

PREMIER MINISTRE

SECRETARIAT 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/9911

Smartcard Integrated Circuit with Embedded Software
Version 2.0

Juillet 1999

Ce document constitue le rapport de certification du profil de protection "Smartcard Integrated Circuit with Embedded Software".

Ce rapport de certification ainsi que le profil de protection associé sont disponibles 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

© SCSSI, France 1999.

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

Ce document est folioté de 1 à 8 et certifiat.

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



CERTIFICAT PP/9911

Protection Profile Smartcard Integrated Circuit with Embedded Software Version 2.0

Exigences d'assurance : EAL4 augmenté

EUROSMART Security Working Group

Le 16 juillet 1999,

Le chef du Service central de la sécurité
des systèmes d'information

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 2.0 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 0.6.

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



Chapitre 1

Introduction

1 Ce document présente le rapport de certification du profil de protection “Smartcard Integrated Circuit with Embedded Software” dont la référence est PP/9911 [6].

2 La version évaluée du profil de protection est la version 2.0 de juin 1999.

3 Le profil de protection dont la référence est PP/9911 a été dérivé de celui-ci afin de couvrir les exigences de sécurité des porte-monnaies électroniques pour les phases d'expérimentation.

4 L'enregistrement du profil de protection a été demandé par :

EUROSMART Security
Working Group

Rue Montoyer, 47
B-1000 BRUXELLES

5 Le profil de protection PP/9911 a été développé par le même organisme

6 Le profil de protection PP/9911 est rédigé en langue anglaise.

7 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.

8 Le contenu d'un profil de protection doit se conformer aux exigences décrites dans la partie 1 des critères communs [1].

9 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.

10 Ce profil de protection, y compris sa partie justificative, est un document public.

1.1 Contexte de l'évaluation

11 L'évaluation du profil de protection a été menée conformément aux critères communs [1] à [4] et à la méthodologie définie dans le document [5].

12 L'évaluation du profil de protection en date du mois de juin 1999 a été conduite par le centre d'évaluation d'AQL. Les résultats de l'évaluation sont repris dans le Rapport Technique d'Evaluation [7].

1.2 Résultats

13 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 [4].

1.3 Enregistrement

14 Ce profil de protection est enregistré dans le catalogue des profils de protection évalués suite à son évaluation par le centre d'évaluation d'AQL.

15 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.

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

17 Sur demande, il pourra être retiré du catalogue des profils de protection évalués conformément aux exigences définies dans le guide technique ECF 11 [8].

18 Ce profil de protection "Smartcard Integrated Circuit with Embedded Software" sera mentionné dans la prochaine version du guide technique ECF 06 [9] dans le catalogue des profils de protection évalués.

1.4 Portée de la certification

19 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.

20 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.

21 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	Smartcard Integrated Circuit with Embedded Software
Statut	Certifié
CESTI	AQL
Version	2.0
Date de parution	Juin 1999
Diffusion du document	Document public
Demande d'enregistrement	EUROSMART Security Working Group
Développeurs	EUROSMART Security Working Group
Évaluation	Juin 1999
Référence d'enregistrement	PP/9911
Langue utilisée	Anglais
Exigences d'assurance	EAL4 augmenté Résistance élevée des fonctions de sécurité

Chapitre 2

Présentation du Profil de Protection

2.1 Description de la cible d'évaluation

22 La cible d'évaluation définie dans ce profil de protection est le microcircuit de carte à puce avec son logiciel embarqué. Le profil de protection PP/9911 impose que le microcircuit soit évalué conformément au profil de protection PP/9806 et définit les exigences complémentaires applicables au logiciel embarqué.

23 Le profil de protection définit la phase de développement du logiciel embarqué, les phases de livraison des éléments nécessaires à la construction de la cible d'évaluation, et la phase d'utilisation de la cible d'évaluation.

2.2 Menaces

24 Les biens à protéger sont les spécifications, la conception, les outils de développement et la technologie des logiciels et matériels, les logiciels embarqués ainsi que les données applicatives de la carte. La cible d'évaluation elle-même est un bien à protéger.

25 Les principales menaces portent sur la divulgation et la modification non autorisées des biens à protéger.

2.3 Exigences fonctionnelles

26 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.

2.4 Exigences d'assurance

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

28 Le tableau ci-après précise les exigences d'assurance qui sont demandées en complément du niveau d'évaluation EAL4.

Exigences d'assurance complémentaires	Type
ADV_IMP.2	Composant hiérarchiquement supérieur au niveau EAL4.
ALC_DVS.2	Composant hiérarchiquement supérieur au niveau EAL4.
AVA_VLA.4	Composant hiérarchiquement supérieur au niveau EAL4.

Annexe A

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-99/008 version 0.6.
- [6] Profil de protection PP/9911, version 2.0, juin 1999.
- [7] Rapport Technique d'Évaluation PP/9911, document non public.
- [8] ECF11, Procédure d'enregistrement des profils de protection version 1.0 du 16 janvier 1997.
- [9] ECF 06, Catalogues, Juin 1998.

