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

PREMIER MINISTRE

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

CERTIFICAT 2001/22

Application M/Chip Select v2.0.5.2

installée sur la plate-forme SLE66CX160M + MULTOS V4 release 1N'

Développeur : Mondex International Limited

EAL1 Augmenté

Commanditaire : Mondex International Limited

Le 22 octobre 2001,

Le Commanditaire :
Le Chief Executive Officer
Mondex International Limited
Richard FLETCHER

L'Organisme de certification :
Le Directeur Central de la Sécurité des Systèmes d'Information
Henri SERRES

Ce produit a été évalué par un centre d'évaluation de la sécurité des TI conformément aux Critères Communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée du produit dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de certification :
Secrétariat Général de la Défense Nationale
DCSSI
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

IT Security Certified

Common Criteria

Chapitre 1

Résumé

1.1 Objet

1 Ce document représente le rapport de certification de l'application M/Chip Select v2.0.5.2 installée sur la plate-forme SLE66CX160M + MULTOS V4 release 1N'.

2 L'application M/Chip Select est une application de débit/crédit conforme aux spécifications EMV. Pour l'évaluation, cette application est installée sur la carte à puce constituée du micro-circuit Infineon SLE66CX160M et du système d'exploitation Keycorp MULTOS V4 release 1N'+AMD 0013v002.

3 Le développeur de la cible d'évaluation est Mondex International Ltd :

- Mondex International Limited
  47-53 Cannon Street
  London EC4M 5SH
  Royaume Uni.

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

5 Le niveau d'assurance atteint est le niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" décrit dans la partie 3 des Critères Communs [CC].

6 L'évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information CEACI :

- CEACI (Thalès Microelectronics - CNES)
  18, avenue Edouard Belin
  31401 Toulouse Cedex 4
  France.

1.2 Contexte de l'évaluation

7 L'évaluation s'est déroulée d'avril à septembre 2001.

8 Le commanditaire de l'évaluation est Mondex International Ltd :

- Mondex International Limited
  47-53 Cannon Street
  London EC4M 5SH
  Royaume Uni.

Chapitre 2

Description de la cible d'évaluation

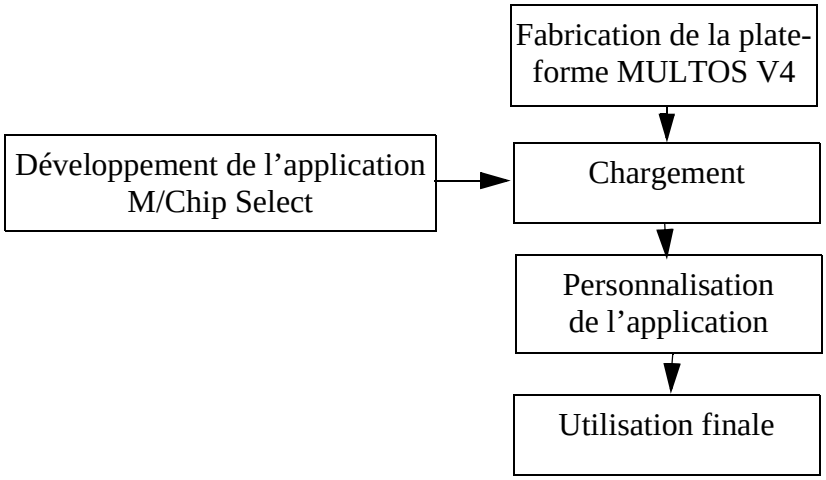
2.1 Périmètre de la cible d'évaluation

9 La cible d'évaluation est l'application M/Chip Select v2.0.5.2 développée en MAL par Mondex International et destinée à être chargée sur une plate-forme MULTOS V4.

10 Pour l'évaluation, cette application est installée sur la plate-forme contituée des éléments suivants :

- le système d'exploitation MULTOS V4 release 1N'+AMD 0013v002 développé par Keycorp Ltd ;
- le micro-circuit SLE66CX160M (version M1401C13 ou M1401C16) développé et fabriqué par Infineon Technologies AG.

2.2 Cycle de vie



2.3 Fonctions de sécurité évaluées

11 Les fonctions de sécurité évaluées sont les suivantes :

- Génération de cryptogrammes pour les commandes GENERATE AC ;
- Authentification dynamique des données ;
- Contrôle d'accès aux clés ;
- Contrôle d'intégrité des clés ;
- Authentification du porteur ;
- Authentification et ré-authentification de l'émetteur ;

- Contrôle des commandes ;
- Anti-rejeu ;
- Gestion sécurisée des données sensibles ;
- Confidentialité et intégrité des données transmises.

12 La fonction d'authentification statique est hors du périmètre de l'évaluation.

2.4 Documentation disponible

13 Le guide disponible pour l'évaluation [GUIDE] décrits les fonctions d'administration et d'utilisation de l'application.

14 L'émetteur des cartes contenant l'application évaluée devra retranscrire les informations présentes dans ce guide dans les manuels qui seront distribués aux responsables du chargement, de la personnalisation et des utilisateurs finaux.

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

Le niveau visé est EAL1 augmenté du composant AVA_VLA.2 «Analyse de vulnérabilités indépendante» :

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	Introduction de la ST (ASE_INT.1) Description de la TOE (ASE_DES.1) Environnement de sécurité (ASE_ENV.1) Objectifs de sécurité (ASE_OBJ.1) Annonce de conformité à un PP (ASE_PPC.1) Exigences de sécurité des TI (ASE_REQ.1) Exigences de sécurité des TI explicitement énoncées (ASE_SRE.1) Spécifications globales de la TOE (ASE_TSS.1)
Gestion de configuration	Numéros de version (ACM_CAP.1)
Livraison et exploitation	Procédures d'installation, de génération et de démarrage (ADO_IGS.1)
Développement	Spécifications fonctionnelles informelles (ADV_FSP.1) Démonstration de correspondance informelle (ADV_RCR.1)
Guides	Guide de l'administrateur (AGD_ADM.1) Guide de l'utilisateur (AGD_USR.1)
Tests	Tests indépendants - conformité (ATE_IND.1)
Estimation des vulnérabilités	Analyse de vulnérabilités indépendante (AVA_VLA.2)

15 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.

16 Le détail des travaux d'évaluation menés est disponible dans le Rapport Technique d'Evaluation [RTE].

17 Conformément au niveau visé, les seules informations de conception qui ont été fournies à l'évaluateur sont les spécifications fonctionnelles des fonctions de sécurité.

18 Pour l'évaluation, les administrateurs des fonctions de sécurité sont les émetteurs des cartes et les utilisateurs sont les utilisateurs finaux. Les guides qui leurs seront distribués doit être conformes au document évalué [GUIDE].

19 Les procédures d'installation, de génération et de démarrage (composant ADO_IGS.1) évaluées sont les procédures de génération des ALU, de chargement de l'application et la réponse au Reset de l'application.

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeur

20 Conformément au niveau d'évaluation visé, le développeur n'a pas eu à fournir sa stratégie de tests fonctionnels.

3.2.2 Tests évaluateur

21 L'évaluateur a réalisé des tests fonctionnels pour s'assurer par échantillonnage que les fonctions de sécurité identifiées dans la cible de sécurité sont bien réalisées par le produit en évaluation.

22 Les tests fonctionnels et les tests de pénétration ont été menés sur le produit constitué de l'application et la plate-forme identifiée au chapitre 2. Les résultats obtenus ne sont pas valables si l'application est installée sur une autre plate-forme.

23 L'évaluateur a également mené une analyse de vulnérabilités, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élémentaire (composant AVA_VLA.2) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation suivants :

- la cible d'évaluation doit pouvoir authentifier le porteur et l'émetteur ;
- la cible d'évaluation doit empêcher les attaques par rejeu ;
- la cible d'évaluation doit empêcher la prédiction des valeurs des données utilisées pour l'authentification notamment ;
- la cible d'évaluation doit protéger en confidentialité et intégrité les clés cryptographiques et les données associées au PIN ;
- la cible d'évaluation doit s'assurer que les données des transactions et des authentifications ne peuvent pas être falsifiées ;
- les services offerts par la cible d'évaluation doivent rester disponibles.

Chapitre 4

Certification

4.1 Verdict

24 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [CC].

4.2 Recommandations

25 L'application M/Chip Select v2.0.5.2 est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat :

a) pour les terminaux :

- les terminaux utilisés doivent fournir les fonctionnalités EMV et être testés et validés ;

c) pour la plate-forme MULTOS 4 :

- la plate-forme doit protéger les données de l'application contre les attaques physiques ;
- la plate-forme doit garantir l'étanchéité entre les différentes applications installées ;
- la plate-forme doit vérifier régulièrement l'intégrité du code de l'application ;
- la plate-forme doit fournir des primitives DES et RSA sûres ;

h) pour l'émetteur :

- des mesures de sécurité doivent être mise en place pour protéger les données sensibles hors de la carte ;
- le personnel en charge des fonctions administratives doit être de confiance et entraîné ;
- l'émetteur doit vérifier dans son système que l'utilisation des ATC est cohérente ;

l) pour le porteur :

- le porteur doit garder confidentielles ses données personnelles.

4.3 Certification

26 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.

27 Le certificat ne s'applique qu'à la version évaluée du produit, identifiée au chapitre 2. La certification d'une version ultérieure de l'application ou sur une autre plate-forme nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Glossaire

ALU	Application Load Unit : Format des applications pour leur chargement sur une plate-forme MULTOS.
Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
ATC	Application Transaction Counter : compteur utilisé dans les transactions.
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.
Emetteur	Banque ou organisme qui émet la carte de débit/crédit.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
MAL	Langage de programmation des applications destinées à être chargées sur les cartes équipées du système d'exploitation MULTOS.
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.
PIN	Personal Identification Number : code d'identification du porteur.

Porteur	Utilisateur final de la carte de débit/crédit.
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] 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.
- Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.
- 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] - M/Chip Select Application Security Target Summary v0-1, réf. mxi-mchip-stg-002, Mondex International Ltd, 26 sept. 2001. (diffusion libre).
- M/Chip Select Application Security Target rev 0-9, réf. mxi-mchip-stg-001, Mondex International Ltd, 3 sept. 2001.

[RTE] Evaluation Technical Report rev 1.0, réf. JAB_RTE, CEACI, 21 sept. 2001 (diffusion contrôlée).

[GUIDE] M/Chip Select Application User and Administrator Guidance rev 0-4, réf. mxi-mchip-gui-001, Mondex International, 18 juil. 2001.

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information à l'adresse suivante :

www.ssi.gouv.fr

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

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau Certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr