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/0307

JICSAP ver2.0 Protection Profile part2,
Protection profile for Smart Cards
with the Application Program Loading Function
version 1.7e

SÉCURITÉ CERTIFICATION

Novembre 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 part2, Protection profile for Smart Cards with the Application Program Loading Function version 1.7e

Emetteur : Japan IC Card System Application Council

Auteur : Electronic Commerce Security Technology Research Association

Centre d'évaluation : CEACI

Le

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 part2, Protection profile for Smart Cards with the Application Program Loading Function", version 1.7e.

This document is the certification report of the "JICSAP ver2.0 Protection Profile part2, Protection profile for Smart Cards with the Application Program Loading Function", version 1.7e.

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 "Protection profile for Smart Cards with the Application Program Loading Function" émis en japonais par New Media Development Association, le 10 décembre 2001. Il exprime les exigences de sécurité liées au système d'exploitation embarqué dans un micro-circuit pour carte à puce. Il fait suite au profil de protection "JICSAP ver.2.0 Protection Profile part 1 multi-Application Secure System LSI Chip Protection Profile" version 2.5, certifié sous la référence PP/0301, qui exprime les exigences de sécurité pour le micro-circuit seul.

This protection profile is the English version of the "Protection profile for Smart Cards with the Application Program Loading Function" issued in Japanese by New Media Development Association on December 10th 2001. It relates the security requirements for the operating system embedded in a microcontroller for smart card. It comes after the "JICSAP ver.2.0 Protection Profile part 1 Multi-Application Secure System LSI Chip Protection Profile" version 2.5 certified under the reference PP/0301, related to the security requirements for the microcontroller alone.

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 le système d'exploitation embarqué dans un micro-circuit électronique destiné à être utilisé dans une carte à puce. Le profil de protection décrit les exigences auxquelles le système d'exploitation (partie logicielle) doit se conformer.

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

8 Les biens à protéger sont constitués des informations qui seront stockées dans la carte. Ces informations doivent être protégées en fonction des droits des applications et des utilisateurs qui y feront appel.

The assets to be protected are the data that will be put in the card. These data shall be protected depending on the rights of the applications and users calling for them.

9 Le profil de protection identifie des hypothèses sur le contexte d'exploitation de la carte à puce :

The protection profile identifies assumption on the exploitation context of the smart card:

- les données sécuritaires du produit doivent être gérées de manière sécurisée en dehors du produit ;
  the product's TSF data shall be securely managed out of the product;
- les personnes en charge de l'exploitation du produit doivent être formées à l'utilisation sûre du produit ;
  the person in charge of the operations of the product shall be trained to a secure usage of the product;
- les applications chargées sur le système d'exploitation sont considérées comme sûres.
  applications loaded on the operating system are considered secured.

10 Le profil de protection identifie les menaces contre lesquelles les biens doivent être protégés :

The protection profile identifies threats against which the assets must be protected:

- modification ou vol des données par des attaques logiques ;
  modification or steal of data by logical attacks;
- contournement des mécanismes d'authentification par des attaques force brute ;
  bypass of authentication mechanism with brute force attacks;
- exposition des données sécuritaires par des interruptions d'opérations ;
  TSF data exposure by operations interruptions;

- récupération de données d'application par l'utilisation illégale d'une autre application ;
  applications data tampering with the illegal use of another application;
- utilisation du terminal spécial pour récupérer des données ;
  use of the special terminal to tamper data;
- utilisation illégale des données avant que l'utilisateur final n'active le produit ;
  abuse of data before the end user activates the product;
- récupération de données par la mise en oeuvre d'attaques sur le micro-circuit.
  data tampering by the mean of attacks on the microcontroller.

11 Le profil de protection identifie des mesures organisationnelles et techniques nécessaires à l'environnement opérationnel du produit :
The protection profile identifies organizational security policies:

- les rôles de gestion de la sécurité du produit doivent être précisément décrits ;
  the roles with respect to security management of the product shall be clearly be defined;
- un canal de communication sécurisé doit exister entre le terminal et la carte à puce.
  a secure communication path shall be established between the smart card and the terminal.

2.2 Exigences fonctionnelles

Functional requirement

12 Les fonctionnalités de sécurité exigées par le profil de protection sont les suivantes :
The security functions required by this protection profile are the following:

- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Subset access control (FDP_ACC.1)
- Security attribute based access control (FDP_ACF.1)
- Subset residual information protection (FDP_RIP.1)
- Authentication failure handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Single-use authentication mechanisms (FIA_UAU.4)

- Multiple authentication mechanisms (FIA_UAU.5)
- Re-authenticating (FIA_UAU.6)
- Timing of identification (FIA_UID.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Security roles (FMT_SMR.1)
- Abstract machine testing (FPT_AMT.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Automated recovery without undue loss (FPT_RCV.3)
- Function recovery (FPT_RCV.4)
- TSF domain separation (FPT_SEP.1)
- TSF testing (FPT_TST.1)

13 Ces fonctionnalités de sécurité sont exprimées par des exigences fonctionnelles de sécurité extraites de la partie 2 des Critères Communs [CC], à l'exception des exigences suivantes qui ont été explicitement énoncées 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 following requirements, which have been explicitly stated in this protection profile:

- Configuration generation (FAU_CFG.1)
- Attribute definition of logical interface and object (FDP_IOA.1)

2.3 Exigences d'assurance

14 Le niveau d'assurance exigé par le profil de protection est EAL 4 augmenté de l'exigence d'assurance de sécurité suivante :

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

- AVA_VLA.4 - Analyse de vulnérabilité, résistance élevée.
  AVA_VLA.4 - Vulnerability analysis, highly resistant.

15 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

16 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)

17 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.

18 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

19 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

20 Les recommandations suivantes s'adressent au développeur d'un produit dont la cible de sécurité se veut conforme à ce profil de protection :

The following recommendations are addressed to the developper of a product which security target claims compliance with this protection profile:

- Le périmètre du profil de protection est la partie logicielle d'une puce. Le profil de protection recommande au développeur de s'assurer que les mesures de sécurité du micro-circuit soient correctement prises en compte dans la conception et l'implémentation du système d'exploitation (OE.Chip).
  The scope of the protection profile is the software part of a chip. The protection profile recommends that the developer ensures that the security measures of the integrated circuit are correctly taken in account in the design and in the implementation of the operating system (OE.Chip).

- Le profil de protection définit une exigence sur le produit pour que celui-ci génère des clés cryptographiques (exigence fonctionnelle FCS_CKM.1). Le système d'exploitation, pour être conforme à cette exigence, doit donc générer lui-même les clés cryptographiques : celles-ci ne doivent pas être générées uniquement pas le micro-circuit, ni être importées (chargées).
  The protection profile defines a requirement for the product to generate cryptographic keys (FCS_CKM.1 functional requirement). The operating system, in order to be compliant with this requirement, shall then generate cryptographic keys by itself: these keys cannot be generated by the microcontroller alone, nor be imported (loaded).

4.3 Certification

21 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

22 Le profil de protection est enregistré comme profil de protection certifié sous la référence PP/0307.

The protection profile is registered as a certified protection profile under the reference PP/0307.

4.5 Limitations

Restrictions

23 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.

24 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

25 Un accord (Common Criteria Arrangement) [MRA] de reconnaissance des certificats basés sur les évaluations jusqu'au niveau EAL4 a été signé en mai 2000. En octobre 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada et l'Australie-Nouvelle Zélande ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Espagne, la Finlande, la Grèce, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, l'Autriche, la Turquie et la Hongrie.

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. In October 2003, the issuing countries that have signed the arrangelent are: France, Germany, United Kingdom, United States, Canada and Australia - New-Zealand; the countries that have signed the arrangement and do not issue certificates are: Spain, Finland, Greece, Israel, Italy, Norway, The Neetherlands, Sweeden, Austria, Turkey and Hungary.

Annexe

Exigences Fonctionnelles

Attention : les descriptions des composants fonctionnels suivants sont donnés à titre indicatif. Seule une lecture attentive du Profil de protection peut apporter la description exacte des exigences fonctionnelles exigées pour le produit.

Class FCS **Cryptographic support**

Cryptographic key management

FCS_CKM.1 *Cryptographic key generation*
Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiés qui peuvent être basés sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].

FCS_CKM.4 *Cryptographic key destruction*
Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].

Cryptographic operation

FCS_COP.1 *Cryptographic operation*
Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).

Class FDP **User data protection**

Access control policy

FDP_ACC.1 *Subset access control*
Chaque règle de contrôle d'accès identifiée doit être mise en place pour un sous-ensemble des opérations qu'il est possible d'effectuer sur un sous-ensemble des objets du produit.

Access control functions

FDP_ACF.1 *Security attribute based access control*
Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.

Residual information protection

FDP_RIP.1 *Subset residual information protection*
Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.

Class FIA **Identification and authentication**

Authentication failures

FIA_AFL.1 *Authentication failure handling*
Le produit doit être capable d'arrêter le processus d'établissement d'une session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il doit aussi, après la clôture du processus d'établissement d'une session, être capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.

User attribute definition

FIA_ATD.1 *User attribute definition*
Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.

User authentication

FIA_UAU.1 *Timing of authentication*
Le produit autorise un utilisateur à exécuter certaines actions, spécifiées dans la cible de sécurité [ST], avant que son identité ne soit authentifiée.

FIA_UAU.4 *Single-use authentication mechanisms*
Le mécanisme d'authentification doit fonctionner avec des données d'authentification à usage unique.

FIA_UAU.5 *Multiple authentication mechanisms*
Différents mécanismes d'authentification doivent être fournis et utilisés pour authentifier les identités d'un utilisateur pour des événements spécifiques.

FIA_UAU.6 *Re-authenticating*
Ce composant permet de spécifier des événements (spécifiés dans la cible de sécurité [ST]) pour lesquels l'utilisateur doit être ré-authentifié.

User identification

FIA_UID.1 *Timing of identification*
Le produit autorise les utilisateurs à exécuter certaines actions, identifiées dans la cible de sécurité [ST], avant d'être identifiés.

Class FMT **Security management**

Management of security attributes

FMT_MSA.1 *Management of security attributes*
Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.

FMT_MSA.2 *Secure security attributes*
Le produit doit garantir que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.

FMT_MSA.3 *Static attribute initialisation*
Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.

Security management roles

FMT_SMR.1 *Security roles*
Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiées dans la cible de sécurité [ST]).

Class FPT **Protection of the TSF**

Underlying abstract machine test

FPT_AMT.1 *Abstract machine testing*
Ce composant définit la façon de tester la machine abstraite sous-jacente.

Fail secure

FPT_FLS.1 *Failure with preservation of secure state*
Le produit doit préserver un état sûr dans le cas de défaillances identifiées.

Trusted recovery

FPT_RCV.3 *Automated recovery without undue loss*
Le produit doit revenir dans un état sûr sans intervention humaine, au moins pour un type d'interruption de service ; la reprise à la suite d'autres types d'interruption peut nécessiter le recours à une intervention humaine. Le produit ne doit pas autoriser pas la perte indue d'objets protégés.

FPT_RCV.4 *Function recovery*
La reprise au niveau de fonctions de sécurité identifiées (dans la cible de sécurité [ST]) doit être garantie, en garantissant soit la réussite finale, soit un retour des données dans un état sûr.

Domain separation

FPT_SEP.1 *TSF domain separation*
Le produit doit offrir un domaine protégé et distinct pour les fonctions de sécurité du produit et procurer une séparation entre sujets.

TSF self test

FPT_TST.1 *TSF testing*
Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.

Références

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

[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-JICSAP project, CEACI, version 2.0L du 22/10/2003, réf: JIC_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