Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Schéma français

d'évaluation et de certification

de la sécurité des technologies de l'information

Rapport de certification PP/0301

JICSAP ver2.0 Protection Profile part1,
Multi-Application Secure System LSI Chip
Protection Profile
version 2.5

Juin 2003

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

CERTIFICAT PP/0301

JICSAP ver2.0 Protection Profile part1, Multi-Application Secure System LSI Chip Protection Profile version 2.5

Emetteur : Japan IC Card System Application Council

Auteur : Electronic Commerce Security Technology Research Association

Centre d'évaluation : CEACI

Le 27 juin 2003,

Le Directeur central de la sécurité
des systèmes d'information
Henri Serres

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information publié au journal officiel de la République française le 19 avril 2002.

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. 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.

Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Chapitre 1

Présentation

Executive Summary

1.1 Objet

Purpose

1 Ce document est le rapport de certification du Profil de protection "JICSAP ver2.0 Protection Profile part1, Multi-Application Secure System LSI Chip" version 2.5.

This document is the certification report of the "JICSAP ver2.0 Protection Profile part1, Multi-Application Secure System LSI Chip" Protection profile version 2.5.

2 Ce profil de protection est émis par JICSAP (Japan IC Card System Application Council) et a été rédigé par ECSEC (Electronic Commerce Security Technology Research Association) :

This protection profile is issued by JICSAP (Japan IC Card System Application Council) and has been written by ECSEC (Electronic Commerce Security Technology Research Association):

- ECSEC
  5322, Endoh,
  Fujisawa, Kanagawa
  Japon 252-0816.

3 L'évaluation a été menée conformément aux Critères Communs [CC] et à la méthodologie définie dans le manuel CEM [CEM].

This evaluation has been performed in conformance with Common Criteria [CC] and with the methodology defined in the CEM [CEM].

1.2 Contexte

Context

4 Ce profil de protection est la traduction anglaise du profil de protection "Multi-Application Secure System LSI Chip Protection Profile" émis en japonais par Information Technology Promotion Agency le 29 août 2002. Ce profil de protection (partie 1) exprime les exigences de sécurité liées au micro-circuit ; un autre profil de protection (partie 2) pourrait être rédigé pour exprimer les exigences de sécurité liées au système d'exploitation.

This protection profile is the English version of the "Multi-Application Secure System LSI Chip Protection Profile" issued by Information Technology Promotion Agency in Japanese on August 29, 2002. This protection profile (part 1) is related to the security requirements for the integrated circuit; another protection profile (part 2) could be written to specify the security requirements for the embedded operating system.

5 Le commanditaire de l'évaluation est ECSEC :

The sponsor of the evaluation is ECSEC:

- ECSEC
  5322, Endoh,
  Fujisawa, Kanagawa
  Japon 252-0816.

6 L'évaluation a été réalisée par le Centre d'Evaluation de la Sécurité des Technologies de l'Information CEACI :

The evaluation has been performed by the Information Technology Security Evaluation Facility CEACI:

- CEACI (Thalès Microelectronics)
  18, avenue Edouard Belin
  31401 Toulouse
  France.

Chapitre 2

Description du profil de protection

Description of the protection profile

2.1 Périmètre du profil de protection

Scope of the protection profile

7 Le produit considéré dans ce profil de protection est un micro-circuit électronique destiné à être utilisé dans une carte à puce. Le profil de protection décrit les exigences auxquelles ce micro-circuit (composant matériel) doit se conformer.

The product considered in this protection profile is a integrated circuit to be used in a smart card. The protection profile describes the requirements to which this integrated circuit (hardware part) must comply.

8 Les biens à protéger sont constitués des informations qui seront stockées dans la carte. Ces informations doivent être protégées lors de leur circulation et stockage dans les différentes parties physiques du micro-circuit (par exemple : les mémoires, les bus de données, les processeurs).

The assets to be protected are the data that will be put in the card. These data shall be protected while they are being transmitted or stored in the physical parts of the integrated circuit (for example: memories, data buses, processing units).

9 Le profil de protection identifie les menaces contre lesquelles les biens doivent être protégés. Les menaces considérées sont celles qui ont pour but d'essayer de récupérer les informations contenues dans le micro-circuit. Ces menaces peuvent être mises en oeuvre par des attaques telles que : modification physique du micro-circuit, injection de faute, analyse de signaux...

The protection profile identifies threats against which the assets must be protected. The considered threats have the aim of retrieving information from the integrated circuit. These threats can be realized by attacks such as: physical modification of the integrated circuit, fault injection, residual information analysis...

2.2 Exigences fonctionnelles

Functional requirement

10 Les principales fonctionnalités de sécurité exigées par le profil de protection sont les suivantes :

The main security functions required by this protection profile are the following:

- Protection physique des données de sécurité,
  Security data physical protection,
- Protection des données pendant leur transfert interne,
  Data protection during internal transfer,
- Mode sûr après défaillance,
  Failure with preservation of secure state,
- Tolérance aux pannes,
  Fault tolerance,

- Politique et fonctions de contrôle d'accès,
  Access control policy and functions,
- Administration et initialisation des attributs de sécurité,
  Management and initialization of security attributes,
- Rôles pour l'administration de la sécurité,
  Security management roles,
- Identification et authentification des utilisateurs,
  User identification and authentication,
- Réduction des fuites d'information.
  Reduce the information leakage.

11 Ces fonctionnalités de sécurité sont exprimées par des exigences fonctionnelles de sécurité extraites de la partie 2 des Critères Communs [CC], à l'exception de l'exigence FDP_RIL.1 "Réduction des fuites d'information" qui a été explicitement énoncée dans ce profil de protection.

These security functions are expressed according to the security functional requirements of Common Criteria part 2 [CC], with the exception of the requirement FDP_RIL.1 «Reduce the information leakage» which has been explicitly stated in this protection profile.

2.3 Exigences d'assurance

12 Le niveau d'assurance exigé par le profil de protection est EAL 4 augmenté des exigences d'assurance de sécurité suivantes :

The assurance level required by this protection profile is EAL 4 augmented with the following security assurance requirements:

- AVA_CCA.1 - Analyse des canaux cachés,
  AVA_CCA.1 - Covert channel analysis,
- AVA_VLA.4 - Analyse de vulnérabilité, résistance élevée.
  AVA_VLA.4 - Vulnerability analysis, highly resistant.

13 Le niveau de résistance des fonctions de sécurité doit être au minimum élevé (SOF-high).

The strength level of the security function shall be SOF-high as a minimum.

Chapitre 3

Résultats de l'évaluation

Evaluation results

14 L'évaluation du profil de protection a été menée sur la base des exigences de la classe APE définie dans la partie 3 des Critères Communs :

The evaluation of the protection profile has been lead on the basis of the requirements defined in the APE class defined in Common Criteria part 3:

Class	Component
APE - Protection profile	PP introduction (APE_INT.1) TOE description (APE_DES.1) Security environment (APE_ENV.1) Security objectives (APE_OBJ.1) IT security requirements (APE_REQ.1) Explicitly stated IT security requirements (APE_SRE.1)

15 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.

For all the above assurance components, a «pass» verdict has been given by the evaluator.

16 La description des travaux d'évaluation menés est présentée dans le Rapport Technique d'Evaluation [RTE].

The description of the evaluation work is in the Evaluation Technical Report [RTE].

Chapitre 4

Certification

Certification

4.1 Verdict

Verdict

17 Ce rapport certifie que le profil de protection satisfait aux exigences des critères d'évaluation des profils de protection définis dans la classe APE de la partie 3 des Critères Communs [CC].

This report certifies that the protection profile satisfies to the protection profile evaluation requirements defined in the APE class of Common Criteria part 3.

4.2 Recommandations

Recommendations

18 La recommandation suivante s'adresse à l'auteur d'une cible de sécurité qui se veut conforme à ce profil de protection :

The following recommendations are addressed to the author of a security target compliant with this protection profile:

- le profil de protection ne fait pas d'hypothèse sur l'utilisation qui pourra être faite du micro-circuit. Une cible de sécurité devra faire apparaître les phases du cycle de vie du produit qui sont considérées en développement et celles qui sont considérées en utilisation.
  as the protection profile does not make assumption on the usage of the integrated circuit, a security target shall clearly identify which phases of the product's life cycle are considered in the development and which are considered in usage.

4.3 Certification

19 Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information, publié au journal officiel de la République française le 19 avril 2002.

This certificate is issued within the scope of the «décret 2002-535» of april 18th, 2002 dealing with the evaluation and the certification of the security provided by IT product and systems. The text of the «décret» was published april 19th, 2002 in the «journal officiel de la République française».

4.4 Enregistrement

Registration

20 Le profil de protection est enregistré comme profil de protection certifié sous la référence PP/0301.

The protection profile is registered as a certified protection profile under the reference PP/0301.

4.5 Limitations

Restrictions

21 Le certificat d'un profil de protection ne s'applique qu'à la version évaluée du profil de protection.

The certificate only applies to the evaluated version of the protection profile.

22 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.

The certificate of a protection profile is not a recommendation of the protection profile by the certification body or by any other organization.

4.6 Reconnaissance internationale

International recognition

4.6.1 CC MRA

23 Un accord (Common Criteria Arrangement) [MRA] de reconnaissance des certificats basés sur les évaluations jusqu'au niveau EAL4 a été signé en mai 2000. Cet accord a été signé par l'Allemagne, l'Australie, l'Autriche, le Canada, l'Espagne, les Etats-Unis, la Finlande, la France, la Grèce, Israël (en novembre 2000), l'Italie, la Norvège, la Nouvelle-Zélande, les Pays-Bas, le Royaume-Uni et la Suède (juin 2002).

An arrangement (Common Criteria Arrangement) [MRA] on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. The arrangement was signed by the national bodies of Australia, Austria, Canada, Finland, France, Germany, Greece, Israel (november 2000), Italy, The Netherlands, New Zealand, Norway, Spain, Sweden (june 2002), United Kingdom and the United States.

Annexe

Références

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- Part 1 : Introduction and general model, august 1999, version 2.1, réf : CCIMB-99-031 ;
- Part 2 : Security functional requirements, august 1999, version 2.1, réf : CCIMB-99-032 ;
- Part 3 : Security assurance requirements, august 1999, version 2.1, réf : CCIMB-99-033.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

[RTE] Evaluation Technical Report of PP-IPA project, CEACI, version 1.2L du 11/06/2003, réf: IPA_RTE_APE. *(diffusion limitée)*

[MRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, mai 2000.

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Centre de Certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr