



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE
DIRECTION CENTRALE 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 PP/0103

Smart Card Security User Group
Smart Card Protection Profile
(SCSUG-SCPP)
version 3.0

Octobre 2001



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

CERTIFICAT PP/0103

Profil de Protection
Smart Card Security User Group
Smart Card Protection Profile
(SCSUG-SCPP)
version 3.0

Commanditaire : Mondex International Ltd

Le 22 octobre 2001,

L'Organisme de certification :
Le Directeur central de la sécurité des systèmes d'information
Henri SERRES

Ce profil de protection 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 profil de protection 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 profil de protection 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 profil de protection 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



Chapitre 1

Résumé

- 1 Ce document représente le rapport de certification du profil de protection «Smart Card Security User Group, Smart Card Protection Profile (SCSUG-SCPP) version 3.0».
- 2 Ce profil de protection est rédigé par le groupe de travail Smart Card Security User Group en langue anglaise. Ce document, y compris sa partie justificative, est un document public.
- 3 Un profil de protection définit pour une catégorie de cibles d'évaluation un ensemble d'exigences et d'objectifs de sécurité des technologies de l'information indépendant de l'implémentation. Les cibles d'évaluation ainsi définies ont pour objet de satisfaire des besoins communs de clients en ce qui concerne la sécurité des technologies de l'information.
- 4 L'enregistrement du profil de protection a été demandé par Mondex International Ltd pour le Smart Card Security User Group :
 - MONDEX International Limited
47-53 Canon Street
London EC4M 3SS
Royaume Uni.
- 5 L'évaluation du profil de protection a été menée conformément aux Critères Communs [CC] et à la méthodologie définie dans le manuel CEM [CEM].
- 6 L'évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information CEACI :
 - CEACI (Thalès Microelectronics)
18, avenue Edouard Belin
31401 Toulouse
France.

Chapitre 2

Description du Profil de Protection

2.1 Périmètre de la cible d'évaluation

- 7 La cible d'évaluation décrite dans le profil de protection est un composant pour cartes à puce constitué d'un micro-circuit et de son système d'exploitation. Cette plate-forme doit avoir la capacité d'établir un canal de communication sûr avec une source de confiance afin de charger des applications.
- 8 Les biens à protéger sont principalement les suivants :
- les données des utilisateurs,
 - les données du porteur,
 - le code des applications chargées sur la cible d'évaluation ;
 - les données de la cible d'évaluation,
 - attributs de sécurité, données d'authentification,
 - clés cryptographiques.
- 9 Les menaces contre lesquelles la cible d'évaluation et son environnement doivent se protéger portent sur la divulgation et la modification non autorisées de ces biens.

2.2 Exigences fonctionnelles

- 10 Les principales fonctionnalités de sécurité exigées par le profil de protection sont les suivantes :
- analyse des attaques potentielles et réponse automatique,
 - opérations cryptographiques et gestion des clés cryptographiques,
 - contrôle d'accès,
 - authentification de données,
 - importation et exportation de données utilisateur,
 - intégrité des données stockées,
 - identification et authentification des utilisateurs,
 - administration de la sécurité,
 - non-observabilité,
 - résistance aux attaques physiques,
 - séparation de domaine,
 - tests des fonctions de sécurité,
 - allocation de ressources.

- 11 Les exigences fonctionnelles présentes dans le profil de protection sont toutes tirées de la partie 2 des Critères Communs [CC].

2.3 Exigences d'assurance

- 12 Le niveau d'assurance exigé par le profil de protection est EAL 4 augmenté des composants suivants :

- AVA_VLA.3 - Résistance moyenne,
- ADV_INT.1 - Modularité.

- 13 Le niveau minimal de résistance des fonctions utilisant des mécanismes probabilistiques ou permutationnels est élevé (SOF-high).

Chapitre 3

Résultats de l'évaluation

L'évaluation du profil de protection a été menée sur la base des exigences de la classe APE définie dans la partie 3 des Critères Communs :

Classe	Composants
Profil de Protection	Introduction du PP (APE_INT.1) Description de la TOE (APE_DES.1) Environnement de sécurité (APE_ENV.1) Objectifs de sécurité (APE_OBJ.1) Exigences de sécurité des TI (APE_REQ.1) Exigences de sécurité des TI explicitement énoncées (APE_SRE.1)

- 14 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.
- 15 Le détail des travaux d'évaluation menés est disponible dans le Rapport Technique d'Evaluation [RTE].

Chapitre 4

Certification

4.1 Verdict

- 16 Ce présent rapport certifie que le profil de protection satisfait aux exigences des critères d'évaluation des profils de protection définis dans la classe APE de la partie 3 des Critères Communs [CC].

4.2 Enregistrement

- 17 Le profil de protection est enregistré dans le catalogue des profils de protection certifiés sous la référence PP/0103.
- 18 Un profil de protection enregistré est un document public dont une copie pourra être téléchargée sur le serveur internet de la Direction centrale de la sécurité des systèmes d'information : www.ssi.gouv.fr.
- 19 Suite à modification, une nouvelle version de ce profil de protection peut être enregistrée.
- 20 Sur demande du commanditaire, il pourra être retiré du catalogue des profils de protection certifiés conformément aux exigences définies dans le guide technique ECF11 [ECF11].

4.3 Certification

- 21 Le certificat d'un profil de protection ne s'applique qu'à la version évaluée du profil de protection selon les modalités décrites dans le présent rapport de certification.
- 22 Le certificat d'un profil de protection ne constitue pas en soi une recommandation du profil de protection par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.
- 23 Le certificat d'un profil de protection n'exprime directement ou indirectement aucune caution du profil par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

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.
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.
- [ECF11] ECF11, Procédure d'enregistrement des profils de protection version 2.0, Service Central de la Sécurité des Systèmes d'Information, 20 décembre 1999.
- [PP/0103] Smart Card Security User Group, Smart Card Protection Profile (SCSUG-SCPP) version 3.0, 9 septembre 2001.
- [RTE] Rapport Technique d'Évaluation HARMONIE, réf: HAR_RTE version 1.3 du 1er octobre 2001 (diffusion contrôlée).

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

La reproduction de tout ou partie de ce document, sans altérations ni coupures, est autorisée.

Tous les noms des produits ou des services de ce document sont des marques déposées de leur propriétaire respectif.