PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/29

IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library

Paris, le 14 décembre 2006

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport 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 cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr

Référence du rapport de certification

2006/29

Nom du produit

IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library

Référence/version du produit

IC version FR00 001, HAL-API v. 22.0, DRNG Library v. 22.0

Conformité à un profil de protection

BSI-PP-02

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur(s)

Fujitsu

1-1 Kamikodanaka 4_Chome, Nakahara-Ku, Kawasaki 211-8588 Japan

Commanditaire

Fujitsu

1-1 Kamikodanaka 4_Chome, Nakahara-Ku, Kawasaki 211-8588 Japan

Centre d'évaluation

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 62 88 28 01, mél : ceaci@cnes.fr

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics. (article 7)
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (article 8)

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library , IC version FR00 001, HAL-API v. 22.0, DRNG Library v. 22.0 » développé par Fujitsu.

Ce produit est une plateforme sans contact pour carte à puce répondant à des besoins de communication ; il comporte le système applicatif pour le transport et la finance. Il est conforme à l'ISO/IEC18092 « Télécommunications et échanges d'information entre systèmes, communication de champ proche (212/424 kbps)».

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation. Les références techniques utilisées dans ce rapport sont identifiées dans la cible de sécurité.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par les éléments suivants :

- Smartcard Integrated Circuit « CXD9861/MB94RS402, version FR00 001 »
- HAL-API version 22.0
- DRNG Library version 22.0

Le produit est physiquement identifié par des caractères et des codes d'identification dessinés sur la couche de métal supérieure :

- Caractère d'identification du Chip
- Sony RC-S960
- FR00 MB94RS402

plus le code de révision matériel sur trois caractères.
Le produit est étiqueté avec différentes appellations cohérentes : MB94RS402, CXD9861, FR00 001.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- SF.RNG : Générateur de nombres aléatoires déterministes (DRNG) qui génère des aléas de 64 bits.
- SF.DES : Co-processeur DES qui est conforme au FIPS46-3, il fournit un processeur DES 1 clé et un processeur triple-DES 2 clés. Il supporte les modes ECB ou CBC pour le chiffrement et le déchiffrement.

- SF.Mal-Detect : Fonction qui détecte si le produit est utilisé en dehors d'un environnement défini en termes de température, fréquence et tension.
- SF.Phy-Detect : Bouclier actif qui détecte les modifications du produit pour le protéger contre le sondage et les manipulations physiques.
- SF.Phy-Protect : Agencement physique qui protège le produit des manipulations et sondage physique et rend difficiles les manipulations.
- SF.TEST : Le test du microcontrôleur est effectué par des fonctions de test qui incluent un logiciel de test dédié au microcontrôleur et des circuits de test qui permettent de s'assurer du fonctionnement correct du produit et de la qualité des opérations du produit. Une fois que les tests sont effectués, les fonctions de test sont invalidées.
- SF.Identification : Capacité d'écrire chaque donnée d'identification du produit et de prépersonnalisation dans la FRAM.
- SF.Memory-Access : Détection du fait qu'un code malicieux ait un accès non autorisé au produit et que les données d'accès DMA sont modifiées délibérément, ceci permet de prévenir la révélation de données confidentielles.
- SF.Memory-Scramble : Protection des données confidentielles stockées en mémoire contre les attaques en manipulation et en sondage. Cette fonction brouille de manière logique les données d'adressage de la mémoire afin de rendre difficile la lecture des données en mémoire depuis l'extérieur.
- SF.Memory-Verification : Fonction CRC qui assure l'intégrité des données en FRAM.

1.2.3. Architecture

Le produit est constitué d'une partie matérielle :
- CPU F2MC-8FX (8-bit CISC at 6.78 MHz),
- Mémoires (48KB ROM, 3KB SRAM, 9KB FRAM),
- Coprocesseur DES,
- Contrôleur DMA,
- Circuit analogique.

Le produit inclut aussi une partie logicielle :
- HAL-API (Hardware Abstraction Layer Application Program Interface),
- DRNG Library.

1.2.4. Cycle de vie

Le cycle de vie du produit est décomposé en sept phases telles que décrites dans [BSI-PP-002] :
- Phase1 : Développement du logiciel embarqué,
- Phase2 : Développement du microcontrôleur,
- Phase3 : Fabrication du microcontrôleur,
- Phase4 et Phase5 : Production des cartes à puce,
- Phase6 : Personnalisation des cartes à puce,
- Phase7 : Utilisation finale.

Le produit a été développé sur les sites suivants :

Développement du microcontrôleur en phase 2

Fujitsu ltd. Kawasaki R&D Facilities

4-1-1, Kamikodanaka, Nakaharaku, Kawasaki, Kanagawa, 211-8588, Japan.

Development du programme de test en phase 2

Fujitsu ltd. Akiruno Technology Center

50 Fuchigami, Akiruno, Tokyo, 197-0833, Japan

Fabrication des masques en phase 2

Dai Nippon Printing Limited. Kamifukuoka plant

2-2-1, Fukuoka, Kamifukuoka-shi, Saitama 356-8507 Japan

Fabrication du microcontrôleur en phase 3

Fujitsu ltd. Mie plant

1500, Mizono, Todo-cho, Kuwana-shi, Mie-Ken, 511-0192, Japan

Pour l'évaluation, l'évaluateur a considéré comme « administrateur du produit » les développeurs, fabricants, personnalisateurs et émetteurs des cartes à puce et comme « utilisateur du produit » le développeur du logiciel embarqué.

1.2.5. Configuration évaluée

Ce rapport de certification porte sur le microcontrôleur et le logiciel identifié en §1.2.1 et décrit en §1.2.3. Tout autre logiciel utilisé pour les besoins de l'évaluation ne fait pas partie de la certification.
Au regard du cycle de vie, le produit évalué est celui qui sort de fabrication (phase 3).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] ont été appliqués.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], délivré à la DCSSI le 1er décembre 2006 détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library , IC version FR00 001, HAL-API v. 22.0, DRNG Library v. 22.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation **EAL 4 augmenté.**

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre1 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit à des attaques qui demeurent fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée qu'au travers de l'évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de cette évaluation.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES] et la documentation de livraison [DEL], notamment :

- le développeur du logiciel embarqué doit faire attention aux règles de nommage des fichiers ROM échangés avec le développeur du microcontrôleur, ceux-ci étant utilisés pour l'identification du produit final ;
- le développeur du logiciel embarqué doit s'assurer que son logiciel respecte les exigences de sécurité des guides.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA] Toutefois, il n'est reconnu qu'au niveau EAL4.

L'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

[2] Les pays signataires de l'accord sont : l'Allemagne, l'Australie, l'Autriche, le Canada, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle Zélande, la Norvège, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**3**	Analysis and testing of insecure states
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécuritéde référence pour l'évaluation : - IC Platform of FeliCa Contactless Smartcard CXD9861 / MB94RS402 Security Target, Version 5, Level 7, 13 Nov 2006. Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IC Platform of FeliCa Contactless Smartcard CXD9861 / MB94RS402 Security Target (Public Version), Version 5, Level 3, Nov 22, 2006
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report Project: CXD9861 / MB94RS402, Ref.: TOR_ETR Revision : 2.0, 1 Déc. 2006. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validée : - ETR LITE for composition CXD9861 / MB94RS402, TOR_ETR_Lite, version 1.0, 1 Déc. 2006
[CONF]	Liste de configuration du produit : - CM list for CC, v30 - Configuration list of the project - Project HAL Configuration list FR00 001(CS), 16 Nov. 2006 - Project Submission List Version 34
[DEL]	ADO - DEL / ROM data acceptance manual 2 - 10-08-2006 / YT
[GUIDES]	Guide d'utilisation du produit : - RC-S960 / MB94RS402 LSI Specifications, MB94RS402_USR_E01, V5L6 - HAL-API Function Specification, MB94RS402_USR_E02, V5L4 - DRNG Library Specifications, MB94RS402_USR_E03, V5L2
[PP-BSI-02]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié sous la référence BSI-PP-0002-2001.*

Annexe 3. Références liées à la certification

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.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.