Aspects Software OS755
for
Renesas XMobile Card Module

Security Policy
FIPS 140-2 Level 3

Version: 1.0
Date: 21 February 2006

TABLE OF CONTENTS

TABLES

FIGURES

1 Scope

The Aspects Software OS755 for Renesas XMobile Card Module is a single chip multi-application cryptographic Java Card module specially designed for XMobile cards.

The Cryptographic Module offers 61.2K of EEPROM and 3.4K of RAM for applications, together with cryptographic services such as:

- DES and Triple DES (using double and triple length DES keys) for encryption and decryption in both ECB and CBC modes, no pad,
- RSA key generation up to 1024 bit key length with strong prime numbers (ANSI X9.31),
- RSA encryption and decryption using PKCS#1 automatic padding,
- RSA signature and verification using PKCS#1 padding method,
- Digest computation using SHA-1 algorithm.

2 Product Overview

Java promises write once, run anywhere™ capability. Aspects OS755 for Renesas XMobile Card, the Aspects' Java Card™ technology and Global Platform Operating System validated against FIPS standards, fulfills that promise for the XMobile card industry.

This Security Policy describes the **Aspects Software OS755 Java Card Platform** validated against **FIPS 140-2 Overall Level 3 on the Renesas AE46C1 chip for XMobile Card Module**. It identifies the cryptographic module that successfully passed the certification and describes software and hardware features of the cryptographic module. It defines roles and services provided to Card Issuers and Applet Providers, describes algorithms implemented following standards recommended by FIPS, Power-up and conditional self-tests.

Aspects OS755 for Renesas XMobile module is built to give Card and Applet Issuers flexibility in the way they work: a blank canvas on which to create XMobile Card products for all market sectors, including those requiring FIPS 140-2 validation. Central to Aspects OS755 is its compliance with the Java Card and Global Platform standards; multiple compliant Java Card applets from any source will run securely on Aspects OS755 enabled silicon. FIPS Applets can be securely loaded and deleted post issuance thanks to Global Platform compliant Issuer Security Domain implementation.

The Module presented for validation does not contain any third party applets.

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
CLK	Clock
CM	Cryptographic Module
CPLC	Card Production Life Cycle
CSP	Critical Security Parameter
DES/TDES	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
KEK	Key Encryption Key
MAC	Message Authentication Code
MONOS	Metal Oxide Nitride Oxide Silicon
OPEN	Open Platform Environment
PIN	Personal Identification Number
RFU	Reserved for Future Use
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
RST	Reset
SPA	Simple Power Analysis

Table 2 – Glossary of Terms

3 Cryptographic Module Specification

The Cryptographic Module is the combination of a Java Card Operating System firmware that implements FIPS approved cryptographic functions and a state-of-the-art secure Single Chip Silicon Hardware.

Aspects Software OS755, the firmware component of the cryptographic module is a standards compliant Java Card 2.1.1 technology and GlobalPlatform 2.1 Operating System.

Aspects OS755 for Renesas XMobile Card Module	
Description:	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:	OS755 version 2.4.6
Hardware Version:	AE46C1 Version 0.1
Operating System:	Global Platform 2.1 Java Card Runtime Environment 2.1.1 (amended for compliance with Global Platform)
APIs:	Global Platform 2.1 API VISA Open Platform 2.0.1' API (deprecated) Java Card API 2.1.1 (options as specified by Global Platform for modules supporting asymmetric cryptography)
Virtual machine:	Java Card Virtual Machine 2.1.1
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 so you always have full use of all available free memory.
Interoperability:	Fully interoperable for Java Card 2.1.1 applets
Approved Algorithms and Operation Modes:	Signature and Cipher: - RSA with PKCS#1 padding ([PKCS1]),[1] - DES and TDES in ECB and CBC modes, no pad, - DES MAC and TDES MAC - SHA-1 (Signature only), Random Number Generator: - ANSI X9.31 Deterministic RNG ([X9.31]), On-board RSA Key Generation (1024 bits key length), All security functions are used in an approved mode of operation.

[1] Note that RSA (PKCS#1) is not used in this module but provided to FIPS applets to be loaded in the future.

Aspects 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 - TDES in ECB and CBC modes, with ISO9797 m1/m2 padding; non compliant

Table 3 – Aspects Software OS755 for Renesas XMobile Card Module

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 Aspects Software OS755 for Renesas XMobile Card Module has been successfully tested against FIPS140-2 requirements and meets an overall security level 3. The following areas have been independently rated.

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

Table 4 – Security Level of Evaluated Areas

5 Modes of operation

The OSS755 FIPS Java Card Platform does not include any third party applets. If any applets are loaded in the module, it will subsequently function in a non-approved mode 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 applets validated to FIPS 140-2.

5.1 How to put the module in the approved mode

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

- Send EXTERNAL AUTHENTICATE command with the C-MAC flag set.

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:

- 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'
ICC manufacturer	2	'3060'
IC embedding date	2	'0000'

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

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,
- Global Platform and Java Card Application Programming Interfaces (APIs), and Java Card Runtime Environment (JCRE) and Virtual Machine (JCVM) as logical interfaces (these interfaces are not currently available as there are no third party applets loaded for this validation).

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
RES	Reset signal
I/O	Input / Output
CLK	Clock signal
VSS	Power Ground
VCC	Power Supply

Table 5 – Physical Interfaces

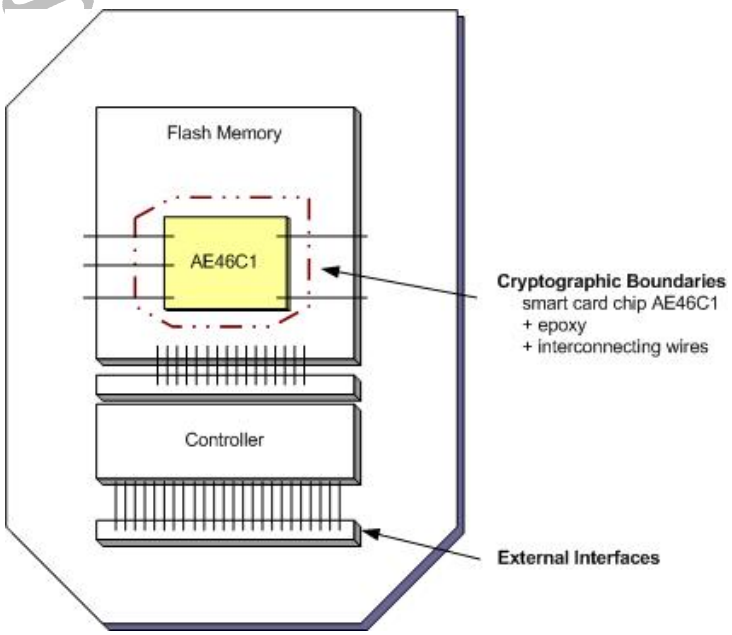

Figure 1 – The Cryptographic Module

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 6 - CM Physical and Electrical Characterstics

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 FIPS 140-2 and ISO7816-4 standards, with the available logical interfaces as follows:

Logical Interfaces	**APDU**	**Physical Interfaces** *(see Table 5 – Physical Interface)*
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 7 – Logical Interface Structure Regarding FIPS 140-2

6.2.2 Logical Interface for Keys and CSPs

The Cryptographic Module never inputs/outputs Keys or CSPs in plain text.

Moreover, the Cryptographic Module enforces encrypted transfer of Keys and CSPs through a logical secure channel following the [GP] 2.1 standard.

7 Roles, Services, and Authentication

This section specifies roles, services, security rules, and CSPs of the cryptographic module.
The Identification/Authentication and Access Control Policies define interrelationships between roles, services and security rules.

7.1 Roles

As defined in the Ports and Interfaces section, the module is interfacing with both external operators and applets outside its boundaries (third party applets), as shown in the following diagram.

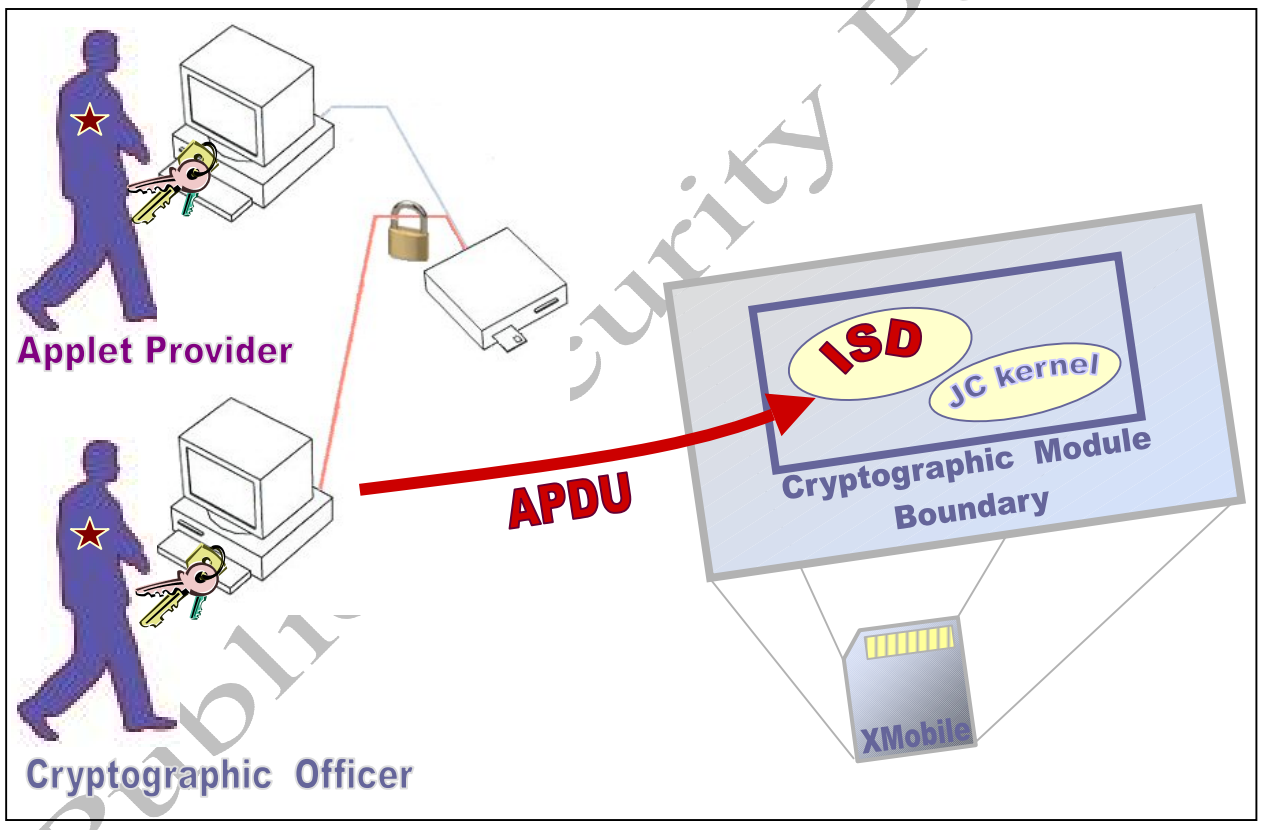

Figure 2 – Cryptographic Module users (★)

The following table describes the roles:

Role	Description
Cryptographic Officer Role	
Cryptographic Officer	**External operator** who knows a **unique TDES key set** to open a **secure channel** [GP] 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 Roles	
Applet Provider	**External operator** who knows a **unique TDES key set** to open a **secure channel** [GP] with the ISD. The Applet Provider is capable of performing the same services as the Cryptographic Officer, which includes the load and instantiation of applets validated FIPS 140-2. Applet instances are associated with a Security Domain (a dedicated one or the ISD).
Maintenance Role	
None	

Table 8 – Cryptographic Module roles description

No third party applets are present in the module for this validation

However applets validated FIPS 140-2 can be loaded at issuance time (loaded at personalization time) and additional applets validated FIPS 140-2 can be loaded anytime at post issuance (SECURED state). All these applets are subjects that operate on behalf of an external operator.
See following figure for interaction of an applet validated FIPS-140-2 with the CM:

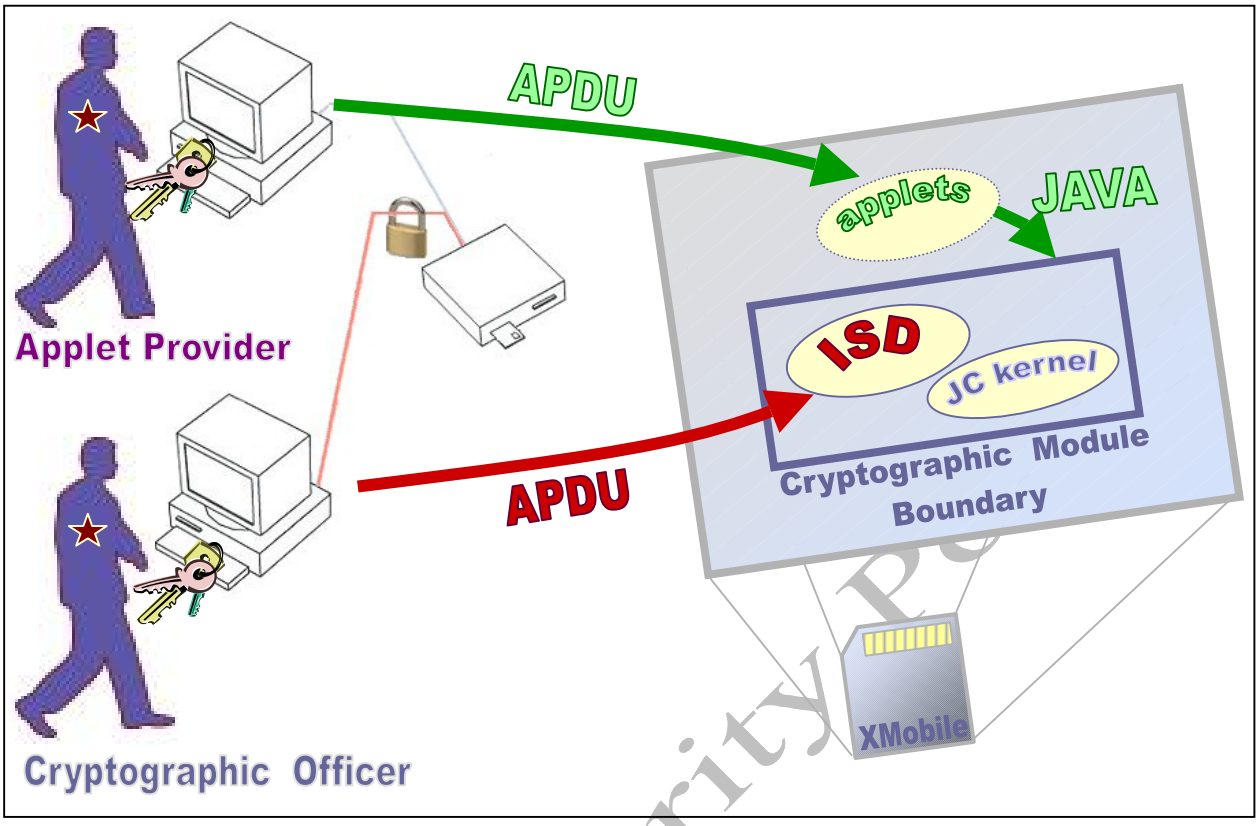

Figure 3 - Cryptographic Module users with applets loaded

7.2 Services

This section is dedicated to the services proposed by the Cryptographic Module.

Service		Description
APDU logical interface [GP]	Show Status Service	
	GET STATUS	External individuals 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.
		Service input: APDU GET STATUS
	GET DATA	External individuals can retrieve public data from the ISD. No CSPs can be read using this service.
		Service input: APDU GET DATA
	Perform Approved Security Function Services	
	INITIALIZE UPDATE	External individuals can initiate the initiation of a Secure Channel session, setting key set version and index.
		Service inputs: APDU INITIALIZE UPDATE
	EXTERNAL AUTHENTICATE	External individuals can open a secure channel with the ISD in order to communicate with it in a secure and confidential way.
		Service inputs: APDU EXTERNAL AUTHENTICATE
	LOAD	External individuals can transfer a Load File to the CM.
		Service input: APDU LOAD
	DELETE (applet)	External individuals 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.
		Service input: APDU DELETE
	SELECT	External individuals can select an application.
		Service input: APDU SELECT
	SET STATUS	External individuals can modify the module Life Cycle State or the Application Life Cycle State.
		Service input: APDU SET STATUS
	INSTALL	External individuals can initiate or perform the various steps required for Module Content management.
		Service input: APDU INSTALL
	PUT KEY	Regarding ISD keys, external individuals can either: - Replace an existing key with a new key - Replace multiple existing keys with new keys - Add a single new key - Add multiple new keys - Key zeroization
		Service input: APDU PUT KEY
	DELETE (Key)	External individuals can delete a uniquely identifiable object such as a key. This service is also used for key zeroization.
		Service input: APDU DELETE
	STORE DATA	External individuals can transfer data to the ISD.
		Service input: APDU STORE DATA
		Service inputs: See both standards for more details

Table 9 – Services provided by the Cryptographic Module

7.3 Identification and Authentication Policy

7.3.1 Introduction

This section contains the description of our identity-based Identification and Authentication Policy. It provides a description of the authentication mechanisms, their interfaces and a set of rules that are enforced at runtime.

The Cryptographic Module provides mechanisms to identify the following roles:

- **Cryptographic Officer**
- **User/Applet Provider**

This policy relies on the identity-based authentication mechanisms presented in the following table:

Mechanism	Description
Identification	
Key	The Cryptographic Officer and the User/Applet Provider have their own unique Key set that is used to identify them to the module: - Key sets are identified by a unique ID and version
	Interface: *INITIALIZE UPDATE APDU command*
Authentication based on identity	
Secure channel opening	The external operator opens a secure channel with the ISD in order to manage the module, becoming the **Cryptographic Officer** or the **User/Applet Provider**, depending on the selected Key Set. This procedure is based on a mutual authentication and requires that each operator and the module generate a cryptogram using a shared nonce and the identified **Keys**. The **Cryptographic Officer** loads these **unique Key Sets** for himself and the **User/Applet Provider** during the personalization phase of the module lifecycle. The CM identifies the **Cryptographic Officer** as being the identity responsible for ISD Key Sets management and use. [GP] describes the mechanism interfaces conditions of use.
	Interfaces: *APDU* **INITIALIZE UPDATE** *Key set selection* *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 10 – Identification and authentication mechanisms description

7.3.2 Security rules

Id	Rule
IAP.1	Identification and authentication of the **Cryptographic Officer** shall fail when the maximum amount of consecutive failures is reached.
IAP.2	Re-identification and re-authentication of the **Cryptographic Officer** shall be required upon closure of the secure channel (intentionally or after reset or corruption of the secure channel)
IAP.3	Identification and authentication of the **User/Applet Provider** shall fail when the maximum amount of consecutive failures is reached.
IAP.4	Re-identification and re-authentication of the **User/Applet Provider** shall be required upon closure of the secure channel (intentionally or after reset or corruption of the secure channel)

Table 11 – Identification and authentication policy rules

7.3.3 Authentication Mechanism Strength

Mechanism	Strength
Secure channel	$\left(\frac{2^{128}}{\max try}\right)$ *max try* initial value = 80 It is the maximum retry counter associated to the ISD secure channel and it can be updated. Authentication strength is based on an 8 byte long cryptogram and an 8 byte long TDES MAC.

Table 12 – Authentication Mechanism Strength

The authentication mechanism provided by the CM does not provide any feedback to the individual or process that is performing the authentication process. The CM communicates authentication status (success or failure) at the end of the process.

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 Identification and Authentication Policy for more details on the way roles are set.

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** and **User/Applet Provider**. *This includes all the services that shall be used within a secure channel. See [GP] for more details.*
ACP.2	Access to the Cryptographic Module services dedicated to module lifecycle management shall be restricted to the **Cryptographic Officer** and the **User/Applet Provider**. *They are able to use respectively the APDU and the Java interfaces.*
ACP.3	Access to GET DATA and SELECT services does not require any role authentication.

Table 13 – Access Policy Rules

7.4.2.1 Service restrictions

The following table shows the access restrictions applied to each service provided by the Cryptographic Module:

Service \ Role	Cryptographic Officer	User / Applet Provider	No role
SELECT	✓	✓	✓
GET DATA	✓	✓	✓
INITIALIZE UPDATE	✓	✓	
EXTERNAL AUTHENTICATE	✓	✓	
LOAD	✓	✓	
DELETE (applet)	✓	✓	
GET STATUS	✓	✓	
SET STATUS	✓	✓	
INSTALL	✓	✓	
PUT KEY	✓	✓	
DELETE (Key)	✓	✓	
STORE DATA	✓	✓	

Table 14 - Services restriction regarding roles

7.5 Critical Security Parameters

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

Data	Description & evolution
CO ISD Key Set	Set of 3 TDES keys used to manage secure communication, as per GP, between the ISD and the Cryptographic Officer: - Secure Channel Encryption Key: **CO S-ENC** - MAC Key: **CO S-MAC** - Data (Secret Keys) Encryption Key: **CO DEK**
	SET *Identity based APDU PUT KEY*
	USED *Identity based APDU INITIALIZE UPDATE* *Identity based APDU EXTERNAL AUTHENTICATE* *Identity based APDU PUT KEY*
	READ *No interface is provided to retrieve ISD key set values*
CO Session Keys	Set of 2 TDES keys generated, as per GP, during the secure channel establishment to secure communications from the Cryptographic Officer to the ISD: - Encryption Key: **CO SK-ENC** - MAC Key: **CO SK-MAC**
	SET *Identity based APDU EXTERNAL AUTHENTICATE*
	USED *Identity based APDUs that are sent within a secure channel*
	READ *No interface is provided to retrieve session key values*
User/Applet Provider ISD Key Set	Set of 3 TDES keys used to manage secure communication, as per GP, between the ISD and the User/Applet Provider: - Encryption Key: **AP S-ENC** - MAC Key: **AP S-MAC** - Key Encryption Key: **AP DEK**
	SET *Identity based APDU PUT KEY*
	USED *Identity based APDU INITIALIZE UPDATE* *Identity based APDU EXTERNAL AUTHENTICATE* *Identity based APDU PUT KEY*
	READ *No interface is provided to retrieve ISD key set values*
User/Applet Provider Session Keys	Set of 2 TDES keys generated, as per GP, during the secure channel establishment to secure communications from the User/Applet Provider to the ISD: - Encryption Key: **AP SK-ENC** - MAC Key: **AP SK-MAC**
	SET *Identity based APDU EXTERNAL AUTHENTICATE*
	USED *Identity based APDUs that are sent within a secure channel*
	READ *No interface is provided to retrieve session key values*
Internal KEK	16-byte TDES key that is used to encrypt secret and private parts of any persistent key. It is generated with the FIPS PRNG when the card is powered up for the first time.
	SET *No interface is provided to set its value*
	USED *Each time a private or secret part of the above CSPs is used*
	READ *No interface is provided to retrieve its value*

Table 15 – Sensitive Data 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.

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.

Keys (ISD TDES key set) are protected within the CM from unauthorized disclosure, modification and substitution.

11.1 Random Number Generators

The CM provides 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.

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

11.2 Key Generation

The CM generates cryptographic keys internally, using an approved key generation method. Generated cryptographic keys are used by approved algorithms and security functions. Compromising the security of the key generation method requires at least as many operations as determining the value of the generated key.

Two session keys are generated upon CM-Host mutual-authentication success:

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

The Internal KEK is generated using the FIPS-PRNG when the CM is reset for the first time: secure storage is part of its initialization process.

11.3 Key Establishment

The CM provides 80-bits of strength for key establishment using a 2-key TDES Approved Algorithm.

11.4 Key Entry and Output

The CM enforces confidentiality while entering keys using key encryption following [GP] (FIPS approved algorithms and operation mode). The CM provides no key

output. All Secret values of keys are entered wrapped with the TDES DEK (Data Encryption Key) identified during the secure channel initialization.

The Internal KEK is never entered or output: it is generated inside the CM and no interface is provided to read or write it.

11.5 Key Storage

The CM is responsible for confidentiality and integrity of sensitive data.
The CM stores Secret and private parts of Keys encrypted in EEPROM. The encryption algorithm that is used is a TDES with a 16-byte Internal KEK.
The CM also applies an integrity checksum to these Keys.

11.6 Key Zeroization

The CM provides a key zeroization mechanism using either the PUT KEY or the DELETE (Key) commands.

The Internal KEK is zeroized by setting the CM card lifecycle state to TERMINATED using dedicated command SET STATUS.

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 Aspects 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.

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 FIPS-DRNG, DES and TDES (CBC in Encrypt and Decrypt modes), RSA-CRT, and SHA-1.

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.*

13.2 Conditional Self-Tests

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

Software Load Test:
Applet loading follows the Global Platform 2.1 specifications (Secure Channel with TDES MAC using SK-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.

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

Errors while performing:

- **KAT :** module is set mute[2],
- **Continuous RNG Tests:** the module is set mute,
- **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,
- **Applet loading:** applet is not loaded.

[2] 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 Aspects OS755 for Renesas XMobile 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 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.

[END OF THE DOCUMENT]