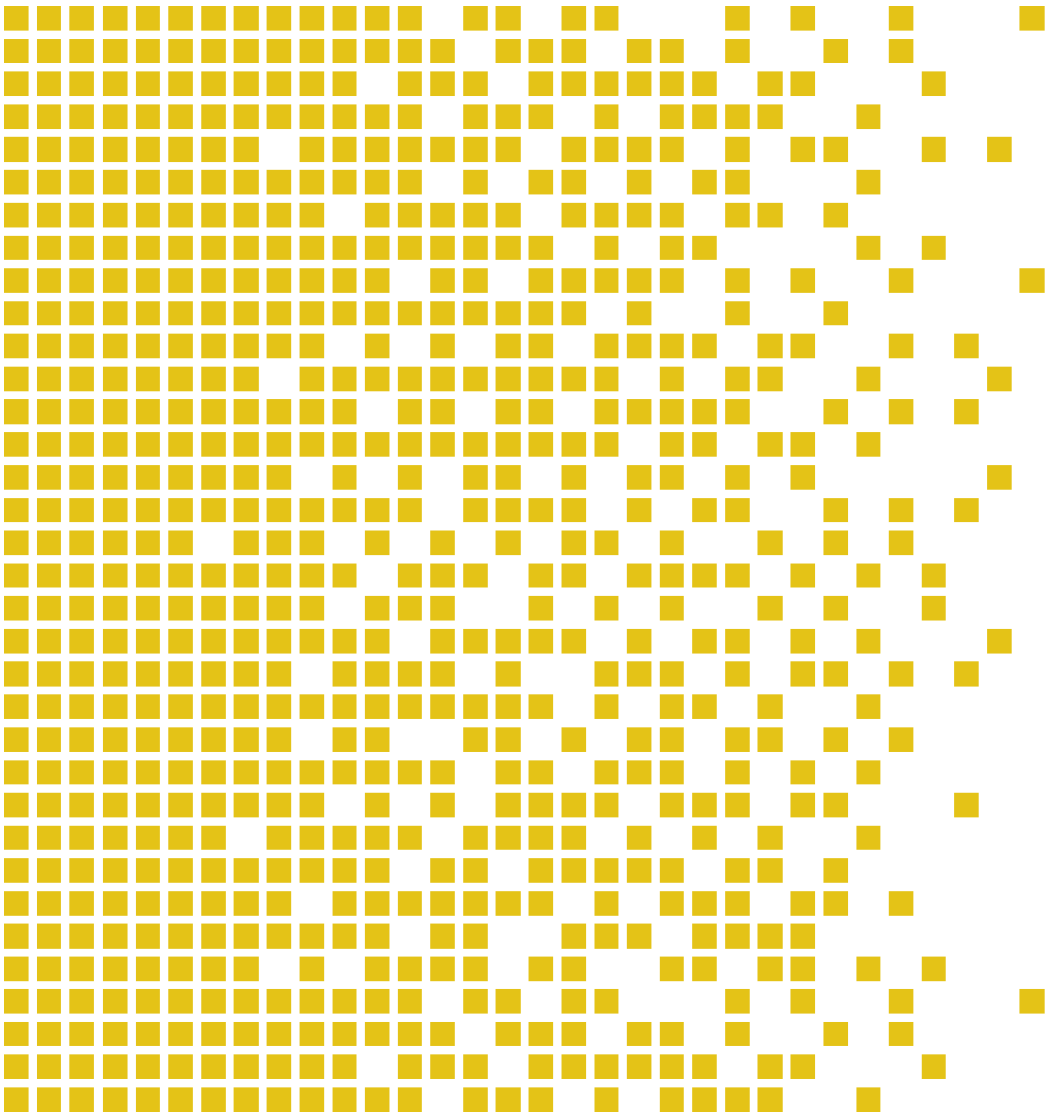
SERTIT-045 CR Certification Report

Issue 1.0 21 August 2013

Toshiba T6NE1 HW version 4



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

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

SERTIT, the Norwegian Certification Authority for IT Security, 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 SERTIT which issued it and the evaluation facility (EVIT) 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. *

* Mutual Recognition under the CC recognition arrangement applies up to EAL 4.

Contents

1 Certification Statement

TOSHIBA CORPORATION Semiconductors Company T6NE1 Integrated Circuit is a integrated circuit with a DES and AES accelerator combined with a IC for communication to realise an electronic purse (people can pay with the TOE embedded in mobile equipment).

T6NE1 Integrated Circuit version 4 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL 5+ (AVA_VAN.5 and ALC_DVS.2) for the specified Common Criteria Part 2 conformant functionality for the specified environment when running on the platforms specified in Annex A.

It has also met the requirements of Protection Profile Security IC Platform Protection Profile, version 1.0.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	21 August 2013

2 Abbreviations

BGA	Ball Grid Array
CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
DEMA	Differential Electro-Magnetic Analysis
CLF	Contactless Front End
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
HW	Hardware
HWC	Hardware Configuration
OSP	Organisational Security Policy
POC	Point of Contact
QP	Qualified Participant
RNG	Random Number Generator
SAM	Security Authentication Module
SEMA	Simple Electro-Magnetic Analysis
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Function Policy
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] T6NE1 Integrated Circuit Security Target, 24 May 2013, Version 0.38.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report Common Criteria EAL5+ Evaluation of Toshiba T6NE1 Integrated Circuit, 27th of May 2013 version 0.3

[8] T6NE1 User guidance overview, version 0.38

[9] Kura2 development specification, version 0.9.2

[10] T6NE1 User Guidance manual, version 0.9.9

[11] Security IC Platform Protection Profile. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, version 1.0, June 15, 2007

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of T6NE1 Integrated Circuit version 4 to the Sponsor, TOSHIBA CORPORATION Semiconductors Company, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was T6NE1 Integrated Circuit HW version 4.

This product is also described in this report as the Target of Evaluation (TOE). The developer was TOSHIBA CORPORATION Semiconductors Company.

The T6NE1 Integrated Circuit (Target of Evaluation – TOE) is an Integrated Circuit (plastic package or wafer) with a DES and AES accelerator. The TOE that is described is a single chip microcontroller (hardware, security IC dedicated software to initialise a number of settings for sensor levels and countermeasures at start-up and security IC dedicated test software) that is used as SAM chip in a cellular phone. The TOE combined with CLF (which is not part of the TOE) realizes a platform for electronic transactions.

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

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.3

4.4 Protection Profile Conformance

The Security Target[1] claimed conformance to the following protection profile:

Security IC Platform Protection Profile, version 1.0[11]

Additional objectives according to the PP's[11] application note 6 are described in the ST[1], chapter 4.1 and. 4.3.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 5, augmented by AVA_VAN.5 and ALC_DVS.2. Common Criteria Part 3[4] describes the scale of

assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in *ST[1] chapter 3.3*

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats, OSP's which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered by the TOE

- Physical Manipulation
- Physical Probing
- Malfunction due to Environmental Stress
- Inherent Information Leakage
- Forced Information Leakage
- Abuse of Functionality
- Deficiency of Random Numbers

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

The assumptions for the TOE are described in the Protection Profile[11], chapter 3.4

4.12 IT Security Objectives

All the IT Security objectives are described in the ST[1], chapter 4.1

4.13 Non-IT Security Objectives

All the IT Security objectives are described in the ST[1], chapter 4.2 and 4.3.

4.14 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- Limited fault tolerance FRU_FLT.2
- Failure with preservation of secure state FPT_FLS.1
- Limited capabilities FMT_LIM.1
- Limited availability FMT_LIM.2
- Audit storage FAU_SAS.1
- Resistance to physical attack FPT_PHP.3
- Basic internal transfer protection FDP_ITT.1
- Subset information flow control FDP_IFC.1
- Basic internal TSF data transfer protection FPT_ITT.1
- Quality metric for random numbers FCS_RNG.1
- Cryptographic operation FCS_COP.1
- Import of user data without security attributes FDP_ITC.1
- Cryptographic key generation FCS_CKM.1
- Cryptographic key destruction FCS_CKM.4
- Secure security attributes FMT_MSA.2
- Subset access control FDP_ACC.1
- Security attribute based access control FDP_ACF.1
- Static attribute initialisation FMT_MSA.3
- Management of security attributes FMT_MSA.1
- Specification of Management Functions FMT_SMF.1

4.15 Security Function Policy

User Data and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT

Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] 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[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT on the 27. May 2013. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 5 assurance package augmented with AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing

	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

Delivery procedures for the TOE are described in the supporting documents[8][9].

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been comprised in delivery.

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting documents[8][9].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance[8][9] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The vulnerability analysis comprised the following steps:

1. The combined set of well-known attacks from the "JIL Attack Methods for Smartcards and Similar Devices" is considered, leading to the list of 9 major attack methods to consider.
2. A theoretical analysis of the TOE type (smartcard hardware compliant to the PP) considers all 9 major attack methods against the SFRs clustered in 8 groups, being the 5 groups from the PP (Malfunctions, Abuse of functionality, Physical Manipulation, Leakage and Random numbers) and 3 extension groups

(Access Control, Cryptography(DES) and Cryptography(AES)). In total 9*8=72 SFR/attack-combinations are possible. The theoretical analysis leads to the exclusion of 38 SFR/attack combinations as not applicable for this type of TOE.

3. Potential vulnerabilities from the other evaluation activities have been gathered and taken into account during the analysis. The potential vulnerabilities in the other IRs indicated that light manipulation should be considered in the perturbation penetration testing.
4. An analysis based on design information analysing SFR/attack-combinations, showing which combinations are not applicable or not possible on this particular TOE, or which need further penetration testing. For 32 of the SFR/attack-combinations sufficient assurance could be found in the design information and other evaluation activities. For 4 SFR/attack-combinations further penetration testing was deemed necessary: light injection (on ROM,RAM,EEPROM, Toshiba registers and ARM registers) on the Malfunction SFRs, voltage manipulation on Malfunction SFR, Power/EM-based Template Attack on EEPROM data transfer and Power/EM-based Template Attack on crypto key loading on Leakage SFRs.

The TSF is resistant against known attacks at the given time of evaluation, but this could change in the future as attack techniques become more sophisticated.

5.6 Developer's Tests

The testing results from the developer show that the TOE exhibits the expected behaviour at TSFI and SFR enforcing module level. The developers test specification are directly linked to its corresponding functional specification, and passing one test shows that that specific functional specification works according to the documentation.

The depth and coverage analysis shows that the developers' tests cover all TSF, and that the TOE has been extensively tested against its functional specification. The developer's testing results lead either to a test is passed, or the test is failed and an error report is created for that error.

The results show that the developer testing requirements are extensive and that the TSF satisfies the TOE security functional requirements.

5.7 Evaluators' Tests

For independent testing, the evaluator has chosen to perform some additional testing although the developer's testing was extensive but some additional assurance could be gained by additional testing.

The evaluator's independent testing was spread over nearly all interfaces involved for implementation of the SFRs to provide good rigour of testing.

5.8 Scheme tests of the random number generator (RNG)

The Norwegian national security authority did extensive tests on the random number generator (RNG) of the chip.

Overall the conclusion was that the random number generator of the chip was of satisfactory quality.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that T6NE1 Integrated Circuit version 4 meet the specified Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 5+ (AVA_VAN.5 and ALC_DVS.2) for the specified Common Criteria Part 2 conformant functionality and the Protection Profile Security IC Platform Protection Profile, version 1.0, in the specified environment.

6.2 Recommendations

Prospective consumers of T6NE1 Integrated Circuit version 4 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

The evaluated TOE configuration is specified in Annex A.

Annex A: Evaluated Configuration

TOE Identification

The T6NE1 Integrated Circuit (Target of Evaluation - TOE) is an Integrated Circuit (plastic package or wafer) with a DES and AES accelerator. The TOE that is described in this ST is a single chip microcontroller (hardware, security IC dedicated software to initialise a number of settings for sensor levels and countermeasures at start-up and security IC dedicated test software) that is used as SAM chip in a cellular phone. The TOE combined with CLF (which is not part of the TOE) realizes a platform for electronic transactions.

CLF is the abbreviation of Contactless Front End. The TOE can connect to an RF interface and interface to a Device Host through a CLF chip.

The TOE has the following interfaces:

- a communication interface;
- a serial interface that receives data from the CLF chip.

The objective of the TOE is to protect the IT security of the IC and embedded software that is intended to be used as an electronic purse (people can pay with the TOE embedded in mobile equipment), ticket or commuter ticket and so on.

The intended usage of the operational TOE is by consumers (end-user), who own/use mobile equipment in which the TOE is embedded.

The TOE is delivered to a composite product manufacturer. The security IC embedded software is developed by the composite product manufacturer. This software is sent to Toshiba. Toshiba develops the IC dedicated test software. Toshiba merges the security IC embedded software and the IC dedicated test software and implements these in the T6NE1. After testing in Toshiba, the IC dedicated test software is made unavailable and becomes inaccessible by the composite product manufacturer or by the end-user after delivery.

TOE Documentation

The supporting guidance documents evaluated were:

[a] T6NE1 User guidance overview, version 0.38

[b] Kura2 development specification, version 0.9.2

[c] T6NE1 User Guidance manual, version 0.9.9

Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

TOE Configuration

The following configuration was used for testing:

Item	Identifier	Version
Hardware	T6NE1 chip	4.0
Software	HWC	0.5
	Test ROM	0.3