PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/18

Sony FeliCa Contactless Smart Card IC Chip RC-S962/1

Paris, le 27 juin 2008

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

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.gouv.fr

Référence du rapport de certification

DCSSI-2008/18

Nom du produit

Sony FeliCa Contactless Smart Card IC Chip RC-S962/1

Référence/version du produit

RC-S962/1

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4

Développeur(s)

Sony Corporation

1-11-1 Osaki Shinagawa-ku, Tokyo, 141-0032, Japon

Fujitsu

1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, 211-8588, Japon

Commanditaire

Sony Corporation

1-11-1 Osaki Shinagawa-ku, Tokyo, 141-0032, Japon

Centre d'évaluation

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 61 28 16 51, mél : ceaci@cnes.fr

Accords de reconnaissance applicables

CCRA

SOG-IS

IT Security Certified

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 la carte à puce sans contact Sony FeliCa RC-S962/1 développé par Sony Corporation.

Les usages possibles de cette carte sont multiples, et peuvent typiquement couvrir les besoins d'applications financières.

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.

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 :

- nom commercial : IC Chip RC-S962/1 version 1.0 ;
- référence du logiciel : FeliCa OS version 3.31 ;
- référence de la ROM du produit : 01 sans patch ;
- référence du microcontrôleur : CXD9916H3/MB94RS403 Version FR01 0001 ;
- référence du logiciel dédié du microcontrôleur : HAL Library Version 01.

Le produit peut être physiquement identifié par ses code d'identification gravé sur la couche de métal supérieure, ou bien logiquement identifié à l'aide des commandes décrites dans les guides (cf. [GUIDES]).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- contrôle d'accès ;
- contrôle des séquences ;
- protection en confidentialité des données de communication ;
- protection en intégrité des données de communication ;
- protection en intégrité des données internes.

1.2.3. Architecture

Le produit évalué est constitué d'un microcontrôleur et d'éléments logiciels dédiés sur lesquels est embarqué le système d'exploitation FeliCa OS, comme résumé dans la figure suivante :

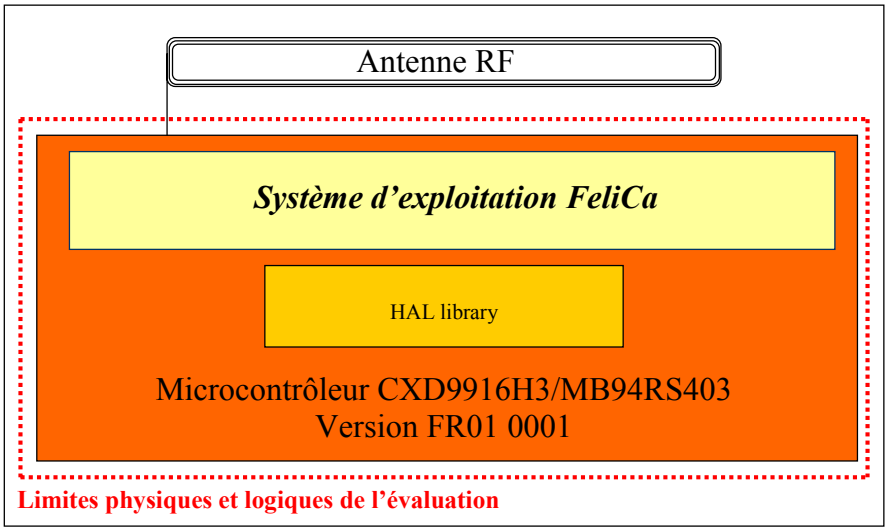

Figure 1 – Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

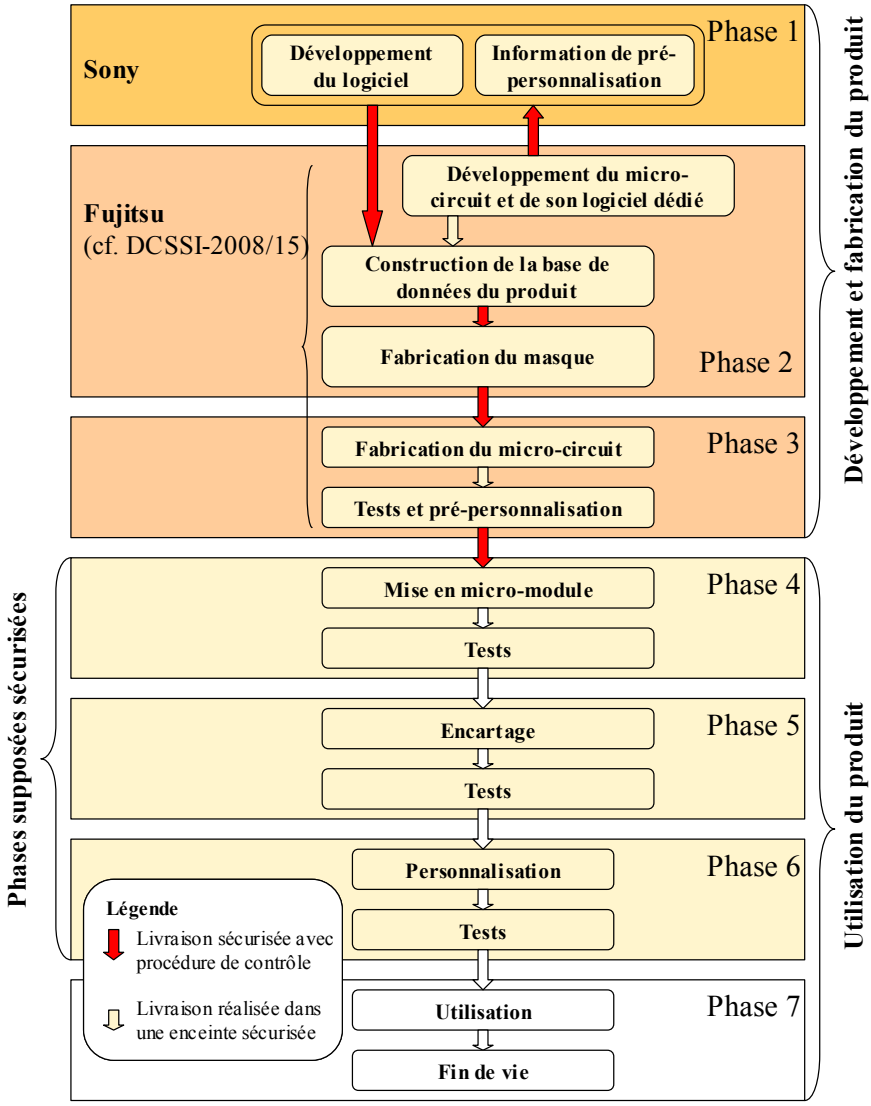

Figure 2 - Cycle de vie du produit

Le design du produit est réalisé par :

Sony Gate City Osaki Office

1-11-1 Osaki Shinagawa-ku,
Tokyo, 141-0032,
Japon

Le produit est délivré par :

Sony Toyosato Plant

130 Koguchimae, Toyosato-cho, Tome-shi,
Miyagi-ken. 987-0362,
Japon

Le microcontrôleur est conçu et fabriqué par :

Fujitsu Microelectronics Limited

1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki, 211-8588,
Japon

1.2.5. Configuration évaluée

Ce rapport de certification porte sur le microcontrôleur et son logiciel embarqué, 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].

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « CXD9916H3/MB94RS403 Version FR01 0001 » au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 26 mai 2008 sous la référence DCSSI-2008/15 (cf. [2008/15]).

L'évaluation s'appuie sur les résultats d'évaluation du produit « Sony FeliCa Contactless Smart Card IC Chip RC-S960/1 » certifié le 28 juin 2007 sous la référence 2007/14 (cf. [2007/14]).

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 11 juin 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour 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 « Sony FeliCa Contactless Smart Card IC Chip RC-S962/1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 .

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

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] au chapitre 4.2.2 et suivre les recommandations se trouvant dans les guides fournis [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 :

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

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], 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 CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, la République de Corée, 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	**1**	Subset of the 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	**1**	Identification 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	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[2007/14]	Rapport de certification DCSSI-2007/14 - Sony FeliCa Contactless Smart Card IC Chip RC-S960/1, 28 juin 2007, SGDN/DCSSI
[2008/15]	Rapport de certification DCSSI-2008/15 - Microcontrôleur CXD9916H3 / MB94RS403 & HAL Library pour carte sans-contact FeliCa, 26 mai 2008, SGDN/DCSSI
[ST]	Cible de sécurité de référence pour l'évaluation : - RC-S962/1 Composite Security Target, Référence : 962-ST-E01-10 version 1.10, Sony Corporation. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - RC-S962/1 Composite Security Target – Public version, Référence : 962-STL-E01-10 version 1.10, Sony Corporation.
[RTE]	Evaluation Technical Report - Project: TYPHON-PETIT, Référence : TYPP_ETR_v1.0 CEACI
[CONF]	RC-S962 Configuration Management List, Référence : 962-CML-E01-10 version 1.10, Sony Corporation.
[GUIDES]	Guide de livraison du produit : - FeliCa Card IC - RC-S962 IC Delivery Rules, Référence : No.962-DEL_IC-E01-20 version 1.20 Sony Corporation. Guide d'utilisation et d'administration du produit : - FeliCa Card IC Security Operation Guidelines, Référence : M292-E0.1-00 version 1.0, Sony Corporation. - FeliCa Card Rewriting Transport key, Référence : Tec01-E01-10 version 1.1, Sony Corporation. - RC-S962 Series Inspection/Verification Procedure, Référence : M427-E01-00 version 1.0, Sony Corporation. - RC-S962 Series FeliCa OS Command Reference Manual, Référence : M417-E01-00 version 1.0, Sony Corporation. - RC-S962 Series FeliCa OS Status Flag Reference, Référence : M418-E01-00 version 1.0, Sony Corporation.

	- RC-S962 Series Manufacture ID Writing Procedure, Référence : M428-E01-00 version 1.0, Sony Corporation.
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) 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. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.