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/9903

Carte à puce billettique avec et sans contact
Version 1.2

Avril 1999

Ce document constitue le rapport de certification du profil de protection “Carte à puce billettique avec et sans contact".

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/9903

Protection Profile
Carte à puce billettique avec et sans contact version 1.2

Exigences d'assurance : EAL4 augmenté

Régie autonome des transports parisiens (RATP)
Société nationale des chemins de fer français (SNCF)

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 “Carte à puce billettique avec et sans contact” dont la référence est PP/9903.

2 La version évaluée du profil de protection est la version 1.2 de février 1999.

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

Régie autonome des transports parisiens (RATP)	Département SIT ISV 102, esplanade de la Commune de Paris F - 93167 Noisy-Le-Grand Cedex
Société nationale des chemins de fer français (SNCF)	Direction du Système d'Information Voyageurs Etudes et Développements 44, rue de Rome F - 75008 Paris

4 Le profil de protection a été développé par ces mêmes sociétés.

5 Le profil de protection PP/9903 est rédigé en langue française.

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 février 1999 a été conduite par le centre d'évaluation de Serma Technologies.

1.2 Résultats

12 Le profil de protection détaillé au chapitre 2 du présent rapport satisfait aux exigences 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 de Serma Technologies.

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 “Carte à puce billettique avec et sans contact” 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	Carte à puce Billettique Avec et Sans Contact
Statut	Certifié
CESTI	Serma Technologies
Version	1.2
Date de parution	Février 1999
Diffusion du document	Document public
Demande d'enregistrement	Société nationale des chemins de fer français (SNCF) Régie autonome des transports parisiens (RATP)
Développeurs	Société nationale des chemins de fer français (SNCF) Régie autonome des transports parisiens (RATP)
Évaluation	Février 1999
Référence d'enregistrement	PP/9903
Langue utilisée	Français
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 est une carte à puce utilisée en billettique multimodale.

22 Les cartes à puce visées par le profil de protection doivent pouvoir fonctionner, soit en insertion (mode à contact), soit en téléalimentation (mode sans contact où la carte ne contient pas de pile).

23 Ce profil de protection concerne la phase de spécification de la carte. Néanmoins, les menaces considérées couvrent tout le cycle de vie de la carte. Les objectifs et les exigences de sécurité de la cible d'évaluation concernent quant à eux uniquement la phase opérationnelle.

24 La cible d'évaluation en phase opérationnelle est constituée des éléments suivants d'une carte à puce fonctionnant en mode "avec contacts" et en mode "sans contact" :

- la partie du circuit intégré, comportant l'application billettique multimodale ainsi que les composants matériels et logiciels de base (système d'exploitation et firmware) ; le circuit intégré ne comporte pas forcément de microprocesseur, il peut être conçu en logique câblée ;

- l'antenne et les composants associés (pour les communications sans contact).

2.2 Menaces

25 Les biens à protéger sont :

- les biens intermédiaires, à savoir les informations relatives à la carte pendant les phases préalables à la phase opérationnelle,

- les biens finaux, à savoir les biens relatifs à la cible d'évaluation pendant sa phase opérationnelle, par exemple les informations applicatives, les éléments secrets et les informations de gestion et de structure.

26 Les principales menaces envisagées dans ce profil de protection portent sur la divulgation et la modification non autorisées des biens de la cible d'évaluation.

2.3 Exigences fonctionnelles

27 Le profil de protection définit pour la phase opérationnelle de la carte les principales fonctionnalités suivantes :

- action en cas de détection d'une violation potentielle de la sécurité,
- non répudiation de l'origine,
- opérations cryptographiques,
- protection de l'intégrité et contrôle d'accès aux biens finaux,
- identification et authentification des porteurs,
- authentification des équipement billettiques,
- notification et résistance aux attaques physiques,
- test des fonctions de sécurité.

2.4 Exigences d'assurance

28 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.

29 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
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/9903, version 1.2 Février 1999.

[7] Rapport Technique d'Évaluation PP/9903, 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.