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 2002/08

Smart Card IC Development flow
Smart Card IC Development Section in Kumamoto
NEC - Japan

(version 1.0)

Juin 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

CERTIFICAT 2002/08

Smart Card IC Development flow
Smart Card IC Development section in Kumamoto
NEC - Japan

(version 1.0)

Développeur : NEC Smart Card IC development Section, Kumamoto

Critères Communs

EAL1 Augmenté

(AVA_VLA.2)

Commanditaire : NEC Smart Card Application Center

Centre d'évaluation : AQL - Groupe Silicomp

Le 12 juin 2002,

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

Ce système 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 et 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 certificat ne s'applique qu'à la version évaluée du système dans sa configuration d'évaluation et 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 système 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 système par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Chapitre 1

Résumé

Executive summary

1.1 Objet

Purpose

1 Ce document est le rapport de certification du «Smart Card IC Development flow, Smart Card IC Development section in Kumamoto, NEC - Japan» (version 1.0).

This document is the certification report of the «Smart card IC development flow, Smart Card IC development section, NEC-Japan» (version 1.0).

2 Ce système a pour but d'assurer le développement de circuits-intégrés pour cartes à puce. Les exigences de sécurité de ce système répondent aux exigences de la phase 2 de développement du profil de protection PP/9806 «Smart card Integrated Circuit Protection Profile v2.0».

The goal of this system is to ensure the development of integrated circuits for smart cards. The security requirements of this system meet the requirements for the development phase 2 of the protection profile PP/9806 «Smart card Integrated Circuit Protection Profile v2.0».

3 Le développeur de la cible d'évaluation est :

The developer of the target of evaluation is:

- Smart Card IC Development Section
  NEC
  Kumamoto
  Japan.

4 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].

5 Le niveau atteint par cette évaluation est le niveau d'assurance EAL 1 augmenté du composant :

This evaluation reaches the assurance level EAL 1 augmented of the component:

- AVA_VLA.2 "Analyse de vulnérabilité indépendante".
  AVA_VLA.2 «Independant vulnerability analysis».

6 L'évaluation du système a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information d'AQL :

The system evaluation has been performed by the Information Technology Security Evaluation Facility of AQL:

- AQL - Groupe Silicomp
  Rue de la chataîgneraie - BP 127
  35513 Cesson-Sévigné Cedex
  France.

1.2 Contexte de l'évaluation

7 L'évaluation s'est déroulée d'octobre 2001 à avril 2002.

The evaluation has been carried out from October 2001 to April 2002.

8 Le commanditaire de l'évaluation est NEC Smart Card Application Center :

The sponsor of the evaluation is NEC Smart Card Application Center:

- NEC SmartCard Application Center
  9, rue Paul Dautier - BP 52
  78142 Vélizy
  France.

Chapitre 2

Description de la cible d'évaluation

Description of the target of evaluation

2.1 Périmètre de la cible d'évaluation

Scope of the target of evaluation

9 La cible d'évaluation est le «Smart Card IC development flow, NEC - Japan» (version 1.0) du site de NEC Kumamoto-Japon pour développer des micro-contrôleurs pour cartes à puce.

The target of evaluation is the «Smart card IC development flow, NEC-Japan» (version 1.0) of the NEC smart card integrated circuit development plant in Kumamoto, Japan.

10 La partie technique de la cible d'évaluation évaluée avec les critères communs est principalement composée de serveurs de fichiers et de stations de travail qui leur sont reliées :

The technical part of the target of evaluation evaluated with common criteria is mainly made up file servers and workstations to which they are connected:

- Serveur de fichiers sous Windows 2000,
  Windows 2000 file server,
- Machines clients du serveur de fichiers sous Windows NT 4.0,
  NT 4.0 client computers of the file server,
- Equipement de test sous Windows NT 4.0,
  NT 4.0 testing equipment,
- Serveurs proxy, mail, Sun et NIS+ sous Solaris 2.7.
  Solaris 2.7 proxy, mail, Sun file and NIS+ servers.

11 L'environnement de la cible d'évaluation est composé de plusieurs lieux dédiés à l'intérieur du site de Kumamoto qui sont des pièces à accès contrôlés :

The environment of the target of evaluation is composed of several dedicated areas within the Kumamoto plant, these are access controlled rooms:

- la salle de sécurité, où les développeurs des micro-contrôleurs travaillent avec les stations de travail,
  the security room, where integrated circuit designers work on computers,
- la salle de tests, où les étapes de tests sont effectuées à la fois pour l'évaluation (validation des échantillons) et pour le test (validation du programme final de test).
  the tester room, where the testing steps are performed for both evaluation (sample product validation) and testing (final testing program validation).

12 La cible d'évaluation a pour objectif de protéger en terme de confidentialité, d'intégrité et de disponibilité les biens suivants répartis en deux familles.

The target of evaluation has to protect in term of confidentiality, integrity and availability the following assets

- Les biens informatiques, sous forme de fichiers électroniques concernant :
- *The computerized assets, electronic files about:*

  - les circuits de sécurité,
    security circuits,
  - les données des circuits,
    circuits data,
  - les données des masques,
    mask data,
  - les schémas d'initialisation de l'EEPROM,
    EEPROM initialization pattern,
  - les logiciels dédiés,
    dedicated software,
  - les résultats des évaluations des circuits,
    evaluation results for security circuits,
  - les données des logiciels embarqués.
    embedded software data.

- Les biens non-informatiques :
- *Non-computerized assets:*

  - les documents sur les circuits de sécurité,
    hard documents for security circuits,
  - les documents sur les données des circuits,
    hard documents for circuits data,
  - les prototypes de produits,
    products samples,
  - les documents des schémas d'initialisation de l'EEPROM,
    hard documents of EEPROM initialization data,
  - les documents des logiciels dédiés,
    hard copy of dedicated software,
  - les documents de résultats des évaluations des circuits,
    hard documents,
  - l'émulateur,
    emulator,
  - le simulateur.
    simulator.

2.2 Fonctions de sécurité évaluées

Evaluated security functions

13 Les fonctions de sécurité réalisées par la partie technique du système évalué sont les suivantes :

The security functions implemented by the technical part of the evaluated system are:

- Identification et authentification des utilisateurs Solaris,
  Identification and authentication of Solaris users,
- Gestion des attributs liés aux utilisateurs de Solaris identifiés,
  Management of attributes associated with identified Solaris users,
- Distinction entre les administrateurs et les opérateurs de Solaris,

Distinction of administrators form operators on Solaris,

- Association des propriétés de fichiers ou de commandes avec les utilisateurs de Solaris authentifiés,
  Property of file or command are associated to authenticated Solaris user,
- Les fichiers ou les commandes héritent des attributs de l'utilisateur Solaris qui les exécute,
  File or command executed by a Solaris user inherits his attributes.
- Gestion des droits d'accès et d'exécution de chaque utilisateur,
  Management of access or execution rights associated to each user,
- Identification et authentification des utilisateurs et administrateurs Windows NT,
  Identification and authentication of Windows NT users and administrators,
- Maintenance de la liste des attributs des utilisateurs Windows NT,
  Maintenance of the list of attributes belonging to Windows NT users.
- Gestion des rôles des utilisateurs de Windows NT,
  Role management of Windows NT users,
- Gestion des propriétés des fichiers et des commandes Windows NT en fonction des utilisateurs,
  Management of files and commands properties depending on Windows NT users,
- Gestion des droits pour les utilisateurs de Windows NT,
  Management of rights for Windows NT users,
- Identification et authentification des administrateurs et utilisateurs Windows 2000,
  Identification and authentication of Windows 2000 administrators and users
- Maintenance de la liste des attributs des utilisateurs Windows 2000,
  Maintenance of the list of attributes belonging to Windows 2000 users,
- Gestion des rôles des utilisateurs de Windows 2000,
  Role management of Windows 2000 users,
- Gestion des propriétés des fichiers et des commandes Windows 2000 en fonction des utilisateurs,
  Management of files and commands properties depending on Windows 2000 users,
- Gestion des droits pour les utilisateurs de Windows 2000.
  Management of rights for Windows 2000 users.

2.3 Mesures de sécurité

Security measures

14 Les mesures de sécurité qui ont été auditées dans le cadre de l'évaluation concernent les aspects suivants :

The security measures that have been audited in the scope of this evaluation are:

- Gestion des biens non-informatiques (stockage sécurisé, identification unique, gestion de configuration, procédure de fin de vie),
  Non-computerized assets management (secure storage, unique identification, configuration management, end of life procedure),
- Non permanence des données de tests et d'évaluation sur les matériels de tests et d'évaluation,
  Non permanence of tests and evaluation data on tests and evaluation materials,
- Gestion des livraisons et des programmes de test,

Management of deliveries and test programs,

- Sauvegarde de secours des résultats d'évaluation,
  Back-up of evaluation results,
- Gestion des rebuts,
  Scrap management,
- Gestion des mots de passe,
  Passwords management,
- Actions correctives vis-à-vis des failles et des non-conformités,
  Security failures and non-conformance corrective actions,
- Gestion des évolutions de la sécurité,
  Security change management,
- Gestion des employés,
  Employees management,
- Gestion du contrôle d'accès,
  Access control management,
- Protection du système informatique,
  Information system protection,
- Gestion des livraisons,
  Delivery management,
- Gestion des commandes,
  Ordering management,
- Gestion des sous-traitants,
  Subcontractors management,
- Gestion des règles de sécurité.
  Security rules management.

Chapitre 3

Résultats de l'évaluation

Evaluation results

3.1 Exigences d'assurance

Assurance requirements

Le système a été évalué au niveau EAL 1 augmenté du composant AVA_VLA.2.

This system has been evaluated EAL 1 augmented with AVA_VLA.2 component.

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	ASE_INT.1 : Introduction de la ST ASE_DES.1 : Description de la TOE ASE_ENV.1 : Environnement de sécurité ASE_OBJ.1 : Objectifs de sécurité ASE_PPC.1 : Annonce de conformité à un PP ASE_REQ.1 : Exigences de sécurité des TI ASE_SRE.1 : Exigences de sécurité des TI explicitement énoncées ASE_TSS.1 : Spécifications globales de la TOE
Gestion de configuration	ACM_CAP.1 : Numéros de version
Livraison et exploitation	ADO_IGS.1 : Procédures d'installation, de génération et de démarrage
Développement	ADV_FSP.1 : Spécifications fonctionnelles informelles ADV_RCR.1 : Démonstration de correspondance informelle
Guides	AGD_ADM.1 : Guide de l'administrateur AGD_USR.1 : Guide de l'utilisateur
Tests	ATE_IND.1 : Tests indépendants - conformité
Analyse de vulnérabilité	AVA_VLA.2 : Analyse de vulnérabilité indépendante

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

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

16 Les travaux d'évaluation menés sont décrits dans le Rapport Technique d'Evaluation [RTE].

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

17 Dans le cadre des travaux d'évaluation, un audit a été réalisé sur le site de développement de Kumamoto ; cet audit a permis de s'assurer de l'application de mesures de sécurité concernant les aspects de sécurité physique, organisationnels et liés au personnel.

In the scope of the evaluation work, an audit has been performed on the development plant of Kumamoto; this audit gave confidence in the application of the security measures concerning physical protection, organisational and employees related aspects.

3.2 Tests fonctionnels et de pénétration

Functional and penetration testing

18 L'évaluateur a mené une analyse de vulnérabilités, confirmée par des tests de pénétration sur site, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élémentaire (composant AVA_VLA.2) ne peut pas remettre en cause l'objectif de sécurité de la cible d'évaluation :

The evaluator lead a vulnerability analysis, confirmed by on-site penetration testing, to ensure that an attacker with a low attack potential (AVA_VLA.2 requirement) cannot bypass the security objective of the security target:

- La cible d'évaluation doit donner accès seulement au personnel autorisé et doit protéger ses parties critiques et biens informatiques contre les accès et les opérations non-autorisés.
  The target of evaluation shall give an access only to authorized personnel and shall protect its security critical parts and «computerized assets» against unauthorized access and operations.

Chapitre 4

Certification

Certification

4.1 Verdict

Verdict

19 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL 1 augmenté du composant AVA_VLA.2, tels que décrits dans la partie 3 des Critères Communs [CC] :

The present report certifies that the target of evaluation satisfies to the requirement of the EAL 1 level augmented with AVA_VLA.2, as described in Common Criteria part 3 [CC]:

- AVA_VLA.2 "Analyse de vulnérabilité indépendante".
  AVA_VLA.2 «Independent vulnerability analysis».

4.2 Recommandations

Recommendations

20 Le système doit être exploité conformément aux procédures d'utilisation et d'administration prescrites dans la cible de sécurité [ST].

The system shall be used in accordance with the usage and administrative procedures prescribed in the security target [ST].

4.3 Certification

Certification

21 La certification ne constitue pas en soi une recommandation du système. Elle ne garantit pas que le système certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

Certification is not in itself a recommendation of the system. It does not guaranty that the certified system is totally exempt of exploitable vulnerabilities: it still subsist a residual probability that exploitable vulnerabilities have not been discovered: this probability is as low as the assurance level is high.

22 Le certificat ne s'applique qu'à la version évaluée du système identifiée au chapitre 2. La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

The certificate only applies to the evaluated version of the system identified in chapter 2. The certification of any subsequent version requires a prior re-evaluation depending on the modifications made.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	Addition d'un ou de plusieurs composants d'assurance de la partie 3 des CC à une échelle prédéfinie d'assurance ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou par son environnement.
Cible d'évaluation	Produit ou système et documentation associée pour (administrateur et utilisateur) qui est l'objet d'une évaluation.
Cible de sécurité	Ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Paquet de composants d'assurance extraits de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	Ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

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

[ST] Security Target for Smart Card IC Development flow - Japan, NEC SCAC, version 2.3, april 2002 (document non public)

[RTE] Evaluation Technical Report CAMELLIA, AQL, version 1.01, may 2002, réf: NEC004-ETR-1.01. (document non public)

[PP9806] "Smartcard Integrated Circuit, Version 2.0", septembre 1998, enregistré au catalogue des profils de protection certifiés sous la référence PP/9806.

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

[SOG-IS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, final version, European Commission, Directoire-General XIII, Telecommunication, Information Market and Exploitation of Research, Security of telecommunication and information systems, SOG-IS (Senior Officials Group Information Systems Security), 21 novembre 1997, réf : 017/97 Final.

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
Bureau Certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr