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
August 31, 2009

Reference
NSCIB-CC-08-10573-CR

Subject

Project number
10573

NSCIB-CC-08-10573

Certification Report

FS Sigma Version 01.01.05 (FSSIGMA)

TNO CERTIFICATION

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

FS Sigma Version 01.01.05,
Assurance Package: EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2
Product and version

FROM

Toshiba Corporation, Tokyo, Japan
Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 2

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 2

IT Security Certified

NSCIB-CC-08-10573-CR2
Certification Report number

THE CERTIFICATE HAS BEEN ISSUED ON

October 27, 2009
1st Issue Date

October 27, 2019
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 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 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 CD8-10573

ACCREDITED BY THE COUNCIL FOR ACCREDITATION

Table of contents

Document Information

Date of issue	31st August 2009
Author	R. Hunter
Version of report	1
Certification ID	NSCIB-CC-08-10573
Sponsor and Developer	Toshiba Corporation
Evaluation Lab	Brightsight BV
TOE name	FS Sigma Version 01.01.05
TOE reference name	FS SIGMA
Report title	Certification Report
Report reference name	NSCIB-CC-08-10573-CR

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 in the Netherlands 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 in the Netherlands 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 FS Sigma version 01.01.05 (FS SIGMA). The developer of this product is Toshiba Corporation located in Tokyo, 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 FS Sigma version 01.01.05 (Target of Evaluation – TOE) is a composite security IC, consisting of the Toshiba Corporation T6NC9 hardware, which is used as the evaluated underlying platform and the FS SIGMA, which is built on this hardware platform. The Toshiba Corporation T6NC9 has been certified by NSCIB Certification Body under certification ID NSCIB-CC-07-09482. The FS SIGMA is a secure operating system on top of the T6NC9. It provides a number of APIs in order to provide a secure application development environment for the application software development.

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

The FS Sigma version 01.01.05 was evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 6 July 2009, 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 7 July 2009 with the preparation 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 FS Sigma version 01.01.05, 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 FS Sigma version 01.01.05 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 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) and ASE_TSS.2 (TOE Summary specification with architectural design summary). The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 2 *[CC]*.

TNO Certification, as the NSCIB Certification Body, declares that the Toshiba FS Sigma version 01.01.05 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.

[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.

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 Toshiba FS Sigma version 01.01.05, from Toshiba Corporation located in Tokyo, Japan.

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

Delivery item type	Identifier	Version	Medium
Hardware	T6NC9	#4.0	COT
Software	FS SIGMA	01.01.05 Refer to the Platform Specification document (MC-SM0721-01) for Mask Version (TOE ID)	ROM of hardware (user area)

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

2.2 Security Policy

The TOE is a composite security IC, consisting of the hardware T6NC9, which is used as the evaluated underlying platform, and the FS SIGMA, which is built on this hardware platform. The T6NC9 is a secure single chip microcontroller with a contact type communication interface. It consists of the central processing unit (CPU), memory element (ROM, RAM, NV memory), and circuit for contact external interface that have been integrated with consideration given to tamper resistance. The software that is incorporated in the memory element is capable of providing security functions for the various applications.

The FS SIGMA is a secure operating system on top of the T6NC9. It provides a number of APIs in order to provide a secure application development environment for the application software development.

The TOE consists of the security functions: Memory access control, Sensitive data with CRC checksum, encrypted key data on NV memory and ISO7816-4 based file system access control.

The memory access control provides function to protect the memory against illegal access during response data transmitting and sensitive data transporting. It uses the HW memory firewall function as a mechanism to help protect the TOE against fault injection attacks (either directly on the TOE or on the optional applications).

The sensitive data with CRC check sum function provides the data integrity. It is possible to get the sensitive data with checking the data's integrity by using CRC checksum.

The encrypted key data on NVM is one of file management function, is useful for storing the data confidentiality. There are function "encryption to NVM" and "decryption from NVM", the application can store and load the key data on/from NVM using these function.

The access control protects the ISO7816-4 based file system by:

- providing the means for the reader to authenticate itself against PINs and/or authentication keys,
- maintaining the current security status of the reader based on its successful authentications

against PINs and/or authentication keys,

- granting or denying access to files based on their access control permissions and the current security status of the reader.

Other security features of the TOE, which are described in more detail in the guidance documentation, are:

- sensitive flags are encoded in and verified against complex data patterns (using more than 2bits)
- a special comparison function for comparison of sensitive data
- software random waitstates
- clearing of the temporary data after cryptogram process
- access control of the card life cycle data

The TOE also includes the security features of the underlying T6NC9 HW platform as described below. These are copied directly from *[HW-ST]*.

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 TOE is designed for use in a smartcard. 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

There are no usage assumptions for the TOE as it is certified.

2.3.2 Environmental assumptions

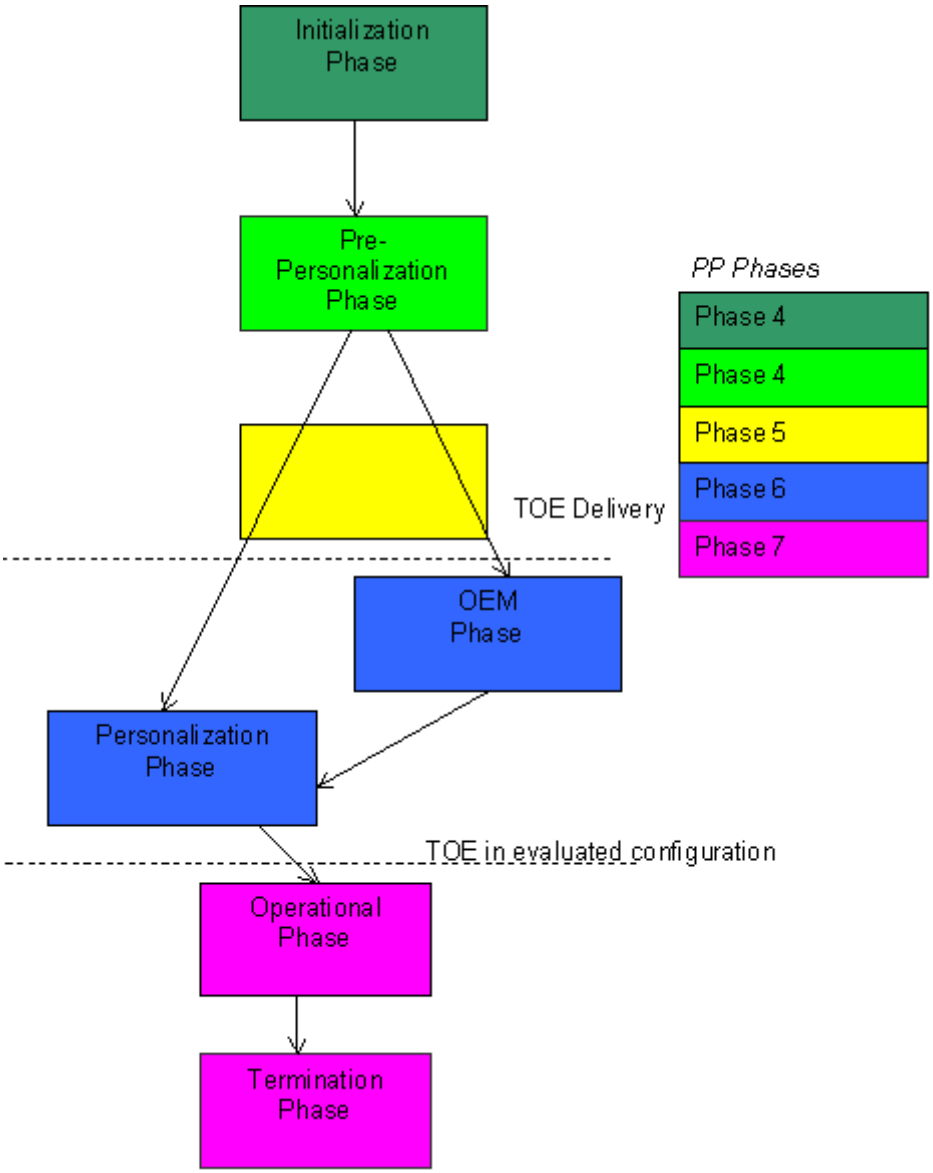
There are no environmental assumptions for the TOE as it is certified. The following environmental assumptions arise for additional optional applications (see figure 1, page 10). For the detailed and precise definition of the assumptions refer to the *[PP]*, chapter 3.4:

2.3.3 Clarification of scope

There are no defined threats for the TOE that require additional measures in the environment, they have all been met by the TOE. There were two objectives for the environment defined in *[HW-ST]* that have been met in the composite TOE in order to meet the requirements of the *[PP]*. These objectives are also valid for any additional optional applications (which are outside the scope of this evaluation) and they should also be met as described above.

2.4 Life cycle

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



The TOE is developed in phase 1. The TOE delivery occurs after phase 5 (or before phase 6), as a chip on tape transport key locked. The TOE is in its evaluated configuration after the card lifecycle state has been set to "Operation", i.e. after phase 6 (or before phase 7).

It is noted that Phases 2, 3 and 5 of the *[PP]* are physical steps and have no impact on the logical phases of the TOE.

The fabrication application is available in "Initialization phase" and "pre-personalization phase" (*[PP]* phase 4) only. The personalization application is available in "OEM Phase" and "Personalization phase" (*[PP]* phase 6) only.

2.5 Architectural Information

The TOE (FS SIGMA) consists of the FS SIGMA OS, HWConfig and crypto library code on the T6NC9 in the form of ROM code. The TOE is compiled from its source code.

At this time, any optional applications (which are not part of the TOE) are also compiled by Toshiba and linked with the TOE. The total ROM code (TOE + non-TOE optional applications) is stored in the User ROM of the T6NC9.

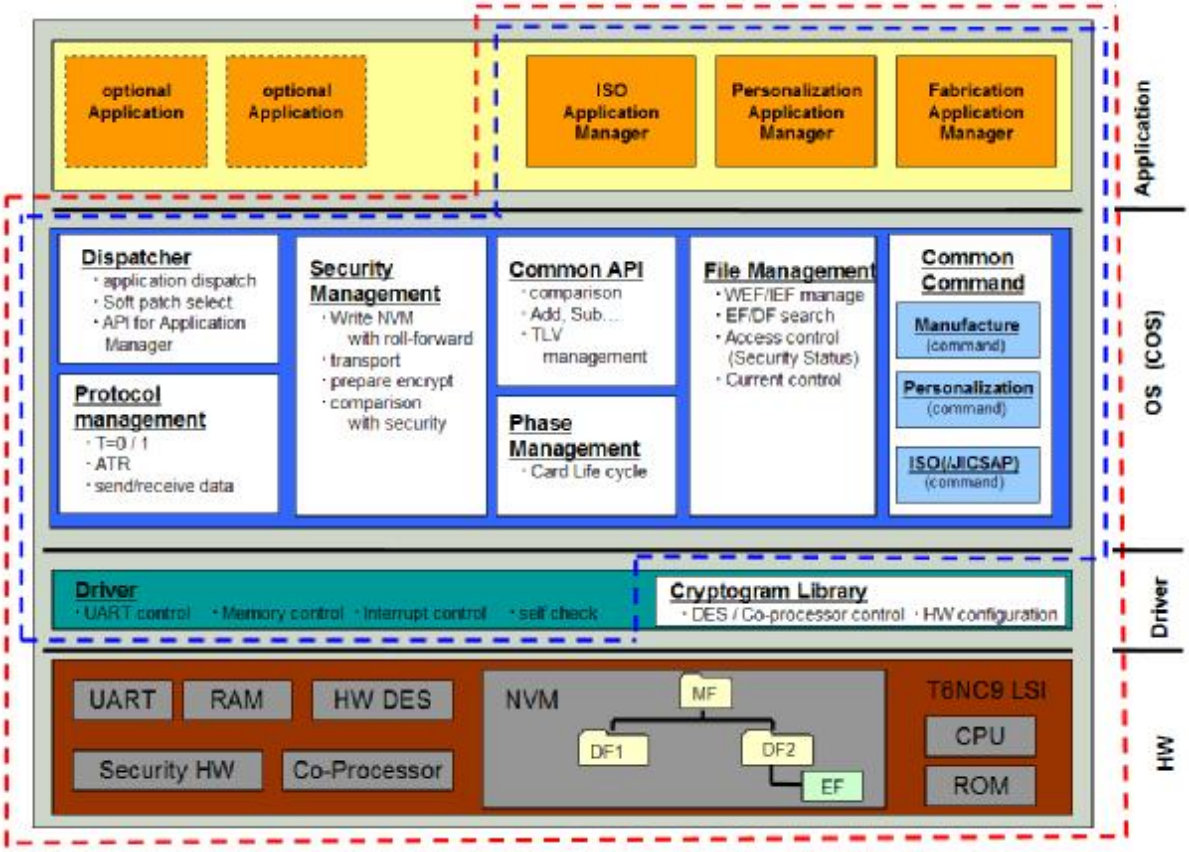


Figure 1: TOE scope (marked by red line) and part additional to hardware (marked by blue line)

The T6NC9 provides the computing platform and cryptographic support by means of co-processors for its Security IC Embedded Software (i.e. the FS SIGMA and the optional applications). The T6NC9 Security Target describes the features of this hardware platform. These also apply to the composite TOE.

The FS SIGMA provides the optional applications with the security functionality listed below in addition to the functionality described in the T6NC9 Security Target:

- Ø Card life-cycle management functions allowing the total card to be terminated at the request of an application.

The FS SIGMA provides the external smartcard readers with the security functionality listed below in addition to the functionality described in the T6NC9 Security Target:

- Ø An application providing an external smartcard reader with a ISO7816-4-based file system, including access control.

- A personalization application providing an external smartcard reader with commands for personalization steps of the card. This application is not available in the operational phase (i.e. it is only available to the personalizer).

The FS SIGMA also satisfies the following requirements the underlying hardware T6NC9 puts on its Security IC Embedded Software i.e. all software running on the platform (including the FS SIGMA and the optional applications):

- Destruction of the cryptographic keys after usage (FCS_CKM.4), as required for the RSA and the DES operations (FCS_COP.1[RSA] and FCS_COP.1[DES])
- Implementation of the T6NC9 user guidance with respect to:
- Enabling the hardware countermeasures
- Anti-perturbation countermeasures (for the FS SIGMA internally, and supporting the optional applications)

Physical parts of the TOE

- T6NC9

Software parts of the TOE

- Hardware configuration (CODE)
- Hardware configuration (Data)
- Co-Processor control library
- DES control library
- TEST ROM software
- FS SIGMA ROM software

Objectives for the environment

The objectives for the environment are all taken from the *[HW-ST]*. There are no additional security objectives for the operational environment. The objectives for the environment in *[HW-ST]* apply to the security IC embedded software (OE.Plat-Appl and OE.Resp-Appl), which are the FS SIGMA and the optional applications. For this evaluation these security objectives for the environment now apply only to the optional applications. One specific result is that these applications are assumed to be non-hostile as these objectives trace back to the assumptions A.Plat-Appl and A.Resp-Appl defined in *[PP]*.

2.6 Documentation

The following electronic documentation is provided with the product in the form of a PDF by the developer to the customer:

Identifier	Version
Guidance Document for Application Builder	MC-SJ0040-02
Application note	MC-SJ0023-03
Guidance Document for Card Issuer	MC-SJ0041-02
Platform Specification	MC-SM0721-01
Pre-Personalization Specification	MC-SM0785-00
Personalization Specification	MC-SM0786-00
Preparative guidance	MC-SJ0042-01
Procedural Request of Security Products Delivery and Receipt	MB-ICCARD-W386

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

Developer Testing
The developer used the following three testing methods:

- Unit tests on module level
- Integration tests on interaction of modules and subsystems
- System tests

The test approach, the TOE configuration and the testing results are described below per test method, as these properties are differently documented for each of the test methods.

Unit testing: Testing approach

Unit testing is performed as part of the development process. Using the development board version of the hardware (also used for the development and testing of the crypto library of the underlying hardware T6NC9), the ROM image is loaded and executed. The debugging functionality of the development board is used to set the registers and any other relevant input variables to a function, and to execute the function. The functional differences between the development board and the actual hardware are documented, the composite TOE developer is aware of these differences. The developer together with the evaluators have analysed the differences and have found no relevant differences for this TOE.

The actual result is inspected by the developer and manually verified against the expected results. Only when a ROM image meets all the expected test results, is it integrated with the underlying hardware and produced as a TOE.

Integration tests on interaction of modules and subsystems and system testing: Testing approach

Integration tests are performed to show complex behaviour on a higher abstraction level then module level, i.e. for the ISO7816-4 based file system access control rules.

The system tests are performed on the entire design using specific personalization settings of customers.

Using the development board version of the hardware (also used for the development and testing of the crypto library of the underlying hardware T6NC9), the ROM image is loaded and executed. All debugging functionality of the development board is disabled and a common card reader is used to communicate to the TOE with command APDUs. All tests except those that require manipulation of the TOE internals (such as simulation of a defective EEPROM) are repeated on engineering samples, i.e. on the actual TOE.

The actual result is inspected by the developer and manually verified against the expected results. Only when a ROM image meets all the expected test results, is it integrated with the underlying hardware and produced as a TOE. Only when the engineering samples meet all expected test results, mass production is authorized.

Evaluator testing

The evaluator re-used the testing methods by the developer, i.e. the following three testing methods:

- Unit tests on module level
- Integration tests on interaction of modules and subsystems
- System tests

Two verification steps were performed:

- The evaluators have observed a re-run of selected tests on the developer's testing setup, i.e. they were performed on the TOE's actual ROM image in the development emulator, and
- The evaluators have repeated these tests on the actual TOE (i.e. in hardware format) using the evaluator's testing setup.

2.7.2 Test Configuration

The evaluator re-run selected tests on the developer's testing setup, i.e. they were performed on the TOE's actual ROM image in the development emulator, and the evaluators also repeated these tests on the actual TOE (i.e. in hardware format) using the evaluator's testing setup.

The following tools were used for testing the TOE:

- The test tools of the developer
- Brightsight voltage manipulation setup
- Brightsight laser setup

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 *[JIL]* is considered and a scheme specific document, 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 6 groups: Those related to the Card Lifecycle, to the requirements from the underlying hardware platform, and those of the Persistent Storage divided in the access control, the try limits, the PIN verification and the External Authentication. In total 11*6=66 SFR/attack-combinations are possible. The theoretical analysis leads to the exclusion of 12 SFR/attack-combinations as covered by the underlying hardware platform's certification, and an additional 21 combinations as not applicable for this type of TOE, leaving 66-12-21=33 combinations for further analysis.
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 32 of the SFR/attack-combinations sufficient assurance could be found in the design information and other evaluation activities. For 1 SFR/attack-combination further penetration testing was deemed necessary: perturbation attacks (using both voltage manipulation and light injection) on the access control mechanism (in particular the updating of the internal security status flags).
4. Potential vulnerabilities from the other evaluation activities have been gathered and analysed whether they are still appropriate. All potential vulnerabilities were already considered or shown to be no longer appropriate. As a result, no significant additions were made to the penetration testing selected.
5. The resulting penetration tests were performed and the individual results analysed according to *[JIL]*.

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

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

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

Based on the above evaluation results the evaluation lab concluded the Toshiba FS Sigma version 01.01.05 to be **CC Part 2 extended**, **CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented by AVA_VAN.5, ALC_DVS.2 and ASE_TSS.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 FS Sigma Security Target, Version 1.9, dated May 18th 2009.

2.10 Evaluator Comments/Recommendations

The FS SIGMA uses all the security characteristics of the T6NC9 IC. As a consequence application builders for the optional applications functionality the TOE provides only have to use the interfaces offered by FS SIGMA to build a secure application.

When the customer is the builder of an optional application this customer must use all the provided platform functionality as described in the guidance document for the application builder (see section 2.6). When the customer is the user of the ISO-7816-4 based file system then there are no recommendations and hints to mention.

3 Security Target

The Security Target, “FS SIGMA Security Target”, Version 1.9.0, dated May 18th 2009, unique ID MC-SM0722 is included here by reference. Please note that for the need of publication a public version of the Security Target, “FS SIGMA Security Target (for public)”, Version 1.9.0, dated May 18th 2009, unique ID MC-SM1046 has been created and verified according to [ST-SAN].

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
EEPROM	Electronically Erasable Programmable Read Only Memory
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
NV	Non-volatile
NVM	Non-volatile Memory
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SPA/DPA	Simple/Differential Power Analysis
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 FSSigma version 01.01.05 (FSSigma) June 26th 2009.
[HW-ST]	Toshiba Corporation, Security Target T6NC9 Integrated Circuit with Crypto Library v1.1, version 2.1, 2 April 2009
[JIL]	JIL Application of Attack Potential to Smart Cards, version 2.5, November 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]	FS Sigma Security Target, Version 1.9.0, dated May 18th 2009.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.