Apollo OS

V4.03

on

SLE66CX680PE m1534-a13 Smart Card Controller IC

Version:	1.11
Date:	2009-06-15
Doc. ID	SP - 1
Author(s):	Ilanit Avioz
FIPS 140-2	Level 3

Table of Contents

1 Introduction

1.1 Purpose

This document defines the Security Policy for the SCsquare Apollo OS V4.03 on SLE66CX680PE m1534-a13[1] smart card controller by Infineon Technologies AG, a single-chip cryptographic module in accordance with FIPS 140-2 Security Level 3 requirements. Included are a description of the security requirements for the module, and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules (both those derived from the security requirements of FIPS 140-2 standard and from the security requirements of the module itself), under which the cryptographic module must operate.

1.2 Scope

The Cryptographic Security Policy specifies the security rules under which the cryptographic module operates and its major properties. It does not describe the requirements for the entire system, which makes use of the cryptographic module.

1.3 Security level

The Apollo OS V4.03 on SLE66CX680PE meets the overall requirements applicable to FIPS140-2 Security Level 3. In the different requirement sections of FIPS 140-2 the following Security Level ratings are achieved:

Security Requirements Section	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Cryptographic Key Management	3

Security Requirements Section	Security Level
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of other attacks	3
Operational environment	N/A

Table 1 – FIPS 140-2 Security Levels achieved

[1] "m1534-a13" is Infineon's product code for the used SLE66CX680PE chips, where "a13" means 13th revision which is manufactured in Dresden, Germany (site code "a"). In absence of other version numbers for the SLE66 series chips therefore this product code is used to unambiguously define the version of the SLE66CX680PE ICs used here.

2 Cryptographic Module Specification

2.1 Cryptographic boundary

Apollo OS V4.03 on SLE66CX680PE is a single-chip implementation of a cryptographic module. The corresponding micro-module (see chapter “Physical Security” hereinafter) is designed to be embedded in a plastic card body to provide an ISO/IEC 7816 compliant smart card. During the manufacturing process, the chip (IC) with electrical contact pads is wire bonded on the inner side of a contact plate, then globe-topped with epoxy resin. The perimeter of the resulting micro-module (i.e. contact plate on one side and epoxy resin cover on the other side) forms the cryptographic boundary of this FIPS140-2 Security Level 3 compliant single-chip cryptographic module (see chapter “Physical Security” hereinafter). The contained hardware and software components are as follows:

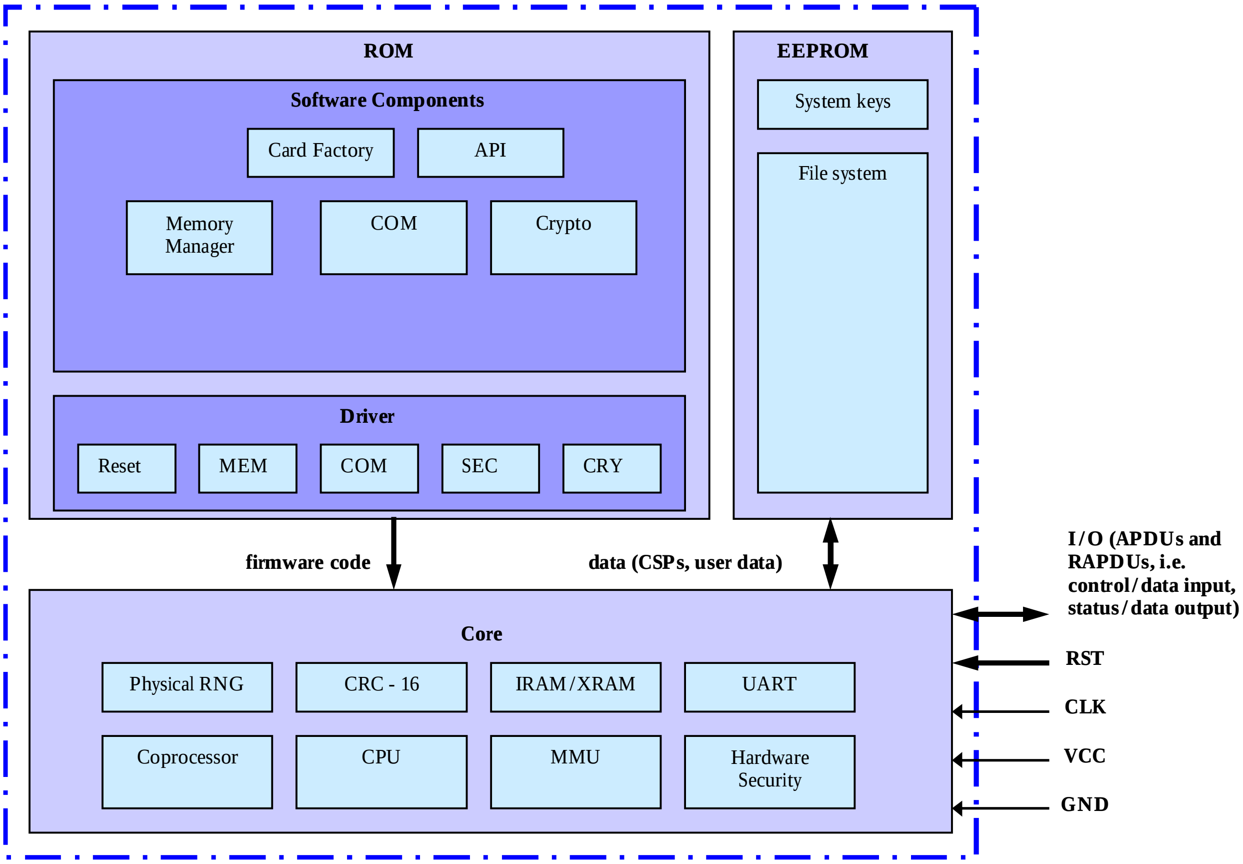


Figure 1 – cryptographic module boundary, major components, major data flows

2.2 Firmware

The Apollo OS V4.03 is firmware is located in the ROM of Infineon SLE66CX680PE smart card controller. This firmware is implemented using high level language (C), a limited number of software modules that require fast processing have been written in low level language (assembly language). The Apollo OS firmware contains the following components:

Item	Description
Software components	
API	ISO API's and proprietary commands
Card Factory	The Card Factory, including OS bootstrap, OS initialization, self-tests, command procedures.
Memory manager	The Memory Manager including services such as memory access, allocation, deallocation.
COM	Communication handler including services, such as ATR, PSS, T=1.
CRYPTO	The Cryptography engines including services such as TDES, SHA-1, SHA-256, HMAC, RSA, DSA.
Drivers Layer	
RESET	OS startup and chip initialization, IT/exception vectors, MMU/banking configuration
MEM	Memory module including NVM access, atomicity and transaction management
COM	Communication module including IO exchanges, timing control
SEC	Security module including counter-measures and fault attack management, CRC, RNG
CRY	Cryptography module including basic primitives for TDES, SHA-1, SHA-256, RSA, and DSA

Table 2 – Firmware components

2.3 Hardware

The cryptographic module is based on the Infineon SLE66CX680PE m1534-a13[2] chip card controller. This is an off-the-shelf smart card IC, which is comprised of:

- Central processing unit, CPU (processes all firmware of the module)
- Memory management unit (MMU)
- 256 byte of internal RAM (IRAM)
- 6 Kbyte extended RAM (XRAM)
- 244 Kbyte ROM (contains the Apollo OS firmware, see chapter "Firmware" above)

[2] "m1534-a13" is Infineon's product code for the used SLE66CX680PE chips, where "a13" means 13th revision which is manufactured in Dresden, Germany (site code "a"). In absence of other version numbers for the SLE66 series chips therefore this product code is used to unambiguously define the version of the SLE66CX680PE ICs used here.

- 68 Kbyte EEPROM (contains CSPs and the file system of the cryptographic module)
- Physical random number generator (PRNG)
- Checksum module (CRC-16)
- Coprocessor providing long integer modular arithmetics (used in RSA and DSA)
- Hardware security components like sensors, filters and active shield

3 Cryptographic Module Port and Interfaces

The Apollo OS V4.03 on SLE66CX680PE restricts all information flow and physical access. The following physical ports and logical interfaces define all entry and exit points to and from the module.

3.1 Physical Ports

The module follows the standards “ISO 7816-1 Physical characteristics” and “ISO/IEC 7816-2 Dimensions and contact location for smart card with a contact interface.

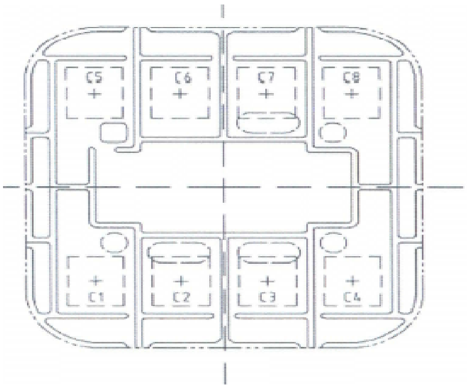


Figure 2 – Contact plate – physical ports

Contact No.	Assignments
C1	VCC (Supply voltage)
C2	RST (Reset signal)
C3	CLK (Clock signal)
C4	Reserved for Future Use
C5	GND (Ground)
C6	Not Used
C7	I/O (Input/Output)
C8	Reserved for Future Use

Table 3 – Contact plate pin list

The electrical signals and transmission protocols follow the ISO/IEC 7816-3 standard. The ranges for the electrical signals are 1.8 V or 3.0 V or 5.0 V for the supply voltage and 1 MHz to 5 MHz for the clock frequency.

3.2 Logical Interfaces

Apollo OS V4.03 on SLE66CX680PE provides services to operators in terms of an APDU command interface. The logical interface categories as defined by FIPS 140-2 map to the physical ports as follows:

Logical Interface	Physical Port(s)
Data input	C7
Data output	C7
Status output	C7
Control input	C2, C3 and C7
Power input	C5

Table 4 – Logical Interfaces vs. Physical Ports
(C1 is part of all ports, as it defines the reference level (ground) for all other signals)

The physical port C7 (I/O) belongs to four logical interfaces. Although these four logical interfaces share physical port C7, the information from the different interface categories is kept logically separate by the structure of APDU commands and response APDUs (RAPDUs) according to ISO/IEC 7816-4 standard.

In the structure of the APDU commands in general control input is comprised of a class byte (“CLA”), an instruction byte (“INS”), two parameter bytes (“P1” and “P2”), in some cases length of the command data field (“Lc”, 1 byte) and in some cases length of expected response data field (“Le”, 1 byte); data input is comprised of command data; data output is comprised of response data field, status output is comprised by two bytes status word (“SW”), parts of the ATR, and in some cases also response data field may contain status information (e.g. about the cause of a self-test error, as a response to Get Data command).

For security reasons, the module inhibits all data output via the data output interface when an error state is reached and while performing self-tests.

The concept of the OS is build on a three-fold process

1. receive command APDU
2. process the corresponding command
3. send response APDU

The command processes are executed in queue. The beginning of one process is depending on the success of the one before. No additional process can be executed while a command is send or processed, until the corresponding status word is received.

4 FIPS Approved Security Functions

The following table gives the list of FIPS Approved security functions that are provided by the Apollo OS.

Security Function	Description
TDES (Cert. #701)	Two-key/three-key Triple-DES (i.e. 2TDES/3TDES) encryption/decryption in CBC mode according to FIPS 46-3
HMAC (Cert. #464)	Keyed-Hash Message Authentication Code using SHA-1 (then MAC length at least 10 Byte) or SHA-256 (then MAC length at least 16 Byte)
SHS (Cert. #839)	Hashing according to FIPS 180-2 (i.e. SHA-1/SHA-256)
RSA (Cert. #406)	Signature generation/verification according to PKCS#1.5 (i.e. RSA 1024 bit)
RNG (Cert. #483)	Deterministic Random Number Generation according to FIPS 186-2
DSA (Cert. #306)	Signature generation/verification according to FIPS 186-2 (i.e. DSA 1024 bit)

Table 5 – FIPS 140-2 approved security functions

5 Non-Approved Security Functions

The following non-Approved security functions are implemented in Apollo OS V4.03 on SLE66CX680PE. These non-Approved security functions are disabled in FIPS approved mode.

Type	Algorithm
Symmetric	2TDES Retail MAC
Asymmetric	RSA acc. to PKCS#1 (1024 bit and 2048 bit), but with padding schemes other than defined by PKCS#1
	ECDSA acc. to FIPS 186-2 (but not validated)

Table 6 – Apollo OS Non-Approved security functions (not available in FIPS Approved mode)

6 FIPS Approved mode of operation

When switching to FIPS Approved mode is invoked (see following chapter to see how this is done), first the card performs a self-test, during which all approved cryptographic functions are tested. If a failure is detected during this self-testing process, all commands and cryptographic functions are blocked and no data can be accessed from the card and the module does not enter FIPS Approved mode. The only command still available in this case is a Get Data command, which can be used to output details about the error.

When self-tests mentioned before are successfully passed, FIPS Approved mode is finally activated, and the module enters a non authenticated state, in which most of the module's functions and services are not available to the operator. The module remains in this state until successful authentication of the operator in terms of a User PIN or a Crypto-Officer PIN.

Only FIPS Approved security functions can be run within FIPS Approved mode and any use of cryptographic functions will require successful verification of one of the upper mentioned PINs.

Only Crypto Officer can create or change CSPs. No key or other CSP (PIN) can be read by any means.

6.1 Invoking the FIPS Approved mode of operation

Activation of FIPS Approved mode requires sending FIPS Mode command. This command is only available in non-Approved mode, and it must be encrypted using SM encryption key and HMAC-protected using SM MAC key (these keys are system keys of non-Approved mode, see chapter 11.1 about system keys hereinafter), its structure is as follows:

CLA	A0h
INS	31h
P1	15h
P2	01h
Lc	01h
Data field	01h
Le	Empty

This command responds with SW 9000h, if FIPS mode is successfully entered. In case of a self-test failure while trying to enter FIPS mode it responds with SW 6701h. For more details please refer to Apollo OS 4.03 on SLE66CX680PE m1534-a13 user guide, chapter 4.33.

6.2 Indication of mode of operation

Besides from the response SW of FIPS Mode command[3], the command Get Data[4] can be used at any time to indicate the operational mode the module is currently in. Byte number 22 in the command response of Get Data (using parameters P1=01h and P2=0Eh) indicates the card mode, if it is 00h the card is in not in FIPS Approved mode, if it is 01h the card is in FIPS Approved mode.

[3] FIPS Mode command is available in Non-Approved mode only. After successful execution of FIPS Mode command the module is in FIPS Approved mode.

[4] Get Data command is available in Non-Approved mode and in FIPS Approved mode and can show – among other information – which mode the module is currently in.

7 Roles, Services and Authentication

7.1 Access controlled items (CPSs and user data)

FIPS system keys[5] **(CSPs):** These are special keys used by the Crypto Officer for administrative purpose, they are comprised of:

- FIPS SM encryption key: 3TDES key (168 bit) for data encryption/decryption in CBC mode (to protect confidentiality of command data and response data when using secure messaging)
- FIPS SM MAC key: HMAC with SHA-1 key (24 byte = 192 bit) for data authentication (to protect data authenticity of command data and response data when using secure messaging)
- FIPS key encryption key: 3TDES key (168 bit), which is used for entering FIPS system keys and user keys (see below for definition) in encrypted form (due to 3TDES used here the key transport method provides 112 bit strength)

Crypto Officer PIN and User PIN (CSPs): These are authentication data for Crypto Officer and User verification. They are stored in a dedicated storage area of EEPROM (together with the FIPS system keys). To make sure that only one operator can assume the Crypto officer role and only one operator can assume the User role (see following chapter “Roles”), each of the PINs must be known by one operator only.

User keys[6] **(CSPs):** These are keys, which may be stored in key objects of the file system. With these keys the approved functions of the module may be used on user data (see below). These keys are known and usable by Crypto Officer and User.

User data: This is information not belonging to CSPs stored in elementary files (EFs) and dedicated files (DFs) in the file system.

N.B. When the module is delivered to the customer, it already contains a set of initial FIPS system keys and initial values for Crypto Officer PIN and User PIN as securely

[5] There is a second, independent set of system keys for Non-Approved mode. In either mode the system keys of the other mode can’t be used or accessed in any way. This is to prevent an overlap of system key usage in Approved and Non-Approved mode.

[6] Switching between FIPS Approved mode and Non-Approved mode needs execution of FIPS Format command, which will zeroize the entire file system. This is to prevent an overlap of user key usage in Approved and Non-Approved mode.

configured by the vendor during module manufacturing and securely delivered to the customer (protected concerning confidentiality and integrity). These initial values may be changed prior to actual usage of the module, but the module also allows operation using the initial values of keys and PINs, and this security policy does not mandate that the initial values must be changed. As the set of initial FIPS system keys contains an initial FIPS key encryption key, the module can import keys in encrypted form immediately after being delivered to the customer.

7.2 Roles

Crypto Officer role: This role is authorized to use cryptographic services, random number generation and secure hashing. Crypto Officer role is also authorized to import keys into the module. The module allows only one operator to assume the Crypto Officer role, and the corresponding Crypto Officer PIN shall be known by one operator (i.e. the Crypto Officer) only.

User role: This role is authorized to use cryptographic services, random number generation and secure hashing. User role is not authorized to import keys into the module. The module allows only one operator to assume the User role, and the corresponding User PIN shall be known by one operator (i.e. the User) only.

Not authenticated role: Upon power-up or reset of the module an operator first assumes this role, until being successfully authenticated (and thus assuming Crypto Officer or User role). This role is authorized to read user data, but this role not authorized to use any of the cryptographic services, random number generation, secure hashing or to import keys into the module.

The module does not implement any maintenance interface, thus there is no maintenance role defined.

7.3 Identification and Authentication policy

The module performs authentication using PIN verification. There is one Crypto Officer PIN and one User PIN, each 8 byte long. Only if an operator presents the correct PIN value to the module, he will be authenticated as Crypto Officer or User, respectively. Due to the fact that the module allows only one operator to assume the Crypto Officer role and only one operator to assume the User role, this way an identity-based authentication of the operator is realized. Besides from that the authentication meets the following rules:

- Power-on or reset of the module puts it into not authenticated state.
- An unsuccessful PIN verification attempt puts the module into not authenticated state, regardless of the authentication state prior to the PIN verification attempt.
- A successful PIN verification puts the module into Crypto Officer authenticated state or User authenticated state, respectively, regardless of the authentication state prior to PIN verification. I.e. it is impossible that Crypto Officer and User are authenticated at the same time.

For Crypto Officer PIN and User PIN separate retry counters are managed by the module, which are limiting the maximum number of consecutive unsuccessful PIN verification attempts to seven (7), meeting the following rules:

- If the retry counter has reached seven, all further attempts to verify the corresponding PIN are rejected (the PIN is blocked), i.e. no more Crypto Officer or User authentication, respectively, is possible.
- Each unsuccessful PIN verification attempt increases the corresponding retry counter by one.
- A successful PIN verification resets the corresponding retry counter to zero.

Role	Type of Authentication	Authentication Data
Not authenticated	N/A	N/A
User	PIN verification	User PIN
Crypto officer	PIN verification	Crypto Officer PIN

Table 7 – Roles and Required Identification and Authentication

Authen-tication Mechanism	Strength of Mechanism
PIN verification	PIN 8 Byte long; 7 wrong attempts at most; worst case assumption that only decimal digits are used: ⇒ probability for a false acceptance in one attempt: $p_1 = 10^{-8} < 10^{-6}$ ⇒ probability for a false acceptance within a one minute period

	(7 attempts at maximum due to retry counter limitation): $p_7 = 1 - \frac{10^8 - 1}{10^8} \times \frac{10^8 - 2}{10^8 - 1} \times \frac{10^8 - 3}{10^8 - 2} \times \frac{10^8 - 4}{10^8 - 3} \times \frac{10^8 - 5}{10^8 - 4} \times \frac{10^8 - 6}{10^8 - 5} \times \frac{10^8 - 7}{10^8 - 6}$ $= 7 \times 10^{-8} < 10^{-5}$

Table 8 – Strength of Authentication Mechanisms

7.4 Access Control Policy

The services provided by the module to each role in terms of commands are specified in the table below (for a brief description of the services see table “CSP Access Rights within Services” hereinafter).

Role	Authorized Services (Commands)	
Crypto Officer role	Activate File Append Record Block command **Change System key** Create File Deactivate File Decrease Delete File **Delete Object** Directory Erase Binary External Authenticate FIPS Format FIPS Verify **FIPS Zeroization** Get Challenge Get Data Give Random Increase	Internal Authenticate Manage Security Environment PSO Hash PSO Compute Digital Signature PSO Verify Digital Signature PSO Encipher PSO Decipher **Put Data** Read Binary Read Record Reset Security State Select File Update Binary Update Record Write Binary Write Record Secure Messaging (usable with commands)
User role	Activate File Append Record Block command Create File Deactivate File Decrease Delete File Directory Erase Binary External Authenticate FIPS Format FIPS Verify FIPS Zeroization (**only in self-test error state**) Get Challenge Get Data Give Random Increase	Internal Authenticate Manage Security Environment PSO Hash PSO Compute Digital Signature PSO Verify Digital Signature PSO Encipher PSO Decipher Read Binary Read Record Reset Security State Select File Update Binary Update Record Write Binary Write Record Secure Messaging (usable with commands)
Not authenticated role	Directory FIPS Zeroization (**only in self-test error state**) FIPS Verify	Get Data Read Binary Read Record Select File

Table 9 – Roles and Authorized Services

Types of CSP access when performing the services are shown in the following table (for more details please refer to Apollo OS V4.03 user guide). There is no read access possible concerning keys and other CSPs (PINs). Keys and PINs can only be written, used and zeroized.

Service (Command)	Service description	Cryptographic keys and CSPs	Types of access (W=write, U=use, Z=zerioze)
Activate File	Activates an EF or a DF	-	-
Append Record	Appends records to a linear variable EF or updates the first record in a cyclic EF	-	-
Block command	Blocks a command	-	-
Change System key	Changes system keys, Crypto Officer PIN or User PIN	FIPS key encryption key	U
		FIPS System keys, Crypto officer PIN, User PIN	W
Create File	Creates a new file (MF, DF or EF)	-	-
Deactivate File	Deactivates an EF or a DF	-	-
Decrease	Decreases the content of a record in an EF	-	-
Delete File	Deletes an existing File (DF or EF)	-	-
Delete Object	Deletes an object	user keys	Z
Directory	Returns information about the files inside the current DF	-	-
Erase Binary	Erases the contents of a transparent (binary) file	-	-
External Authenticate	Performs an external authentication procedure (performs Approved security function TDES, RSA or HMAC)	user keys	U
FIPS Format	Zeroizes entire file system (containing MF, DFs, EFs and user key objects)	user keys	Z
FIPS Verify	Compares and verifies a given FIPS PIN with a stored FIPS PIN	Crypto Officer PIN, User PIN	U
FIPS Zeroization	Zeroize FIPS keys and CSPs	FIPS System keys, Crypto officer PIN, User PIN	Z
Get Challenge	Generates a random number and exports it to the outer world (performs Approved security function RNG)	-	-

Service (Command)	Service description	Cryptographic keys and CSPs	Types of access (W=write, U=use, Z=zerioze)
Get Data	Gets system information	-	-
Give Random	Loads an external random number to the module	-	-
Increase	Increments the contents of a record in the currently selected cyclic fixed EF	-	-
Internal Authenticate	Performs an internal authentication procedure (performs approved security function RSA, DSA, TDES or HMAC)	user keys	U
Manage Security Environment	Configures references to user keys (configures, which user keys will be used with the corresponding commands)	-	-
PSO Hash	Calculates a Hash (performs approved security function SHA-1, SHA-256 or HMAC)	user keys	U
PSO Compute Digital Signature	Generates a digital signature (performs approved security function RSA or DSA)	user keys	U
PSO Verify Digital Signature	Verifies a digital signature (performs Approved security function RSA or DSA)	user keys	U
PSO Encipher	Encrypts data (performs Approved security function TDES)	user keys	U
PSO Decipher	Decrypts data (performs Approved security function TDES)	user keys	U
Put Data	Storing/updating user keys	FIPS key encryption key	U
		user keys	W
Read Binary, Read Record	Reads data from a selected EF	-	-
Reset Security State	Resets the security status of the current DF	-	-
Select File	Selects a file (EF or DF)	-	-
Update Binary, Update Record	Updates data in a selected EF	-	-
Write Binary, Write Record	Initiates writing to an EF	-	-
Secure Messaging (usable with commands)	Decryption/encryption and/or MAC verification/generation (performs Approved functions TDES and/or HMAC)	FIPS SM encryption key, FIPS SM MAC key	U

Table 10 – CSP Access Rights within Services

Besides from access rights to services and CSPs as described above, the implemented APDU command interface has got the following properties:

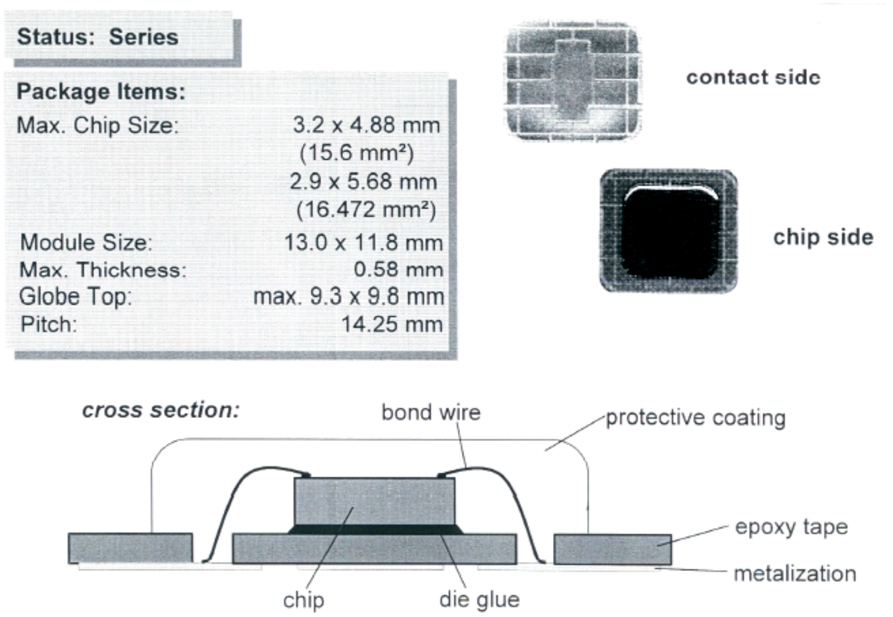
- The module does not provide a means to output keys or other CSPs.
- The module does not provide a bypass mode.
- The module does not provide a maintenance interface.
- The module does not provide a software/firmware loading.

8 Finite State Model

The Apollo OS V4.03 on SLE66CX680PE is designed using a finite state machine model that explicitly specifies every operational and error state. The cryptographic module includes Power on/off states, Cryptographic Officer states, User states, Self-test states and Error states. An additional document (Finite State model document) identifies and describes all the states of the module including all corresponding state transitions.

9 Physical Security

The platform for Apollo OS V4.03, the Infineon SLE66CX680PE m1534-a13 chip card controller is a single chip in a smart card micro-module package. The micro-module consists on one side of a metal contact plate providing ISO/IEC 7816 compliant contacts, on the other side there is a hard opaque epoxy resin cover. The micro-module finally will be embedded in a plastic card body during smart card manufacturing.



Status: Series

Package Items:	
Max. Chip Size:	3.2 x 4.88 mm (15.6 mm²) 2.9 x 5.68 mm (16.472 mm²)
Module Size:	13.0 x 11.8 mm
Max. Thickness:	0.58 mm
Globe Top:	max. 9.3 x 9.8 mm
Pitch:	14.25 mm

Figure 3 – Physical form factor (chip card micro-module)

9.1 Physical Security mechanisms as required by FIPS 140-2

The thermal black resin technology consists in an epoxy resin that is applied on top of the chip at the back side of the micro-module after the connection (bonding) of the chip to the back side of the contact plates has been completed. This resin is applied in a semi-liquid form and is polymerized by temperature. This resin is characterized by its black color and opacity that makes observation of the silicon chip impossible when the micro-module is finished (the substrate side of the chip is covered by the opaque metal contact plate).

The hardness of the resin and of the metal contact plate provides efficient mechanical protection and tamper evidence for the micro-module. Attempts to mechanically open it will first result in visible damage. A continued attempt of tampering, trying to get access to the chip's surface, will result in a non-functioning module by breaking of either silicon chip and/or bond wires with high likelihood, regardless whether the contact side or the side covered by the resin is subject to tampering.

For the finished smart card, i.e. a hard plastic card body with the embedded micro-module, the same is valid: tamper attempts will result in visible damage of the card body and/or the contact plate, and when trying to access the surface of the chip inside the card, again the micro-module has to be opened.

Physical Security Mechanism(s)	**Recommended Frequency of Inspection/Test**	**Inspection/Test Guidance Details**
Tamper evidence provided by hard opaque epoxy coating on chip	During smart card fabrication, when micro-modules are embedded into card bodies (During usage phase the epoxy coating is hidden in the embedded smart card and tamper evidence will be provided by the hard plastic card body instead.)	Check of epoxy coating, whether it is physically intact
Tamper evidence provided by metal contact plate	During usage phase, before inserting smart card into card reader	Check of contact plate, whether it is physically intact
Tamper evidence provided by plastic card body	During usage phase, before inserting smart card into card reader	Check of card body, in particular opposite to the contact plate, whether it is physically intact

Physical Security Mechanism(s)	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper resistance provided by combination of hard opaque epoxy coating, metal contact plate, and bond wiring	No inspection/test needed (attempts to mechanically open the module will result in visible damage and/or loss of functionality by breaking of either silicon chip and/or bond wires)	N/A

Table 11 – Inspection/Testing of Physical Security Mechanisms

9.2 Additional Hardware Security Mechanisms

The circuitry surface of the SLE66CX680PE chip is protected with an **active shield**. Attacks over the surface are detected when the shield lines are cut or get in contact to each other. The attempt to use an opened device will be detected.

All operating **signals are filtered** to prevent malfunction.

In addition the operating state is monitored with **sensors for the operating voltage, voltage glitches, clock frequency, and temperature**[7]. The chip falls into a defined secure state (chip internal reset) in case of a detected value outside the specified range violation.

The light intensity on the surface of the security controller is monitored by **light sensors**. The light sensors are hidden by the top metal layers of the circuit and cannot be distinguished by simple observation. A security reset is activated if a light attack is detected.

[7] Although the IC includes sensors concerning voltage and temperature, EFP/EFT according to FIPS PUB 140-2 is not claimed for this module.

10 Operational Environment

The Operational Environment requirement section of FIPS 140-2 is not applicable for Apollo OS V4.03 on SLE66CX680PE, as Apollo OS is a self-contained firmware stored in the ROM of SLE66CX680PE IC and cannot be dynamically written or modified during execution.

Furthermore Apollo OS is not based on some operating system, but it is an operating system by itself (still it can’t be modified, as all executable code is located in ROM and as the file system (made up by DFs and EFs) may only contain user data, but no executable code.

11 Cryptographic Key Management

11.1 System Keys and PINs (CSPs)

The cryptographic module includes system keys and PINs for card administration purposes. There are two sets of system keys and PINs, one set that is used in FIPS Approved mode of operation (i.e. FIPS system keys and Crypto Officer PIN and User PIN), and a separate set that is used in Non-Approved mode. In either mode, there is no way to use or access the system keys or PINs of the other mode, to prevent any overlap of usage of CSPs in the two modes. The FIPS system keys are comprised of:

- FIPS SM encryption key: 3TDES key (168 bit) for data encryption/decryption in CBC mode (to protect confidentiality of command data and response data when using secure messaging)
- FIPS SM MAC key: HMAC with SHA-1 key (24 byte = 192 bit) for data authentication (to protect data authenticity of command data and response data when using secure messaging)
- FIPS key encryption key: 3TDES key (168 bit), which is used for entering FIPS system keys and user keys in encrypted form (thus the key transport method provides 112 bit strength)

N.B. When the module is delivered to the customer, it already contains a set of initial FIPS system keys and initial values for Crypto Officer PIN and User PIN as securely configured by the vendor during module manufacturing and securely delivered to the customer (protected concerning confidentiality and integrity). These initial values may be changed prior to actual usage of the module, but the module also allows operation using the initial values of keys and PINs, and this security policy does not mandate that the initial values must be changed.

11.2 User Keys (CSPs)

The Crypto Officer, after being successfully authenticated, may enter user keys into objects stored in the file system. The keys supported are:

- HMAC user keys: HMAC with SHA-1 keys (minimum 10 byte = 80 bit) and HMAC with SHA-256 keys (minimum 16 byte = 128 bit) for HMAC generation/verification

- RSA private/public user keys: RSA (1024 bit) private and/or public keys for signature generation/verification according to PKCS#1 V1.5
- DSA private/public user keys: DSA (1024 bit) private and/or public keys for signature generation/verification
- TDES user keys: 2TDES keys (112 bit) or 3TDES keys (168 bit) for encryption/decryption in CBC mode

11.3 Key Generation

The module does not provide key generation functionality.

11.4 Key Entry and Output

The module implements key entry with keys being entered securely in encrypted form (3TDES-encrypted with the FIPS key encryption key). During key entry also an EDC (16 bit CRC defined in ISO/IEC 13239) generated over the key data is transmitted together with the corresponding key, and key entry is only accepted when the entered EDC matches the entered key data. Furthermore, commands used for key entry (CHANGE SYSTEM KEY for system keys and PUT DATA for user keys) are protected by secure messaging, in particular these are HMAC-protected. If the HMAC does not match the data field, the command is not executed, i.e. key entry is denied.

Key output from the module is impossible (command interface and access control prevent this).

N.B. As the set of initial FIPS system keys (see chapter “System Keys and PINs” above) contains an initial FIPS key encryption key, the module can import keys in encrypted form immediately after being delivered to the customer.

11.5 Key Storage

The FIPS system keys and the Crypto Officer PIN and the User PIN are stored in a dedicated space of the EEPROM. User keys (if any) are stored in key objects in the file system (different part of EEPROM).

Initial values for the FIPS system keys and the Crypto Officer PIN and User PIN are written to the module during production and these values are securely transmitted to the

Crypto Officer, who is able (but not required) to change the values from the initial ones to their own values.

11.6 Key Zeroization

The cryptographic module provides two commands with the capability to overwrite all bytes of plaintext cryptographic keys and other critical security parameters within the module with the value FFh.

The first command is FIPS Format, which will overwrite the entire file system space in EEPROM and therefore zeroize all user keys stored in the file system (if any).

The second command is FIPS Zeroization, which will overwrite the FIPS System keys and Crypto Officer PIN and User PIN with byte values FFh.

After zeroization the module automatically switches to Non-Approved mode.

Once FIPS system keys and User PIN and Crypto Officer PIN have been zeriozed, it is impossible to switch back to FIPS Approved mode again.

12 Self-Tests

The Apollo OS V4.03 on SLE66CX680PE performs the following self-tests to ensure that the module works properly:

Self-test	Execution time
Cryptographic algorithm test (known-answer tests for HMAC, TDES, SHA, RSA, and RNG, pair-wise consistency test for DSA)	At power-up or after a reset
Software/firmware integrity test	At power-up or after a reset
Pseudo Random Number Generator test (known-Answer Test for deterministic RNG output)	At power-up or after a reset
Critical functions test: testing for hardware security error (e.g. due to a breach of the active shield of the hardware)[8]	At power-up or after a reset
Critical functions test: testing hardware sensors by calling corresponding hardware functionality[8]	At power-up or after a reset
Continuous random number generator test.	Conditional, each time a random number is requested

Table 12 – Self-tests

12.1 Power-up Self-Test Execution

After Apollo OS is powered up or has been reset and before executing any cryptographic operation, the module enters the self-test state and performs the entire cryptographic algorithm and software integrity self-tests as required by FIPS 140-2.

These tests are conducted automatically as part of the normal functions of the cryptographic module. They do not require any additional operator intervention.

After a reset, power-up self-tests are executed after the first APDU command is received, but before this command is executed[9]. The cryptographic module start-up

[8] The critical functions tests as defined here will make sure that at power-up or after a reset physical modifications of the hardware will be detected. This is to strengthen all functionality of the module that operates on keys and other CSPs, by making sure that those cannot be compromised by a physical attack on the IC platform.

[9] It is not possible to perform the self-tests directly upon a reset, as according to ISO/IEC 7816-3, ch. 5.3.2 and 5.3.3 the module has to respond with the ATR (Answer To Reset) in a certain limited time, which is too short to complete the tests. After reception of a APDU command ISO/IEC 7816-3 allows a longer time for card processing until the response has to be send back, therefore self-tests are performed at this time and

process has been designed in such a way that it cannot be bypassed. This enforces the execution of self-tests before allowing any use of the module, thus guaranteeing a secure execution of the module's cryptographic services.

If and only if all self-tests are passed successfully, the cryptographic module performs the command procedure according to the first APDU (received before power-up self-tests started) and returns the corresponding response and status word via the data output interface and status output interface (and then further incoming APDU commands are processed). All data output via the output interface is inhibited while any power-up and conditional self-test is running.

Resetting the cryptographic module provides a means by which the operator can perform the power-up self-tests on demand.

12.2 Conditional Self-Tests Execution

The module implements the Continuous Random Number Generator (CRNG) self-test as specified in FIPS 140-2 for the implemented Approved RNG.

As during start-up of the module the Approved RNG is initialized with a seed generated by the physical RNG provided by SLE66CX680PE controller, the module furthermore implements the Continuous Random Number Generator (CRNG) self-test as specified in FIPS 140-2 for the physical RNG.

12.3 Self-Test Failure

If any start-up self-test or conditional self-test fails the module enters a self-test error state. No cryptographic operations can be processed and no data can be output via the data output interface, while the module is in the self-test error state. This is achieved by blocking all subsequent commands (status word 6701h will be returned without executing the corresponding command procedure), except for the following three commands, which are still allowed in self-test error state:

- Get Data (with P1=01h and P2=7Fh): This specific command is used to return an indicator describing the cause of the failure; this command can be performed by all

have to be successfully passed before any command would be executed or any related cryptographic service would be called.

roles. It is explicitly allowed in self-test error state to prevent that retrieving status information about the error cannot be retrieved by the operator.

- FIPS Format command: This command is used to zeroize file system data and to exit FIPS Approved mode. It is explicitly allowed in self-test error state to prevent that zeroization of file system data could be blocked by persistent self-test errors.
- FIPS Zeroization: this command is used to zeroize all FIPS System keys and Crypto Officer PIN and User PIN. It is explicitly allowed in self-test error state to prevent that zeroization of FIPS System keys, Crypto Officer PIN and User PIN could be blocked by persistent self-test errors.

The module can be recovered from a self-test error state by performing a reset. If all self-tests pass successfully after the reset, the module will be fully operational again. If after the reset the error persists, the module will re-enter self-test error state.

13 EMI/EMC

The Apollo OS V4.03 on SLE66CX680PE m1534-a13 cryptographic module has been successfully tested by Hermon Laboratories Ltd. to meet the EMI/EMC requirements according to FCC 47 CFR part 15:2006, subpart B, class B, and received the corresponding certificate of conformity No SCCEMC_FCC.17997C.

14 Mitigation of Other Attacks

Other Attack	Mitigation Mechanism	Specific limitation
Fault attack on cryptographic calculations	When a cryptographic calculation (e.g. an encryption) is performed inside the module, additionally the inverse cryptographic calculation (e.g., the corresponding decryption) is performed as a check operation. If the initial input cannot be restored, a fault attack on the cryptographic calculation is assumed and the module zeroizes all RAM contents and enters an infinite loop (until it is powered off or reset). When a hash calculation is performed, additionally the same hashing operation is performed a second time as a check operation. If the two resulting hash values differ, a fault attack on the hash calculation is assumed and the module zeroizes all RAM contents and enters an infinite loop (until it is powered off or reset). By doing so, it is prevented that the module will use or output results of faulty cryptographic operations. This way, among other attacks, a DFA (Differential Fault Attack) is mitigated.	None
SPA/DPA/ EMA/DEMA	To mitigate all side-channel attacks exploiting information leakage in power consumption or electromagnetic emanation of the chip, Apollo OS activates the corresponding hardware countermeasures of SLE66CX680PE (e.g. CURSE to randomize the power consumption and therefore also the electromagnetic emanation of the chip). Furthermore SLE66CX680PE employs chip-individual and dynamic memory and bus encryption[10], which makes interpretation of power consumption or electromagnetic emanation signals resulting from memory access or bus data transfer more difficult (as the attacker cannot predict the internally used values).	None

Table 13 – Mitigation of Other Attacks

[10] This encryption is not using an Approved algorithm.

15 Design Assurance

15.1 Configuration Management

The Apollo OS was designed and developed using a configuration management system that is clearly ruled and operated.

The definition methods, mechanisms and tools that allow identifying and placing under control all the data and information are specified in the “Apollo OS configuration management” document.

15.2 Delivery and Operation

The “Apollo OS delivery and operation” documentation and the “Apollo OS User Guide” define and describe the steps necessary to deliver and operate Apollo OS securely.

15.3 Guidance Documents

“Apollo OS User Guide” document was designed to allow a secure operation of Apollo OS by its users as defined in the ‘Roles, Services and Authentication’ chapter and in the scope of the SP boundaries.

16 Acronym Definitions

2TDES	Two-key Triple Data Encryption Standard (using 112 bit key)
3TDES	Three-key Triple Data Encryption Standard (using 168 bit key)
CRC	Cycling Redundancy Check
CRNG	Continuous Random Number Generator (test)
DES	Data Encryption Standard
DF	Dedicated File (directory in the file systems, containing EFs and/or DFs)
DEMA	Differential Electromagnetic Analysis
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
EF	Elementary File (file in the file system, containing data)
EEPROM	Electrically Erasable Programmable Read Only Memory
EMA	Electromagnetic Analysis
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
HMAC	Keyed-hash Message Authentication Code
ICC	Integrated Circuit Card
ISO	International Standards Organization
MF	Master File (root directory of the file system, containing EFs and/or DFs)
MAC	Message Authentication Code
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read only Memory
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SM	Secure Messaging
SPA	Simple Power Analysis
TDES	Triple Data Encryption Standard