Certification Report

T6ND1 Integrated Circuit with Crypto Library v6.0

Sponsor and developer: ***Toshiba Corporation Semiconductor Company***
1-1-1, Shibaura,
Minato-ku, Tokyo
JAPAN

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-08-10492-CR**
Report version:	**1**
Project number:	**NSCIB-CC-08-10492**
Authors(s):	**NLNCSA**
Date:	**March 4, 2011**
Number of pages:	**20**
Number of appendices:	**0**

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Eindhoven:
De Rondom 1
P.O. Box 6235
5600 HE Eindhoven
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)40 265 0 302

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 2
Certificate number	**C11-10492**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder	**Toshiba Corporation Semiconductor Company, Japan**
Product and type	*T6ND1 Integrated Circuit with Crypto Library v6.0* Assurance Package: ▪ EAL4 augmented with AVA_VAN.5 and ALC_DVS.2
Dossier number	**NSCIB-CC-08-10492-CR**
Testing laboratory	**Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 2

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 2 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 2. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of issue	: **11-3-2011**
	Certificate expiry	: **11-3-2021**

Registration number
Notified Body 0336

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

Version: 20101101

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products in the technical domain of Smart cards and similar Devices. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the T6ND1 Integrated Circuit with Crypto Library v6.0 (T6ND1). The developer of this product is Toshiba Corporation Semiconductor Company located in Yokohama, Japan and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The T6ND1 Integrated Circuit with Crypto Library v6.0 (Target of Evaluation – TOE) is an Integrated Circuit (diced wafer) with a crypto library providing DES, RSA, Diffie-Hellman and ECDSA crypto operations. The TOE is a single chip microcontroller (hardware, security IC dedicated software and security IC dedicated test software) that is used in smartcards. While a smartcard may utilise the contact type or contact less type communication methods, this TOE utilises only the contact type communication method. Any other security IC embedded software is not part of the TOE.

The commercial TOE name is preceded with the letters [JEB] e.g. JT6DN1 and depends on the TOE form factor. J stands for chip, E stand for wafer and B stands for bump pad. The only difference between the form factors is the way the chip dies are prepared for further processing. The TOE can be delivered as complete wafer or as single chips, with aluminum pads for bonding or bump pad for flip4 chip assembly. Because the functional and electrical characteristics of the pads and bumps are the same the different form factors are security irrelevant.

For example:

JT6ND1 is aluminum pad and chip tray shipment.

JBT6ND1 is bump pad and chip tray shipment.

JET6ND1 is sawn wafer (but each chip is attached on a tape), aluminum pad product and wafer case shipment.

JEBT6ND1 is sawn wafer (but each chip is attached on a tape), bump pad and wafer case shipment.

The ST and the TOE claim conformance to the Security IC Platform Protection Profile that was registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.

The T6ND1 Integrated Circuit with Crypto Library v6.0 was originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 4 March 2011, The certification procedure was conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on 4 March 2011 with the preparation of version one of this Certification Report.

The scope of the evaluation is defined by the security target *[ST]*, that identifies assumptions made during the evaluation, the intended environment for the T6ND1 Integrated Circuit with Crypto Library v6.0, the security requirements and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the T6ND1 Integrated Circuit with Crypto Library v6.0 are advised to verify that their own environment is consistent with the security target and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* for this product provide sufficient evidence that it meets the Evaluation Assurance Level 4 augmented (EAL 4+) assurance requirements for the evaluated security functionality. The assurance level is augmented with: AVA_VAN.5 (Advanced methodical vulnerability analysis) and ALC_DVS.2 (Sufficiency of security measures). The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 1 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 2 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Toshiba T6ND1 Integrated Circuit with Crypto Library v6.0 evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4+ evaluation is the T6ND1 Integrated Circuit with Crypto Library v6.0, from Toshiba Corporation Semiconductor Company located in Yokohama, Japan.

This report pertains to the TOE, which comprises the following main components:

Delivery item type	Identifier	Version	Medium	additional information
Hardware	T6ND1	#5.0	Chip (bump or aluminum pad) / Wafer (bump or aluminum pad)	Aluminum pad samples contains 33pF and Bump pad samples contains 0pF tuning Capacitors.
Software	Hardware configuration (CODE)	0.94	Electrical data	T6ND1_HWconfig.lib SHA-256 = d728e6bb93d57daa606c8ae9f391b824118dab2841d046bb2a36363c89c1fee5
	Boot ROM	0.93	Electrical data	
	Hardware configuration (Data)	0.94	EEPROM in delivered T6ND1 hardware	
	Co-Processor control library	1.04	Electrical data	CryptoLibrary.lib. SHA-256 value = a229e515d7578ca268bc791d356c6d20ed7ac8a2ce146f79645422e2bda1474b Crypto_global.h SHA-256 value = 3ae2868ecc3fc8c5fc26e701e3dcaf6d38f83d4bb963348c6a82f03c51d5e0e0 RSA, DH, SHA, DES libraries are included.
	ECC library	1.01	Electrical data	EccLibrary.lib SHA-256 value= a492bf2d41710bb99d7a2e4275001d986ba4fe674655a9f22a96545ed0e7442e
	TEST ROM software	1.3	ROM of hardware (test area)	

To ensure secure usage, a set of guidance documents is provided together with the T6ND1. Details can be found in section 2.6 of this report.

2.2 Security Policy

The TOE - T6ND1 series Integrated Circuit with Crypto Library is a LSI chip designed for devices such as smartcard equipped with wireless communication interface. The TOE is capable to install user application programs and provides security functionality to protect stored data or executable code in the TOE.

The main components of the TOE are a 16bit CPU (TLCS-900/L1), 60kB of user ROM, 6kB of RAM, 80kB of non-volatile memory and a co-processor for 2048-bit modular exponential operations. The TOE also has an RF external interface compliant to ISO/IEC 14443 Type B. An external antenna is attached to the TOE for wireless communication.

The TOE is a platform for “the security IC Embedded software”. The primary purpose of the TOE is to provide safeguard for information stored in the TOE (e.g., personal data, secret number or user program). To protect the information, the TOE involves cryptographic functionality - triple DES, RSA, ECDSA signature verification, EC-Diffie-Hellman key exchange, Diffie-Hellman, SHA-256/SHA-1. The TOE also prepares the other security components to protect data in the TOE and the TOE itself from physical attacks.

The SHA-1 can be used as a building block, e.g. for session key generation in an e-passport application. However the cryptographic strength of SHA-1 is not considered to be sufficient on level AVA_VAN.5.

Further, it is noted that the TOE does not support the generation of hashes from SHA-256/SHA-1 that are confidential in nature.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

The customer must follow the guidance. For the embedded software programmer, the following requirements are important:

- Call the Boot program as first item after reset to ensure proper self-testing and trimming of the chip.
- Call HWConfig early in the start up sequence of the embedded software, to ensure the T6ND1 is in its evaluated configuration.
- Any further modifications of the registers described in section 5.1 of the T6ND1 User guidance overview must comply with the secure values described therein.
- Use the crypto library for cryptographic operations within the limits set by the guidance documents.
- Add sufficient anti-perturbation countermeasures.
- Verify the hash values of the library as provided, to ensure that the correct version is used.
- Use the SHA-256 functionality for non-confidential data only.

2.3.2 Environmental assumptions

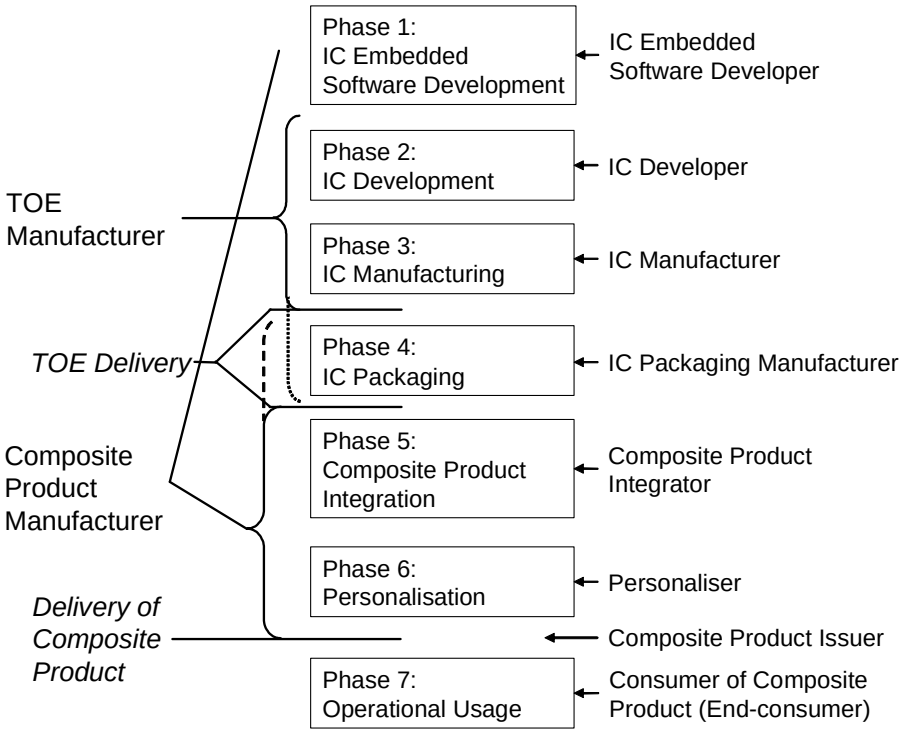
- The following assumptions about the environmental aspects defined by the Security Target have to be met (for the detailed and precise definitions refer to the *[ST]*, chapter 4.2 and 4.3):
- OE.Plat-Appl Usage of Hardware Platform
- OE.Resp-Appl Treatment of User Data
- OE.Process-Sec-IC Protection during composite product manufacturing

2.3.3 Clarification of scope

There are no defined threats that require additional measures in the environment, they are all met by the TOE. There are three objectives for the environment that must be realised in order to meet the requirements of the *[PP]*.

2.4 Life Cycle

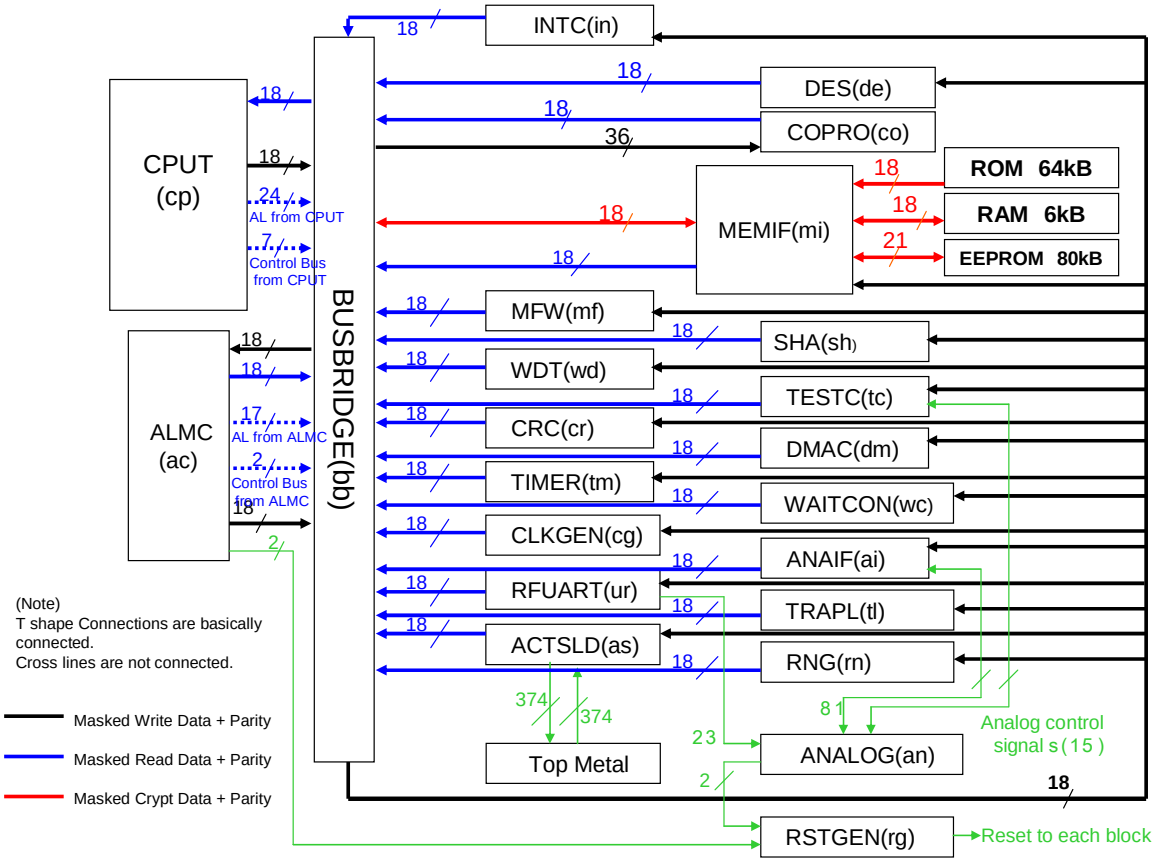
The Life-cycle model followed is that of the *[PP]*:



The TOE is delivered after Phase 3.

2.5 Architectural Information

The physical components of the TOE are depicted in the figure below.



Supplementary information for the above figure:

- Connection from COPRO to BUSBRIDGE line number has 18 lines.
- And the lines to BUSBRIDGE to COPRO are 36 lines.
- DMAC controls memories by BUSBRIDGE.
- The green 2bit signal between ALMC and RSTGEN are reset signals of ALMC when alarm happens. One of these reset signals is a reset signal for RFUART and COPRO. The other is a reset signal for CPUT.
- The green signal between ANALOG and RFUART are 23 lines as input signals to ANALOG.
- The green signal between ANALOG and RSTGEN are 2 signals.
- The green “Analog control signal” are control signals of 15 lines.
- The red 18bit “Crypt data” bus between MEMIF and BUSBRIDGE is the crypt data. That is common for both
- EEPROM ,RAM and ROM.

The first group of security features are functions to protect the TOE itself, as well as data in the TOE, from physical attacks. Those security functions listed below are implemented by hardware circuitry. The figure above represents the construction of hardware blocks of the TOE (includes non-security parts and not consistent to the contents of the security function list below by name). The basic configuration elements of the TOE are the CPUT, peripheral circuits (MFW, RFUART, INTC, MEMIF, DMAC, TIMER, CLKGEN, ACTSLD, TRAPL, ANAIF, WDT, ALMC, BUSBRIDGE), various memory

elements (EEPROM, ROM, RAM), security function circuits (CRC, RNG, DES, COPRO, SHA), various types of detection circuits (ANALOG) and others (TESTC).

Detection for:

- trap latch (light sensor)
- power supply glitch
- clock frequency, out of the range
- internal/rectified supply and current, out of the range
- temperature, out of the range
- signal line error
- illegal access to the memories
- illegal configuration on test mode
- undefined instruction to CPU or co-processor
- access to vacant addresses
- active shield error

Countermeasures for physical probing to the TSF:

- bus scrambling
- memory address scrambling
- memory ciphering
- active shield

The following components are used:

- CPUT: TLCS900-L1 Toshiba original 16bit CPU
- MFW: Memory firewall
- RAM, ROM, EEPROM: 6kbyte RAM, 64kbyte (User 60kbyte) ROM, 80kbyte non-volatile memory
- DES: triple des (single des circuit and cyclically used)
- COPRO: coprocessor for RSA, Diffie-Hellman, ECDSA signature verification and ECDH key exchange
- CRC: cyclic redundancy check
- RNG: Random number generator. True random number generator, LFSR random number generator, Triple des type random number generator
- ANALOG: Analog circuit for RFUART,.shunt regulator
- TESTC: test circuit
- RFUART: RF external interface with compliant to ISO/IEC 14443 type B
- DMAC: DMA controller
- MEMIF: Memory interface
- ANAIF: analog interface
- INTC: interrupt controller
- TIMER: timer
- WDT: watch dog timer
- SHA: secure hash
- TRAPL: trap latch

- ACTSLD: active shield
- CLKGEN: clock generator
- ALMC : alarm controller
- BUSBRIDGE: bus controller
- RSTGEN: reset generator
- WAITCON: random wait controller

2.6 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version	Medium
T6ND1 User guidance overview	0.21	Electronic document
T6ND1 User specification	0.962	Electronic document
T6ND1 Software Security Guidance	0.953	Electronic document
Next-generation IC Sheet Crypt Library Interface Specification	1.0.4	Electronic document

2.7 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.7.1 Testing approach

The developer used the following testing methods:

- Simulation tests on individual modules/subsystems (M1)
- Simulation tests on the entire design (M2)
- On-chip testing as part of the production (M3)
- Software library testing on engineering samples (M4)
- Testing on engineering samples (M5)

The test approach are described below per test method, as these properties are differently documented for each of the test methods. The testing methods were applied as follows on the TOE components:

<table>
<tr><td colspan="3">Crypto Library, ECC library</td><td>M4</td></tr>
<tr><td>HWConfig (Code)</td><td>Boot program (Code)</td><td>TestROM</td><td>M2</td></tr>
<tr><td colspan="3">Hardware</td><td>M1, M3, M5</td></tr>
</table>

M1 and M2: Simulation testing

The M1 and M2 test methods were performed with simulation on the hardware component of the TOE in order to test during development, and also on the final TOE design for the functionality that is not accessible for testing in the TOE itself.

M1 and M2: Testing approach

The M1 and M2 tests methods both apply logic and analogue simulation of the TOE. This is used during development for many parts of the hardware component of the TOE. M1 tests were performed on modules and subsystems individually; M2 tests were performed on the entire design.

M3: In-production hardware testing

The M3 test method is the main method of testing for the hardware component of the TOE.

M3: Testing approach

M3 testing is performed as part of the production process for all products using automated IC testers (also known as wafer testers). These automated testers execute test patterns, which stimulate the respective interfaces, subsystems and modules, and automatically determine whether the expected test results are met. Only when a product meets all the expected test results, is it delivered as a TOE. This provides the user of a TOE assurance that that specific TOE is tested individually, i.e. all delivered TOEs have passed all tests.

M4: Software library testing

The M4 test method tests the cryptographic library (DES, DH, RSA and SHA) and the ECC library on engineering samples of the TOE. The developer uses an in-house developed test tool to verify the proper execution of the cryptographic algorithms. This test tool uses Bouncy Castle, an open source API for cryptographic functions, for the generation of test vectors for the tests. This Bouncy Castle API is used in many applications and proved to be a reliable reference implementation in the past.

M4: Testing approach

The M4 test method tests the cryptographic library (DES, DH, RSA and SHA) and the ECC library using a test application on the TOE. The software is executed using test commands using a card reader via the contactless interface. The result is read sent back to the card reader and compared with the expected results.

M5: Testing on engineering samples

The M5 testing method provides additional tests of a selection of hardware sensors on engineering samples.

M5: Testing approach

The M5 tests method applies physical stimulation to samples of the TOE. This is used to verify the correct operation of a selection of hardware sensors.

The developer uses testing on the TOE in production (M3) testing on the actual TOE hardware component engineering-sample tests (M4) on the actual TOE software component and engineering-sample tests (M5) on a selection of TOE sensors to show proper behaviour. Simulation tests on the final TOE design are used to show proper behaviour of the Hardware Configuration (Code) and TESTROM components.

Developer function testing repeated by the evaluator

Considering the extensive and fully automated testing performed by the developer during production (the M3 testing during production, as described in the summary of the developer testing), and the fact that this testing is successfully performed on each delivered TOE, the evaluators judged that validation testing provided very limited additional assurance. Nevertheless the following developer tests were repeated as they have innovative features: Undefined instruction detector checking.

Evaluator independent functional testing

The evaluator's testing was spread over nearly all interfaces involved for implementation of the SFRs to provide good rigour of testing. Summarized, this testing covers the interfaces involved in the implementation of the SFRs, with the exception of:

- HWConfig (code) (covered by code review in ADV_IMP),
- The interfaces involved in duplicated signal handling, signal error monitoring, undefined instruction monitoring and the memory firewall (all tested by the developer in a way that evaluator testing will not add assurance),
- The test lock mechanism and the leakage countermeasures (functional testing by the developer is sufficient and penetration testing by the evaluator will cover the robustness against attacks).
- The total test set contains 4 tests to verify the TOE component versions and 4 extensive tests to verify functionality.

2.7.2 Test Configuration

For testing the TOE the following equipment was used:

- TOE on testboard.
- Brightsight laser setup.
- Brightsight DPA setup.
- Brightsight EMA setup.
- Optical Microscope

2.7.3 Independent Penetration Testing

Based on the examination of the developer's vulnerability analysis and test activities and also on the evaluators own vulnerability analysis, a number of possible vulnerabilities were identified. Penetration tests were performed by the evaluation lab to assess those identified possible vulnerabilities.

The vulnerability analysis has followed the following steps:

- The combined set of well-known attacks from *[ISCI]* is considered, leading to the list of 11 major attack methods to consider.
- A theoretical analysis of the TOE type (smartcard hardware compliant to *[PP]*) considers all 11 major attack methods against the SFRs clustered in 7 groups, being the 5 from *[PP]* (Malfunctions, Abuse of functionality, Physical Manipulation, Leakage and Random numbers) and 2 extensions common (Cryptography(DES) and Cryptography(RSA). In total 11*7=77 SFR/attack-combinations are possible. The theoretical analysis led to the exclusion of 63 SFR/attack-combinations as not being applicable for this type of TOE.
- Potential vulnerabilities from the other evaluation activities were 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.
- 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 64 of the SFR/attack-combinations sufficient assurance could be found in the design information and other evaluation activities. For 5 SFR/attack-combinations further penetration testing was deemed necessary: for light injection on the FCS_COP.1(DES), FCS_COP.1(RSA) and FCS_COP.1(ECDSA), and SPA on RSA and DEMA on DES for the FDP_ITT.1/FPT_ITT.1/FDP_IFC.1 SFRs.

The resulting penetration tests were performed and the individual results analysed.

2.7.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with a references to the documents containing the full details.

The testing results from the developer shows that the TOE exhibits the expected behaviour at TSFI, subsystem and SFR-enforcing module level.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in the Security Target at SFR-enforcing module level.

No exploitable vulnerabilities were found with the independent penetration tests.

2.8 Evaluated Configuration

For setting up / configuring the TOE all guidance documents was followed (refer to section 2.6 of this report).

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[1] which references several Intermediate Reports. The verdict of each claimed assurance requirement is given in the following tables:

Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.4	Pass
Implementation representation	ADV_IMP.1	Pass
TOE design	ADV_TDS.3	Pass

Guidance documents		**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

Life-cycle support		**Pass**
Configuration Management capabilities	ALC_CMC.4	Pass
Configuration Management scope	ALC_CMS.4	Pass
Delivery	ALC_DEL.1	Pass
Development security	ALC_DVS.2	Pass
Life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass

Security Target	**Pass**

Tests		**Pass**
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.2	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		**Pass**
Vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the Toshiba T6ND1 Integrated Circuit with Crypto Library v6.0 to be CC Part 2 extended, CC Part 3 conformant, and to meet the requirements of EAL 4 augmented by AVA_VAN.5 and ALC_DVS.2 as required by the Security IC Platform Protection Profile, BSI-PP-0035, Version 1.0, 15.06.2007.

This implies that the product satisfies the security technical requirements specified in the T6ND1 Integrated Circuit with Crypto Library v6.0 Security Target, Version 2.16, date 28th December 2010.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2.10 Evaluator Comments/Recommendations

2.10.1 Obligations and hints for the developer

None.

2.10.2 Recommendations and hints for the customer

For the embedded software programmer, the following requirements are important:

- Call the Boot program as first item after reset to ensure proper self-testing and trimming of the chip.
- Call HWConfig early in the start up sequence of the embedded software, to ensure the T6ND1 is in its evaluated configuration.
- Any further modifications of the registers described in section 5.1 of the T6ND1 User guidance overview must comply with the secure values described therein.
- Use the crypto library for cryptographic operations within the limits set by the guidance documents.
- Add sufficient anti-perturbation countermeasures.
- Verify the hash values of the library as provided, to ensure that the correct version is used.
- Use the SHA-256 functionality for non-confidential data only.

The following assumptions about the environmental aspects defined by the Security Target have to be met (for the detailed and precise definitions refer to the *[ST]*, chapter 4.2 and 4.3):

- OE.Plat-Appl Usage of Hardware Platform
- OE.Resp-Appl Treatment of User Data
- OE.Process-Sec-IC Protection during composite product manufacturing.

3 Security Target

The Security Target, “T6ND1 Integrated Circuit with Crypto Library v6.0 Security Target”, Version 2.16, date 28th December 2010 is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CC	Common Criteria
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
EEP	Electronically Erasable Programmable Read Only Memory
ITSEF	IT Security Evaluation Facility
MEMC	Memory Cipher Circuit
MFW	Memory Firewall
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
NV	Non-volatile
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SPA/DPA	Simple/Differential Power Analysis
UART	Universal Asynchronous Receiver/Transmitter
TNO	Netherlands Organization for Applied Scientific Research
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 2, September 2007.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 2, September 2007

[ETR] Evaluation Technical Report T6ND1 Integrated Circuit with Crypto Library version 6.0 (T6ND1) EAL4+, Febraury 21st 2011.

[ISCI] JIL Attack methods for smart cards and similar devices, version 1.3, April 2007

[JIL] JIL Application of Attack Potential to Smart Cards, version 2.4, April 2007

[NSCIB] Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.

[PP] Security IC Platform Protection Profile, version 1.0, 15 June 2007 (BSI-PP-0035).

[ST] T6ND1 Integrated Circuit with Crypto Library v6.0 Security Target, Version 2.16, 28th December 2010.

[TOE] T6ND1 Integrated Circuit with Crypto Library v6.0.

(This is the end of this report).