UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P240

SONY IC Chip with Operating System for Mobile CXD3715GG/GU-x
Version 0701

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

January 2006

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, GL51 0EX
United Kingdom

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

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:

CERTIFICATION STATEMENT

Sony CXD3715GG/GU-x Version 0701 is an Integrated Circuit intended primarily for use within mobile devices (such as a telephone) and can be used for applications such as transport and finance. It operates using both a contactless and a contact interface.

Sony CXD3715GG/GU-x Version 0701, composed of Integrated Circuit (version 2.1) and embedded operating system (Mobile FeliCa OS version 1.0), has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality.

Originator	**CESG** Certifier
Reviewer	**CESG** Certifier UK IT Security Evaluation and Certification Scheme
Date authorised	24 January 2006

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CC	Common Criteria
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
IC	Integrated Circuit
ROM	Read Only Memory
SFR	Security Functional Requirement
SoF	Strength of Functions
SRAM	Static Random Access Memory
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UART	Universal Asynchronous Receive Transmit
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. CXD3715GG/GU-x Security Target (Public Version),
Revision 1.04, 26 January 2006

b. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-001, Version 22, January 2004

c. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-002, Version 2.2, January 2004.

d. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-003, Version 2.2, January 2004.

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

f. CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

g. CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.0, October 2003.

h. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-004, Version 2.2, January 2004.

i. Application of Attack Potential to Smartcards (Common Criteria Supporting Document),
Version 1.1,July 2002.

j. Application of Common Criteria to Integrated Circuits (Common Criteria Supporting
Document), Version 1.2, July 2002.

k. CXD3751GG/GU-X with Mobile FeliCa OS Hardware Evaluation Technical Report,
SiVenture,
FLN2-TR-0001, Version 1.0, 5 December 2005.

l. Evaluation Technical Report,
LogicaCMG,
CLEF.201196/7.2/1, Version 1.0, 5 December 2005.

m. CXD3751GG/GU-x Important Notice for Customers,
Sony Corporation, Version 1.4, 13 January 2006.

n. CXD3751GG/GU-x Secure Operation Guidelines,
Sony Corporation, Version 1.3, 9 December 2005.

o. Functionality Classes and evaluation methodology for deterministic random number generators,
Bundesamt fur Sicherheit in der Informationstechnik (BSI),
Version 1, 2 December 1999.

p. Security Reference Manual Changing Key Package Generation, Sony Corporation, SR-030-004E, Version 1.00, August 2004

q. Security Reference Manual Group Service Key & User Service Key Generation, Sony Corporation, SR-030-001E, Version 1.00, August 2004

r. Security Reference Manual Issue/Delete Package Type 2 [Generation Procedure], Sony Corporation, SR-030-005, Version 1.01, 8 November 2005

s. Security Reference Manual Issuing Package Generation, Sony Corporation, SR-030-003E, Version 1.00, August 2004

t. Security Reference Manual Key Change Package Type 2 [Generation Procedure], Sony Corporation, SR-030-006, Version 1.01, 8 November 2005

u. Security Reference Manual Mutual Authentication Lock Function, Sony Corporation, SR-030-007, Version 1.01, 8 November 2005

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Sony CXD3715GG/GU-x Version 0701, composed of Integrated Circuit (version 2.1) and embedded operating system (Mobile FeliCa OS version 1.0), 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. The certification relates to the composite product, comprised of IC and operating system, for its intended use as defined by the Security Target [a]. It cannot be reused for the IC or operating system used separately or in other applications.

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

4. They should also note that the product has been evaluated against a low Attack Potential (as required for EAL4). This means that threats from attackers with more time and resources were not considered. Common Criteria supporting documents were used to calculate Attack Potential for a given approach [i]. Therefore, customers should ensure that this level of protection is appropriate for their requirements.

5. It is important that customers also ensure that the guidance available from Sony is obtained and followed to avoid potential problems [m and n].

Evaluated Product

6. The version of the product evaluated was:

   Sony CXD3715GG/GU-x Version 0701, composed of Integrated Circuit (version 2.1) and embedded operating system (Mobile FeliCa OS version 1.0)

7. This product is also described in this report as the Target of Evaluation (TOE). The Developer was Sony Corporation.

8. The TOE is an IC with embedded operating system that is designed to be installed primarily in mobile devices such as telephones. It has a wired interface to the host device and power supply and a contactless interface (13.56 MHz) to a read/write device. The read/write device could be installed for example at railway stations (for electronic ticketing applications) or at points of sale (electronic purse applications).

9. Communication and authentication to and from the TOE is protected using encryption and protected against replay attacks using random number generation. See the Security Target [a] for more details of the product and its claimed security functionality.

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

11. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

12. The boundary of the TOE is its contactless and contact (UART) interfaces. The reader/writer device, host device and any other supporting IT infrastructure are out of scope. The TOE comprises the operating system and IC hardware (Mask ROM, SRAM, EEPROM, Logic circuits and analogue circuits).

13. The development of the hardware and software were both within scope of the evaluation and the developer procedures and site security were evaluated as required by Common Criteria EAL4. However the configuration and personalisation of the TOE by the issuer is out of scope, as is the operation of the transport or payment scheme etc.

14. The contactless and contact interfaces were within the scope, as was the entire physical surface of the IC itself. It was assumed that invasive physical attacks might be attempted against the IC and the full range of such attacks were considered up to low Attack Potential [i & j].

15. The main assumptions are around the components surrounding the TOE e.g. trust in privileged administrators, cryptographic key support, the external reader/writer and the internal controller (in the host device – but only if that controller was permitted access).

16. For more details on the scope and assumptions please see the Security Target [a].

Protection Profile Conformance

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

Assurance

18. The Security Target [a] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL4 was used. Common Criteria Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

19. The minimum Strength of Function (SoF) was SoF-Basic. This was claimed for authentication and Random Number Generation.

20. The cryptographic mechanism contained in the TOE is publicly known (3DES and DES) and as such it is the policy of the national authority for cryptographic mechanisms, (CESG), not to comment on its appropriateness or strength. The Random Number Generator was found to meet the statistical tests defined for functionality class K2 in [o].

Security Policy

21. The TOE security policies are detailed in the Security Target [a].

22. In addition, customers should familiarise themselves with the guidance provided by Sony [m & n].

Security Claims

23. The Security Target [a] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional requirements and security functions to elaborate the objectives. Most of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

Evaluation Conduct

24. 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 [e - g]. The Scheme has established a Certification Body which is managed by CESG 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 Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

25. 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. Both parts of the evaluation were performed in accordance with CC Part 3 [d] and the Common Evaluation Methodology (CEM) [h]. Common Criteria Supporting documents [i & j] were used.

26. The Certification Body monitored the evaluation which was carried out by the LogicaCMG (for the Software) and SiVenture (for the Hardware) Commercial Evaluation Facilities (CLEFs). The evaluation was completed when the CLEFs submitted the final Evaluation Technical Reports (ETRs) [k,l] to the Certification Body in December, 2005. The Certification Body then produced this Certification Report.

General Points

27. 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.

28. 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.

29. As required by Common Criteria, the evaluation included site visits for both hardware and software developers.

30. For EAL4, only attacks up to the level of 'low Attack Potential' were considered. See [i] for more details. Residual vulnerabilities may exist above this level.

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

II. EVALUATION FINDINGS

Introduction

32. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETRs [k & l] under the CC Part 3 [d] 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.

Delivery

33. On receipt of the TOE, it is recommended that the consumer checks that the evaluated version has been supplied, and that the security of the TOE has not been compromised in delivery.

34. The normal process is to make use of a transport key protecting against modification and also to check the hash of data on the chip. It is obviously important to safeguard transport keys.

35. More guidance from Sony is available [m & n].

Installation and Guidance Documentation

36. Full reference manuals are available from Sony [p-u]. In addition, customers should read [m & n], which highlight important security guidance.

Strength of Function

37. The SoF claim for the TOE was as given above under “Strength of Function Claims”.

Vulnerability Analysis

38. The Evaluators’ vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

39. The evaluators considered the full range of issues as required for Common Criteria [h & i]. No vulnerabilities were found for a low Attack Potential (as described in [i]).

Assurance Maintenance and Re-evaluation Issues

40. Not applicable.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

41. After due consideration of the ETR [k and l], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Sony CXD3715GG/GU-x Version 0701 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on the platforms specified in Annex A.

42. The Certification Body has also determined that the TOE meets the minimum SoF claim of SoF-Basic given above under "Strength of Function Claims".

Recommendations

43. Prospective consumers of Sony CXD3715GG/GU-x Version 0701 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.

44. 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'.

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

46. The above 'Evaluation Findings' include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE. See [m and n] for more details.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of: Integrated circuit (CXD3715GG/GU-x version 2.1) and embedded operating system (Mobile FeliCa OS version 1.0).

TOE Documentation

2. A discussion of the supporting guidance material is given in Section II under the heading 'Installation and Guidance Documentation'.

TOE Configuration

3. There is no special evaluated configuration for the TOE. The customer can set up access to files (and obviously has to do this sensibly but this is an assumption and does not affect the evaluated configuration of the TOE).

Annex A

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report.

Architectural Features

2. The hardware architecture is based on a CPU, volatile and non-volatile memory, a random number generator and DES encryption engine.

3. The operating system provides a simple security functionality. The TOE's memory is partitioned into several files and these are configured in a hierarchical structure. Files can be defined as open access for reading and writing or can be protected using an access key as required.

Design Subsystems

4. The software subsystems carry out the following functionality: File Management, Mutual Authentication, Control of Access to Blocks, Sequence Control, Encryption of Command/Response Packet Data, Memory protection (at interruption), Data Block Management, Packet Generation, Key Information Change, Transitions between Card Modes, Anti-DPA measures.

5. The hardware design incorporates a number of security features to counter possible attacks.

Hardware and Firmware Dependencies

6. There are no dependencies on unevaluated components. All of the software and hardware within the TOE boundary has been evaluated.

TSF Interfaces

7. The contactless interface with the reader / writer and the UART interface with the host device make up the TSF Interface (TSFI). These are protected by mutual authentication and encryption.

Annex B

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing

1. A subset of developer tests was repeated by the evaluators (for both hardware and software). This subset was spread across all of the relevant security related sub-systems. In addition to this, penetration testing was carried out (again for both hardware and software) according to the guidance laid down in [h, i, & j].

2. Vulnerabilities were searched for up to the low Attack Potential level but none were found. However, customers should be aware that it is important that authorised read/write devices are configured to follow the guidance in [m]. Customers should also be aware that attacks may be possible above the low level.

Platform Issues

3. Not applicable.

Annex C

(This page is intentionally left blank)