PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2003/10

Application M/Chip 4 version 1.0.1.1 pour MULTOS (sur émulateur)

Paris, le 8 septembre 2003

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en terme d'objectifs de sécurité.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par l'organisme de certification, et ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables.

Avant-propos

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendu public (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

www.commoncriteria.org

Accords de reconnaissance des certificats

L'**accord de reconnaissance** européen du SOG-IS de 1999 permet la reconnaissance entre les états signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

La direction centrale de la sécurité des systèmes d'information passe aussi des **accords de reconnaissance** avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de la Communauté européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties.

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, le Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

L'accord du Common Criteria Recognition Arrangement, permet la reconnaissance, par les pays signataires de l'accord[1], des certificats délivrés dans le cadre du schéma Critères Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

Pays	Organisme certificateur	Site web
France	DCSSI	www.ssi.gouv.fr
Royaume-Uni	CESG	www.cesg.gov.uk
Allemagne	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australie-Nouvelle Zélande	AISEP	www.dsd.gov.au/infosec
Etats-Unis	NIAP	www.niap.nist.gov

[1] En janvier 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada et l'Australie-Nouvelle Zélande ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Espagne, la Finlande, la Grèce, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, l'Autriche et le Japon.

Table des matières

1. LE PRODUIT EVALUE 6

1.1. IDENTIFICATION DU PRODUIT 6
1.2. LE DEVELOPPEUR 6
1.3. DESCRIPTION DU PRODUIT EVALUE 6
1.3.1. Architecture 6
1.3.2. Cycle de vie standard d'une carte à puce 7
1.3.3. Périmètre et limites du produit évalué 7
1.4. UTILISATION ET ADMINISTRATION 8
1.4.1. Utilisation 8
1.4.2. Administration 8

2. L'EVALUATION 9

2.1. CENTRE D'EVALUATION 9
2.2. COMMANDITAIRE 9
2.3. REFERENTIELS D'EVALUATION 9
2.4. EVALUATION DE LA CIBLE DE SECURITE 9
2.5. EVALUATION DU PRODUIT 9
2.5.1. Développement du produit 9
2.5.2. Documentation 10
2.5.3. Livraison et installation 10
2.5.4. L'environnement de développement 10
2.5.5. Tests fonctionnels 11
2.5.6. Estimation des vulnérabilités 11

3. CONCLUSIONS DE L'EVALUATION 12

3.1. RAPPORT TECHNIQUE D'EVALUATION 12
3.2. NIVEAU D'EVALUATION 12
3.3. EXIGENCES FONCTIONNELLES 13
3.4. RESISTANCE DES FONCTIONS 14
3.5. ANALYSE DES MECANISMES CRYPTOGRAPHIQUES 14
3.6. CONFORMITE A UN PROFIL DE PROTECTION 14
3.7. RECONNAISSANCE EUROPEENNE (SOG-IS) 14
3.8. RECONNAISSANCE INTERNATIONALE (CC RA) 14
3.9. RESTRICTIONS D'USAGE 14
3.10. OBJECTIFS DE SECURITE SUR L'ENVIRONNEMENT 14
3.11. SYNTHESE DES RESULTATS 15

ANNEXE 1. RAPPORT DE VISITE DU SITE DE LONDRES DE MONDEX 16

ANNEXE 2. ANALYSE DES MECANISMES CRYPTOGRAPHIQUES 17

ANNEXE 3. EXIGENCES FONCTIONNELLES DE SECURITE DU PRODUIT EVALUE .. 18

ANNEXE 4. NIVEAUX D'ASSURANCE PREDEFINIS IS 15408 OU CC 20

ANNEXE 5. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 21

ANNEXE 6. REFERENCES LIEES A LA CERTIFICATION 24

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est l'**application M/Chip 4 version 1.0.1.1** pour MULTOS développée par **Mondex International Limited**.

1.2. Le développeur

Mondex International Limited

47-53 Canon Street
London EC4M 55Q
Angleterre

1.3. Description du produit évalué

Le produit évalué est une application pour cartes à puce permettant de réaliser des transactions de débit et de crédit dans des terminaux. L'application, et plus généralement la carte à puce, est associée à un compte bancaire du porteur de la carte. L'application est conforme[1] aux spécifications EMV (Europay MasterCard Visa).
Pour être utilisée, l'application doit être chargée et installée sur une plate-forme MULTOS (conforme aux spécifications MULTOS version 4).
Elle comporte deux modes d'utilisation : M/Chip 4 Select et M/Chip 4 Lite. Le mode d'utilisation est choisi par le terminal de paiement (en fonction de ses capacités) avant d'initier la transaction. Le premier mode, M/Chip 4 Select, permet l'ensemble des fonctionnalités offertes par le produit (notamment des transactions en mode DDA (Authentification Dynamique de Données)), tandis que le mode M/Chip 4 Lite ne permet ni d'Authentification Dynamique de Données, ni de Combinaison DDA/AC (Application Cryptogram) (CDA) ni de transmission chiffrée du code PIN.

1.3.1. Architecture

Le produit s'intègre de la manière suivante sur un émulateur MULTOS (cf § 1.3.3) :

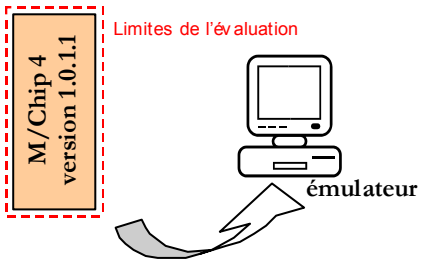

Figure 1 - Application M/Chip 4 sur émulateur

[1] Toutefois, le présent rapport de certification n'atteste pas que le produit est *effectivement* conforme aux spécifications EMV.

Une description détaillée de l'architecture de l'application se trouve dans le document [HLD].

1.3.2. Cycle de vie standard d'une carte à puce

Le cycle de vie standard d'une carte à puce est le suivant. Il a été rajouté le développement et le chargement de l'application M/Chip 4 dans ce cycle de vie afin de montrer comment ils interviennent dans un cycle de vie de carte à puce :

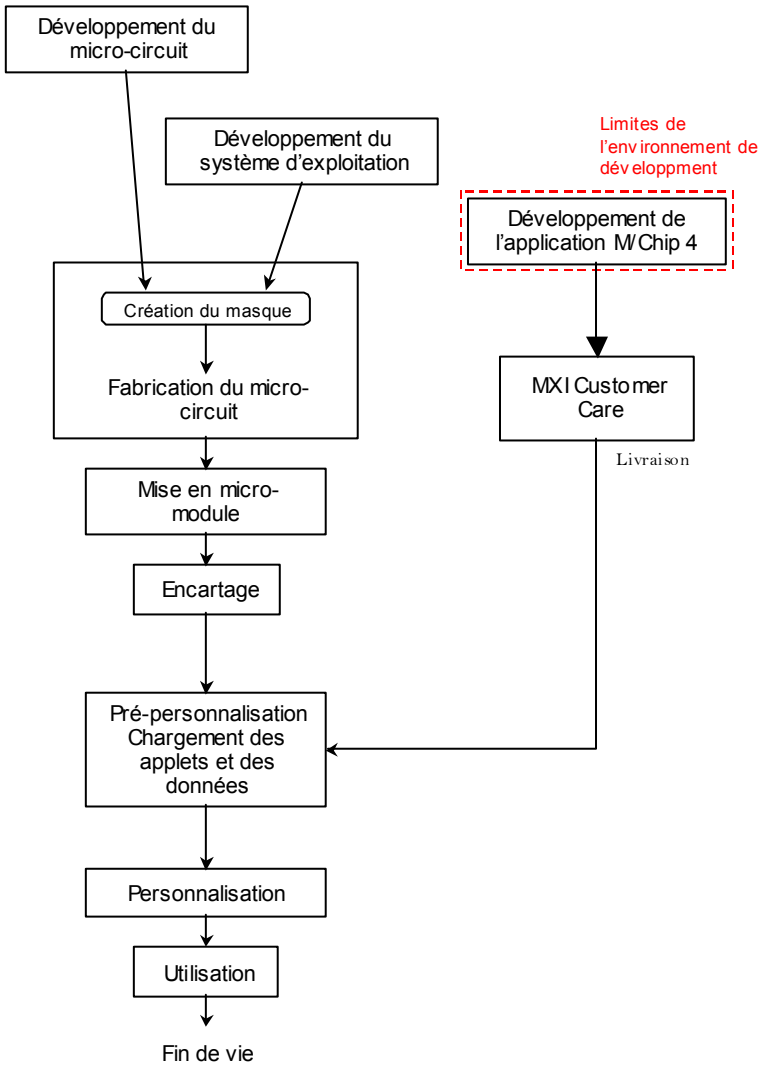

Figure 2 - Cycle de vie standard d'une carte à puce

Le chargement de l'application se fait dans la phase de pré-personnalisation.

1.3.3. Périmètre et limites du produit évalué

Seule l'application M/Chip 4 version 1.0.1.1 (Figure 1) a fait l'objet d'une évaluation. Toutefois pour les besoins de cette dernière, l'application a été chargée sur un émulateur. Cet émulateur a été la plate-forme MULTOS I4C (1-0-2) (incluant le patch AMD 0029v002) de Keycorp Ltd, avec le micro-circuit SLE66CX322P m1484/a23 développé et fabriqué par Infineon Technologies AG. La plate-forme ne fait pas partie du périmètre d'évaluation.

1.4. Utilisation et administration

1.4.1. Utilisation

L'utilisateur du produit M/Chip 4 est le porteur de la carte à puce comportant l'application. Les fonctions de sécurité disponibles pour les utilisateurs sont l'entrée du code PIN, le changement du code PIN (si autorisé par l'émetteur de la carte à puce) et effectuer une transaction financière avec la carte. Ces informations se trouvent dans le guide utilisateur [USR] qui décrit aussi les actions à effectuer par l'utilisateur lorsqu'une transaction financière est arrêtée, lorsque l'application ne fonctionne plus, lorsque le code PIN n'est plus accepté par l'application ou encore lorsque les transactions financières sont systématiquement refusées (suite par exemple au blocage de l'application).

1.4.2. Administration

Les administrateurs de l'application sont le responsable du chargement de l'application sur une plate-forme MULTOS, l'émetteur de la carte et le personnalisateur de l'application.

Pour la phase de chargement de l'application la fonction de sécurité principale est le chargement de l'application décrite dans le document [IGS].

L'émetteur de la carte peut bloquer et débloquer l'application, changer et débloquer le code PIN et il peut modifier les données spécifiques à l'application. Il est aussi en charge de livrer les cartes aux futurs utilisateurs et de prendre en charge les cartes qui lui sont retournées par les utilisateurs. Le document [ADM] décrit les opérations à effectuer pour ces différentes fonctions.

Et en phase de personnalisation de l'application, les recommandations et instructions à respecter sont spécifiées dans les documents [ADM] et [IGS].

2. L'évaluation

2.1. Centre d'évaluation

CEACI (Thalès Microelectronics – CNES)

18 avenue Edouard Belin
31401 Toulouse Cedex 4

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

L'évaluation s'est déroulée de **juin 2002** à **avril 2003**.

2.2. Commanditaire

Mondex International Limited

47-53 Canon Street
London EC4M 55Q
Royaume-Uni

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

2.5.1. Développement du produit

La classe d'assurance ADV – développement – définit les exigences de raffinement pas à pas des fonctions de sécurité du produit depuis ses spécifications globales dans la cible de sécurité [ST] jusqu'à l'implémentation. Chacune des représentations des fonctions de sécurité du produit qui résulte de ce processus fournit des informations qui aident l'évaluateur à déterminer si les exigences fonctionnelles du produit ont été satisfaites.
L'analyse des documents associés à la classe ADV montre que les exigences fonctionnelles sont correctement et complètement raffinées dans les différents niveaux de représentation du

produit (spécifications fonctionnelles (FSP), sous-systèmes (HLD), modules (LLD) et implémentation (IMP)), jusqu'à l'implémentation de ses fonctions de sécurité.
Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.2. Documentation

Du point de vue de l'évaluation, les administrateurs sont le responsable du chargement de l'application (guide [IGS]), l'émetteur de la carte (guide [ADM]) et le personnalisateur de l'application (guides [ADM] et [IGS]).
Du point de vue de l'évaluation, les utilisateurs considérés sont les porteurs de carte à puce comportant l'application M/Chip 4 (guide [USR]).
Les guides utilisateur [USR] et administrateur [ADM et IGS] répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.3. Livraison et installation

La livraison est considérée juste après le développement du produit. L'application développée est livrée au site de Mondex à Warrington, pour être ensuite livrée à un client sur son site de pré-personnalisation de carte afin de charger l'application sur la plate-forme MULTOS.
La procédure [DEL] de livraison au site de Warrington est suffisante pour répondre aux exigences demandées : elle permet de connaître l'origine de la livraison et de détecter une modification du produit pendant la livraison.
L'installation du produit correspond au chargement de l'application sur la plate-forme. Les procédures d'installation, de génération et de démarrage [IGS] permettent d'obtenir une configuration sûre de l'application.
Les documents fournis pour la classe ADO – livraison et opération – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.4. L'environnement de développement

Le système de gestion de configuration est utilisé conformément au plan de gestion de configuration [ACM].
La liste de configuration [LGC] identifie les éléments tracés par le système de gestion de configuration. Les éléments de configuration identifiés dans la liste de configuration sont maintenus par le système de gestion de configuration. Les procédures de génération de l'application sont efficaces pour s'assurer que les bons éléments de configuration sont utilisés pour générer l'application.
Le produit est développé sur le site de Mondex International Limited situé :

47-53 Canon Street
London EC4M 55Q
Royaume-Uni

Les mesures de sécurité décrites dans les procédures fournissent le niveau nécessaire de protection pour maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.

La vérification de la mise en œuvre des procédures de développement et de gestion de configuration a été effectuée lors de l'audit du site de Mondex International Limited ci-dessus (cf Annexe 1). Le rapport d'audit se trouve sous la référence [Audit].
Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.5. Tests fonctionnels

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test. Il a vérifié aussi que toutes les caractéristiques fonctionnelles de chaque fonction de sécurité, telle qu'elles sont décrites dans la conception de haut niveau [HLD], sont couvertes par les tests du développeur.
Les tests ont été réalisés sur la plate-forme MULTOS I4C (version 1-0-2) (incluant le patch AMD 0029v002) développée par Keycorp Ltd. L'application M/Chip 4 version 1.0.1.1 était chargée sur cette plate-forme.

2.5.6. Estimation des vulnérabilités

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement couvertes.
L'évaluateur a réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités supplémentaires.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation de l'application M/Chip 4 version 1.0.1.1.

3.2. Niveau d'évaluation

L'application M/Chip 4 version 1.0.1.1 sur émulateur a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants du niveau d'évaluation du produit, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up	Réussite

[1] En Annexe 4 se trouve un tableau récapitulant les différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

	procedures	
Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** [ST chapitre 5] suivantes[1] :

- Enforced proof of origin (FCO_NRO.2)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failures handling (FIA_AFL.1)
- Timing of authentication (FIA_UAU.1)
- Single-use authentication mechanisms (FIA_UAU.4)

[1] En Annexe 3 se trouve un tableau complet explicitant les exigences fonctionnelles de sécurité du produit évalué.

- Re-authenticating (FIA_UAU.6)
- Management of TOE security functions data (FMT_MTD.1)
- Security management roles (FMT_SMR.1)
- Trusted Path (FTP_TRP.1)

3.4. Résistance des fonctions

Seules les fonctions d'authentification (du porteur et de l'émetteur de la carte à puce) ont fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance de ces fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse des mécanismes cryptographiques

Aucun mécanisme cryptographique n'a été coté dans le cadre de l'évaluation (cf Annexe 2).

3.6. Conformité à un profil de protection

(Sans objet)[1]

3.7. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité.

3.8. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité.
Les augmentations suivantes ne sont par reconnues dans le cadre du CC RA [CC RA] : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4 (Tableau 1).

3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides utilisateur [USR] et administrateur [ADM et IGS].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.10. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST § 4.2] :

- Le terminal doit supporter les fonctionnalités du système EMV et doit être testé et approuvé de façon appropriée. Le terminal communique avec l'application via la plate-forme MULTOS. Le terminal doit assurer que la vérification des

[1] La cible de sécurité [ST] du produit ne revendique pas de conformité à un profil de protection.

données du porteur sont constamment gardées confidentielles et effacées de manière sécurisée dès qu'elles ne sont plus utilisées (OE.TERMINAL) ;

- L'émetteur et le porteur de la carte à puce sur laquelle se trouve l'application doivent appliquer la politique de sécurité du système. L'émetteur doit communiquer au porteur les règles d'utilisation de l'application (OE.SYSTEM) ;
- L'émetteur doit s'assurer que l'application est délivrée et installée de manière sécurisée, y compris pour l'identifiant du compte auquel est rattaché l'application et les données SDA (OE.INSTALL) ;
- L'émetteur doit assurer que l'application est gérée, administrée et exploitée de manière sécurisée (OE.MANAGE) ;
- La plate-forme sur laquelle s'exécute l'application doit être résistante aux attaques physiques afin que les données sensibles ne puissent être lues, modifiées ou déduites à l'aide de telles attaques (OE.TAMPER) ;
- La plate-forme sur laquelle s'exécute l'application doit être un domaine séparé des autres applications. La plate-forme doit protéger (de manière logique) l'application contre toute modification non autorisée de son code source et de ses données (OE.DOMAIN) ;
- La plate-forme MULTOS sur laquelle s'exécute l'application doit fournir une primitive permettant de bloquer la carte (OE.BLOCK) ;
- Les données sensibles non stockées sur la carte doivent être protégées en confidentialité (OE.DATA_SEC) ;
- Le personnel responsable de l'administration de l'application sont des personnes de confiance et compétentes (OE.ADM_SEC) ;
- La plate-forme MULTOS sur laquelle s'exécute l'application doit vérifier l'intégrité du code de l'application à la sélection de cette dernière (OE.INTEGRITY) ;
- Le code PIN doit être délivré au porteur de manière sécurisée et séparément de la carte sur laquelle se trouve l'application (OE.CHV_INSTALL) ;
- La plate-forme MULTOS doit fournir des primitives DES et RSA pour l'application, s'exécutant correctement et sans fuite d'information sur les clés (OE.FCS_COP) ;
- Le système de l'émetteur doit contrôler les cryptogrammes ATC (Application Transaction Counter) afin de s'assurer qu'un même ATC n'est pas utilisé par la même carte pour des transactions différentes et que l'utilisation des ATC pour une carte donnée ne se contredise pas (OE.ATC) ;
- Le terminal doit exécuter les transactions en ligne s'il ne peut pas exécuter une authentification dynamique des données (DDA) (OE.ONLINE).

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que l'**application M/Chip 4 version 1.0.1.1** identifiée au paragraphe 1.1 et décrite au paragraphe 1.3 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. rapport de visite du site de Londres de Mondex

Le site de développement de **Mondex International Limited situé 47-53 Canon Street London EC4M 55Q, Royaume-Uni**, a fait l'objet, dans le cadre de l'évaluation de l'application M/Chip 4 version 1.0.1.1 pour MULTOS sur émulateur, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4)
- la livraison : **ADO** (ADO_DEL.2)
- le support au cycle de vie : **ALC** (ALC_DVS.2)

La visite par le centre d'évaluation accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 2. Analyse des mécanismes cryptographiques

L'application M/Chip 4 version 1.0.1.1 reprend les spécifications cryptographiques du système EMV. Aucun mécanisme cryptographique spécifique n'a été coté dans le cadre de l'évaluation de cette application.

Il est recommandé toutefois de ne pas utiliser de clés RSA de taille plus petite que 1024 bits.

Annexe 3. Exigences fonctionnelles de sécurité du produit evalué

Attention : les descriptions des composants fonctionnels suivants sont donnés à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles auxquelles répond le produit.

Class FCO	**Communication**
Non-repudiation of origin	
FCO_NRO.2	*Enforced proof of origin* Le produit doit générer systématiquement la preuve de l'origine des informations transmises (la liste de ces informations est spécifiée dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
FDP_IFC.1	Subset *information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'information.
Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Stored data integrity	
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions (spécifiées dans la cible de sécurité [ST]) suite à une détection d'erreur.
Class FIA	**Identification and authentication**
Authentication failures	

FIA_AFL.1	*Authentication failure handling* Le produit doit être capable d'arrêter le processus d'établissement d'une session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il doit aussi, après la clôture du processus d'établissement d'une session, être capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.
User authentication	
FIA_UAU.1	*Timing of authentication* Le produit autorise un utilisateur à exécuter certaines actions, spécifiées dans la cible de sécurité [ST], avant que son identité ne soit authentifiée.
FIA_UAU.4	*Single-use authentication mechanisms* Le mécanisme d'authentification doit fonctionner avec des données d'authentification à usage unique.
FIA_UAU.6	*Re-authenticating* Ce composant permet de spécifier des événements (spécifiés dans la cible de sécurité [ST]) pour lesquels l'utilisateur doit être ré-authentifié.
Class FMT	**Security management**
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiées dans la cible de sécurité [ST]).
Class FTP	**Trusted path/channels**
Trusted path	
FTP_TRP.1	*Trusted path* Un chemin de confiance entre le produit et un utilisateur doit être fourni pour un ensemble d'événements défini. Soit l'utilisateur soit le produit initie le chemin de confiance.

Annexe 4. Niveaux d'assurance prédéfinis IS 15408 ou CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 5. Références documentaires du produit évalué

[ACM]	Les procédures associées à la gestion de configuration sont : ▪ MXI Project Procedures – Document Review Procedures Référence mxi-general-prc-003 Version 3-0 12 février 2003 Mondex International ▪ MXI Project Procedures – Change Control Procedures Référence mxi-general-prc-004 Version 2-0 04 avril 2000 Mondex International ▪ Configuration Management Processes and Procedures Référence mxi-general-prc-005 Version 2-0 10 décembre 1999 Mondex International ▪ MXI Project Procedures Fault Control Procedures Référence mxi-general-prc-006 Version 2-0 28 avril 2000 Mondex International ▪ M/Chip 4 for MULTOS Version 4.0 Build A Project Definition Document Référence mxi-mchip-pdd-001 Version 2-0 08 mai 2002 Mondex International ▪ M/Chip Version 4 EAL 4+ Project Definition Document Référence mxi-mchip-pdd-006 Version 3-0 16 juillet 2002 Mondex International ▪ M/Chip 4 for MULTOS Application PVCS Configuration Référence mxi-mchip4-doc-007 Version 0-2 16 juillet 2002 Mondex International ▪ PVCS VM I-NET Guide Référence mxi-pvcs-usg-001 Version 0-3 01 mars 2001 Mondex International

	▪ M/Chip 4 for MULTOS Version 4.0 Code Build and Delivery Procedure Référence mxi-mchip4-bld-001 Version 1-0 16 décembre 2002 Mondex International ▪ MXI Project Procedures Document Naming Conventions *Référence* mxi-general-prc-007 *Version* 2-0 04 avril 2000 Mondex International
[ADM]	M/Chip 4 form MULTOS application User and Administration Guidance Référence mxi-mchip-gui-003 Version 1-1 28 avril 2003 Mondex International
[Audit]	Visit Report Référence JB2_RDV_MXI_v1.0, version 1.0 13 décembre 2002 CEACI
[DEL]	M/Chip 4 for MULTOS version 4.0 Code Build and Delivery Procedure Référence mxi-chip4-bld-001 Version 2-0 Mondex International M/Chip 4 for MULTOS Lifecycle Overview Référence mxi-mchip4-doc-008 Version 1-0 Mondex International
[HLD]	M/Chip 4 for MULTOS High Level Design Specification Référence mxi-mchip-hld-001 Version 6-0 16 janvier 2003 Mondex International
[IGS]	M/Chip 4 for MULTOS Card Production Guide Reference mxi-chip4-usg-001 Version 0.2 29 août 2002 Mondex International
[LGC]	M/Chip 4 for MULTOS Configuration List Version 1.2 17 mars 2003 Mondex International

[RTE]	Rapport Technique d'Evaluation Référence JB2_RTE Version 1.1L 16 juin 2003 CEACI
[ST]	M/Chip 4 for MULTOS Application Security Target Reference mxi-mchip-stg-003 Version 4-1 10 mars 2003 Mondex International
[USR]	M/Chip 4 form MULTOS application User and Administration Guidance Reference mxi-mchip-gui-003 Version 1-1 28 avril 2003 Mondex International

Annexe 6. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
Décret 2001-272 du 30 mars 2001- Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Norme IS/IEC 15408 :1999, comportant 3 documents : ▪ IS 15408–1: (Part 1) Introduction and general model ; ▪ IS 15408–2: (Part 2) Security functional requirements ; ▪ IS 15408–3: (Part 3) Security assurance requirements ;
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, may 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[MQ]	Manuel qualité du centre de certification Référence SGDN/DCSSI/SDR/MQ.01 Version 1.0 SGDN/DCSSI
[CER/P/01]	Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information Référence CER/P/01.1 Version 1 SGDN/DCSSI

Toute correspondance relative à ce rapport 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 cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr