TNO CERTIFICATION

Laan van Westenenk 501
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

Phone +31 55 5493468
Fax +31 55 5493288
E-mail: Certification@certi.tno.nl

BTW/VAT NR NL8003.32.167.B01
Bank ING at Delft
Bank account 66.77.18.141
stating 'TNO Certification'
BIC of the ING Bank: INGBNL2A
IBAN: NL81INGB0667718141

Date
June 13, 2009

Reference
NSCIB-CC-07-09482-CR2

Subject

Project number
9482

NSCIB-CC-07-09482

Certification Report

T6NC9 Integrated Circuit with Crypto Library v1.1

TNO CERTIFICATION

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

T6NC9 Integrated Circuit with Crypto Library v1.1, Assurance Package: EAL4 augmented with AVA_VAN.5 and ALC_DVS.2
Product and version

FROM

Toshiba Corporation Semiconductor Company, Japan
Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 1

Certification guidelines or standards

AS DEMONSTRATED BY / EVALUATION PERFORMED BY

Brightsight BV, located in Delft, the Netherlands
Testing Laboratory

APPLYING THE

Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 1

IT Security Certified

NSCIB-CC-07-09482-CR
NSCIB-CC-07-09482-CR2
Certification Report numbers

THE CERTIFICATE HAS BEEN ISSUED ON

September 9th, 2008
1st Issue Date

June 25th, 2009
Revision Date

September 9th, 2018
Expiry Date

ISSUED IN: Apeldoorn, the Netherlands

DIRECTOR TNO CERTIFICATION

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 1 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 1. 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 TNO Certification or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

CERTIFICATE NUMBER C07-09482

ACCREDITED BY THE COUNCIL FOR ACCREDITATION

Table of contents

Document Information

Date of issue	13 June 2009
Version of report	2
Certification ID	NSCIB-CC-07-09482
Sponsor and Developer	Toshiba Corporation Semiconductor Company
Evaluation Lab	Brightsight BV
TOE name	T6NC9 Integrated Circuit with Crypto Library v1.1
TOE reference name	T6NC9
Report title	Certification Report
Report reference name	NSCIB-CC-07-09482-CR2

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 the NSCIB, TNO Certification 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 TNO Certification in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF is a commercial facility that has been licensed by TNO Certification 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, TNO Certification 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 Recognition Agreement approved by the SOG-IS in April 1999 provides mutual recognition of ITSEC and Common Criteria certificates for all evaluation levels (E6, resp. EAL7). This agreement was originally signed by Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the T6NC9 Integrated Circuit with Crypto Library v1.1 (T6NC9). 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.

This security evaluation re-used the evaluation results of the recently performed evaluation of the T6NC9 Integrated Circuit with Crypto Library v1.0. Version 1.0 of the T6NC9 Integrated Circuit with Crypto Library was certified on September 10th 2008 under the certification identifier NSCIB-07-09482 with an certification report identified as 'version 1'. The difference between version 1.1 and version 1.0 of the TOE is that this certificate now covers the delivery of the T6NC9 in diced wafer form in addition to the T6NC9 delivered as a packed die. The original certificate that covered T6NC9 Integrated Circuit with Crypto Library v1.0 identified as in the certification report NSCIB-CC-07-09482 version 1 has now been extended to cover the T6NC9 Integrated Circuit with Crypto Library version 1.1 as described in this document, certification report NSCIB-CC-07-09482 version 2.

The T6NC9 Integrated Circuit with Crypto Library v1.1 (Target of Evaluation – TOE) is an Integrated Circuit (diced wafer) with a DES and RSA crypto library. 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 ST and the TOE claim conformance to the Security IC Platform Protection Profile which was registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.

The T6NC9 Integrated Circuit with Crypto Library v1.0 was originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 5 September 2008, 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 5 September 2008 with the preparation of version one of this Certification Report.

The T6NC9 Integrated Circuit with Crypto Library v1.1 in diced wafer format has be re-evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on May 20th 2009 with the delivery of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on June 13th 2009 with the issuing of version two 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 T6NC9 Integrated Circuit with Crypto Library v1.1, 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 T6NC9 Integrated Circuit with Crypto Library v1.1 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]*[1] for this product provide sufficient

[1] The evaluation technical report is a NSCIB document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

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 1 *[CC]*.

TNO Certification, as the NSCIB Certification Body, declares that the Toshiba T6NC9 Integrated Circuit with Crypto Library v1.1 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 T6NC9 Integrated Circuit with Crypto Library v1.1, 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	T6NC9	#4.0	Chip	Delivery formats: packaged die or diced wafer
Software	Hardware configuration (CODE)	1.02	Electrical data	HWCONFIG.REL 's HASH VALUE (SHA-256) = 0563a5685308a6b706176268704215f8f62b96e83e037a819f3c9aa3851bef8d
	Hardware configuration (Data)	1.0	EEPROM in delivered T6NC9 hardware	
	Co-Processor control library	1.0.1	Electrical data	CRYPTO.REL(Co-Processor control
	DES control library	1.0.1	Electrical data	Library and DES control library)'s HASH VALUE (SHA-256) = 2b87c7391f45ba5c61276463b28ba5864cdb0aaa1a663a2921678f72a53cdd2e
	TEST ROM software	1.2	ROM of hardware (test area)	

To ensure secure usage, a set of guidance documents is provided together with the T6NC9. Details can be found in section 2.6 of this report.

2.2 Security Policy

The TOE is a highly functional and security single chip microcontroller with a contact type communication interface. The objective of the TOE is to protect the IT security of the smartcard usage that are intended to be used for banking, finance or electronic commerce, etc. The intended usage of the operational TOE is by consumers (end-user). The TOE is delivered to a composite product manufacturer to load security IC embedded software in the ROM. The TOE does not allow access to security IC dedicated test software when the TOE is delivered to the composite product manufacturer or used by the end-user.

Protected information is in general secret data as Personal Identification Numbers, Balance Value (Stored Value Cards), and Personal Data Files. Other protected information is the data representing the access rights; these include any cryptographic algorithms and keys needed for accessing and using the services provided by the system through use of the smartcard.

The IC, that is used in a smartcard, consists of the central processing unit (CPU), memory element (ROM, RAM, NV memory) and circuitry for the external contact interface that have been integrated with consideration given to tamper resistance. The security IC dedicated software, which is incorporated in the memory element, is capable of providing security functions for the various security IC embedded software.

The increase in the number and complexity of applications in the smartcard market is reflected in the increase of the level of data security required. The security needs for a smartcard can be summarised as being able to counter those who want to defraud, gain unauthorised access to data and control a system using a smartcard. Therefore it is mandatory to:

- maintain the integrity and the confidentiality of the content of the smartcard memory as required by the security IC embedded software the smartcard is built for and
- maintain the correct execution of the security IC embedded software residing on the card.

This requires that the smartcard integrated circuit especially maintains the integrity and the confidentiality of its security enforcing and security relevant architectural components.

The TOE consists also of security IC dedicated software: a DES library and a RSA library.

The DES library provides functions to perform primitive operations such as Triple DES ECB and CBC using the hardware. Secondly this library adds defensive mechanisms to help protect the TOE against fault injection attacks as well as attacks aimed at circumventing critical steps in the cryptographic processing.

The RSA provides functions to perform primitive operations such as CRT and non CRT RSA calculations using the hardware coprocessor. Secondly this library adds defensive mechanisms to help protect the TOE against fault injection attacks as well as attacks aimed at circumventing critical steps in the cryptographic processing.

Other security features of the TOE are:

- Bus and memory encryption
- Clock filter
- Detection Warm/Cold reset, Power supply voltage, Temperature, Input clock frequency, Power supply glitch, Metal cover removal, Light.
- Duplicated signals
- EEPROM error correction
- Memory firewall
- Metal cover
- Random number generator
- Random wait insertion circuit
- Undefined instruction monitoring
- Vacant address access guard

The intended environment is very large; and generally once issued the smartcard can be stored and used anywhere in the world, at any time, and no control can be applied to the smartcard and the card operational environment.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

Based on the assumptions which are relevant for the TOE the following usage assumptions arise (for the detailed and precise definition of the assumptions refer to the *[PP]*, chapter 3.4):

- Usage of Hardware Platform - The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.
- Treatment of User Data - All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

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 definition of the assumptions refer to the *[PP]*, chapter 3.4):

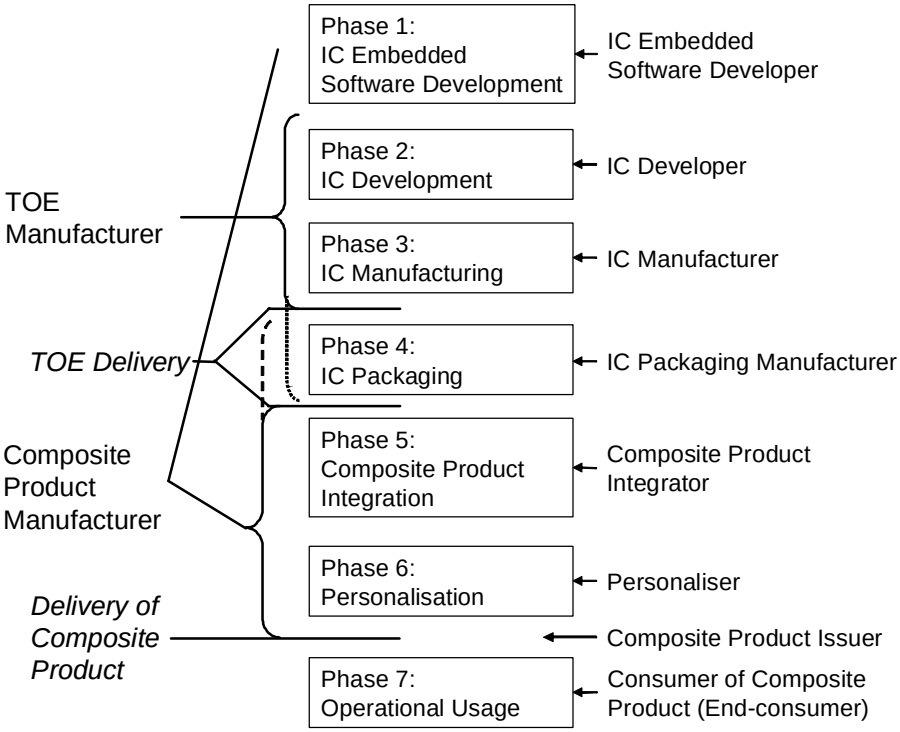
- Protection during Packaging, Finishing and Personalisation - It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

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]*:

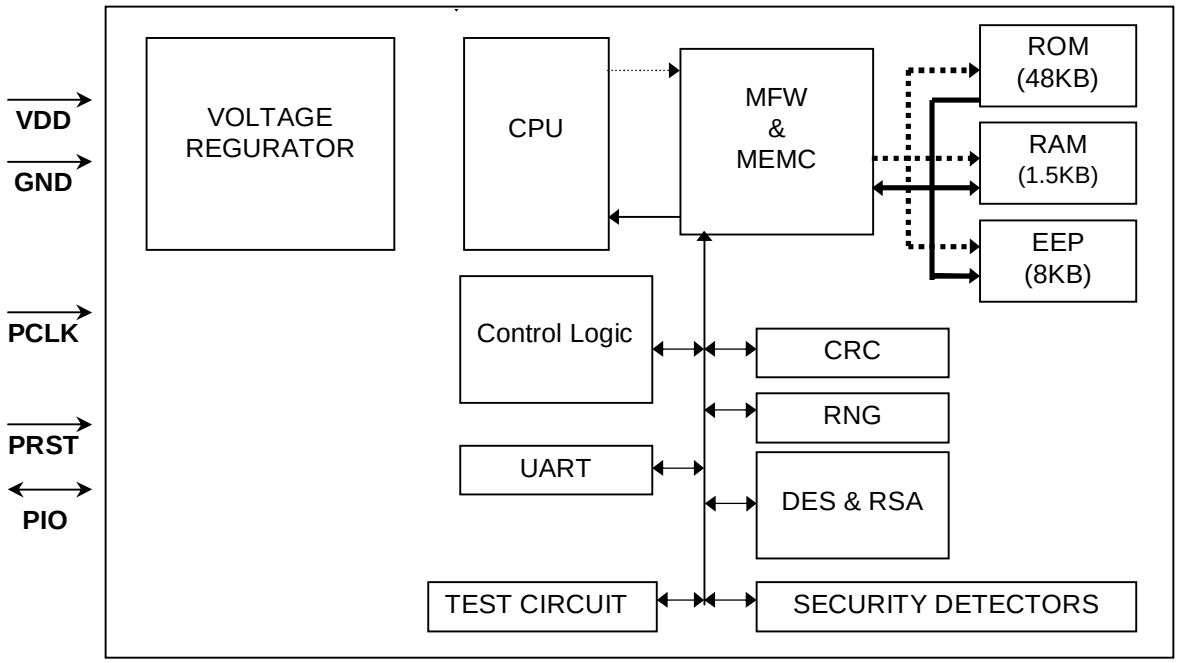


The TOE is delivered after Phase 3.

Note that as common in IC production processes, the actual TOE hardware has a test mode that is enabled during Phase 3 for testing purposes. This test mode allows the test machines in the production process to access special test functionality in the TOE hardware. At the end of the testing, the test mode is permanently disabled and the T6NC9 will automatically only operate in user mode from that time forward. Any attempt to access the test functionality will fail and result in the temporary muting of the T6NC9. Hence, the T6NC9 as TOE (i.e. after Phase 3) is only available in user mode and its test functionality is not available.

2.5 Architectural Information

The physical components of the TOE are depicted below. The basic configuration elements of the TOE are the CPU, the CPU peripheral circuits (MFW, MEMC, UART, Control Logic), the various memory elements (EEP, ROM, RAM), security function circuit (CRC, RNG, DES, RSA), various types of detection circuits (SECURITY DETECTORS), and others (TEST CIRCUIT, etc.).



The logical security features offered by the TOE are the following:

1. Triple-DES:
   a. ECB mode, Triple DES 2KEY,Encryption/Decryption
   b. ECB mode, Triple DES 3KEY,Encryption/Decryption
   c. CBC mode, initial value: 0,Triple DES 2KEY,Encryption/Decryption
   d. CBC mode, initial value: 0,Triple DES 3KEY,Encryption/Decryption
   e. CBC mode, initial value: arbitrary, Triple DES 2KEY,Encryption/Decryption
   f. CBC mode, initial value: arbitrary, Triple DES 3KEY,Encryption/Decryption

2. RSA:
   pRSA_CRT. Exponential reminder calculations by CRT are performed to the input data with the secret key. Key length is up to 1408 bit. Anti-tamper measures are implemented because the secret key is used for these calculations. Calculation result is same bit length as key(N) length. The size of key e is less than 10 bytes and the errors occurs more than 10 bytes.

3. Physically seeded random number generator:
   A physical noise source provides seeding for a deterministic random number generator built from recursive calls to Triple DES, conformant to AIS20 Class K3. The seeding must be performed before use (i.e. at least after each power on, more often if desired). The quality of the noise source is monitored during this seeding process for total failure of the noise source. The whole construction (physical noise source, total failure tests, Triple DES in recursive mode) is completely implemented in hardware, and the actual entropy is provided by physical random processes.

The following components are used.

- CPU — Z80TM CPU
- MFW — Memory Fire Wall
- MEMC — Memory Cipher Circuit

- Ø RAM, ROM,EEP 1.5KB RAM, 48KB USER ROM, 8KB EEPROM
- Ø Control Logic
- Ø DES
- Ø RSA
- Ø CRC ISO 3309 (16 bit CRC)
- Ø RNG Random number generator
- Ø VOLTAGE REGURATOR
- Ø SECURITY DETECTOR
- Ø TEST CIRCUIT
- Ø UART

2.6 Documentation

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

Identifier	Version	Medium
User guidance overview	1.0	Electronic document
T6NC9 User Specification	0.92	Electronic document
T6NC9 Software Security Guidance	1.03	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 four testing methods:

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

The developer uses testing on the TOE in production (M3) testing of the actual TOE hardware component and simulated hardware tests (M4) on the actual TOE software component 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.

The evaluator has chosen to test the majority of the interfaces involved in the implementation of SFRs: even though the developer's testing was extensive some additional assurance could be gained by additional testing. Some tests were added at the request from the NSCIB.

2.7.2 Test Configuration

The following TOE configurations were tested:

- Ø TOE in test mode (for the RNG quality test, the developer's unused address detector test and

also for verification of the TOE hardware component version)

- User mode sample with evaluation code (for all other tests)

For testing the TOE the following equipment was used:

- TOE on testboard
- Brightsight voltage manipulation setup
- 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:

1. The combined set of well-known attacks from *[ISCI]* is considered, leading to the list of 11 major attack methods to consider.
2. 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 leads to the exclusion of 33 SFR/attack-combinations as not applicable for this type of TOE.
3. 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 40 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: for voltage manipulation and light injection on the FRU_FLT.2/FPT_FLS.1 SFRs, and SPA/DPA on DES, EMA on DES, SPA on RSA for the FDP_ITT.1/FPT_ITT.1/FDP_IFC.1 SFRs.
4. Potential vulnerabilities from the other evaluation activities have been gathered and analysed whether they are still appropriate. The potential vulnerabilities in the other Intermediate Reports indicated that positive voltage glitches should be considered in the voltage manipulation penetration testing. No significant additions were made to the penetration testing selected (positive glitches were highlighted but already considered).
5. 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]*[2] which references several Intermediate Reports. The verdict of each claimed assurance requirement is given in the following table:

Security Target		**Pass**

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

Guidance documents		**Pass**
Operational	AGD_OPE.1	Pass
Preparative	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
Lifecycle definition	ALC_DEL.1	Pass
Tools and Techniques	ALC_TAT.1	Pass

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

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

Vulnerability assessment		Pass
Vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the Toshiba Integrated Circuit with Crypto Library v1.1 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 T6NC9 Integrated Circuit with Crypto Library v1.1 Security Target, Version 2.1, date 2 April 2009.

2.10 Results of the IAR assessment

This security evaluation re-used the evaluation results of the recently performed evaluation of the T6NC9 Integrated Circuit with Crypto Library v1.0. Version 1.0 of the T6NC9 Integrated Circuit with Crypto Library was certified on September 10th 2008 under the certification identifier NSCIB-07-09482 with an certification report identified as 'version 1'.

On April 27th 2009, Toshiba, the developer of the T6NC9 Integrated Circuit with Crypto Library v1.0 submitted an Impact Analysis Report *[IAR]* to the NSCIB Certification Body requesting to re-issue the certificate for their updated v1.1 T6NC9 product. The IAR is intended to satisfy the requirements outlined in the document Assurance Continuity: CCRA Requirements *[CCRA-AC]*. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

The difference between version 1.1 and version 1.0 of the TOE is that this certificate now covers the delivery of the T6NC9 in diced wafer form in addition to the T6NC9 delivered as a packed die. The guidance has been updated (and therefore the TOE physical scope). The TOE identifier has changed from T6NC9 Integrated Circuit with Crypto Library v1.0 to T6NC9 Integrated Circuit with Crypto Library v1.1. The guidance now covers the secure handling of the diced wafer form. The updated ETR includes the analysis of the T6NC9 Integrated Circuit with Crypto Library version 1.1 that represents the T6NC9 product delivered in diced wafer form and in packed die form. The assessment of the IAR by the evaluation lab in the ETR indicated that the original evaluation results were still valid and could be fully reused. The evaluation lab also confirmed in the ETR that the change had no impact on the security functionality and had no negative effect on the Vulnerability Analysis performed on version 1.0 of the T6NC9.

The original certificate that covered T6NC9 Integrated Circuit with Crypto Library v1.0 identified as in the certification report NSCIB-CC-07-09482 version 1 has now been extended to cover the T6NC9 Integrated Circuit with Crypto Library version 1.1 as described in this document, certification report NSCIB-CC-07-09482 version 2.

2.11 Evaluator Comments/Recommendations

The T6NC9's countermeasures are for the larger part automatically and always activated, as a result all the embedded software has to do to put the T6NC9 into the evaluated configuration by executing the HWConfig(code), that automatically applies all remaining security relevant settings. This makes the T6NC9 easy to use for embedded software developers, but also easier to test by the evaluators.

The customer must fulfil the objectives for the environment as defined in the Security Target:

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

When the customer in his activities as an Composite Product Manufacturer develops software for the T6NC9, especially the following requirements from the guidance documents are important:

- Call HWConfig.h early in the start up sequence of the embedded software, to ensure the T6NC9 is in its evaluated configuration (as described in T6NC9 Software Security Guidance, sections “Startup sequence” and “HW Configuration”),
- Use the crypto library for cryptographic operations within the limits set by the guidance documents (as described in T6NC9 Software Security Guidance, section “Cryptograph”),
- Add anti-perturbation countermeasures (as described in T6NC9 Software Security Guidance, sections “Tamper detection counter”, “Cryptograph”, “SFR and memory access”, “Memory Firewall”, and “CRC Check”),
- Verify the hash values of the library as provided, to ensure that the correct version is used (as described in T6NC9 User Specification, section “TOE Identification”).

For the Smartcard IC module manufacturers, the requirement that non-operational dices are incinerated (at high temperature) before disposal is important in the case of the diced wafer form factor.

3 Security Target

The Security Target, "T6NC9 Integrated Circuit with Crypto Library v1.1 Security Target", Version 2.1, date 2 April 2009 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 1, September 2006.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 1, CCMB-2006-06-004, September 2006
[ETR]	Evaluation Technical Report T6NC9 Integrated Circuit with Crypto Library version 5.0 (T6NC9) EAL4+, May 20th 2009.
[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 2.3, 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]	T6NC9 Integrated Circuit with Crypto Library v1.1 Security Target, Version 2.10, 2 April 2009.
[TOE]	T6NC9 Integrated Circuit with Crypto Library v1.1.