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/9810

Smartcard Embedded Software Version 1.2

Avril 1999

Ce document constitue le rapport de certification du profil de protection “Smartcard Embedded Software Version 1.2".

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

Ce document est folioté de 1 à 8 et certificat.

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

CERTIFICAT PP/9810

Protection Profile
Smartcard Embedded Software Version 1.2

Exigences d'assurance : EAL4 augmenté

SCHLUMBERGER

Le 19 avril 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 Embedded Software Version 1.2” dont la référence est PP/9810.

2 La version évaluée du profil de protection est la version 1.2 de novembre 1998.

3 L'enregistrement du profil de protection a été demandé par la société :

Schlumberger	50, avenue Jean Jaurès 92542 Montrouge Cedex France

4 Le profil de protection a été également développé par Schlumberger.

5 Le profil de protection PP/9810 est rédigé en langue anglaise.

6 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.

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

8 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.

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

1.1 Contexte de l’évaluation

10 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].

11 L' évaluation du profil de protection en date du mois de novembre 1998 a été conduite par le centre d'évaluation de la sécurité des technologies de l'information d'AQL.

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 [4].

1.3 Enregistrement

13 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.

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 évalués conformément aux exigences définies dans le guide technique ECF 11 [8].

17 Ce profil de protection “Smartcard Embedded Software Version 1.2” 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

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	Smartcard Embedded Software
Statut	Certifié
CESTI	AQL
Version	1.2
Date de parution	Novembre 1998
Diffusion du document	Document public
Demande d'enregistrement	Schlumberger
Développeur	Schlumberger
Évaluation	Novembre 1998
Référence d'enregistrement	PP/9810
Langue utilisée	Anglais
Exigences d'assurance	EAL4 augmenté Résistance élevée des fonctions de sécurité

Chapitre 2

Présentation des résultats

2.1 Description de la cible d'évaluation

21 La cible d'évaluation définie dans ce profil de protection correspond au logiciel masqué sur un microcircuit de carte à puce. Le microcircuit est externe à la cible d'évaluation et fait partie intégrante de l'environnement de la cible.

22 Le profil de protection définit la phase de développement du logiciel embarqué ainsi que la phase de livraison de la cible d'évaluation auprès du fabricant de microcircuits.

2.2 Menaces

23 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.

24 Les principales menaces portent sur la divulgation et la modification non autorisées des biens de la cible d'évaluation.

2.3 Exigences fonctionnelles

25 Les principales fonctionnalités de sécurité définies pour le logiciel masqué sont les suivantes :

- identification et authentification des utilisateurs,
- contrôle d'accès,
- authentification de données,
- exportation et importation de donnés utilisateur,
- intégrité des données stockées,
- opérations cryptographiques et gestion des clés cryptographiques,
- administration de la sécurité,
- analyse des attaques potentielles et réponse automatique,
- non-observabilité,
- résistance aux attaques physiques,
- séparation de domaine,
- tests des fonctions de sécurité.

2.4 Exigences d'assurance

26 Le niveau d'assurance exigé par ce profil de protection est le niveau EAL4 augmenté. La cotation de la résistance minimum des fonctions de sécurité est le niveau de résistance élevé.

27 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_IMP2	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/9810, November 19th 1998.

[7] Rapport Technique d'Évaluation PP/9810, 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.