Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 for Renesas XMobile Card Module

Security Policy
FIPS 140-2 Level 2

Date: 22 March 2007
Version: 6.0

TABLE OF CONTENTS

1 INTRODUCTION 4

2 HITACHI PRODUCT OVERVIEW 5

2.1 REFERENCES 6
2.2 GLOSSARY OF TERMS 7

3 CRYPTOGRAPHIC MODULE SPECIFICATION 8

4 SECURITY LEVEL 10

5 MODES OF OPERATION 11

5.1 HOW TO PUT THE MODULE IN THE APPROVED MODE 11
5.2 HOW TO VERIFY THAT THE MODULE IS IN APPROVED MODE 11

6 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES 13

6.1 PHYSICAL INTERFACES 13
6.2 LOGICAL INTERFACES 14
6.2.1 Platform Logical Interface 14
6.2.2 Logical Interface for Keys and CSPs 14

7 ROLES, SERVICES, AND AUTHENTICATION 15

7.1 ROLES 15
7.2 SERVICES 17
7.2.1 Approved Security Functions 17
7.3 AUTHENTICATION POLICY 20
7.3.1 Cryptographic officer authentication 20
7.3.2 Cardholder authentication 21
7.4 ACCESS CONTROL POLICY 23
7.4.1 Introduction 23
7.4.2 Security Rules 23
7.5 CRITICAL SECURITY PARAMETERS 25
7.6 PUBLIC KEYS 27

8 FINITE STATE MODEL 28

9 PHYSICAL SECURITY 29

10 OPERATIONAL ENVIRONMENT 30

11 CRYPTOGRAPHIC KEY MANAGEMENT 31

11.1 RANDOM NUMBER GENERATORS 31
11.2 KEY GENERATION 32
11.3 KEY ENTRY AND OUTPUT 32
11.4 KEY STORAGE 33
11.5 KEY ZEROIZATION 33

12 ELECTROMAGNETIC INTERFERENCE/COMPATIBILITY (EMI/EMC) 35

13 SELF-TESTS 36

13.1 POWER-UP SELF-TESTS 36
13.2 CONDITIONAL SELF-TESTS 37
13.3 ERRORS WHILE PERFORMING TESTS 37

14 MITIGATION OF OTHER ATTACKS 38

TABLES

Table 1 - Reference documents 6
Table 2 – Glossary of Terms 7

Table 3 – Cryptographic Module details 9
Table 4 – Security Level of Tested Areas 10
Table 5 – Physical Interfaces 13
Table 6 – Logical Interface Structure Regarding FIPS 140-2 14
Table 7 – Cryptographic Module roles description 16
Table 8 – Services provided by the Cryptographic Module 19
Table 9 – Cryptographic Officer Authentication mechanism 20
Table 10 – C.O. Authentication Security rules 21
Table 11 – C.O. Authentication Mechanism Strength 21
Table 12 – Cardholder authentication mechanism 22
Table 13 – Cardholder Authentication security rules 22
Table 14 – Cardholder Authentication Mechanism Strength 22
Table 15 – Access Policy Rules 23
Table 16 - Services restriction regarding roles 24
Table 17 – Sensitive Data Description and Evolution 26
Table 18 – Public Keys Description and Evolution 27
Table 19 - CM Physical and Electrical Characterstics 29

FIGURES

Figure 1 – The Cryptographic Module 4
Figure 2 – Cryptographic Module roles 15
Figure 3 - Key Management 31

1 Introduction

This Security Policy describes the Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 Java Card Platform for Renesas XMobile Card Module. It identifies the module that successfully passed the validation and describes software and hardware features. It defines the roles and services provided to Card Issuers and Applet Users. It also describes the algorithms implemented following the standards recommended by FIPS for power-up and conditional self-tests.

The cryptographic module is a single chip multi-application cryptographic Java Card module specially designed for XMobile cards loaded with the One-Passport PKI Card Application Java Card applet.

Two versions of Card AP are validated: version 03-00 and version CX 03-00. This second version is version 03-00 (base product) augmented with one APDU command "DATA INITIALIZE" for specific customer needs.

The Cryptographic Module offers cryptographic services such as:

- T-DES encryption and decryption in CBC mode with no padding
- 1024-bit RSA key generation with strong prime numbers (ANSI X9.31)
- RSA CRT signature using PKCS#1 automatic padding

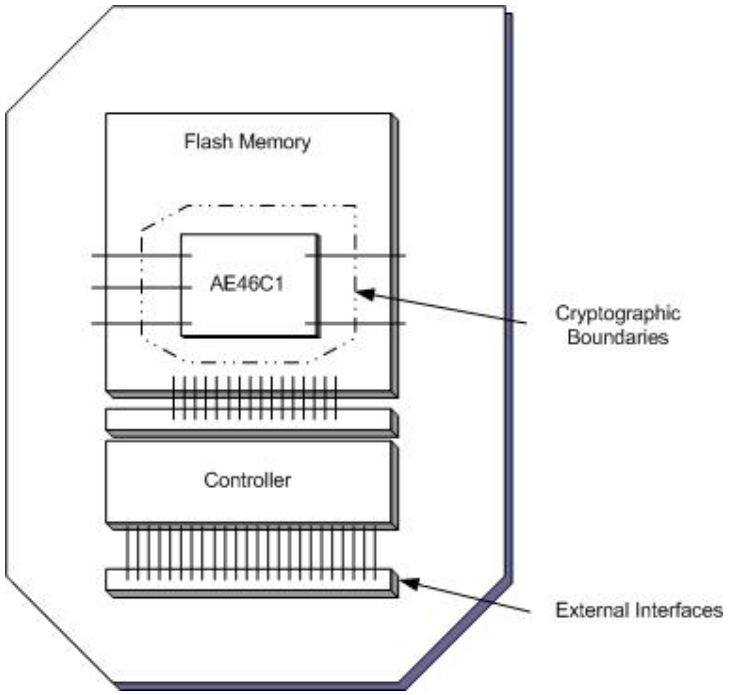

Figure 1 – The Cryptographic Module

2 Hitachi Product Overview

In recent years, mobile devices are getting important in order to pursue customers business. As working styles become increasingly diversified, such as telecommuting and use of satellite offices, the need for remote access from places outside offices is increasing.
The One-Passport PKI product solution provides remote access environment through Internet for general commercial use by private companies. Under the One-Passport PKI environment, employees such as sales persons can access to their corporate mail servers and other corporate information from satellite office, their home and other places outside office. In order to avoid unexpected leakage of information during such remote access, the One-Passport PKI solution uses VPN technique and PKI based authentication method.

The One-Passport PKI solution consists of the following items:

- One-Passport PKI Card which is the validated Cryptographic Module (Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 for Renesas XMobile Card Module)
- One-Passport PKI PC Software
- One-Passport PDA Software

The cryptographic module provides users ways to manage and protect applications such secure emails, smart logon, connection to web servers… the Cryptographic Module offers means to manage secure access to remote servers, unlock workstations and exchange signed information between users.

The XMobile card module is a smart card with flash memory and SD card interface. It is available for both PC and PDA with a SD card slot or an external reader/writer. The loaded One-Passport PKI Card Application applet can store digital certificates on its smart card area so that it can be used for external applications on PC or PDA.

The corresponding mirror application for PC is software, which works on Windows 2000 and Windows XP. OnepassportCSP, which is a constituent element of the One-Passport PC Software, supports the standard security interface both Crypto API and PKCS#11. Using the PC software, the user application such as Internet Explorer, VPN applications, etc. can access the XMobile Card. The PC software application has management functions such as changing User PIN information of the XMobile card and inserting and deleting digital certificates into the XMobile card using the management function.

The corresponding mirror application for PDA provides the PKCS#11 interface for VPN applications, which works on Pocket PC 2003 operating system in collaboration with Card AP. VPN applications access cards by using PKCS#11 interface of the PDA software application. The PDA software has no cryptographic engine, but enables cryptographic functions of the XMobile card. The PDA software also has management function such as changing User PIN on user's PDA.

2.1 References

Reference	[Ref]
Global Platform - Card Specification http://www.globalplatform.org/showpage.asp?code=cardspec	[GP]
Java Card http://java.sun.com/products/javacard/specs.html	
- Application Programming Interface	[JCAPI]
– Virtual Machine Specification	[JCVM]
– Runtime Environment	[JCRE]
FIPS - Federal Information Processing Standards http://csrc.nist.gov/publications/fips/	
– FIPS140-2	[FIPS140-2]
– FIPS140-2 Implementation Guide	[FIPS140-2IG]
– FIPS140-2 Derived Test Requirement	[FIPS_DTR]
– FIPS_PUB_46-3 - DES Implementation	[FIPS46-3]
– FIPS_PUB_180-2 – SHA	[FIPS180-2]
– FIPS PUB 81 – DES Modes of Operation	[FIPS81]
ANSI X9.31 – Random Number Generator http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E31%2D1998	[X9.31]
PKCS #1: RSA Cryptography Standard ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf	[PKCS1]

Table 1 - Reference documents

2.2 Glossary of Terms

The following table provides definitions of common acronyms used throughout this security policy.

Abbreviation	Definition
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
Card AP	One-Passport PKI Card Application
CLK	Clock
CM	Cryptographic Module
CPLC	Card Production Life Cycle
CSP	Critical Security Parameter
DES/T-DES	Data Encryption Standard/Triple DES
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
EEPROM	Electrically Erasable Programmable Read Only Memory
FIPS	Federal Information Processing Standards
GP	Global Platform
IC	Integrated Circuit
ICC	Integrated Circuit Card
ISD	Issuer Security Domain
ISO	International Organization for Standardization
JCRE	Java Card Runtime Environment
KAT	Known Answer Test
MAC	Message Authentication Code
MONOS	Metal Oxide Nitride Oxide Silicon
OPEN	Open Platform Environment
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RFU	Reserved for Future Use
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
RST	Reset
SD	Secure Digital
SPA	Simple Power Analysis
VPN	Virtual Private Network

Table 2 – Glossary of Terms

3 Cryptographic Module Specification

The validated cryptographic module is the Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 for Renesas XMobile Card Module.

This CM is the combination a firmware – One-Passport PKI Card Application Java Card applet running on a Java Card Operating System - that implements FIPS approved cryptographic functions and a state-of-the-art secure Single Chip Silicon Hardware. A single version of the Card AP will be loaded on each product, and a single instance of each applet will be installed before Card is issued to the end user.

The security requirements specified in the FIPS140-2 standard relate to the secure design and implementation of the cryptographic module.
The CM offers cryptographic services to cryptographic officers and users through its role-based authentication policy as described in the dedicated section above.

No other applet than the Hitachi One-Passport PKI Card Application is present in the module for this validation, however additional applets can be loaded anytime at post issuance (SECURED state). Such addition would require entering into a FIPS validation process.

Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 for Renesas XMobile Card Module	
Description	Java Card Applet that runs on Java Card 2.1.1 and Global Platform 2.1 compliant Operating System. Full multi-application support including post-issuance loading and deletion of FIPS-approved applets.
Firmware Version	Applet: Application Program Product C-9550-702 One-Passport PKI Card Application version 03-00 and CX 03-00 OS: OS755 version 2.4.7
Hardware Version	AE46C1 Version 0.1
Approved Algorithms and Operation Modes	Approved 1024-bit RSA algorithm: - RSA PKCS#1 sign/verify with private CRT key Other approved algorithms: - SHA-1 hashing - T-DES encrypt / decrypt in CBC mode, no padding (*Key Wrapping Only; key establishment methodology provides 80-bits of encryption strength*) Approved Random Number Generator: - ANSI X9.31 Deterministic RNG ([X9.31]), On-board RSA CRT Key Pair Generation (1024-bit key length) Non-Approved algorithm used in Approved mode: - RSA encrypt / decrypt (*Key Wrapping Only; key establishment methodology provides 80-bits of encryption strength*)

Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 for Renesas XMobile Card Module	
Non approved Algorithms and Operation Modes	Any FIPS-Approved applet that uses the following algorithms will behave in a non Approved mode of operations: - Raw RSA (no pad), - RSA (Cipher only) with ISO9796 padding, - DES in ECB and CBC modes, with ISO9797 m1/m1 padding; non compliant - T-DES in ECB and CBC modes, with ISO9797 m1/m2 padding; non compliant
Card Content Management System	Global Platform compliant Java Card package / applet load and delete through selected security domain. Full Global Platform functionality is supported, including delegated management and DAP verification.
Memory Management	Full reclaim of memory on package / applet deletion and memory de-fragmentation allowing full use of all available free memory.

Table 3 – Cryptographic Module details

The physical component of the cryptographic module is the assembly of an IC chip (Renesas AE46C1) protected by a hard opaque tamper-evident resin encapsulant.

The Renesas AE46C1 is ideally suited for high security applications, in which security has been built in from the start, to form an integral part of the whole Cryptographic Module design concept. The whole development process is constantly reviewed in order to maximize the overall security package. The AE46C1 can be delivered as pre-packaged modules ready for embedding into an XMobile Card.

Many security features such as integrated sensors, distributed layout, random number generation, DES engine and power analysis attack protection are all included providing a strong on-chip hardware security structure.

Uniquely, Renesas chips are fabricated using a MONOS (Metal Oxide Nitride Oxide Silicon) EEPROM structure. MONOS advantages compared to standard EEPROM structures are high resistance to radiation disturbance, high endurance and reliability.

A high performance modular multiplication co-processor is complementary to the design concept, and ensures final operating system efficiency, application integrity and performance that meet tomorrow's needs today.

The AE46C1 has been validated against the Common Criteria scheme (BSI-DSZ-CC-0229-2004 certificate).

4 Security Level

The Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 for Renesas XMobile Card Module has been successfully tested against FIPS140-2 requirements and meets an overall security level 2. The following areas have been independently rated.

Tested Areas	Security Level
Cryptographic Module Specification	2 overall
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	3
Operational Environment	NA
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 4 – Security Level of Tested Areas

5 Modes of operation

The Cryptographic Officer, see Roles section, is responsible for initializing the module in the approved mode of operation and for ensuring that the module:

- only loads FIPS validated versions of Card AP
- only loads FIPS-approved Keys

This applies to both versions of the Card AP.

5.1 How to put the module in the approved mode

The operator must perform one of the following actions to ensure that the module is in the approved mode of operation:

- Select the ISD and start a GP Secure Channel with Integrity option
  - Send SELECT with the AID of the Card Manager (ISD applet)
  - Send INITIALIZE UPDATE command
  - Send EXTERNAL AUTHENTICATE command with the C-MAC flag set
- Select the Hitachi One-Passport PKI Card Application
  - Send SELECT with the AID of the Card Application

The module is not in an approved mode of operation if any of these actions failed (card goes mute or returns an error status word).

The operator will communicate with the ISD being the Cryptographic Officer. Complementarily, the operator will communicate with the Hitachi One-Passport PKI Card Application being any other role.

5.2 How to verify that the module is in approved mode

The operator needs to perform the following tests to ensure that the module is in approved mode of operation:

1. Send GET DATA command with the CPLC flag set and verify that the returned data include the following information:

Data Element	**Length**	**Die Individual Value or default** *(x=any)*
IC fabricator	2	'3060'
IC type	2	'4643'
Operating system identifier	2	'0755'
Operating system release date	2	'xxxx' In the format specified by Visa GP
Operating system release level	2	'0246'
IC fabrication date	2	'xxxx'
IC serial number	4	'xxxx'
IC batch identifier	2	'xxxx'
IC module fabricator	2	'xxxx'
IC module packaging date	2	'xxxx'

Data Element	Length	Die Individual Value or default *(x=any)*
ICC manufacturer	2	'3060'
IC embedding date	2	'0000'

2. Send GET DATA command without including a MAC and verify that the returned status indicates that a MAC is required in the current Secure Session.

3. Send GET VERSION INFO command and check that returned version-revision is

   - '0300' for the version 03-00 of the Card AP

OR

   - '034A' for the version CX 03-00 of the Card AP

Note: *Test 2 is done if the currently selected application is the ISD and test 3 is done if the currently selected application is the Hitachi One-Passport PKI Card Application.*

6 Cryptographic Module Ports and Interfaces

This section describes the physical and logical interfaces.

The Cryptographic Module has:
- The four FIPS 140-2 required logical interfaces (data in/out, control in, status output) are provided,
- Three associated physical interfaces.

These interfaces are provided identically by both versions of Card AP.

6.1 Physical Interfaces

The physical interfaces of the Cryptographic Module depend on the physical characteristics of the module itself.
Renesas XMobile module provides the following interfaces:

Interface	Description
RST	Reset signal
I/O	Input / Output
CLK	Clock signal
PWR	Power
GRD	Ground

Table 5 – Physical Interfaces

6.2 Logical Interfaces

6.2.1 Platform Logical Interface

The following logical interface is considered as an entry point to the Java Card platform:

1. External operators send APDU structured messages following ISO7816-4 standard.

Note: *Logical output interface is inhibited when an error state exists, during self-tests, and while performing key generation or key Zeroization.*

Information crossing the interface is structured as defined in the FIPS140-2 and ISO7816-4 standards, with the available logical interfaces as follows:

Logical Interfaces	**APDU**	**Physical Interfaces** *(see Table 5 – Physical Interfaces)*
Structure	ISO7816-4 standard	*Not Applicable*
Input Data Interface	APDU data field	I/O wire
Output Data Interface	APDU data field	I/O wire
Control Input Interface	APDU fields : - CLA - INS - P1 - P2 - Le	I/O, CLK, and RST wires
Status Output Interface	Status Words (SW1 SW2)	I/O wire

Table 6 – Logical Interface Structure Regarding FIPS 140-2

6.2.2 Logical Interface for Keys and CSPs

The Cryptographic Module enforces encrypted transfer of Issuer Security Domain Keys through a logical GP Secure Channel following the [GP] 2.1 standard.

The One-Passport PKI Card Application applet provides cryptographic key components and CSPs. The PC or PDA software using the cryptographic module must enter and output any private key encrypted after establishing a Card AP Secure Communication with the CM. Other CSPs (authentication data and public keys) can either be entered in plaintext or encrypted. No output of any authentication data is possible.

7 Roles, Services, and Authentication

The cryptographic module supports authorized roles (Cryptographic Officer and Cardholder) for operators and corresponding services within each role. Authorized operators are authenticated within the cryptographic module to access services part of the module access control policy. The CM verifies that the operator is authorized to assume the requested role and perform the services within the role.

7.1 Roles

The CM is interfacing with a cryptographic officer responsible for card content management including applet loading, initialization and deletion. The CM also interfaces with a User (Cardholder) and provides services related to the One-Passport PKI Card Application.

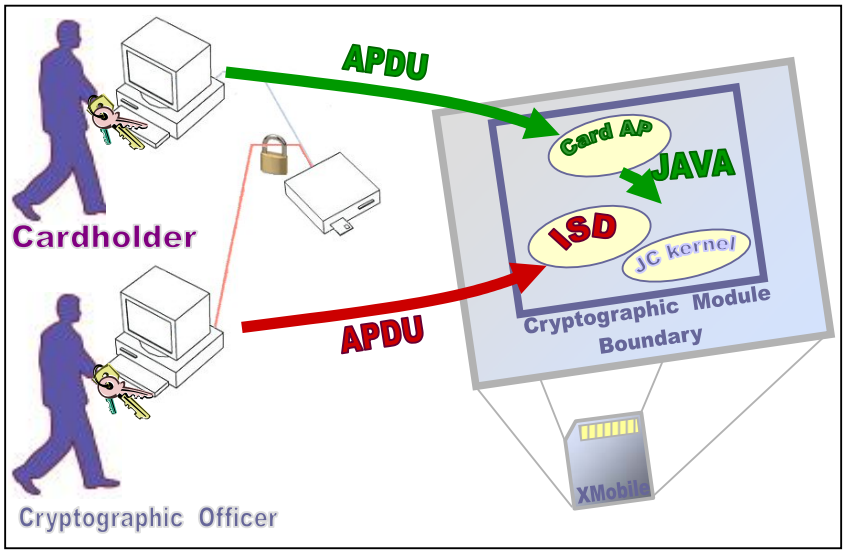

Figure 2 – Cryptographic Module roles

Roles are the same for both versions of Card AP.

Role	Description
Cryptographic Officer Role	
Cryptographic Officer	**External operator** who knows a **T-DES key set** to open a **GP Secure Channel** ([GP] commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATE) with the Issuer Security Domain (ISD). Per the GP standard the Cryptographic Officer is responsible for: - Generating and loading the initial key sets for himself and the Applet Provider, - Enforcing standards and policies for Applet Provider governing all aspects of Applications to be provided to the Card Issuer or operated on the Card Issuer's cards, - Working with Applet Provider to create and initialize Security Domains other than the Issuer Security Domain (ISD), - Determining policy with regards to card and card content Life Cycle management, Application privileges, and other security parameters, - Managing the application code loading and installing on Post-Issuance basis, and - Performing cryptographically authorized load, install, and extradition (See [GP] Section 6.4.3 for a description).
User Role	
Cardholder	Operator who knows all the PINs stored in the module. The Cardholder knows an initial PIN and is able to store additional PINs. Each PIN or PIN combination allows Cardholder to: - Control PINs (store, verify, update…) - Control data (store, read, remove…) - Control Key Pairs (store, output, use for signature…) - Control root certificates (store, read, associate…) The PIN Authentication command (Check PIN) and the other services are provided by the One-Passport PKI Card Application.
No Role	
No-role	User who does not know any secrets related to the One-Passport PKI Card Application or the ISD. This non-authenticated user can access services provided by Card AP and the ISD that do not require any prior authentication.
Maintenance Role	
None	The CM does not support any maintenance role.

Table 7 – Cryptographic Module roles description

7.2 Services

This section provides services that can be performed by the cryptographic module. Services interfaces are APDU commands with data in inputs and data out outputs. All services are provided in an approved mode of operation.

Self-tests services are described in the dedicated section below. Show status and Approved security functions are listed here below.

The distinction between the two versions of Card AP is made from the delivered services as follows:

- Card AP version 03-00 is the base product
- Card AP version CX 03-00 provides, in addition to base product, one APDU command that is DATA INITIALIZE

7.2.1 Approved Security Functions

Note: *the following table contains references to the following terms, described as:*

Super PIN	*Group of PINs which "Super" flag has been set by the Cardholder. Super PIN verification allows Cardholder to access restricted services.*
Permission	*Combination of 15 PINs (all owned by the Cardholder) associated to Card AP Keys and PINs as access control conditions.*

ISD related commands	
Get Status	Operator can retrieve Life Cycle status information of the ISD, Executable Load File, Executable Module, Application or Security Domain. No CSPs can be read using this service.
Get Data	Operator can retrieve public data from the ISD. No CSPs can be read using this service.
Initialize Update	CO can initiate the initiation of a GP Secure Channel session, setting key set version and index.
External Authenticate	CO can open a GP Secure Channel with the ISD in order to communicate with it in a secure and confidential way.
Load	CO can transfer a Load File to the CM.
Delete (applet)	CO can delete a uniquely identifiable object such as an Executable Load File (library), an Application (applet), optionally an Executable Load File and its related Applications.
Select	Operator can select an application.
Set Status	CO can modify the module Life Cycle State or the Application Life Cycle State.
Install	CO can initiate or perform the various steps required for Module Content management.
Put Key	Regarding ISD keys, CO can either: - Replace an existing ISD key with a new key - Replace multiple existing ISD keys with new keys - Add a single new ISD key - Add multiple new ISD keys - Zeroize ISD Keys
Delete (key)	CO can delete a uniquely identifiable ISD object such as a key. This service is also used for ISD keys zeroization.
Store Data	CO can transfer data to the ISD.

Card Application management related commands	
Initialize	To set Card AP PIN properties (Card AP Super PIN), number of times the private RSA keys output is possible (Backup), and the version number. Requires prior successful Super PIN verification.
Card Application public commands	
Get Version Info	Get the version number of the current installed and selected Card Application.
Get Data Area Number	To get the data area number, key pair number, Root certification number.
Data Initialize	**ONLY AVAILABLE ON CARD AP version CX 03-00** To initialize the value of PIN number 4 (4th entry in the table) to "passphrase" and clear the key containers but for the 3rd area.
Card Application activation related commands	
Activate	To Activate/deactivate the One-Passport PKI Card Application, in order to protect the application during delivery. Requires a successful activation PIN verification: - Set Card AP status from inactive to active - Set Card AP status from active to inactive - change Card AP activation key value to new value
Card AP Secure Communication related commands	
Generate Session Key	Generates a T-DES session key for Card AP Secure Communication. This session key is generated from FIPS-DRNG rather than derived. By the way, the module has to return it to the external user. This output is ensured by wrapping the session key with an RSA public key. This Key (Cardholder RSA Public Key) is sent as input data of the APDU command.
Set Enc Communication Mode	Sets communication mode to plaintext or encrypted, on demand. Typically follows the Generate session key APDU command. When encrypted mode is set, all APDU commands shall be encrypted (data field) with the T-DES session key
Card AP RSA Keys related commands	
Set Public Key Pair	To import and zeroized Card AP key pair components. Requires sending multiple consecutive APDU commands to set an entire RSA Key pair: public components and private CRT components. RSA keys must be 1024-bits minimum and they are input wrapped with the current Card AP Session Key.
RSA Signature	To process RSA PKCS #1 signature of incoming data using the private CRT components of a designated RSA key pair of the CM. (see section 9.17 of the manual for more details)
Set Encryption Auth Pattern	Sets "use" or "set" permission in the Key table for RSA key pair.
Generate Backup Private Key	To export the private CRT components of a designated RSA Key Pair wrapped with the current Card AP Session Key.
Get Key Length	To get the modulus length of an identified RSA key pair.
Get Public Key	Returns the public key component (modulus and exponent) of an identified RSA key pair, plaintext.
Delete Public Key	To delete the RSA Key Pair information and public key components from the attribute and storage tables. Used for Card AP RSA Keys zeroization.

Get Key Pair Attributes	To get information from the RSA Key Pair attribute table.
Generate Public Key Pair	To generate an RSA CRT Key Pair including its public and private components. Generated values are not output.
Data related commands	
Read Data	To read a data stored in the data table of the "special protected area". Requires validation of data "read" permission.
Write Data	To write in the data table. Requires validation of data "write" permission.
Get Data Length	To get data length of an identified record of the data table. Requires validation of data "read" permission.
Set Management Table	To change the permissions of an identified data (at input entry in Data table) to input permission. Requires Super PIN validation.
Set Certificate	To store a certificate and associate it with identified RSA key pair. Requires data "write" and Key Pair "set" permissions validation.
Root certificate related commands	
Root Certificate Input	To store an input root certificate in the Management table.
Delete Root Certificate	To delete the root certificate: set root certificate first and last numbers to zero in the Root Certificate Management table.
Get Root Certificate Position	To get the position of the root certificate identified by input number (0x01 to 0x0C).
PINs related commands	
Check PIN	To compare an identified stored PIN with input PIN. If comparison succeeds, retry counter is reset and associated authentication flag is set to 1. (see manual sections 9.1 and 9.2 for more details)
Set PIN	To change the value of an identified stored PIN. Requires validation of PIN "write" permission. (see sections 9.3 and 9.4 of the manual for more details)
Unlock	To unlock all PINs by resetting each retry counter to its corresponding limit counter. Requires Super PIN validation.
Unlock 2	To unlock an identified PIN (at input entry in PIN table) by resetting the retry counter to its corresponding limit counter. Requires validation of PIN "unlock" permission.
Set PIN Attribute	To change the "read" and "write" permissions of all PINs (1-8) to an input pattern. Requires Super PIN validation. (see sections 9.12 of the manual for more details)
Set PIN Attribute 2	To change the "write" permission of all PINs (1-15) to an input pattern. Requires Super PIN validation. (see section 9.13)
Set PIN Protection Attribute	To change the limit counter, valid period and "unlock" permission of a PIN. Requires Super PIN validation. (see section 9.14)
Access Default PIN Container Number	To get the number or set the default PIN container (Cardholder default PIN). (see section 9.30)

Table 8 – Services provided by the Cryptographic Module

7.3 Authentication Policy

Role-based authentication mechanisms within the cryptographic module authenticate the Cryptographic Officer and the Cardholder accessing the module and verify that the operators are authorized to assume the requested roles and perform services within those roles.
Results of previous authentications are not retained at power-off/on. The operator must be re-authenticated to access authorized services.
This section contains the description of both the Issuer Security Domain and Card AP role-based Authentication Policies. It provides a description of the authentication mechanisms, their interfaces and a set of rules that are enforced at runtime.

Authentication policy is identical for both versions of Card AP.

7.3.1 Cryptographic officer authentication

This authentication policy relies on the following role-based authentication mechanisms, security rules and mechanism strength:

Mechanism	Description
Identification	
Key	The Cryptographic Officer owns a unique Key set that is used for authentication to the module: - Key sets are identified by a unique ID and version
	Interface: *INITIALIZE UPDATE APDU command*
Authentication based on role	
GP Secure Channel opening	The external operator opens a GP secure channel with the ISD in order to manage the module and becoming the **Cryptographic Officer**. This procedure is based on a mutual authentication and requires that the operator and the module generate a cryptogram using a shared nonce and the identified **Keys**. The **ISD Key Set** is loaded during the personalization phase of the module lifecycle. The CM identifies the **Cryptographic Officer** as being the role responsible for ISD Key Set management and use. [GP] describes the mechanism interfaces conditions of use.
	Interfaces: *APDU* **INITIALIZE UPDATE** *Key set selection* *GP Secure channel initialization based on nonce and cryptogram exchange (session keys generation).* *APDU* **EXTERNAL AUTHENTICATE** *Operator authentication and establishment of the level of security required for all subsequent commands.*

Table 9 – Cryptographic Officer Authentication mechanism

Id	Rule

Id	Rule
IAP.1	Role-based authentication of the **Cryptographic Officer** shall fail when the maximum amount of consecutive failures is reached.
IAP.2	Role-based authentication of the **Cryptographic Officer** shall be required again upon closure of the GP secure channel (intentionally or after reset or corruption of the secure channel)

Table 10 – C.O. Authentication Security rules

The following table shows that the Module meets the requirements regarding authentication mechanism strength:

- For each attempt to use the authentication mechanism, the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur
- For multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.
- No feedback of authentication data is provided to an operator apart from success or failure status at the end of processing

Mechanism	Strength
GP Secure channel	Success probability = $\left(\frac{GP\_retry}{2^{80}}\right)$ *GP_retry* is the maximum retry counter associated to the ISD GP secure channel. It is initially equal to 80. Authentication strength is based on an 8 byte long cryptogram and an 8 byte long T-DES MAC.

Table 11 – C.O. Authentication Mechanism Strength

7.3.2 Cardholder authentication

This authentication policy relies on the following role-based authentication mechanisms, security rules and mechanism strength:

Mechanism	Description
Role-based authentication	
Check PIN	The Cardholder owns all initialized PINs within the CM Card AP. PINs are identified by a unique ID. The CM identifies the cardholder by verifying that the submitted PIN is equal to the corresponding PIN stored within the "Key storage table". PINs are loaded at personalization time, and can be changed by the Cardholder. The CM identifies the **Cardholder** as being the role responsible for managing the PINs and performing the approved services that require prior authentication.
	Interfaces: *APDU* **CHECK PIN** *As any PIN verification, the CM receives a value in*

Mechanism	Description
	entry and compares it with the value within the dedicated storage table. *(CLA = 90 and INS = 5E or 80)*

Table 12 – Cardholder authentication mechanism

Id	Rule
IAP.1	Role-based authentication of the **Cardholder** shall fail when the maximum amount of consecutive failures is reached (PIN try limit).
IAP.2	Role-based authentication of the **Cardholder** shall be required again upon the CM reset.

Table 13 – Cardholder Authentication security rules

The following table shows that the Module meets the requirements regarding authentication mechanism strength:

- For each attempt to use the authentication mechanism, the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur
- For multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.
- No feedback of authentication data is provided to an operator apart from success or failure status at the end of processing

Mechanism	Strength
Check PIN	Success probability = $\left(\frac{Limit\_counter}{2^{128}}\right)$
	Limit counter is the maximum retry counter associated to each PIN of the Card AP. As specified, it can be up to 255 (0xFF) and PINs are 16 byte long binary strings (that is 128 bits of secret). Each byte may contain a value from 0x00 through 0xFF.

Table 14 – Cardholder Authentication Mechanism Strength

The Card AP authentication mechanism provides at the end of the process:

- authentication status (success or failure)
- remaining tries (only for Check PIN Command 2 where INS= 80h)

7.4 Access Control Policy

7.4.1 Introduction

This section contains the description of our Access Control Policy. This policy includes the rules that restrict the availability of some services provided by the Cryptographic Module to particular roles. See Authentication Policy for more details on the way roles are set.

Access Control policy is identical for both versions of Card AP.

7.4.2 Security Rules

Id	Rule
ACP.1	Access to the Cryptographic Module services dedicated to module administration shall be restricted to the **Cryptographic Officer.** *This includes all the services that shall be used within a GP secure channel.*
ACP.2	Access to the Card AP services dedicated to application usage shall be restricted to the **Cardholder.** *This includes all the services that shall be used after a successful PIN verification.*
ACP.3	Access to some services, as listed in the table below, does not require any role authentication.
ACP.4	Some services are available only if the Card AP is activated.

Table 15 – Access Policy Rules

7.4.2.1 Service restrictions

This section provides the CM services to the authorized roles. It also provides services that can be performed by the CM for which the operator is not required to assume an authorized role (no-role).
In addition, the Card AP proposes different services, depending if it is in an "Activated" state or not. This state is managed by the Cardholder using dedicated commands.

Service	Cryptographic Officer	Cardholder	No Role
Get Status	-	-	✓
Get Data	-	-	✓
Initialize Update	✓	-	-
External Authenticate	✓	-	-
Load	✓	-	-
Delete (applet)	✓	-	-
Select	-	-	✓
Set Status	✓	-	-
Install	✓	-	-
Put Key	✓	-	-
Delete (key)	✓	-	-

Service	Cryptographic Officer	Cardholder	No Role
Store Data	✓	-	-
Get Version	-	-	✓
Get Data Area	-	-	✓
Data Initialize	-	-	✓
Activate	-	✓ (*)	-
Services Proposed when Card AP is "**Activated**" only			
Initialize	-	✓ (*)	-
Generate Session Key	-	-	✓
Set Enc Communications Mode	-	-	✓
Set Public Key Pair	-	✓	-
RSA Signature	-	✓	-
Set Encryption Auth Pattern	-	✓ (*)	-
Generate Backup Private Key	-	✓	-
Get Key Length	-	-	✓
Get Public Key	-	-	✓
Delete Public Key	-	✓	-
Get Key Pair Attributes	-	-	✓
Generate Public Key Pair	-	✓	-
Read Data	-	✓	-
Write Data	-	✓	-
Get Data Length	-	✓	-
Set Management Table	-	✓ (*)	-
Set Certificate	-	✓	-
Root Certificate Input	-	✓	-
Delete Root Certificate	-	✓	-
Get Root Certificate Position	-	-	✓
Check PIN	-	-	✓
Set PIN	-	✓ (*)	-
Unlock	-	✓ (*)	-
Unlock 2	-	✓	-
Set PIN Attribute	-	✓ (*)	-
Set PIN Attribute 2		✓ (*)	
Set PIN Protection Attribute	-	✓ (*)	-
Access Default PIN Container Number	-	-	✓

Table 16 - Services restriction regarding roles

Note: *The services marked with a (*) correspond to services requiring presentation of Super PIN (see CSP description of* Card AP Cardholder PINs*)*

7.5 Critical Security Parameters

This section contains the description of the sensitive data managed by the Cryptographic Module that are involved in the security enforcement.

Critical Security Parameters are identical for both versions of Card AP.

Data	Description & evolution	
CO ISD Key Set	Set of 3 T-DES keys used to manage GP Secure Channel, between the ISD and the Cryptographic Officer: - **CO-K**enc: Used to derive CO session Key that will wrap data (except keys) within a secure channel with ENCRYPTION mode set - **CO-K**mac: Used to derive CO session Key that will guarantee integrity of any data within a secure channel with MAC mode set - **CO-K**kek: Key Encryption Key used to wrap the additional CO ISD Key Sets that are loaded in the CM with PUT KEY command within a secure channel.	
	LOAD	*Role based APDU PUT KEY*
	USE	*Role based APDU INITIALIZE UPDATE* *Role based APDU EXTERNAL AUTHENTICATE* *Role based APDU PUT KEY*
	OUTPUT	*No interface is provided to retrieve these Keys*
	ZEROIZE	*Role based APDU DELETE*
CO session Key Set	Set of 2 T-DES keys derived during the GP Secure Channel establishment from a selected CO ISD Key Set. These two keys are used to secure exchanges from the Cryptographic Officer to the ISD: - **CO-S**enc: Encryption Session Key used to wrap data (except keys) exchanged within a secure channel with ENCRYPTION mode set - **CO-S**mac: MAC Session Key used to guarantee integrity of any data exchanged within a secure channel with MAC mode set	
	GENERATION	*Role based APDU EXTERNAL AUTHENTICATE*
	USE	*Role based APDUs [GP] sent within secure channel*
	OUTPUT	*No interface is provided to retrieve these Keys*
	ZEROIZE	*Card Reset* *Role based APDU SELECT (OTHER APPLET AID)*
Card AP RSA Private Keys (1024-bit)	Set of RSA Private Keys used to sign data sent by the Cardholder. These Keys can be externally loaded or internally generated by the module. The output and load of these keys is submitted to authentication (PIN based access control), limitation of authorized backup amount, and Card AP Secure Communication (encryption with current Card AP Session Key is required).	
	GENERATE	*Role based APDU GENERATE PUBLIC KEY PAIR*
	SET	*Role based APDU SET PUBLIC KEY PAIR*
	USE	*Role based APDU RSA SIGNATURE*
	OUTPUT	*Role based APDU GENERATE BACKUP PRIVATE KEY*
	ZEROIZE	*Role based APDU DELETE PUBLIC KEY PAIR*

Data	Description & evolution	
Card AP Session Key	Session key derived from the FIPS-DRNG during the initialization of the Card AP Secure Communication: - T-DES Session Key When derived, this Key is also output wrapped with a RSA public key that was transmitted as input data of the command. This public key is part of an RSA Key Pair of the external user.	
	GENERATE	*Role based APDU GENERATE SESSION KEY*
	USE	*Role based APDUs that are sent to Card AP within a secure communication in encrypted mode*
	OUTPUT	*Role based APDU GENERATE SESSION KEY*
	ZEROIZE	*Card Reset* *Role based APDU SELECT (OTHER APPLET AID)*
Card AP Cardholder PINs	Set of up to 15 PINs, 16 bytes long (see Table 14), that can be either normal PINs or super PIN, and that must be verified prior to access specific cardholder services: - PINs: PIN 1 to PIN 15 - Super PINs: combination of PIN 1 to PIN 15 with the 'Super' flag set PINs are used to enforce Access Control (AC) on Card AP PINs and Keys. Super PIN is used to strengthen AC on some sensitive services provided by Card AP (see services marked with (*) in Table 16).	
	LOAD	*Role based APDU SET PIN*
	MANAGE	*Role based APDU INITIALIZE* *Role based APDU SET PIN ATTRIBUTE* *Role based APDU SET PIN PROTECTION ATTRIBUTE* *Role based APDU UNLOCK* *Role based APDU UNLOCK 2*
	USE	*Role based APDU ACTIVATE* *Role based APDU CHECK PIN*
	OUTPUT	*No interface is provided to retrieve any PIN value*
	ZEROIZE	*Role based APDU SET PIN (ALL-0)*
Card AP Activation PIN	The activation PIN is a 16-bytes long PIN (see Table 14) used by the Cardholder to activate and deactivate Card AP. Its value is associated to a retry counter, and both are stored plaintext.	
	SET	*Role based APDU ACTIVATE*
	USE	*Role based APDU ACTIVATE*
	ZEROIZE	*Role based APDU ACTIVATE*
	OUTPUT	*No interface is provided to retrieve any PIN value*
Secure Storage Key	This key (SSK) is a 16-bytes T-DES Key used to encrypt CO ISD Key Set values when stored in EEPROM.	
	SET	*At first reset of the card using the FIPS-approved RNG*
	USED	*Each time a* CO ISD Key Set *is used or set*
	OUTPUT	*No interface is provided to retrieve this Key*
	ZEROIZE	*Role based APDU SET STATUS (TERMINATED)*

Table 17 – Sensitive Data Description and Evolution

7.6 Public Keys

The following public keys are handled by the module:

Data	Description & evolution	
Cardholder RSA Public Key	This Key is transmitted by the Cardholder to CM when requesting Card AP to generate Card AP Secure Communication session key. It is transmitted plaintext in the command APDU data field and used to encrypt the generated T-DES Card AP Session Key before it is output. This Key is not kept by the CM: it is received, used, then overwritten with output information.	
	USE	*Role based APDU GENERATE SESSION KEY*
Card AP RSA Public Keys	These Keys correspond to the public part of the Card AP RSA Private Keys (see table 17) and are stored in the same table, plaintext. They can be internally loaded by the Cardholder or internally generated by the module. The module only stores these Keys: it does not provide any service that uses them. On demand, the module outputs such keys plaintext.	
	GENERATE	*Role based APDU GENERATE PUBLIC KEY PAIR*
	SET	*Role based APDU SET PUBLIC KEY PAIR*
	USE	*No interface is provided to use these Keys*
	OUTPUT	*Role based APDU GET PUBLIC KEY*
	ZEROIZE	*Role based APDU DELETE PUBLIC KEY PAIR*

Table 18 – Public Keys Description and Evolution

8 Finite State Model

CM operations are specified using a finite state model represented by a state transition diagram.

The state transition diagram includes:

- All operational and error states of the CM,
- The corresponding transitions from one state to another,
- The input events that cause transitions from one state to another, and
- The output events resulting from transitions from one state to another.

The CM includes the following operational and error states:

- Power on/off states
- Crypto officer states
- Key/CSP entry states
- User states
- Self-test states
- Error states

9 Physical Security

The Cryptographic Module (CM) is a single-chip implementation which Cryptographic boundaries encompass the chip, the interconnection wires and an encapsulant epoxy. The physical component of CM is protected by a hard opaque tamper-evident resin cover.

The CM employs physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module (including substitution of the entire module) when installed. All hardware and firmware within the cryptographic boundary are protected.

Physical security features meet FIPS-140-2 level 3 requirements with:

- Production-grade component including passivation techniques (hard opaque tamper-evident resin cover on chip) and state-of-the-art physical security features (detection of out-of-range supplied voltage, frequency or temperature, detection of illegal address or instruction, and physical security measures within the layout of the whole circuitry)
- Opaque coating on chip that deter direct observation within the visible spectrum,
- Hard tamper-evident coating that provides evidence of tampering (visible signs on the resin cover and/or contact face plates), with high probability of causing serious damage to the chip while attempting to probe it or remove it from the module.
- The epoxy that covers the Cryptographic Module is resistant to commonly available solvents.

The CM physical security features consider the following physical and electrical ranges:

Item	Range
Supply voltage	2.7V to 3.6V
Frequency	1MHz to 10MHz
Temperature	-25 to + 85°C

Table 19 - CM Physical and Electrical Characterstics

10 Operational Environment

The Operational Environment of this module is considered a limited one that can only load FIPS validated applications. As such, this section is non-applicable.

11 Cryptographic Key Management

The Cryptographic Key Management services include approved random number and key generation, key establishment, storage and Zeroization mechanisms.

Cryptographic Key Management is identical for both versions of Card AP.

The CM contains T-DES keys owned by the [GP] Issuer Security Domain and managed by the OS755. These keys (and only these) are stored encrypted with a T-DES key called SSK in EEPROM.

The CM also contains RSA keys and PINs that belong to the Card AP.
The Card AP owns RSA key Pairs, a T-DES session key and PINs. It provides services related to their management to the Cardholder, including their generation, storage and zeroization. RSA Key Pair generation and Random Number generation (used for generating new session key values) in provided by the OS755 to Card AP.
Card AP key management services are provided through dedicated APDU commands.

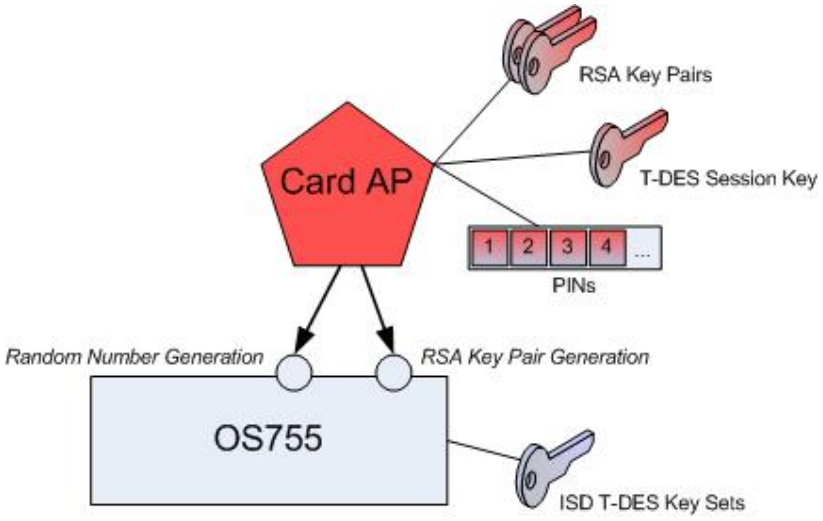

Figure 3 - Key Management

11.1 Random Number Generators

The CM includes a FIPS approved ANSI X9.31 Random Number Generator ([X9.31]), implementing the continuous random number generator test. This FIPS-DRNG is used for the on-board generation of cryptographic keys such as the T-DES Secure Communication session key of the Card AP.

Note: *The chip hardware RNG is used for the purpose of generating seeds for the FIPS-DRNG.*

11.2 Key Generation

Three groups of Keys can be generated using the CM:

Secure Storage Key
The SSK is generated at first reset of the card using the FIPS-DRNG.

ISD Session Key
[GP] Issuer Security Domain Session keys are generated by OS755 upon CM-Host mutual-authentication success:

- S-MAC Session Key: generated from S-MAC, used for protecting data integrity in GP Secure Channel secure mode (MAC).
- S-ENC Session Key: generated from S-ENC, used for protection data confidentiality in GP Secure Channel mode (Encryption).

Card AP RSA Private Keys
The OS755 provides Card AP with an on-board 1024-bit key generation that uses an approved key generation method.

Card AP T-DES Session Key
The Card AP generates a 24-bytes T-DES key upon Card AP Secure Communication initiation success. This Key is called "session key", but it is stored in a fixed area in EEPROM. Card AP is responsible for clearing it when it is re-selected (after power up). The generation of each value of this Key is generated using the FIPS approved random number generator provided by the CM.

11.3 Key Entry and Output

Two groups of keys can be entered and output in the CM:

ISD T-DES Key Sets
The CM offers the PUT KEY APDU command for:

- Replacing an existing key with a new ISD key
- Replacing existing key set with new ISD key set
- Adding a single new ISD key
- Adding a new ISD key set

The CM enforces confidentiality while entering Issuer Security Domain secret keys using key encryption following [GP] (FIPS approved algorithms and operation mode). The CM provides no ISD secret key output. All Secret values of keys are entered wrapped with the T-DES **CO-K**kek identified during the GP Secure Channel initialization, when one of the ISD Key set is selected.

Card AP RSA Private Keys
The Card AP offers APDU commands for:

- Outputting RSA Private Keys
- Entering RSA Private Keys

Card AP enforces encryption (FIPS approved algorithms and operation mode) for entering and outputting RSA private keys (Card AP Secure Communication mode).
Only entry of 1024-bit length RSA Private Keys are accepted by the Card AP related APDU command.

11.4 Key Storage

Key storage is detailed for all persistent keys managed by the CM:

Secure Storage Key
The SSK is stored in EEPROM plaintext.

ISD T-DES Key Sets
Issuer Security Domain T-DES secret keys are stored in EEPROM encrypted with the T-DES key SSK. The CM also applies an integrity checksum to these Keys.

Card AP RSA Private Keys
One-Passport PKI Card Application RSA Private Keys are stored plaintext with no checksum in Card AP buffers: key access control is fully managed by the Card AP.
Access to the Card AP RSA key Pairs is protected with Read/Write permissions that are combination of 15 PINs (all owned by the Cardholder). This mechanism guarantees that RSA Key Pairs can only be changed by the Cardholder.
The PINs are used as multiple lockers on a safe. The Cardholder will associate multiple PINs to very secret RSA Key Pairs that he wants to highly protect: all associated PINs shall be verified prior using/updating the RSA Key Pair.

Card AP T-DES Session keys
The One-Passport PKI card Application T-DES Session key is persistent key stored in EEPROM. Session keys will not be cleared at power-off, but when you will start-up the CM again: power up and Card AP selection.

11.5 Key Zeroization

The CM offers services to zeroize all the persistent keys:

Key Encryption Key
The SSK is zeroized when Card lifecycle state is set to TERMINATED using the SET STATUS APDU command provided by [GP] layer of the Card OS or setting the card in insecure and irrecoverable state (corrupting a cryptographic algorithm for example).

ISD T-DES Key Sets
The CM offers Issuer Security Domain [GP] APDU commands for zeroizing all the associated Keys in ISD Key Sets.
The CM provides a key zeroization mechanism using either the PUT KEY or the DELETE (Key) commands to zeroize the Issuer Security Domain related keys.

Card AP RSA Private Keys
The CM offers Card AP APDU commands for zeroizing RSA Private Keys.

The One-Passport PKI card Application RSA key pairs can be zeroized by deleting the key reference and forcing the public and private keys to all-1 values using the DELETE PUBLIC KEY PAIR and the SET PUBLIC KEY PAIR APDU commands (all-1 modulus and all-1 public exponent or all-1 private exponent):

- clear header to allow Key Pair value zeroization DELETE PUBLIC KEY PAIR
- clear all private values of the Key Pair SET PUBLIC KEY PAIR (3 APDUs)
- disable key pair access DELETE PUBLIC KEY PAIR

This zeroization technique is performed in a time that is not sufficient to compromise plaintext secret and private keys: 2.2 s in average.

The CM also offers Card AP APDU commands for zeroizing the T-DES session key. The One-Passport PKI card Application T-DES session key is zeroized when it is started: upon reception of the SELECT APDU command.

12 Electromagnetic Interference/Compatibility (EMI/EMC)

The Cryptographic Module conforms to the EMI/EMC requirements specified by 57 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, and Class B.

13 Self-Tests

FIPS140-2 defines Self-Tests. The Hitachi One-Passport PKI Card Application on Athena Smartcard Solutions OS755 for Renesas XMobile Card Module implements the following:

- Power-up self-tests are launched when the CM is reset
- Conditional self-tests are performed when the related cryptographic function is to be used.

Self-tests are identical for both versions of Card AP.

13.1 Power-up Self-Tests

Cryptographic Algorithms:
Known Answer Tests (KATs) are conducted for each cryptographic function and in each mode of operation. Input Data and Known Answers are recorded in ROM.
KATs are related to:

- ANSI X9.31 Deterministic RNG KAT,
- T-DES (CBC mode; Encrypt and Decrypt),
- SHA-1,
- RSA PKCS#1 (Signature and verification with private/public CRT key),
- RSA PKCS#1 (encryption and decryption with private/public CRT key).

The self-tests are processed one by one as first thing prior to completion of first selection of the One-Passport PKI Card Application. If one of the KAT under control of the OS755 fails (3 first categories), the card goes mute. If the last power-up KAT fails, the Card AP returns an error.

Software Integrity:
A 16 bit checksum is used to verify that no FIPS applications present in EEPROM have been modified. It also checks the integrity of all additions and corrections that have been added to the module (patch code and patch table). ROM code is excluded from Software integrity verification.

Note: *Power-up self-tests are performed between the module power-up and processing of the first APDU command by the Card AP.*

13.2 Conditional Self-Tests

Key Pair-Wise Consistency Test:
This test is performed during RSA Key Pair generation once the CM has generated the RSA Key Pair values (both signature/verification and encryption/decryption are tested).

Software/Firmware Load Test:
Applet loading follows the Global Platform 2.1 specifications (GP Secure Channel with T-DES MAC), See [GP].

Continuous RNG Tests:
The FIPS-DRNG and the Hardware random number generator are tested for failure to a constant value of 64 bits.

First a 64-bit block is generated, and then a second 64-bit block is generated and compared to the first. If they are equal, the test fails.

A Continuous RNG Test is performed every time a new block of bits is generated.

Note: *Power-up self–tests on demand: resetting the module is an approved self-test on demand function.*

13.3 Errors while performing tests

- **KAT :** module is set mute[1] or returns an error,
- **Software Integrity Self-Test:** the module is placed in a terminated lifecycle state and set mute,
- **Key Pair-Wise Consistency Test**: the module is set mute,
- **Software/Firmware Load Test:** software/firmware is not loaded.
- **Continuous RNG Tests:** the module is set mute.

[1] When card is set Mute, the card does not output any data or process subsequent commands. The only mean to exit this state is to reset the card.

14 Mitigation of Other Attacks

Typical XMobile Card attacks are Single Power Analysis, Differential Power Analysis, Timing Analysis, Fault Induction that may lead to revealing sensitive information such as PIN and Keys by monitoring the module power consumption and timing of operations or bypass sensitive operations.

The Athena Smartcard Solutions OS755 for Renesas XMobile Card Module is protected against **SPA, DPA, Timing Analysis and Fault Induction** by combining State of the Art Software and Hardware counter-measures.

The Cryptographic Module is protected from attacks on the operation of the IC hardware. The protection features include detection of out-of-range supply voltages, frequencies or temperatures, detection of illegal address or instruction, and physical security.

All cryptographic computations and sensitive operations such as PIN comparison provided by the Cryptographic Module are designed to be resistant to timing and power analysis. Sensitive information of the embedded Operating System is securely stored and integrity protected. Sensitive operations are performed in constant time, regardless of the execution context (parameters, keys, etc…), owing to a combination of hardware and firmware features.

The Cryptographic Module does not operate in abnormal conditions such as extreme temperature, power and external clock, increasing its protection against fault induction.

Mitigation of Other Attacks applies to both versions of Card AP.

[END OF THE DOCUMENT]