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/0002

Transactional Smartcard Reader
Version 2.0

Février 2000

Ce document constitue le rapport de certification du profil de protection “Transactional Smartcard Reader”.

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/0002

Protection Profile
Transactional Smartcard Reader

Version 2.0

Exigences d'assurance : EAL4 augmenté

Cyber-COMM

Le 10 février 2000,

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 “Transactional Smartcard Reader” dont la référence est PP/0002 [5].

2 La version évaluée du profil de protection est la version 2.0 de janvier 2000.

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

Cyber-COMM	29, rue de Berri 75008 PARIS

4 Le profil de protection PP/0002 a été développé par le même organisme.

5 Le profil de protection PP/0002 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 [3] et à la méthodologie définie dans le document [4].

11 L' évaluation du profil de protection en date du mois de janvier 2000 a été conduite par le centre d'évaluation d'AQL. 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 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 certifiés conformément aux exigences définies dans le guide technique ECF 11 [7].

17 Ce profil de protection "Transactional Smartcard Reader" 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	Transactional Smartcard Reader
Statut	Certifié
CESTI	AQL
Version	2.0
Date de parution	Janvier 2000
Diffusion du document	Document public
Demande d'enregistrement	Cyber-COMM
Développeurs	Cyber-COMM
Évaluation	Janvier 2000
Référence d'enregistrement	PP/0002
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

21 La cible d'évaluation définie dans ce profil de protection est un lecteur transactionnel de cartes à puce. Ce lecteur est conçu autour de l'utilisation d'un module de sécurité qui contient les fonctions de sécurité liés au traitement de la carte à puce.

22 Le lecteur doit être capable d'interagir avec une carte à puce et d'exécuter une application. Il reçoit des informations de transaction et des données d'authentification, et les transmet à l'application pour générer une transaction sûre.

23 Le profil de protection définit les phases de développement, de production, et d'utilisation du lecteur transactionnel de cartes à puce.

2.2 Menaces

24 Les biens à protéger sont séparées entre les données internes à la cible d'évaluation et les données externes.

25 Les données internes sont constituées du firmware, des ressources cryptographiques du module de sécurité, des clés cryptographiques et des mémoires du module de sécurité où ces clés sont stockées, ainsi que les connections entre ces mémoires et l'unité de traitement du lecteur.

26 Les données internes sont constituées des logiciels applicatifs, des données et clés associées.

27 Les principales menaces portent sur la divulgation et la modification non autorisées des biens à protéger. Le firmware et les applications pouvant être téléchargées, ce PP couvre aussi la menace de téléchargement d'un firmware ou d'une application frauduleux.

2.3 Exigences fonctionnelles

28 Les principales fonctionnalités de sécurité définies dans ce profil de protection sont les suivantes :

- opérations cryptographiques et gestion des clés cryptographiques,
- authentification de données,
- authentification des applications et du firmware avant téléchargement,
- identification des applications téléchargées,

- administration de la sécurité,
- tolérance aux pannes et reprise sur erreur,
- protection de données internes lors de leur transfert,
- résistance aux attaques physiques,
- tests des fonctions de sécurité.

2.4 Exigences d'assurance

29 Le niveau d'assurance exigé par ce profil de protection est le niveau EAL4 augmenté des exigences d'assurance dont la liste est donnée dans le tableau ci-après :

Exigences d'assurance complémentaires	Type
ADV_IMP.2	Composant hiérarchiquement supérieur au niveau EAL4.
AVA_VLA.3	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-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 PP/0002, version 2.0, janvier 2000.

[6] Rapport Technique d'Évaluation PP/0002, document non public.

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