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

Profil de Protection

Rapport de certification PP/0010

Smart Card IC with Multi-Application Secure Platform

Version 2.0

Janvier 2001

Ce document constitue le rapport de certification du profil de protection"Smart Card IC with Multi-Application Secure Platform".

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 :

Secrétariat Général de la Défense Nationale
Service Central de la Sécurité des Systèmes d'Information
51, boulevard de Latour-Maubourg
F-75700 PARIS 07 SP

mél : ssi20@calva.net

Ce document est folioté de 1 à 8 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

CERTIFICAT PP/0010

Profil de Protection
Smart Card IC with Multi-Application Secure Platform
Version 2.0

Exigences d'assurance : EAL4 augmenté

EUROSMART

Le 5 janvier 2001,

Le Directeur Chargé de la Sécurité
des Systèmes d'Information

M. 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 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 par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de Certification :
SGDN/SCSSI
51, boulevard de Latour-Maubourg
F-75700 PARIS 07 SP

Common Criteria

Chapitre 1

Introduction

1 Ce document présente le rapport de certification du profil de protection “Smartcard IC with Multi-Application Secure Platform” dont la référence est PP/0010 [5].

2 Ce profil de protection est dérivé du profil de protection PP/9911 pour prendre en compte les nouvelles menaces liées aux cartes à puce multi-applicatives.

3 L'enregistrement du profil de protection a été demandé par EUROSMART.

EUROSMART
Rue Montoyer, 47
B-1000 BRUXELLES

4 Le profil de protection PP/0010 a été développé par le même organisme et est rédigé en langue anglaise.

5 Un profil de protection définit pour une catégorie de cibles d’évaluation un ensemble d’exigences et d’objectifs de sécurité des TI 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 TI.

6 Le contenu d’un profil de protection doit se conformer aux exigences décrites dans la partie 1 des Critères Communs [1].

7 Un profil de protection est un document constitué de deux parties :

- le corps du document définissant pour la catégorie de cibles d'évaluation envisagées les objectifs et les exigences de sécurité,

- une partie justificative constituée des éléments de preuve nécessaires à l'évaluation du profil de protection. Cette partie peut être fournie séparément si cela s'avère nécessaire.

8 Le profil de protection, y compris sa partie justificative, est un document public.

1.1 Contexte de l’évaluation

9 L’évaluation du profil de protection a été menée conformément aux Critères Communs [1] à [3] et à sa méthodologie associée [4].

10 L' évaluation du profil de protection en date du mois de novembre 2000 a été conduite par le centre d’évaluation de SERMA Technologies.

SERMA Technologies
30 Avenue Gustave Eiffel
F-33608 PESSAC

11 Les résultats de l'évaluation sont repris dans le Rapport Technique d'Evaluation [6].

1.2 Résultats

12 Le profil de protection détaillé au chapitre 2 du présent rapport satisfait aux exigences des critères d'évaluation des profils de protection définis dans la classe APE de la partie 3 des Critères Communs [3].

1.3 Enregistrement

13 Ce profil de protection est enregistré dans le catalogue des profils de protection certifiés.

14 Un profil de protection enregistré est un document public dont une copie pourra être transmise à tout organisme qui en fera la demande auprès de l'organisme de certification.

15 Suite à modification, une nouvelle version de ce profil de protection peut être enregistrée.

16 Sur demande, il pourra être retiré du catalogue des profils de protection certifiés conformément aux exigences définies dans le guide technique ECF11 [7].

17 Ce profil de protection "Smartcard IC with Multi-Application Secure Platform" sera mentionné dans le catalogue des profils de protection certifiés sur le site internet du SCSSI à l'adresse suivante : www.scssi.gouv.fr.

1.4 Portée de la certification

18 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 rapport de certification associé.

19 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.

20 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.

1.5 Fiche signalétique du profil de protection

Profil de protection	Smart Card IC with Multi-Application Secure Platform
Statut	Certifié
CESTI	SERMA Technologies
Version	2.0
Date de parution	Novembre 2000
Diffusion du document	Document public
Demande d'enregistrement	EUROSMART
Développeur	EUROSMART
Évaluation	Novembre 2000
Référence d'enregistrement	PP/0010
Langue utilisée	Anglais
Exigences d'assurance	EAL4 augmenté (ALC_DVS.2 : Caractère suffisant des mesures de sécurité, ADV_IMP.2 : Implémentation de la TSF, AVA_VLA.4 : Résistance élevée) Résistance élevée des fonctions de sécurité

Chapitre 2

Présentation du Profil de Protection

2.1 Description de la cible d'évaluation

21 La cible d'évaluation définie dans ce profil de protection est un micro-circuit pour carte à puce avec son logiciel embarqué permettant l'installation de multiples applications. Le logiciel embarqué est constitué d'un système d'exploitation et d'une interface système pour les applications qui seront chargées sur la carte.

22 Le profil de protection PP/0010 impose que le composant électronique utilisé soit évalué conformément au profil de protection PP/9806.

2.2 Menaces

23 Les biens à protéger sont principalement les suivants :

a) les biens associés au composant et au logiciel embarqué :

- les spécifications, les outils et la documentation de développement du composant, du logiciel dédié et du logiciel embarqué,
- le code du logiciel dédié,
- le code du logiciel embarqué,
- les données utilisées par le composant et le logiciel embarqué,

b) les biens associés aux applications installées :

- le code des applications,
- les données utilisées par les applications,

c) les données utilisateurs,

d) les ressources système (espace mémoire, CPU).

24 Les menaces portent sur la divulgation et la modification non autorisées de ces biens dans leurs environnements de développement et en exploitation.

2.3 Exigences fonctionnelles

25 Les principales fonctionnalités de sécurité définies dans ce 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.

2.4 Exigences d'assurance

26 Le niveau d'assurance exigé par ce profil de protection est le niveau EAL4 augmenté.

27 Le tableau ci-après précise les exigences d'assurance qui sont demandées en augmentation du niveau d'évaluation EAL4 :

Exigence d'assurance	Nom
ADV_IMP.2	Implémentation de la TSF.
ALC_DVS.2	Caractère suffisant des mesures de sécurité.
AVA_VLA.4	Résistance élevée.

Annexe A

Références

[1] [CC-1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIB-99-031, version 2.1 August 1999.

[2] [CC-2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIB-99-032, version 2.1 August 1999.

[3] [CC-3] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIB-99-033, version 2.1 August 1999.

[4] [CEM] Common Methodology for Information Technology Security Evaluation CEM-99/045 version 1.0 August 1999.

[5] Profil de protection “Smart Card IC with Multi-Application Secure Platform”, version 2.0, novembre 2000.

[6] Rapport Technique d’Évaluation, APE_EUROSMART_V2.0, novembre 2000 (document non public).

[7] ECF11, Procédure d'enregistrement des profils de protection version 2.0 du 20 décembre 1999.