4].

5.2.1 ASE_DES Description de la TOE

46 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

47 La cible d'évaluation (TOE) est le porte-monnaie électronique "Mondex Purse 2", constitué du micro-circuit électronique SLE66CX160S, du système d'exploitation MULTOS version 4.1N et de l'applet porte-monnaie proprement dite "Mondex Purse 2", version 0203.

48 La description de la cible d'évaluation est précisée au chapitre 3 du présent rapport de certification.

5.2.2 ASE_ENV Environnement de sécurité

49 Les critères d'évaluation sont définis par les sections ASE_ENV.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

50 Les hypothèses d'utilisation et d'environnement du produit, les menaces auxquelles doit faire face le produit ainsi que les politiques de sécurité organisationnelles sont décrites dans la cible de sécurité [6]. Ces caractéristiques de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.3 ASE_INT Introduction de la ST

51 Les critères d'évaluation sont définis par les sections ASE_INT.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

52 L'introduction de la cible de sécurité [6] précise l'identification du produit et contient une vue d'ensemble de la cible de sécurité, ainsi qu'une annonce de conformité aux critères communs.

5.2.4 ASE_OBJ Objectifs de sécurité

53 Les critères d'évaluation sont définis par les sections ASE_OBJ.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

54 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrites dans la cible de sécurité [6]. Ces objectifs de sécurité sont repris en annexe A du présent rapport de certification.

5.2.5 ASE_PPC Annonce de conformité à un PP

55 Les critères d'évaluation sont définis par les sections ASE_PPC.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

56 La cible de sécurité [6] ne fait aucune annonce de conformité à un profil de protection ; les critères d'évaluation ci-dessus ne sont pas applicables.

5.2.6 ASE_REQ Exigences de sécurité des TI

57 Les critères d'évaluation sont définis par les sections ASE_REQ.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

58 Les exigences de sécurité des TI fonctionnelles ou d'assurance sont décrites dans la cible de sécurité [6]. Ces exigences de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.7 ASE_SRE Exigences de sécurité des TI déclarées explicitement

59 Les critères d'évaluation sont définis par les sections ASE_SRE.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

60 La cible de sécurité [6] ne contient pas d'exigences de sécurité des TI déclarées explicitement qui ne font pas référence à la partie 2 des critères communs [2].

5.2.8 ASE_TSS.1 Spécifications de haut niveau de la TOE

61 Les critères d'évaluation sont définis par les sections ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

62 La cible de sécurité [6] contient un résumé des spécifications des fonctions de sécurité du produit ainsi que les mesures d'assurance prises pour satisfaire les exigences d'assurance. L'évaluateur s'est assuré que ces fonctions de sécurité sont une représentation correcte des exigences fonctionnelles de sécurité et que les mesures d'assurance prises couvrent les exigences du niveau EAL1 augmenté.

5.3 Résultats de l'évaluation du produit

63 Le produit répond aux exigences des critères communs pour le niveau EAL1 augmenté du composant AVA_VLA.2 "Analyse de vulnérabilités effectuée de manière indépendante".

5.3.1 ADV_FSP.1 : Spécifications fonctionnelles informelles

64 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 [4].

65 Le développeur a fourni la documentation spécifiant les fonctions de sécurité du produit (conception de haut niveau des fonctions de sécurité). Les interfaces externes sont également décrites.

66 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.

5.3.2 ADV_RCR.1 : Démonstration de correspondance informelle

67 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 [4].

68 Le développeur a fourni une documentation indiquant la correspondance entre les fonctions de sécurité telles qu'elles sont définies dans les spécifications (ADV_FSP) et la cible de sécurité (ASE_TSS).

69 Deux représentations des fonctions de sécurité ont donc été analysées par l'évaluateur ; celui-ci s'est assuré que les spécifications fonctionnelles (ADV_FSP) correspondent à une image complète et cohérente des fonctions de sécurité décrites dans la cible de sécurité [6] (ASE_TSS).

5.3.3 ACM_CAP.1 : Numéros de version

70 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 [4].

71 Le produit évalué porte la référence "Mondex Purse 2" (version 0203, composant SLE66CX160S, système d'exploitation MULTOS version 4.1N), telle que définie dans l'annexe B du présent rapport.

72 L'évaluateur s'est également assuré de l'absence d'incohérence dans la documentation fournie.

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

73 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 [4].

74 L'installation et la génération de la cible d'évaluation sont appliquées une seule fois ; dans ce cas, comme l'indique la méthodologie d'évaluation [5], les critères correspondants ne sont pas applicables.

75 Les procédures de démarrage du porte-monnaie électronique ont été analysées ; l'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures conduisent à une configuration sûre du produit.

5.3.5 AGD_ADM.1 : Guide de l'administrateur

76 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 [4].

77 L'administrateur du produit est la banque émettrice de la carte. 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.

5.3.6 AGD_USR.1 : Guide de l'utilisateur

78 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 [4].

79 L'utilisateur du produit est le porteur du porte-monnaie électronique d'une part et le commerçant d'autre part. La documentation utilisateur est constituée des spécifications d'interface du produit. Cette documentation précise un ensemble de recommandations d'utilisation des fonctions de sécurité.

80 L'évaluateur s'est assuré que cette documentation correspondait à une utilisation sûre du produit.

5.3.7 ATE_IND.1 Tests effectués de manière indépendante - conformité

81 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 [4].

82 Les évaluateurs ont effectué un ensemble de tests sur la carte afin de vérifier par échantillonnage la conformité des fonctions de sécurité aux exigences fonctionnelles de sécurité.

83 Ces tests ont porté sur les logiciels embarqués et également sur le composant. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL1.

5.3.8 AVA_VLA.2 : Analyse de vulnérabilités effectuée de manière indépendante

84 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 [4].

85 L'évaluateur a réalisé des tests de pénétration de manière indépendante, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit résiste aux

attaques correspondant à un potentiel de l'attaquant tel que défini par le composant AVA_VLA.2. Ces tests de pénétration ont porté sur les logiciels embarqués ainsi que sur le composant. Les attaques de nature évidente, incluant donc celles du domaine public, ont été également prises en compte dans cette analyse.

5.3.9 Verdicts

86 Pour tous les aspects des critères communs identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 6

Recommandations d’utilisation

87 Le produit “porte-monnaie électronique Mondex Purse 2 (composant SLE66CX160S ; système d’exploitation MULTOS version 4.1N)” est soumis aux recommandations d’utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

88 Le produit doit être utilisé conformément à l’environnement d’utilisation prévu dans la cible de sécurité [6].

89 Les processus d’encartage et de personnalisation sont des étapes critiques destinées à configurer le produit de manière sûre.

90 Les processus d’encartage et de personnalisation doivent être strictement définis et contrôlés ; des mesures de sécurité doivent être appliquées au cours de ces phases afin de pouvoir garantir l’intégrité et la confidentialité des biens à protéger du produit (codes et clés secrètes).

Chapitre 7

Certification

7.1 Objet

91 Le produit dont les caractéristiques de sécurité sont définies dans la cible de sécurité [6], satisfait aux exigences du niveau d'évaluation **EAL1 augmenté** du composant d'assurance **AVA_VLA.2** "Analyse de vulnérabilités effectuée de manière indépendante".

92 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'attaques tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.**

7.2 Portée de la certification

93 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.

94 Le certificat ne s'applique qu'à la version évaluée du produit, telle qu'elle est définie en annexe B de ce rapport.

95 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Caractéristiques de sécurité

96 Les caractéristiques de sécurité évaluées sont décrites dans la cible de sécurité [6] qui est la référence pour l'évaluation. Compte-tenu du caractère confidentiel de la cible de sécurité, un résumé public de la cible de sécurité a été rédigé [7].

97 La cible de sécurité étant rédigée en langue anglaise, les paragraphes ci-après sont une traduction française des politiques de sécurité organisationnelles, des hypothèses, des menaces ainsi que des objectifs et des exigences de sécurité.

1.1 Politiques de sécurité organisationnelles

OSP.PH_BEHAV	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.
OSP.A_LA_TRUSTED	L'acquéreur et l'agent de chargement sont des agents autorisés par l'émetteur de valeur électronique.
OSP.EV_INDIC	Il doit exister un moyen pour indiquer au porteur le montant de valeur électronique des transactions.
OSP.INTENT_TRANS	Chaque transaction électronique doit être une action intentionnelle du porteur. Une procédure doit être définie par le fournisseur du porte-monnaie électronique afin de permettre au porteur d'accepter ou de refuser les transactions.
OSP.IEP_ID	Le porte-monnaie électronique doit avoir une identification unique dans le système.
OSP.IEP_PD	L'équipement d'acceptation du commerçant doit avoir une identification unique pour l'équipement acquéreur.
OSP.LINK_SP_PD	Le commerçant doit être associé à son équipement d'acceptation (son compte bancaire doit être crédité une seule fois par remise).
OSP.SP_A_CLT	Le commerçant ne peut être collecté que par sa banque acquéreur.
OSP.ROLE	La cible d'évaluation doit administrer des rôles de sécurité et ces rôles doivent être indépendants.
OSP.EX_LOG	Les enregistrements des fichiers "exception logs" doivent être occasionnellement supprimés des porte-monnaie électroniques ; ceux-ci doivent donc être enregistrés ailleurs dans le système avant leur destruction. Les enregistrements doivent pouvoir comptabiliser la valeur électronique qui aurait été perdue durant les transferts incomplets.

OSP.COLLECT	Le commerçant doit garantir qu'une opération de collecte est effectuée avant que le fichier de "payment log" soit rempli, la précédente opération de collecte sera réinscrite (nature "tournante" du fichier de payment log).
OSP.LICENSE	Les licences représentent les mécanismes pour contrôler l'accès aux opérations réservées. Chaque licence contient un numéro de séquence pour s'assurer qu'elle ne peut être utilisée qu'une seule fois. La génération des licences pour les opérations réservées doit être effectuée dans un environnement sécurisé et conformément à des procédures appropriées pour détecter tout abus non autorisé.

1.2 Menaces

1.2.1 Blanchiment d'argent

T.LAUND_MON	Blanchiment d'argent afin de cacher les sources réelles de l'argent.

1.2.2 Usurpation d'identité

T.USP_LA_LD	Usurpation de l'identité de l'agent de chargement : chargement d'un porte-monnaie électronique avec de la fausse valeur électronique.
T.USP_IEP_LD	Usurpation de l'identité d'un porte-monnaie électronique : chargement de vraie valeur électronique dans un faux porte-monnaie.
T.USP_PP_EVP_PCH	Usurpation de l'identité du fournisseur de porte-monnaie ainsi que de l'émetteur de valeur électronique : paiement par un faux porte-monnaie électronique contenant de la fausse valeur électronique.
T.USP_PP_PCH_IEP	Usurpation de l'identité du fournisseur de porte-monnaie : paiement par un faux porte-monnaie électronique contenant de la vraie valeur électronique.
T.USP_PP_PCH_PD	Usurpation de l'identité du fournisseur de porte-monnaie : paiement par un porte-monnaie électronique contenant de la vraie valeur électronique avec un équipement d'acceptation frauduleux.
T.USP_PP_EVP_CLT	Usurpation de l'identité du fournisseur de porte-monnaie ainsi que de l'émetteur de valeur électronique : remise de fausse valeur électronique à l'acquéreur par un équipement d'acceptation frauduleux.
T.USP_A_CLT	Usurpation de l'identité de l'acquéreur : remise de valeur électronique dans un équipement acquéreur frauduleux.

1.2.3 Rejeu

T.RPLY_LD	Rejeu d'un chargement.
T.RPLY_PCH_C	Rejeu d'un paiement conduisant à une création de valeur électronique.
T.RPLY_PCH_L	Rejeu d'un paiement conduisant à une perte de valeur électronique.
T.RPLY_CLT	Rejeu d'une remise.

1.2.4 Défaillances

T.FAIL_PCH	Défaillances durant une transaction de paiement.
T.FAIL_CLT	Défaillances durant une transaction de remise.
T.FAIL_LD	Défaillances durant une transaction de chargement.

1.2.5 Contre-façon

T.FORG_LD_C	Contre-façon d'une transaction de chargement conduisant à une création de valeur électronique.
T.FORG_LD_L	Contre-façon d'une transaction de chargement conduisant à une perte de valeur électronique.
T.FORG_PCH_C	Contre-façon d'une transaction de paiement conduisant à une création de valeur électronique.
T.FORG_PCH_L	Contre-façon d'une transaction de paiement conduisant à une perte de valeur électronique.
T.FORG_CLT_C	Contre-façon d'une transaction de remise conduisant à une création de valeur électronique.
T.FORG_CLT_L	Contre-façon d'une transaction de remise conduisant à une perte de valeur électronique.

1.2.6 Perte d'intégrité

T.INTEG_EV	Modification non autorisée de valeur électronique.
T.INTEG_TD	Modification non autorisée des données des fichiers "exception logs".
T.INTEG_PARA	Modification non autorisée des paramètres du porte-monnaie électronique.

1.3 Hypothèses sur l'environnement

A.AD	L'équipement acquéreur préserve un état sûr lorqu'une erreur survient au cours d'une transaction de remise, ou en cas de transactions illicites.
A.LA	L'équipement de chargement préserve un état sûr lorqu'une erreur survient au cours d'une transaction de chargement, ou en cas de transactions illicites.

1.4 Objectifs pour la cible d'évaluation

O.EV	La TSF doit offrir les moyens pour éviter la création ou la perte de valeur électronique.
O.INTEG_DATA	La TSF doit offrir les moyens pour éviter la modification non autorisée de la valeur électronique, des données des fichiers "exception logs" ou des paramètres du porte-monnaie électronique et de l'équipement d'acceptation.
O.LOGICAL	La TSF doit prévenir contre l'accès non autorisé à la cible d'évaluation et contre le contournement du modèle de flux de valeur électronique.
O.AUTH	La TSF doit assurer l'authentification de la cible d'évaluation vis-à-vis des équipements de chargement ou acquéreurs.
O.ACCESS	La TSF doit assurer le contrôle des données utilisateurs aux seuls utilisateurs autorisés.
O.OPERATE	La TSF doit assurer la continuité de la sécurité en cas de rupture de transactions.
O.REPLAY	La TSF doit assurer que les transactions illicites (rejeu) sont détectées et contrées.
O.TAMPER	La TSF doit se prémunir contre les attaques physiques.
O.DOMAIN	La TSF doit maintenir une séparation des domaines entre l'application porte-monnaie électronique et d'autres applications.

1.5 Objectifs pour l'environnement

O.SYSTEM	L'émetteur de valeur électronique doit garantir la valeur électronique dans le système sur la base d'une politique de sécurité.
O.EV_DISTRIB	Les équipements de chargement et acquéreur ne doivent pas créer de valeur électronique.
O.LA_FAIL	L'équipement de chargement doit préserver un état sûr en cas d'erreurs de transactions, ou de transactions illicites.
O.AUTH2	Les équipements de chargement et acquéreurs doivent se prémunir contre l'accès d'utilisateurs non autorisés.
O. INSTALL	Le fournisseur de porte-monnaie électronique doit s'assurer que la cible d'évaluation est livrée et installée de manière sûre.
O. MANAGE	Le fournisseur de porte-monnaie électronique doit s'assurer que la cible d'évaluation est administrée de manière sûre.
O.ACQ	L'équipement acquéreur doit préserver un état sûr en cas d'erreurs de transactions, ou de transactions illicites.

1.6 Exigences fonctionnelles de sécurité

Audit de Sécurité	FAU_GEN.1	Génération de données d'audit..
	FAU_STG.1	Stockage protégé de traces d'audit.
Communication	FCO_NRO.2	Preuve systématique de l'origine.
	FCO_NRR.2	Preuve systématique de la réception.
Cryptographie	FCS_COP.1	Opération cryptographique.
Protection des données utilisateur	FDP_ACC.2	Contrôle d'accès complet.
	FDP_ACF.1	Contrôle d'accès basé sur les attributs de sécurité.
	FDP_DAU.1	Authentification de données élémentaire.
	FDP_ETC.1	Exportation de données de l'utilisateur sans attributs.
	FDP_IFC.1	Contrôle de flux d'information partiel.
	FDP_IFF.1	Attributs de sécurité simple.
	FDP_ITC.1	Importation de données de l'utilisateur sans attributs.
	FDP_SDI.1	Contrôle de l'intégrité des données stockées.
Identification et authentification	FIA_UID.1	Timing de l'identification.
	FIA_UAU.1	Timing de l'authentification.
	FIA_UAU.3	Authenfication infalsifiable.
	FIA_UAU.4	Mécanismes d'authentification.
	FIA_UAU.6	Réauthentification.
Protection des fonctions de sécurité	FPT_FLS.1	Défaillance avec préservation d'un état sûr.
	FPT_PHP.2	Notification d'une attaque physique.
	FPT_PHP.3	Résistance à une attaque physique.
	FPT_RCV.4	Reprise de fonction.
	FPT_RPL.1	Détection de rejeu.
	FPT_RVM.1	Capacité de la TSP à ne pas être court-circuitée.
	FPT_SEP.1	Séparation des domaines de la TSF.

1.7 Exigences d'assurance

Cible de sécurité	ASE	Évaluation de la cible de sécurité.
EAL1	ACM_CAP.1	Numéros de version.
	ADO_IGS.1	Procédures d'installation, de génération et de démarrage.
	ADV_FSP.1	Spécifications fonctionnelles informelles.
	ADV_RCR.1	Démonstration de correspondance informelle.
	AGD_ADM.1	Guide de l'administrateur.
	AGD_USR.1	Guide de l'utilisateur.
	ATE_IND.1	Tests effectués de manière indépendante - conformité.
Augmentation	AVA_VLA.2	Analyse de vulnérabilités effectuée de manière indépendante.

Annexe B

Configuration de la cible d'évaluation

98 La cible d'évaluation est constituée du microcircuit destiné à être inséré dans une carte porte-monnaie électronique "Mondex Purse 2".

99 Elle est référencée de la manière suivante :

Composant	Système d'exploitation	Version d'application
SLE66CX160S	MULTOS V4 masque 1N	0203

100 La documentation disponible pour le produit comprend notamment le document :

- Mondex Purse 2.0/4-Guidelines for Card Issuers.

Annexe C

Glossaire

C.1 Abréviations

CC	(Common Criteria) - Critères Communs, l'intitulé utilisé historiquement pour la présente norme à la place de l'intitulé officiel de l'ISO 15408: "Critères d'évaluation de la sécurité des technologies de l'information"
EAL	(Evaluation Assurance Level) - Niveau d'assurance de l'évaluation
PP	(Protection Profile) - Profil de protection
SF	(Security Function) - Fonction de sécurité
SFP	(Security Function Policy) - Politique d'une fonction de sécurité
ST	(Security Target) - Cible de sécurité
TI	(IT : Information Technology) - Technologie de l'Information
TOE	(Target of Evaluation) - Cible d'évaluation
TSF	(TOE Security Functions) - Ensemble des fonctions de sécurité de la TOE

C.2 Glossaire

Acquéreur	Agent autorisé de l'émetteur de valeur électronique qui est responsable de la collecte de valeur électronique auprès des équipements d'acceptation des commerçants.
Affectation	La spécification d'un paramètre identifié dans un composant.
Agent de chargement	Agent autorisé de l'émetteur de valeur électronique qui est responsable du chargement des porte-monnaie électroniques par de la valeur électronique créée préalablement par l'émetteur de valeur électronique.
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 les contre-mesures d'une TOE.
Cible d'évaluation (TOE)	Un produit ou un système TI et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité (ST)	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Classe	Un groupement de familles qui partagent un thème commun.
Composant	Le plus petit ensemble sélectionnable d'éléments qui peut être inclus dans un PP, une ST ou un paquet.
Émetteur de valeur électronique	L'émetteur de valeur électronique garantit la valeur électronique dans le système. Dans ce but, l'émetteur de valeur électronique crée la valeur électronique et la diffuse en échange de fonds, la collecte et la détruit en retour.
Équipement acquéreur	Afin de pouvoir collecter l'ensemble des transactions de valeur électronique, l'acquéreur dispose d'un ou plusieurs équipements acquéreurs.

Équipement d'acceptation	Équipement du commerçant utilisé pour accepter les paiements lors d'une transaction de paiement par porte-monnaie électronique.
Évaluation	Estimation d'un PP, d'une ST ou d'une TOE par rapport à des critères définis.
Fournisseur du porte-monnaie électronique	Le fournisseur de porte-monnaie électronique est responsable de la sécurité du système de porte-monnaie (ici Mondex International).
Fonction de sécurité	Une partie ou des parties de la TOE sur lesquelles on s'appuie pour appliquer un sous-ensemble étroitement imbriqué de règles tirées de la TSP.
Informel	Qui est exprimé à l'aide d'un langage naturel.
Itération	L'utilisation multiple d'un composant avec des opérations différentes.
Niveau d'assurance de l'évaluation	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 TI qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Raffinement	L'addition de détails à un composant.
Sélection	La spécification d'une ou de plusieurs entités à partir d'une liste au sein d'un composant.
Utilisateur	Toute entité (utilisateur humain ou entité TI externe) hors de la TOE qui interagit avec elle.
Valeur électronique	Contre-partie des fonds reçus par l'émetteur de valeur électronique ; elle est définie par l'identité de l'émetteur de valeur électronique, le montant et la devise.

Annexe D

Références

[1] [CC-1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIB-98-026, version 2.0 May 1998.

[2] [CC-2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIB-98-027, version 2.0 May 1998.

[3] [CC-2B] Common Criteria for Information Technology Security Evaluation Part 2 annexes CCIB-98-027A, version 2.0 May 1998.

[4] [CC-3] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIB-98-028, version 2.0 May 1998.

[5] [CEM] Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0.

[6] Cible de sécurité “EAL1 Common Criteria Security Target for the Mondex Purse”, référencée mxi-alberto-doc-001, version 1.1 du 22/10/99, document non public.

[7] Résumé de la cible de sécurité “Mondex Purse 2.0/4 Alberto Security Target Summary”, référencée mxi-alberto-doc-009, version 0.1 du 15/11/99, document public.

[8] Rapport Technique d’Évaluation, référencée RTE_AL, version 1.0 du 3/11/99, document non public.