UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UKAS
PRODUCT
CERTIFICATION
122-B

CERTIFICATION REPORT No. P165

Sony FeliCa Contactless Smart Card
RC-S860

Sony CXD9559, ROM Version 6, OS Version 3.1

has been evaluated under the terms of the Scheme

and complies with the requirements for

EAL4 COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL

Issue 1.0

March 2002

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

ARRANGEMENT ON THE
MUTUAL RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

(CCRA)

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Trademarks:

The following trademarks are acknowledged:

Sony Corporation

All other product or company names are used for identification purposes only and may be trademarks of their respective owners.

CERTIFICATION STATEMENT

FeliCa RC-S860 is a Contactless Smart Card developed by Sony Corporation.

FeliCa RC-S860 (Sony CXD9559, ROM Version 6, OS Version 3.1) has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met Common Criteria Part 3 requirements of Assurance Level EAL4 for the specified Common Criteria Part 2 functionality. The Security Target did not invoke CC augmented assurance or extended functionality.

Protection Profile claims were not invoked in the Security Target.

Given the nature of threats to smartcards, the “Important Notice for Customers FeliCa RC-S860” [z] and “Sony FeliCa RC-S860 Hardware Evaluation Report, Datacard Group” [o] should be consulted to allow a proper risk analysis to be performed before FeliCa RC-S860 is deployed.

Originator	**A W Borrett** Certifier
Approval **and Authorisation**	**Dr R Pizer** Head of the Certification Body
Date authorised	4 March 2002

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CMP	Chemo-Mechanical Polishing
CPU	Central Processing Unit
CCRA	Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security
CSM	Confocal Scanning Microscope
DES	Data Encryption Standard
3DES	Triple DES operation. A 3DES encryption uses two keys in an Encrypt-Decrypt-Encrypt sequence.
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
FD	Floppy Disk
FIB	Focused Ion Beam
GPIB	General Purpose Interface Bus
IC	Integrated Circuit
ID	Identity
IDm	Manufacturer ID
ITSEC	Information Technology Security Evaluation Criteria
JIL	Joint Interpretation Library

LFSR	Linear Feedback Shift Register
LSI	Large Scale Integration
OR	Observation Report
OSP	Organizational Security Policy
PET	Poly Ethylene Terephthalate
PGP	Pretty Good Privacy
PP	Protection Profile
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
RNG	Random Number Generator
ROM	Read Only Memory
RF	Radio Frequency
SFR	Security Functional Requirement
SoF	Strength of Function
SPM	Security Policy Model
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication

REFERENCES

a. FeliCa RC-S860 Contactless Smart Card Security Target,
Sony Corporation,
Version 2.0, 860-ST-E02-00, 12 December 2001.

b. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

c. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

d. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

e. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

f. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

h. Common Criteria: Interpretation-069: Informal Security Policy Model, 30 March 2001.

i. Joint Interpretation Library, The Application of CC to Integrated Circuits,
JIL,
V1.0, January 2000.

j. Joint Interpretation Library, Integrated Circuit Hardware Evaluation Methodology,
Vulnerability Assessment,
JIL,
Version 1.3, April 2000.

k. Final Evaluation Technical Report for LFL/T141,
Logica CLEF,
Issue 1.0, CLEF.25909/7.2/2, 22 June 2001.

l. Evaluation Technical Report Addendum for LFL/T141,
Logica CLEF,
Issue 1.0, CLEF.25909/7.2/3, 9 July 2001.

m. EAL4 Evaluation Technical Report for LFL/T141,
Logica CLEF,
Issue 1.0, CLEF.25909/7.2/4, 9 November 2001.

n. EAL4 Evaluation Technical Report Addendum for LFL/T141,
Logica CLEF,
CLEF.25909/7.2/5, Issue 1.0, 13 December 2001.

o. Sony FeliCa RC-S860 Hardware Evaluation Report,
Datacard Group,
Issue 1.0, HDCR-DCG-TR-0001, Issue 1.0, 12 December 2001.

p. Errata for LFL/T141 Hardware Evaluation Report,
Datacard Group,
25 January 2002.

q. DES Function Test Procedure for FeliCa RC-S860,
Sony Corporation,
860-DTP-E01-00, v1.00, 2 October 2001.

r. DES Function Test Result for FeliCa RC-S860,
Sony Corporation,
860-DTR-E01-00, v1.00, 2 October 2001.

s. DES Function Test Specification for FeliCa RC-S860,
Sony Corporation,
860-DTS-E01-00, v1.00, 1 October 2001.

t. Differential Fault Analysis of Secret Key Cryptosystems,
Technion – Computer Science Department,
Technical Report 0910 (Revised 1997)
E Biham & A Shamir, 1997.

u. Differential Power Analysis,
Cryptography Research Inc.,
P Kocher & J Jaffe & B Jun.

v. FeliCa RC-S860 Developer Vulnerability Analysis,
Sony Corporation,
860-VA-E01-20, v1.2, 12 December 2001.

w. Federal Information Processing Standards Publication,
NIST,
Security Requirements for Cryptographic Modules, FIPS PUB 140-1, 11 January 1994.

x. Function Specification FeliCa RC-S860,
Sony Corporation,
860-FS-E02-00, v2.0, 10 December 2001.

y. High Level Design FeliCa RC-S860,
Sony Corporation,
860-HD-E02-00, v2.0, 10 December 2001.

z. Important Notice for Customers FeliCa RC-S860,
Sony Corporation,
860-IN-E01-10, v1.1, 20 December 2001.

aa. Development Specification Document Product Code: CXD9559-06, 955906-DS-E01-20 (pre-issue),
Sony Corporation,
Rev. 1.2, March 2001.

bb. CXD9559 Mass-Production Test Description,
Sony Corporation,
860- MTD-E01-00, v1.0, 1 Oct 2001.

cc. Random Number Generator Function Test Procedure for FeliCa RC-S860,
Sony Corporation,
860-RTP-E01-00, v1.00, 2 October 2001.

dd. Random Number Generator Function Test Result for FeliCa RC-S860,
Sony Corporation,
860-RTR-E01-00, v1.00, 2 October 2001.

ee. Random Number Generator Function Test Specification for FeliCa RC-S860,
Sony Corporation,
860-RTS-E01-00, v1.00, 1 October 2001.

ff. RC-S860 Strength Of Function Analysis,
Sony Corporation,
860-SOF-E01-20, Version 1.2, November 20, 2000.

gg. FeliCa Security Reference Manual,
Sony Corporation,
M10-E01-20, Version 1.2. December 2001.

hh. FeliCa Card User's Manual,
Sony Corporation,
M09-E02-01, v2.1, December 2001.

ii. FeliCa RC-S860 Delivery Procedure,
Sony Corporation,
M12-E02-00, V. 2.0 Draft 1, 13 August 2001.

jj. ISO7810: 1995 Identification Cards – Physical Characteristics
ISO.

kk. Rewriting Transport Key,
Sony Corporation,
FeliCa RC-S860, Tec 10-E01-00, Version 1.0, March 2001.

ll. Card Issue Procedure RC-S860,
Sony Corporation,
860-CI-E02-00, Version 2.0, Draft 2, 13 August 2001.

mm. Errata to Sony FeliCa RC-S860 Hardware Evaluation Report,
Datacard Group,
Version 1-0, 5 February 2002.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Sony FeliCa RC-S860, Sony CXD9559, ROM Version 6, OS Version 3.1 to the Sponsor, Sony Corporation, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

Sony FeliCa RC-S860, Sony CXD9559, ROM Version 6, OS Version 3.1.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Sony Corporation. Sony subcontracted IC layout and fabrication.

4. The Sony RC-S860 contactless smart card is a compact card, conforming to ISO/IEC7810ID-1 dimensions [jj]. An IC chip and antenna are built into the card. The card itself operates from low-power electromagnetic signals received from a reader/writer. The card contains an 8-bit RISC CPU, combining built-in EEPROM, RAM, ROM, encryption processing and RF functions.

5. The Sony RC-S860 can facilitate unique access rights set by several different service providers. Hence, a single card can be used for a variety of applications whilst assuring individual security. Separate, unique keys, providing individual access rights to different memory areas on the card, control both dedicated and common files.

6. Details of the evaluated configuration, including the TOE’s supporting guidance documentation, are given in Annex A.

7. An overview of the TOE’s security architecture can be found in Annex B.

TOE Scope

8. The Security Target [a] does not identify specific hardware functions as Security Functions. Rather, the Security Functions of [a] are implemented in firmware. These Security Functions were evaluated to EAL4 by the Logica CLEF.

9. The DES processor and random number generator (RNG) are intrinsic to the implementation of other security functions in the Security Target. Assurance in respect of their operation was derived from Developer test evidence and software functional and penetration testing. Hardware evaluation to support the Security Target [a] was carried out by Datacard

Consult p7. The results of the hardware evaluation were only to establish the resistance of the IC attacks in the context of the composed TOE represented in [a].

Protection Profile Conformance

10. The Security Target [a] did not claim conformance to any protection profile.

Assurance

11. The Security Target [a] specified the assurance requirements for the evaluation. The predefined evaluation assurance level EAL4 with straight VLA.2 was used. Common Criteria Part 3 [f] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7 (where EAL0 represents no assurance). An overview of CC is given in CC Part 1 [d].

Strength of Function Claims

12. The minimum Strength of Function (SoF), applied to cryptographic protocol, was SoF-basic. SoF-basic was tied to the use of VLA.2 as in reference [j].

13. The cryptographic mechanisms contained in the TOE, DES and 3DES, are publicly known. As such it is the policy of the national authority for cryptographic mechanisms, CESG, not to comment on appropriateness or strength. Hence, no comment on the strength of function of DES and 3DES by the TOE in respect of encryption/decryption for confidentiality or mutual authentication are given.

Security Policy

14. The TOE security policies are detailed in [a]. These cover: identification, data access, secure communication and cryptographic standards.

Security Claims

15. The Security Target [a] fully specifies the TOE’s security objectives, threats, OSPs and security functional requirements, and security functions to elaborate the objectives. All of the SFRs are taken from CC Part 2 [e]; use of this standard facilitates comparison with other evaluated products.

16. CC Security Functional Requirements (SFRs) were either tailored, refined or restated to reflect the security of the TOE. Security Functions for the TOE were as follows:

a. Cryptographic key generation, FCS_CKM.1

b. Cryptographic key destruction, FCS_CKM.4

c. Cryptographic operation, FCS_COP.1

d. Subset access control, FDP_ACC.1

e. Security attribute based access control, FDP_ACF.1

f. Basic data authentication, FDP_DAU.1

g. Export of user data without security attributes, FDP_ETC.1

h. Subset information flow control, FDP_IFC.1

i. Simple security attributes, FDP_IFF.1

j. Import of user data without security attributes, FDP_ITC.1

k. Stored data integrity monitoring, FDP_SDI.1

l. Underlying abstract machine test, FPT_AMT.1

m. Failure with preservation of secure state, FPT_FLS.1

n. Inter-TSF confidentiality during transmission, FPT_ITC.1

o. Inter-TSF detection of modification, FPT_ITI.1

p. Function recovery, FPT_RCV.4

q. Replay detection, FPT_RPL.1

r. Inter-TSF trusted channel, FTP.ITC.1

Evaluation Conduct

17. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [b, c]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group and the Department of Trade and Industry on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

18. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. The evaluation was performed in accordance with CC Part 3 [f] and the Common Evaluation Methodology (CEM) [g]. Additionally, [i, j] were used to interpret CC for ICs.

19. EAL3 evaluation of the TOE, excluding some vulnerability analyses and hardware penetration testing, commenced in November 2000 and ended in June 2001. Complete vulnerability analyses and the hardware and EAL4 delta evaluations (to include some additional security functions), started in July 2001 and completed in December 2001.

20. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF) and Datacard Consult p7. The evaluation was completed when the CLEF submitted the Addendum to the Evaluation Technical Report (ETR) [m] and Datacard Consult p7 submitted the Hardware Evaluation Report [o] to the Certification Body in November and December 2001 respectively. Following the CLEF and Datacard's response [n, p, mm] to a request for further information, the Certification Body then produced this Certification Report.

Certification Result

21. For the certification result see the "Evaluation Outcome" Section.

General Points

22. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

23. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been evaluated and certified.

24. The issue of a Certification Report is not an endorsement of a product.

II. EVALUATION FINDINGS

Introduction

25. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [k, l, m, n, o, p, mm] under the CC Part 3 [f] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Architectural Information

26. The CPU connects the device's various memory (ROM, RAM, EEPROM) via an 8-bit data bus. The device contains a voltage regulator with high voltage detector. RNG is a pseudo-random number generator implemented in the random logic portion of the IC. (See references [x, y, aa].) Refer to Annex B for an overview of software and hardware architecture.

Security Policy Model

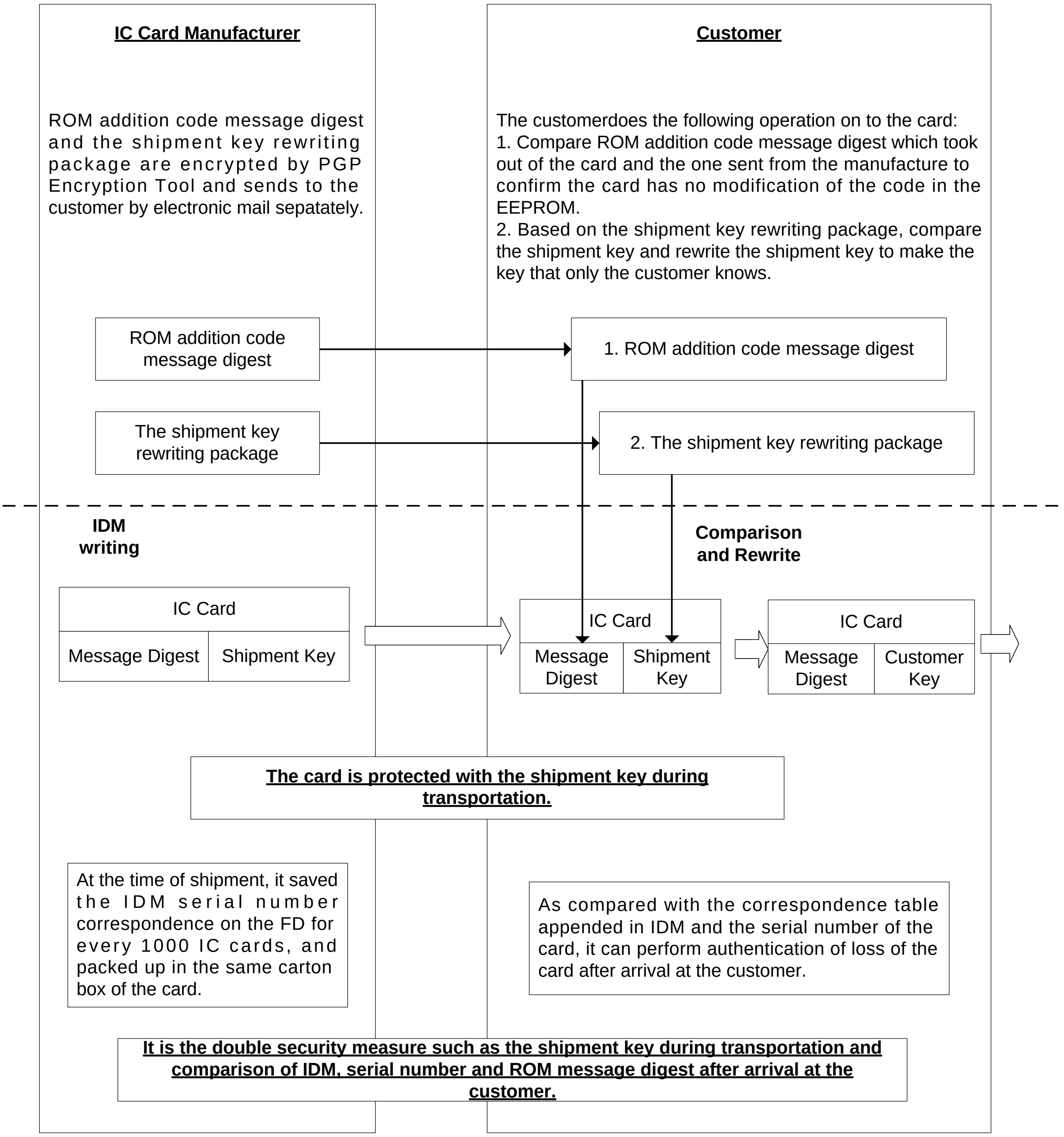
27. Common Criteria: Interpretation-069 [h] was followed, allowing the Security Target [a] to be taken as providing the Informal Security Policy Model (SPM). The Evaluators confirmed that the SPM clearly articulated the security behaviour of the TOE. They noted that although the CEM [g] does not require a check of the internal consistency of the informal SPM, the evidence for such was provided as part of the Security Target evaluation.

Delivery

28. Customers of the TOE need to be aware of the delivery guidance procedures as detailed by Sony in [a, gg, ii, z].

29. The shipping key is required to establish an authentic IC. PGP is used as the distribution mechanism for the ROM addition code message digest and the shipping key from the manufacturer to the customer.

30. The following diagram illustrates trusted delivery flow procedures. The IC manufacturing key protects the IC chip during the manufacturing process. The manufacturing key is required whenever information needs to be changed on the card. The IC manufacturing key is changed to a shipping key before transportation for protection during transportation. The shipping key is changed by the customer to their own customer key before the card can be set-up. Only the customer key can be used to set-up the card.



ROM addition code message digest and the shipment key rewriting package are encrypted by PGP Encryption Tool and sends to the customer by electronic mail sepatately.

The customerdoes the following operation on to the card:
1. Compare ROM addition code message digest which took out of the card and the one sent from the manufacture to confirm the card has no modification of the code in the EEPROM.
2. Based on the shipment key rewriting package, compare the shipment key and rewrite the shipment key to make the key that only the customer knows.

ROM addition code message digest
1. ROM addition code message digest
The shipment key rewriting package
2. The shipment key rewriting package
IDM writing
Comparison and Rewrite
IC Card
Message Digest
Shipment Key
IC Card
Message Digest
Shipment Key
IC Card
Message Digest
Customer Key

The card is protected with the shipment key during transportation.

At the time of shipment, it saved the IDM serial number correspondence on the FD for every 1000 IC cards, and packed up in the same carton box of the card.

As compared with the correspondence table appended in IDM and the serial number of the card, it can perform authentication of loss of the card after arrival at the customer.

It is the double security measure such as the shipment key during transportation and comparison of IDM, serial number and ROM message digest after arrival at the customer.

Guidance Documentation

31. References [gg, hh] should be adhered to when developing applications for use with the TOE or deploying the TOE operationally; it should be noted, however, that the TOE does not support application download. The Certifier draws particular attention to Reference [z], which alerts customers to the need to consider certain technical attacks when carrying out their risk analysis.

Strength of Function

32. The SoF claim for the TOE was as given above under “Strength of Function Claims”. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE other than DES, 3DES and RNG, and that therefore the SoF claim of SoF-basic was upheld as claimed in [ff].

Vulnerability Analysis

33. The Evaluators’ vulnerability analysis was based on public domain sources, Developer supplied evidence [v] and the visibility of the TOE given by the evaluation process [k, l, m, n, o, p, z].

IT Product Testing

34. The correspondence between the tests specified in the Developer’s test documentation and the IT Security Functions specified in the Functional Specification [x], and between the tests and the High Level Design [y], was complete and accurate in terms of the coverage of the Security Functions and High Level Design. Although the Evaluators identified some additional tests in the test documentation that were not identified in the Developer’s mappings, the Evaluators were nevertheless satisfied that the tests were suitable to demonstrate the expected behaviour of the Security Functions. These tests were subsequently brought under the Developer’s configuration control procedures. For each command used in a test, the Developer tested for correct operation, error conditions, incorrect entry of the command, incorrect parameters (where appropriate) and parameters out of range (where appropriate).

35. The test documentation included the Test Plan and Analysis document, which detailed the test descriptions/procedures (including the pre-requisites, test order dependencies and expected results), the mapping of Security Functions to test cases, the mapping of High Level Design to test cases, the mapping of interfaces to test cases, the test environments, the test tools and the actual test results. The test results included the results of regression testing and all test results were found to be consistent with the expected results. The Evaluators noted that the test environment was consistent with the security environment requirements and assumptions stated in the Security Target [a]. (See references [r, bb, cc, dd, ee].)

Software Testing

36. The evaluation was performed in two stages: EAL3; EAL4 top-up. The evaluators examined the Internet for any publicly known vulnerabilities on the TOE: no generic vulnerabilities relevant to this type of TOE were discovered. CLEF vulnerability analysis and

penetration testing was carried out at the EAL3 [k, l] stage and after the hardware evaluation had concluded [n, o, p, z]. This comprised:

a. Exploiting the capabilities of interfaces to the TOE, or utilities which might interact with the TOE;

b. Examining privileges inheritance or other capabilities that should otherwise be denied;

c. Looking for data stored or inadequately copied to protected areas;

d. Behaviour examination of the TOE when start-up, closedown or recovery is activated;

e. Behaviour examination of the TOE under extreme circumstances, particularly where this could lead to the de-activation or disablement of Security Function;

f. Investigation of attempts to use the Test Enable command.

37. No exploitable vulnerabilities arose from these tests.

Hardware Testing

38. Datacard Consult p7 carried out testing in the following respects (see references [q, r, s, t, u, v, w, x, y, z, aa, bb, cc, dd, ee, ff, gg, hh, ii]):

a. Operational Envelope. Die with antenna were tested by carrying out DES calculations at a range of temperatures between –41^{o}C and +85^{o}C, and with variation of the distance between card and reader/writer. The intention of this testing was to identify conditions which would induce faults in DES calculation (for use in differential fault analysis) or which led to unexpected behaviour of the TOE.

b. Sensor. Visual inspection of the die to identify features that might lead an attacker to disable the regulation of voltage by the TOE was conducted.

c. Differential Fault Analysis. The evaluators attempted to introduce faults into DES calculations carried out by the IC.

d. Timing and Power Analysis.

e. Bus probing. Probing was carried out to examine the ability to extract or modify critical data in transit on the bus (e.g. between the CPU and EEPROM).

f. Test Mode. The TOE passes through a number of test modes during its manufacturing process [bb]. In particular, one of the modes enables reading and writing of EEPROM. The evaluators found that certain alterations to the IC could be made which might enable some sorts of attacks.

III. EVALUATION OUTCOME

Certification Result

39. After due consideration of the ETR [k, l, m, n, o, p, mm], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Sony FeliCa RC-S860, Sony CXD9559, OS Version 3.1 meets Common Criteria Part 3 requirements for Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 conformant functionality.

40. The minimum strength of function was SoF-basic. The VLA level was VLA.2.

41. The Certification Body has also determined that the TOE meets the minimum SoF claim of SoF-basic given above under paragraph 33 (See [ff].).

42. Given the nature of threats to smartcards, the “Important Notice for Customers FeliCa RC-S860” [z] and “Sony FeliCa RC-S860 Hardware Evaluation Report, Datacard Group” [o] should be consulted to allow a proper risk analysis to be performed before FeliCa RC-S860 is deployed.

Recommendations

42. Prospective consumers of Sony FeliCa RC-S860, Sony CXD9559, OS Version 3.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target. Particular attention should be paid to [z], which alerts customers to the need to consider certain technical attacks when carrying out their risk analysis.

43. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under ‘TOE Scope’ and ‘Evaluation Findings’.

44. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

41. The above ‘Evaluation Findings’ include a number of recommendations relating to the secure receipt and operation of the TOE (See paragraphs 28 to 31).

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of:

    a. Sony FeliCa RC-S860 Contactless Smart Card

    b. IC chip specification: Sony CXD9559

    c. ROM: Version 6

    d. FeliCa OS: Version 3.1.

2. The supporting guidance documents evaluated were:

    a. FeliCa Security Reference Manual, [gg]

    b. FeliCa Card User's Manual, [hh]

    c. FeliCa RC-S860 Delivery Procedure, [ii]

    d. Rewriting transport Key, [kk]

    e. Card Issue Procedure RC-S860, [ll]

    f. Important Notice for Customers FeliCa RC-S860 [z].

3. Further discussion of the supporting guidance material is given in Section II under the heading Guidance Documentation.

TOE Configuration

4. Not applicable.

Environmental Configuration

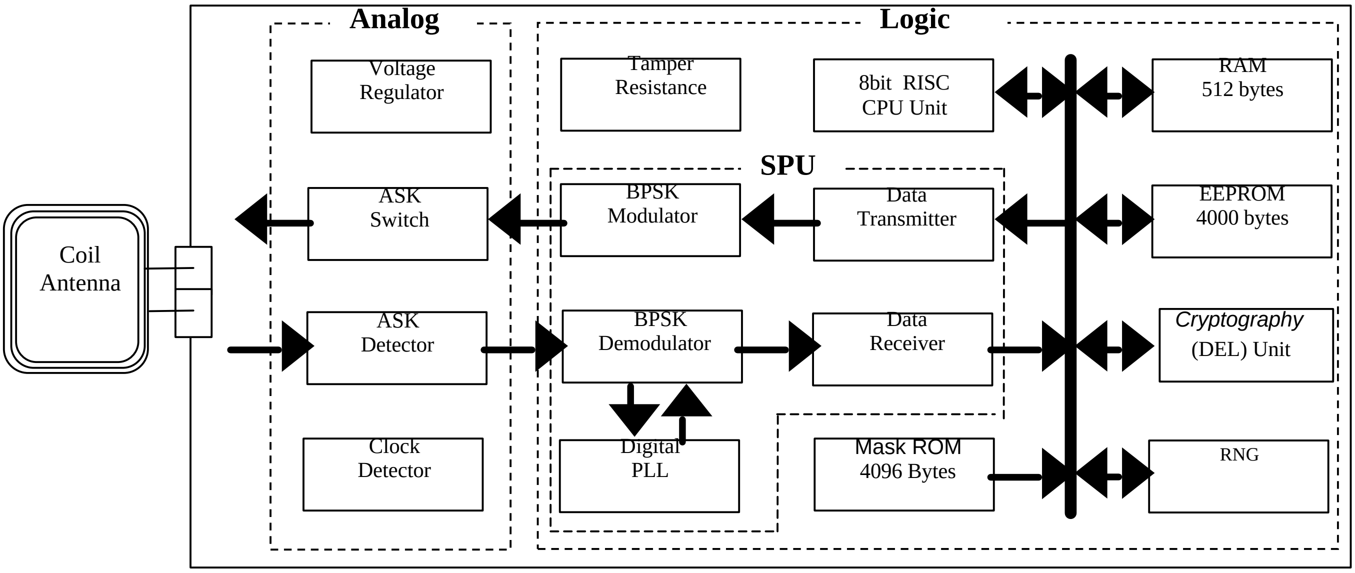
5. The immediate environment for the TOE is the PET carrier in which the IC is embedded. This can be applied with printing, a magnetic stripe and security features such as holograms.

6. In general, a smart card is assumed to be in the uncontrolled possession of the card holder and its environment is therefore application dependent.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the product architectural features that are relevant to the security of the TOE. Other details relating to the scope of evaluation are given in the main body of the report [and in Annex A]. Major components of the TOE are represented in the figure below.



Major Architectural Features

Software

2. The TOE comprises 116 modules. Each of these performs a particular function. The relevant module is called when the TOE performs a particular function: twenty modules directly correspond to the set of commands that are used to communicate between the TOE and a Reader/Writer; these in turn call other modules to, if necessary, implement the required card functionality and generate response packets. Software functions include:

a. checking the card IDm and mode;

b. listing the available area and service file codes;

c. performing data encryption/decryption;

d. parity checks;

e. key changes;

f. mutual authentication;

g. file and system diagnostics;

h. system registration;

i. area and service files;

j. reading and writing;

k. calculation of message digests;

l. enabling test mode;

m. card separation.

3. The RC-S860 Contactless card supports memory separation by logical means: the memory of the card is partitioned into a hierarchical structure. This allows for isolation of information stored by different providers on different virtual cards. The TOE also supports a special separation function that divides the card memory into two independent areas, thereby forming two “virtual” cards.

Hardware

4. The Sony FeliCa RC-S860 contactless smart card comprises a 2-metal layer integrated circuit with 0.6 μm feature size.

5. The CPU connects the device’s various memory (ROM, RAM, EEPROM) via an 8-bit data bus. The device contains a voltage regulator with high voltage detector. RNG is a pseudo-random number generator implemented in the random logic portion of the IC.

Hardware and Firmware Dependencies

6. Hardware: IC chip specification CXD9559 ROM Version 6.0.

7. Firmware: FeliCa OS Version 3.1.

(This page is intentionally left blank)