FS SIGMA
Security Target
(for public)

May, 18, 2009

Version 1.9.0

TOSHIBA CORPORATION

Software Design Group
Smart Card Systems Department
Komukai Operations

Change History

No	Version	Date	chapter	content	name
1	1.0.0	2008-07-25	all	New release, Rev.00	Ishibashi
2	1.9.0	2009-05-18		Based on approved ST	Ishibashi

Table of contents

1. Introduction

1.1. Common Criteria requirements

This document addressed the following requirements of the Common Criteria:

- ASE: Security Target Evaluation

1.2. Definitions and abbreviations

This document uses the following terms:

Configuration Items	Components, files and documents used in the development process of the TOE
FS SIGMA	OS name, used instead of FSΣ
JICSAP	The Specification based on ISO7816-4

This document uses the following abbreviations:

CC	Common Criteria
IC	Integrated Circuit
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
TOE	Target of Evaluation
OSP	Organizational Security Policy
APDU	Application Data Unit
NVM	Non Volatile Memory (=EEPROM)

2. ST introduction

This chapter presents the ST reference, a TOE reference, a TOE overview and a TOE description.

2.1. ST identifiers

Title:	FS SIGMA Security Target
Version:	Version 1.9.0
Date of issue:	18 May 2009
TOE identification:	FS SIGMA (FSΣ)
TOE version:	Version 01.01.05 (=MC-SM0300-04)
Produced by:	TOSHIBA CORPORATION Social Infrastructure Company

Evaluation Assurance Level: EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 and ASE_TSS.2.

2.2. TOE overview

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 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 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

(See the guidance documentation for details)

And there are security features of the HW below, these are direct copy 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. TOE description

2.3.1. Physical scope of the TOE

The TOE physically consists of the following.

Note that the optional applications are outside of the logical scope of the TOE, but as they are part of the final User ROM image, they will be physically inside the TOE when they are composed (similar to the situation that the T6NC9 is certified with a User ROM image, not a specific one).

Delivery item type	Identifier	Version	Medium
Hardware	T6NC9	#4.0	COT
Software	FS SIGMA	Ver.01.01.05 (Refer to the Guidance document [AGD Platform Spec] for Mask Version (TOE ID))	ROM of hardware (user area)
Guidance (for Application Builder)	Guidance Document for Application Builder	MC-SJ0040-02	Document / pdf
	Application note	MC-SJ0023-03	Document / pdf
Guidance (for Card Issuer)	Guidance Document for Card Issuer	MC-SJ0041-02	Document / pdf
	Platform Specification	MC-SM0721-01	Document / pdf
	Pre-Personalization Specification	MC-SM0785-00	Document / pdf
	Personalization Specification	MC-SM0786-00	Document / pdf
	Preparative guidance	MC-SJ0042-01	Document / pdf
	Procedural Request of Security Products Delivery and Receipt	MB-ICCARD-W386	Document / pdf

2.3.2. Logical scope of the TOE

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.

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.

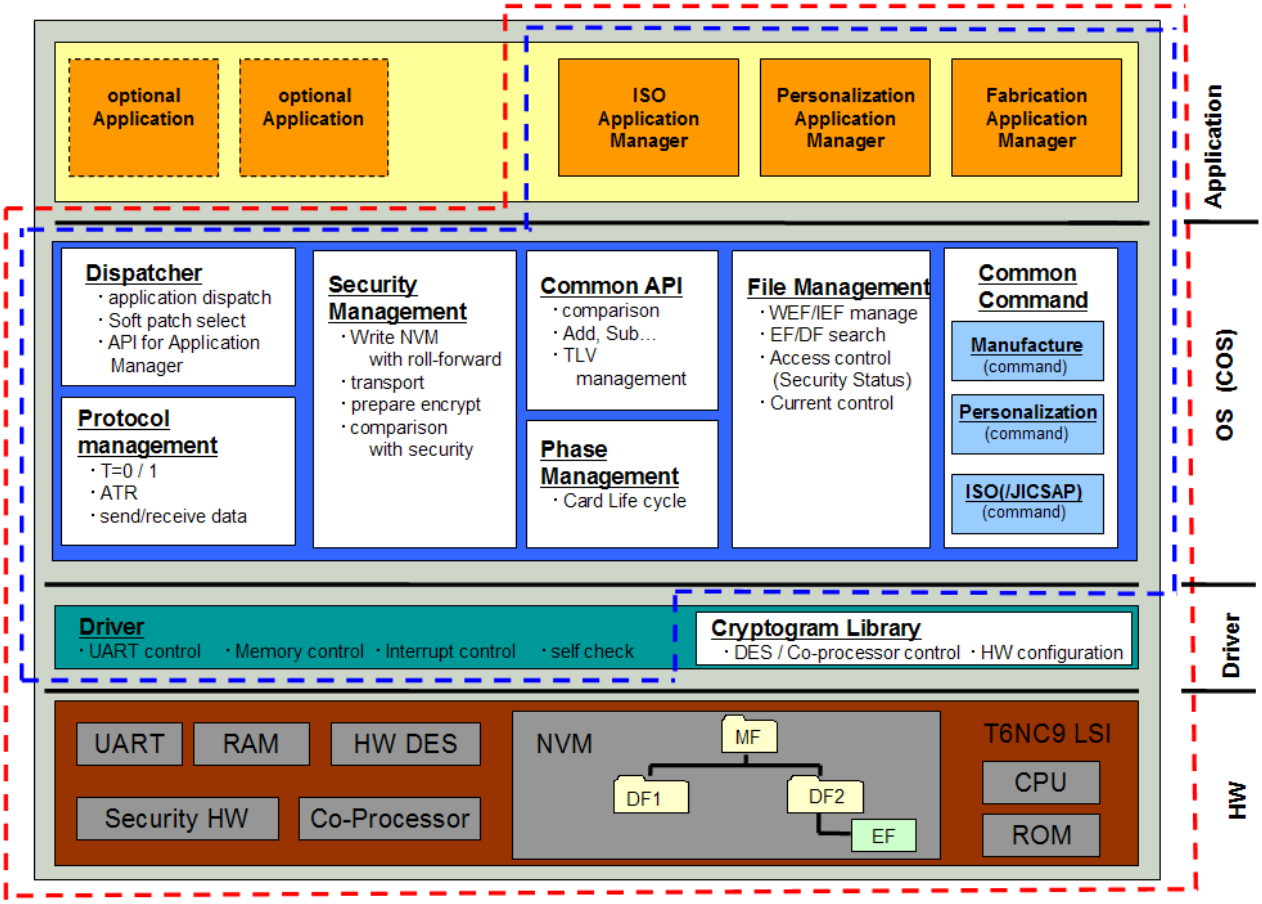

Figure 1: TOE scope (marked by red line) and part additional to hardware (marked by blue line)

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

- 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:

- An application providing an external smartcard reader with 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)

2.3.3. Life cycle Boundaries of the TOE

The TOE life cycle follows the life cycle described in 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).

The following figure relates the in the TOE defined logical phases to the phases as defined in the [PP]. 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.

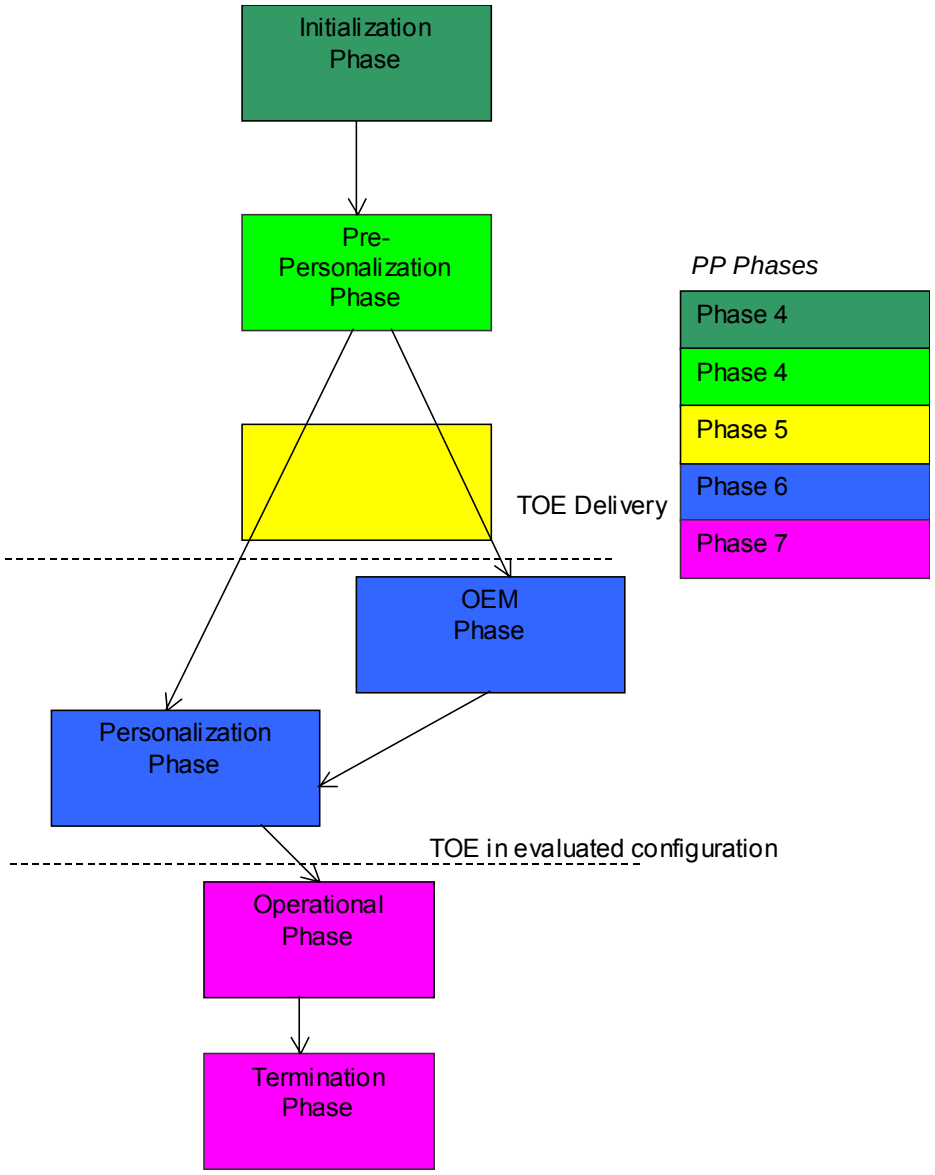

Figure 2 Life-cycle boundaries of the TOE

3. Conformance claim and rationale

3.1. Conformance claim

This Security Target claims conformance to the Common Criteria version 3.1 Revision 2 September 2007.
Furthermore it claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in [PP] Chapter 5.

This Security Target claims conformance to [PP]. This Security Target builds on [HW-ST], which is also conformance to this [PP].

3.2. Conformance claim rationale

The [PP] requires strict compliance.

This Security Target contains all SARs from [HW-ST] and therefore of [PP], augmented with ASE_TSS.2.
This Security Target contains all SFRs from [HW-ST] by reference (see Section 6.1.1), and augments these with SFRs for the FS SIGMA (see Section 6.1.2).

The TOE type of [PP] is "*The Target of Evaluation (TOE) is a security integrated circuit (security IC) […]. The TOE may also include IC Developer/Manufacturer proprietary IC Dedicated Software as long as it is delivered by the IC Manufacturer.*" This Security Target describes the TOE as "a composite security IC or smartcard TOE" with the FS SIGMA delivered by the manufacturer, therefore the TOE type is consistent with the TOE type of [PP]

The security problem definition in Chapter 4 refers to the security problem definition of [HW-ST] (which is compliant with [PP]) and augments this with OSP.Lifecycle and OSP.JICSAP.
The security objectives in Chapter 5 refer to the security objectives of [HW-ST] (which is compliant with [PP]) and augments this with O.Lifecycle and O.JICSAP.

4. Security problem definition

The Security Problem Definition builds on the Security Problem Definition of [HW-ST]. As such, this Security Target refers to [HW-ST] for the Threats, OSPs and Assumptions, defined there.

Only the additional Assets, Subjects, Threat Agents, External Entities, Objects, Operations and Security Attributes associated with the [PP]-augmentations OSP.JICSAP and OSP.Lifecycle are listed in this Security Target.

4.1. Definition of subjects, objects and operations

To facilitate easy definition of threats, OSPs, assumptions, security objectives and security requirements, we define the subjects, objects and operations to be used in the ST first.

4.1.1. Subjects

See also [HW-ST]. The additional subjects are (in alphabetical order):

Identification	Description
S.Application	An (optionally installed) smartcard application running on the TOE.
S.Reader	The representation of a smartcard reader communicating to the TOE via the ISO-7816 contact interface, using APDUs.

4.1.2. Security Attributes

See also [HW-ST]. The additional security attributes of the subjects are (in alphabetical order):

Identification	Description
SA.Reader_security_status	The current security status of the S.Reader, as defined in JICSAP.

4.1.3. Objects

See also [HW-ST]. The additional objects are (in alphabetical order):

Identification	Description
D.JICSAP_files	The user data stored via the JICSAP application, in JICSAP MF/DF/EF/IEFs.
D.Card_Lifecycle_State	The total smartcards lifecycle state, which can be “Operation” or “Termination” in the evaluated configuration.

4.1.4. Operations

See also [HW-ST]. The additional operations that are performed by the TOE are (in alphabetical order):

Identification	Description

Op.APDU_Generic	S.Reader requests other operations then Op.APDU_GetCardInformation from the TOE via APDUs.
Op.APDU_GetCardInformation	S.Reader retrieves general card data from the TOE via APDUs.
Op.JICSAP	The reading, writing, updating, deletion and changing of access control conditions by the S.Reader on D.JICSAP_files

4.2. Assumptions about operational environment of TOE

See also [HW-ST]. There are no additional assumptions about the operational environment of the TOE. Note that the [HW-ST]'s assumptions on the environment A.Plat-Appl and A.Resp-Appl applied to the T6NC9's Security IC Embedded Software developer, which is here the FS SIGMA and the optional applications. For this evaluation these assumptions on the environment now apply only to the optional applications (the TOE part is of course evaluated).

4.3. Threats

See also [HW-ST]. There are no additional threats.

4.4. Organizational Security Policies

See also [HW-ST]. The additional organizational security policies that are to be delivered by the TOE are (in alphabetical order):

Identification	Description
OSP.JICSAP	The TOE shall provide a JICSAP compliant 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.
OSP.Lifecycle	The TOE shall provide an "Operation" and a "Termination" state. In the Termination state, the only commands allowed are those for reading the card lifecycle information. In Operation state, both the reading of the card lifecycle information, as well as the generic APDUs are allowed. The (optionally installed) applications can set the state to Termination.

5. Personalization/Initialization Security Objectives

5.1. TOE Security Objectives

See also [HW-ST]. The additional TOE Security Objectives are (in alphabetical order):

Identification	Description
O.JICSAP	The TOE shall provide a JICSAP compliant 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.
O.Lifecycle	The TOE shall provide an “Operation” and a “Termination” state. In the Termination state, the only commands allowed are those for reading the card lifecycle information. In Operation state, both the reading of the card lifecycle information, as well as the generic APDUs are allowed. The (optionally installed) applications can set the state to Termination.

5.2. Security Objectives for the operational environment

See [HW-ST]. There are no additional security objectives for the operational environment. Note that the [HW-ST]’s Security objectives for the security IC embedded software development environment (OE.Plat-Appl and OE.Resp-Appl) applied to the T6NC9’s Security IC Embedded Software: 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].

6. Security Requirements

6.1. Security Functional Requirements

The SFRs are split in two categories, the SFRs from [HW-ST] that are imported by reference in this Security Target, and the SFRs added in this ST.

6.1.1. SFRs from the underlying hardware platform

Below are the SFRs from [HW-ST], all of which also apply to this (composite) TOE. They are listed here by name for convenience, the full description is in [HW-ST].

SFRs underlying hardware platform	Described in	Implemented in	Notes
FRU_FLT.2 Limited fault tolerance	[HW-ST]	HW	-
FPT_FLS.1 Failure with preservation of secure state	[HW-ST]	HW	-
FMT_LIM.1 Limited capabilities[1]	[HW-ST]	HW, SW	The SFR is unchanged, however the TOE scope has increased and covers the testing functionality present in the FS SIGMA.
FMT_LIM.2 Limited availability[2]	[HW-ST]	HW, SW	See FMT_LIM.1
FAU_SAS.1 Audit storage[3]	[HW-ST]	HW	-
FPT_PHP.3 Resistance to physical attack	[HW-ST]	HW	-
FDP_ITT.1 Basic internal transfer protection	[HW-ST]	HW	-
FPT_ITT.1 Basic internal TSF data transfer protection	[HW-ST]	HW	-
FDP_IFC.1 Subset information flow control	[HW-ST]	HW	
FCS_RNG.1 Random number generation[4]	[HW-ST]	HW	-
FCS_COP.1[DES] Cryptographic operation	[HW-ST]	HW	-
FCS_COP.1[RSA] Cryptographic operation	[HW-ST]	HW	-

[1] Common Criteria Part 2 extended, see section 5.2 of the Eurosmart PP.

[2] Common Criteria Part 2 extended, see section 5.2 of the Eurosmart PP.

[3] Common Criteria Part 2 extended, see section 5.3 of the Eurosmart PP.

[4] Common Criteria Part 2 extended, see section 5.1 of the Eurosmart PP.

6.1.2. SFRs additional the underlying hardware platform

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
Card Lifecycle (O.Lifecycle)					
FDP_ACC.1 [Card Lifecycle] Subset access control	FDP_ACF.1 Security attribute based access control	Yes, by FDP_ACF.1[Card Lifecycle]	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].	[assignment: access control SFP] Card Lifecycle access control policy [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP] S.Reader, D.Card_Lifecycle_State, Op.APDU_GetCardInformation and Op.APDU_Generic	
FDP_ACF.1 [Card Lifecycle] Security attribute based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Yes by FDP_ACC.1[Card Lifecycle], FMT_MSA.3[Card Lifecycle]	The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]. The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled	[assignment: access control SFP] Card Lifecycle access control policy [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes] Subjects and attributes: S.Reader Objects: D.Card_Lifecycle_State Operations: Op.APDU_GetCardInformation and Op.APDU_Generic [assignment: rules governing access among controlled subjects and controlled objects using controlled	Note that S.Application cannot be activated by S.Reader once O.Card_Lifecycle_State is set to Terminated by S.Application, as Op.APDU_Generic is not available in Terminated state and this is the only way to activate S.Application.

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
			objects]. The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]. The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].	operations on controlled objects]. Op.APDU_Generic is allowed if D.Card_Lifecycle_State is in Operational state [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] Op.APDU_GetCardInformation is allowed in if D.Card_Lifecycle_State is in Operational and Terminated state. [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] All operations by S.Reader not explicitly allowed are denied.	
FMT_SMF.1 [Card Lifecycle] Specification of Management Functions	-		The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].	[assignment: list of management functions to be provided by the TSF] only S.Application can change D.Card_Lifecycle_State from Operational to Terminated.	

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
FMT_MSA.3 [Card Lifecycle] Static attribute initialisation	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FMT_MSA.1: Not applicable, there are no security roles, so there is also no management of the security attributes of these roles. FMT_SMR.1: Not applicable, there are no subjects that can change the default value, so there are also no security roles for them.	The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP. The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.	[assignment: access control SFP, information flow control SFP] Card Lifecycle access control policy [selection, choose one of: restrictive, permissive, [assignment: other property]] “Operation state” [assignment: the authorised identified roles] None	
Persistent storage (O.JICSAP)					
FDP_ACC.1 [JICSAP] Subset access control	FDP_ACF.1 Security attribute based access control	Yes, by FDP_ACF.1 [JICSAP]	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].	[assignment: access control SFP] JICSAP access control policy [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP] S.Reader, D.JICSAP_files, Op.JICSAP	
FDP_ACF.1 [JICSAP] Security attribute	FDP_ACC.1 Subset access control	Yes, by FDP_ACC.1[JICSAP] and	The TSF shall enforce the [assignment: access control SFP] to objects based on the	[assignment: access control SFP] JICSAP access control policy	

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
based access control	FMT_MSA.3 Static attribute initialisation	FMT_MSA.3 [JICSAP]	following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].	[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes] Subjects and attributes: S.Reader, with attribute SA.Reader_security_status	
			The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].	Objects: D.JICSAP_files Operations: Op.JICSAP [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]. The operation requested by S.Reader is allowed if the SA.Reader_Security_Status fulfils the requirements as stated in [JICSAP] Section 5.1 “Security attributes and security status” for that operation.	
			The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].	[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] None	
			The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny	[assignment: rules, based on security attributes, that explicitly deny access of	

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
			access of subjects to objects].	subjects to objects] All operations not explicitly allowed are denied.	
FIA_AFL.1 [JICSAP] Authentication failure handling	FIA_UAU.1 Timing of authentication	Yes, by FIA_UAU.1 [JICSAP]	The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events]. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions].	[selection: [assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]] an administrator configurable positive integer within the range 1-255 or unlimited, as defined in the maximum error counter (we call Try Limit) [assignment: list of authentication events] PIN or authorization key [assignment: list of actions] block further authentication attempts to that PIN or authorization key	
FIA_UAU.1 [JICSAP] Timing of authentication	FIA_UID.1 Timing of identification	FIA_UID.1: Not applicable, as there is only one subject that can authenticate itself to the TOE, S.Reader. There is no identification of different	The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated. The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.	[assignment: list of TSF mediated actions] SELECT, GET CHALLENGE, GET DATA, INTERNAL AUTHENTICATE	

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
		readers.			
FIA_UAU.4 [JICSAP] Single-use authentication mechanisms	-		The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(s)].	[assignment: identified authentication mechanism(s)] EXTERNAL AUTHENTICATE	
FIA_USB.1 [JICSAP] User-subject binding	FIA_ATD.1 User attribute definition	FIA_ATD.1 [JICSAP]	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes]. The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes]. The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].	[assignment: list of user security attributes] S.Reader, with attribute SA.Reader_security_status [assignment: rules for the initial association of attributes]. The SA.Reader_security_status initial value is set to “not authenticated” for all PINs and authentication keys [assignment: rules for the changing of attributes] If S.Reader successfully authenticates against a PIN or key, the SA.Reader_security_status is updated to show what this PIN or key is authenticated.	
FIA_SOS.2 [JICSAP] TSF Generation of secrets	-		FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [assignment: a defined	[assignment: a defined quality metric] the requirements of Class K3 of [AIS20]	

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
			quality metric]. The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions].	[assignment: list of TSF functions] GET CHALLENGE, EXTERNAL AUTHENTICATE	
FMT_MSA.3 [JICSAP] Static attribute initialisation	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FMT_MSA.1: Not applicable, there are no security roles, so there is also no management of the security attributes of these roles. FMT_SMR.1: Not applicable, there are no subjects that can change the default value, so there are also no security roles for them.	The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP. The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.	[assignment: access control SFP, information flow control SFP] JICSAP access control policy [selection, choose one of: restrictive, permissive, [assignment: other property]] restrictive [assignment: the authorised identified roles] None	
FIA_ATD.1 [JICSAP] User attribute	-		The TSF shall maintain the following list of security attributes belonging to	[assignment: list of security attributes] SA.Reader_security_status	

SFR	Dep.	Met?	Text of CC part 2	Selection, operation, assignment	Remark
definition			individual users: [assignment: list of security attributes].		
Requirements from underlying hardware platform					
FCS_CKM.4 Cryptographic key destruction	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Crypto-graphic key generation] FMT_MSA.2 Secure security attributes	These dependencies are left to the Security IC Embedded Software (see [HW-ST] “Security Requirements for the Environment”)	The TSF shall destroy cryptographic keys in accordance with a **specified cryptographic key destruction method** [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].	[assignment: cryptographic key destruction method] overwrite once [assignment: list of standards] None	Fulfils the dependencies of FCS_COP.1[DES] and FCS_COP.1[RSA] from [HW-ST].

6.2. TOE Security Assurance Requirements

The TOE security assurance requirements are conformant to the CC Evaluation Assurance Level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 and ASE_TSS.2.

6.3. Explicitly stated requirements

See [PP] Chapter 5.

7. Rationale

7.1. Security Objectives Rationale

For the assumptions, threats and OSPs from [HW-ST], see [HW-ST].

There are two additional OSPs, OSP.JICSAP and OSP.Lifecycle. For each of these additional OSPs we demonstrate that it is met by the security objectives.

The individual rationales demonstrating that the objectives are as follows:

OSP.JICSAP

This policy is directly implemented by O.JICSAP

OSP.Lifecycle

This policy is directly implemented by O.Lifecycle.

7.2. Security Requirements Rationale

The purpose of the Security Requirements Rationale is to demonstrate that the security requirements are suitable to meet the Security Objectives.

7.2.1. The SFRs meet the Security Objectives for the TOE

For the SFRs meeting the Security Objectives from [HW-ST], see [HW-ST]. In addition to the mapping of FCS_COP.1[DES] and FCS_COP.1[RSA] for meeting O.Add-functionality, FCS_CKM.4 is now also supporting this Security Objective for the TOE in the composite TOE.

For each additional Security Objective for the TOE (O.JICSAP and O.Lifecycle) we demonstrate that it is met by the SFRs. The tracings are provided by the SFRs.

O.JICSAP

FDP_ACC.1[JICSAP] and FDP_ACF.1[JICSAP] defines access control compliant with the JICSAP access control conditions based on the current security status of the reader. FIA_ATD.1[JICSAP] describes that this security status of the reader is considered to be a security attribute of S.Reader. FIA_USB.1[JICSAP] describes that the security status is updated based on successful authentications against PINs and authentication keys. FIA_AFL.1[JICSAP] describes the limits on these authentications tries. Authentications against authentication keys require SELECT and GET CHALLENGE to generate the challenge. FIA_UAU.1[JICSAP] describes that only these commands are allowed prior to authentication. FIA_UAU.4[JICSAP] and FIA_SOS.2[JICSAP] describe that this

mechanism is a challenge-response mechanism with random challenges (which are therefore one time use).

O.Lifecycle

FDP_ACC.1[Card Lifecycle] and FDP_ACF.1[Card Lifecycle] define the access control in terms of an "Operation" and a "Termination" state as stored in D.Card_Lifecycle_State. It defines that in the Termination state, the only commands allowed are those for reading the card lifecycle information. In Operation state, both the reading of the card lifecycle information, as well as the generic APDUs are allowed.

FMT_SMF.1[Card Lifecycle] defines that only the (optionally installed) applications can set the state to Terminated.

Note that generic APDUs (in particular, the SELECT command) are needed to activate the (optionally installed) applications. As these are not allowed in Termination state, the applications cannot be activated in Termination state.

7.2.2. Reason for choosing Security Assurance Requirements

The Security Assurance Requirements have been chosen to meet the requirements of [PP]. This was augmented with ASE_TSS.2 to provide the potential consumers of this TOE a clearer view on the protection provided against bypassing and modification of the TOE.

7.2.3. All dependencies have been met

The dependency analysis of the SFRs from the underlying hardware platform have been analyzed in [ST-HW]. The dependency on FCS_CKM.4 by FCS_COP.1[DES] and FCS_COP.1[RSA] is left to the Security IC Embedded Software in [ST-HW], but is met in this composite TOE.

For the SFRS additional to the underlying hardware platform, the section "SFRs additional the underlying hardware platform" shows that all dependencies have been met or are not applicable.

7.3. TOE Summary Specification

7.3.1. TOE meets the SFRs

For each SFR we demonstrate that it is met by the TOE. The tracings are provided implicitly by the rationales.

Card Lifecycle (O.Lifecycle)

The TOE maintains a card life cycle state value in its EEPROM. At the moment of delivery of the TOE, this value is "Operation" (FMT_MSA.3[Card Lifecycle]). If the card life cycle

state is Operation, the Dispatcher dispatches all APDUs to the currently selected application, allowing both the generic APDUs and those for reading the card lifecycle data to proceed. If the card life cycle state is "Termination", all APDUs are dispatched to ISO/JICSAP Application manager that only support the commands necessary for retrieving the card lifecycle data. In particular, it does not support selection (and therefore activation) of other applications. Thereby it implements the FDP_ACC.1[Card Lifecycle] and FDP_ACF.1[Card Lifecycle] requirements.
The (optionally installed) applications can call a function in the FS SIGMA API to request the card life-cycle state to be set to Terminated (FMT_SMF.1[Card Lifecycle]).

Persistent storage (O.JICSAP)
The TOE contains a JICSAP application manager that implements the JICSAP commands by calling the appropriate subsystems in FS SIGMA OS layer. In particular, the access control rules are checked by querying the File Management subsystem's Access control module. Based on the return value of these functions, the current security status of the reader is updated and access is granted or denied. The Access Control module therefore implements the management of the user subject binding (FIA_USB.1[JICSAP] and FIA_ATD.1[JICSAP]) and the access control calculation (FDP_ACC.1[JICSAP] and FDP_ACF.1[JICSAP]).
The authentication against PINs and authentication keys are implemented in the Common Command subsystem, the ISO/JICSAP module, implementing VERIFY and EXTERNAL AUTHENTICATE functionality. This includes the enforcement of the configurable amount of unsuccessful authentication attempts (FIA_AFL.1[JICSAP]).
The EXTERNAL AUTHENTICATE command requires that the reader has done a GET CHALLENGE for retrieving the challenge. The response of the reader via the EXTERNAL AUTHENTICATE command has to match this challenge. The random value for this challenge is generated from the random number generator of the underlying hardware platform. This RNG meets AIS K2 and K3 class requirements, therefore the challenge also meets these requirements (FIA_SOS.2[JICSAP]). As this is a challenge-response mechanism based on a random challenge generated by the TOE, it is a single-use authentication mechanism (FIA_UAU.4[JICSAP]).

The TOE does not allow changes of the JICSAP access control policy (FMT_MSA.3[JICSAP]). Note that the JICSAP access control policy covers access to the security attributes of files, which includes, amongst others, the amount of authentication tries allowed. This is considered part of the access control policy FDP_ACC.1[JICSAP] and FDP_ACF.1[JICSAP].

The SELECT and GET CHALLENGE are not prohibited by the JICSAP access control policy , therefore they are available before authentication (FIA_UAU.1[JICSAP])

Requirements from underlying hardware platform

The TOE provides cryptographic functions to the applications. The cryptographic calculations are implemented in the cryptographic library of the underlying hardware platform. The TOE automatically overwrites the used buffers before returning the data to the calling application (FCS_CKM.4)

The other SFRs (which is from the underlying hardware component) are met by the TOE as described in [HW-ST].

7.3.2. TOE protects itself against interference and logical tampering

The interaction of the underlying hardware platform and FS SIGMA together provides the required protection. The potential effects of attacks are varied, and so are the security measures to counter them. FS SIGMA depends on the underlying hardware platform to provide a first line of defense by providing detection and prevention mechanisms, and a secondary set of defenses that seek to randomize the results of perturbation attacks. FS SIGMA augments this by providing additional detection mechanisms, which have a high chance to detect perturbation attacks.

The software runs in four different memory firewall configurations: “application”, “transmission”, “OS”, and one specifically “memory copy”. The settings of the memory firewall are chosen such that an application cannot access the OS areas where sensitive data is stored, including the cryptographic coprocessor RAM. FS SIGMA OS ensures that during transmission, the only areas accessible are those necessary for the transmission, so no accidental access to the general RAM and EEPROM and coprocessors is possible.
For the copying of sensitive data, the memory firewall is used to ensure that copying outside the address bounds is detected.
The underlying hardware platform reacts to access outside the configured boundaries with a hardware security reset.

The integrity of sensitive data being copied from memory to the CPU registers is verified by CRC before committing the operation. During a memory copy the data is verified one by one. Just before the use of sensitive data, the integrity of the data is verified. Data whose integrity is incorrect is not used for the operation. Sensitive data in return values is encoded in complex patterns to make successful modification attacks unlikely.
Depending on the function and error, a failed integrity check leads to an error message or a

card mute.

All files and meta-data are stored with automatic data integrity protection by the FS SIGMA OS's File Management subsystem. Failure of the integrity checks causes this subsystem to return an appropriate error message to the calling application.

FS SIGMA protects against the logical tampering after the pre-PERSONALIZATION phase. It means that it is impossible for FS SIGMA to add, delete and modify the program code, and to load the temporary new application after the TOE is delivered.

The writing of important data uses the atomic transaction. The written target will be in either the state before writing, or the state where all were written in, by using this atomic transaction, if the abnormalities of power supply interception or other attack occur. After writing, it is verified whether the written data is right. And only if the data is correct, it is committed.

FS SIGMA OS is compliant to the T6NC9 user guidance. So the required hardware countermeasures are appropriately enabled to suitable timing. And other additional anti-perturbation countermeasures are implemented

7.3.3. TOE protects itself against bypass

The underlying hardware platform protects itself and FS SIGMA (and the optionally installed applications) against bypass via physical means. To augment this protection, the FS SIGMA OS stores all internal files (IEFs) with automatic encryption/decryption such that they are stored encrypted in NVM.

The underlying hardware platform protects itself and FS SIGMA (and the optionally installed applications) against bypass via sidechannel analysis. To augment this protection, FS SIGMA incorporates additional timing countermeasures surrounding sensitive operations, performs comparisons of sensitive data in a time constant way with additional blinding of the values compared.

After start-up of the underlying hardware platform, the FS SIGMA OS is always executed because it is in the startpoint of the user ROM. The FS SIGMA OS handles the I/O up to APDU level and, based on the card lifecycle state, dispatches the APDU to the appropriate application manager. This mechanism is already described under the Lifecycle-SFRs, and forms its own bypass protection with regard to these SFRs.

No application except the JICSAP application will access the JICSAP data. The JICSAP application implements the access control rules already described under the JICSAP-SFRs, and forms its own bypass protection with regard to these SFRs.

8. Reference

No	Title	Date	Version	publisher	Document number
HW-ST	T6NC9 Integrated Circuit with Crypto Library v1.1 Security Target	2 April 2009	2.1	TOSHIBA CORPORATION	CC-T6NC9-ST-ENG-002
JICSAP	Specification of IC cards with contacts Complying with Japanese Industrial Standard	1998	1.1	Japan Ic Card System Application council (JICSAP)	
PP	IC Platform Protection Profile	15.06.2007	1.0	Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI-PP-0035
AGD Platform Spec	Platform Specification	***	***	TOSHIBA	***

End of Document

