athena
Smartcard

Athena IDProtect
FIPS 140-2 Cryptographic Module
Security Policy

Version: 0.3

Date: 14 February 2011

Athena Smartcard Inc., 20380 Town Center Lane, Suite 240, Cupertino, CA 95014

CONTENTS

List of Figures

List of tables

1 CRYPTOGRAPHIC MODULE OVERVIEW

1.1 INTRODUCTION

This document defines the Security Policy for the Athena IDProtect Cryptographic Module (CM). This module is validated to overall FIPS 140-2 level 3.

This document contains a description of the CM, its interfaces and services, the intended operators and the security policies enforced in the approved mode of operation.

The primary purpose of this device is to provide data security for government and enterprise personnel identification. The CM is specifically designed to resist non-evident tampering by both physical and electronic means.

The CM is a single Integrated Circuit Chip containing an operating system. As such it is the intention that applications will need to be loaded to provide the necessary business functionality. The design allows for multiple applications to be concurrently loaded and securely separated by a firewall.

The CM is designed such that loading a FIPS 140-2 validated application enables a re-validation to be performed in a short time with the minimum risk possible; that is, the new CM is easily submitted for re-validation. However, this validation is limited in scope to the CM with no loaded applications and as the loading of an application takes the module out of the approved mode of operation a new validation will always be required.

The CM operating system is an implementation of the GlobalPlatform version 2.1.1 and Java Card™ version 2.2.2 specifications. These high level and all low-level services, inclusive of communications, non-volatile and volatile memory management, cryptographic algorithms and physical security are addressed.

Java Card services can be accessed by a loaded application using the Java Card™ Application Programming Interface (API).

GlobalPlatform services are provided to an external operator through the Issuer Security Domain and to a loaded application using the GlobalPlatform API.

***Firmware*:**

Athena IDProtect Version 010B.9288.0303

***Hardware*:**

Atmel AT90SC28872RCU Revision G

1.2 PHYSICAL CRYPTOGRAPHIC MODULE

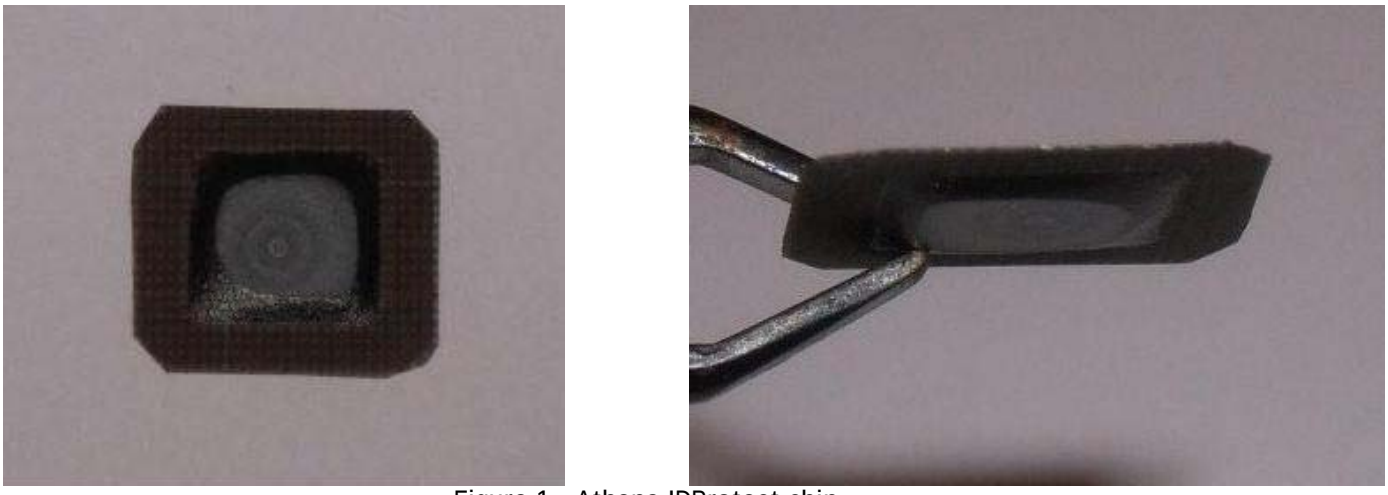


Figure 1 - Athena IDProtect chip

1.3 CRYPTOGRAPHIC MODULE BOUNDARY

The CM will typically be embedded into a plastic smart card body and connected to an ISO 7816 compliant contact plate. The CM boundary separates the chip from the card and contact plate.

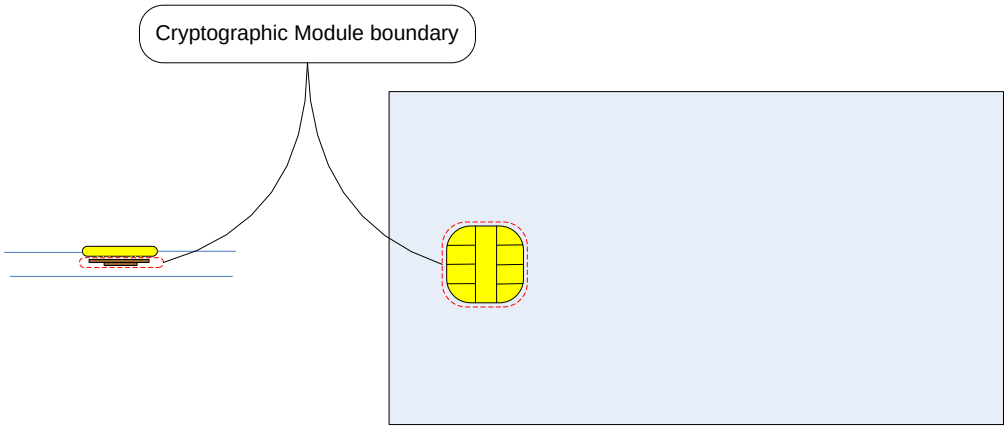


Figure 2 - Athena IDProtect CM and connectors

1.4 HARDWARE

The AT90SC28872RCU Revision G is a low-power, high-performance, 8-/16-bit microcontroller with ROM program memory, EEPROM code or data memory, based on the secure AVR enhanced RISC architecture and with a contact interface.

The cryptographic boundary is the edge of the chip itself, and not the entire smart card.

By executing powerful instructions in a single clock cycle, the AT90SC28872RCU Revision G achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the Arithmetic Logical Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

The AT90SC28872RCU Revision G uses the secure AVR architecture that allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of new functional and security features.

The AT90SC28872RCU Revision G features 72K bytes of high-performance EEPROM (fast erase/write time, high endurance).This allows system developers to offer their customers a true 64K bytes EEPROM, while still being able to use the remaining 8K bytes for their own purposes (customization and patches, for example). The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system.

The cryptographic accelerator featured in the AT90SC28872RCU Revision G is the new AdvX, an N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the secure AVR core which uses the AdvX accelerator during encryption/ decryption. AdvX is based on a 32-bit technology, thus enabling fast computation and low power operation. AdvX supports standard finite field arithmetic functions (including RSA) and arithmetic functions.

This product is specifically designed for smart cards and targets ID applications.

1.5 FIRMWARE

The embedded operating system is GlobalPlatform and Java Card compliant, is loaded on a contact interface smart card chip and supports communication protocols T=0 and T=1.

GlobalPlatform

- GlobalPlatform, Card Specification, Version 2.1.1, March 2003
- GlobalPlatform, Card Specification 2.1.1, Amendment A, March 2004

Java Card

- Runtime Environment Specification, Java Card Platform, Version 2.2.2, March 2006
- Application Programming Interface, Java Card Platform, Version 2.2.2, March 2006
- Virtual Machine Specification, Java Card Platform, Version 2.2.2, March 2006

Communication

- Protocol T=0 with PPS for speed enhancement
- Protocol T=1 with PPS for speed enhancement

The GlobalPlatform external interface and internal API allows for application loading and unloading, for secure communication between an application and a terminal and for the use of a PIN in the context of the entire CM. In particular, it allows for the loading of a special application called a Supplementary Security Domain that allows an Application Provider to separate their key space from the Card Administrator.

The Java Card API provides a large set of cryptographic related services. Some of these services rely on hardware.

Support for Random Numbers	DRNG	ANSI X9.31 two key TDES deterministic RNG seeded with the hardware RNG
Support for Message Digest	SHA-1	FIPS 180-2 Secure Hash Standard compliant hashing algorithms
	SHA-256	
Support for Signature	RSA PKCS#1	1024- to 2048-bit in 32-bit increments
Support for Cipher	TDES	112- and 168-bit ECB and CBC
	TDES MAC	Vendor affirmed
	AES	128-, 192- and 256-bit ECB and CBC
	RSA	1024- to 2048-bit in 32-bit increments
Support for On-Card Key Generation	RSA PKCS#1	1024- to 2048-bit in 32-bit increments

Table 1 – Supported Cryptographic Services

Note that SHA-1, SHA-256, AES, RSA, and RSA PKCS#1 key generation are only available to loaded applications; they are not used by the CM.

2 SECURITY LEVEL

This section details the security level met by this Cryptographic Module for each Security Requirement.

Security Requirement	Security Level
Cryptographic Module Specification	3 overall
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 2 – Security Level of Security Requirements

3 CRYPTOGRAPHIC MODULE SPECIFICATION

This module includes the Issuer Security Domain which allows the Card Issuer to manage the operating system and card content.

The Issuer Security Domain is the on-card representative of the Card Issuer. The ISD has application characteristics such as application AID, application privileges, and Life Cycle State (the Issuer Security Domain inherits the Life Cycle State of the card).

If additional applications are loaded into this module, then these applications require a separate FIPS 140-2 validation.

3.1 PHYSICAL INTERFACES

The physical interfaces of the Cryptographic Module depend on the physical characteristics of the module itself. This module provides the following physical interfaces for contact mode (ISO/IEC 7816 parts 2 and 3):

Interface	Description
RST	External Reset signal
I/O	Input/Output
CLK	External Clock signal 1 – 10.1MHz
VCC	Supply Voltage Power 1.62 – 5V
GRD	Ground

Table 3 – Physical Interfaces for contact mode

This module supports two transmission half-duplex oriented ISO protocols: T=0 and T=1.

Up to 256 bytes of data can be exchanged through one APDU command.

3.2 LOGICAL INTERFACES

The cryptographic module functions as a slave processor to process and respond to the reader commands. The I/O ports of the platform provide the following logical interfaces:

Interface	ISO 7816
Data In	I/O Pin
Data Out	I/O Pin
Status Out	I/O Pin
Control In	I/O, CLK and RST Pins

Table 4 – Logical Interfaces for all modes

4 MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the Athena IDProtect CM is to provide cryptographic services.

4.1 RANDOM NUMBER GENERATORS

The module includes the following random number generators:

- An ANSI X9.31 112-bit key TDES deterministic random number generator (DRNG).
  CAVP RNG Certificate #774
- A hardware random number generator (HRNG) that is used for seeding the DRNG.

4.2 CRYPTOGRAPHIC ALGORITHMS

The module includes the following cryptographic algorithms:

- SHA-1 and SHA-256
  CAVP SHS Certificate #1282
- TDES
  CAVP TDES Certificate #965
  - Encrypt/decrypt (for confidentiality purposes)
  - MAC (vendor affirmed, for integrity and authentication purposes)
  - CBC and ECB modes
  - 112- and 168-bit key lengths
- AES
  CAVP AES Certificate #1412
  - Encrypt/decrypt
  - CBC and ECB modes
  - 128-, 192- and 256-bit key lengths
- RSA
  CAVP RSA Certificate #688
  - PKCS#1 sign/verify
  - 1024- and 2048-bit key lengths

The module supports the following non-FIPS Approved algorithms:

- RSA encrypt/decrypt (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength)

4.3 CRITICAL SECURITY PARAMETERS

This module includes the following CSPs.

No interface is provided to retrieve any of these CSPs.

TDES Keys

Key Secure Storage Key

This CSP (KSSK) is a 16-byte TDES Key used to encrypt all other secret and private keys of this module when stored in EEPROM (that is, all TDES, AES and RSA keys).

It is generated at first reset of the card using the DRNG.

Keys secured with the KSSK are encrypted when created and decrypted each time they are used.

PIN Secure Storage Key

This CSP (PSSK) is a 16-byte TDES Key used to encrypt all PINs of this module when stored in EEPROM (that is, the GlobalPlatform Global PIN and Java Card OwnerPIN objects).

It is generated at first reset of the card using the DRNG.

PIN values are encrypted when created and never decrypted. Candidate PINs are encrypted with PSSK to perform the comparison.

CA ISD Key Set

This CSP is a set of three TDES keys used to manage GlobalPlatform Secure Channel Sessions between the ISD and the Card Administrator:

- CA-Kenc: Used to derive CA Session Key that will encrypt command data within a Secure Channel Session with C-DECRYPTION Security Level.
- CA-Kmac: Used to derive CA Session Key that will guarantee integrity of any data within a Secure Channel Session with C-MAC Security Level.
- CA-Kkek: Key Encryption Key used to encrypt the CA ISD Key Sets that are loaded in the CM with the PUT KEY command within a Secure Channel Session.

CA Session Key Set

This CSP is a set of two TDES keys derived during the GlobalPlatform Secure Channel Session establishment from a selected CA ISD Key Set. These two keys are used to secure exchanges from the Card Administrator to the ISD:

- CA-Senc: Encryption Session Key used to encrypt data exchanged within a Secure Channel Session with C-DECRYPTION Security Level.
- CA-Smac: MAC Session Key used to guarantee integrity of any data exchanged within a Secure Channel Session with C-MAC Security Level and to authenticate the Card Administrator.

AP SD Key Set

This CSP is a set of three TDES keys used to manage GlobalPlatform Secure Channel Sessions between a Security Domain (ISD or SSD) and the Application Provider:

- AP-Kenc: Used to derive AP Session Key that will encrypt command data within a Secure Channel Session with C-DECRYPTION Security Level.
- AP-Kmac: Used to derive AP Session Key that will guarantee integrity of any data within a Secure Channel Session with C-MAC Security Level.
- AP-Kkek: Key Encryption Key used to encrypt the AP ISD Key Sets that are loaded in the CM with the PUT KEY command within a Secure Channel Session.

AP Session Key Set

This CSP is a set of two TDES keys derived during the GlobalPlatform Secure Channel Session establishment from a selected AP SD Key Set. These two keys are used to secure exchanges from the Application Provider to the Security Domain:

- AP-Senc: Encryption Session Key used to encrypt data exchanged within a Secure Channel Session with C-DECRYPTION Security Level.
- AP-Smac: MAC Session Key used to guarantee integrity of any data exchanged within a Secure Channel Session with C-MAC Security Level and to authenticate the Application Provider.

PINs

Global PIN

This CSP is the GlobalPlatform Global PIN available on the GlobalPlatform API. It is created by the CM but is only available to loaded applications; it is not used by the CM.

RNG Seed Values

DRNG Seed and DRNG Seed Key

This CSP is an internal value computed using the HRNG and stored in the processor RAM. These values are not accessible to any user. The hardware processor overwrites all RAM during reset which will destroy any prior values of the DRNG Seed and DRNG Seed Key. The DRNG is the only card service that uses these values.

5 ROLES AND SERVICES

5.1 ROLES

Cryptographic Officer Roles	
Card Administrator	This role is responsible for managing the security configuration of the module. The Card Administrator authenticates to the module through the GlobalPlatform mutual authentication protocol. This protocol is based on the sharing of a TDES key set between him and the embedded Issuer Security Domain (ISD). Once authenticated, the Card Administrator is able to execute the services provided by the ISD in a Secure Channel Session (see [GP] for more details).
User Roles	
Application Provider	This role is responsible for managing the security configuration of a loaded application. The Application Provider authenticates to the module through the GlobalPlatform mutual authentication protocol. This protocol is based on the sharing of a TDES key set between him and the embedded Security Domain (SD) associated with the application. Once authenticated, the Application Provider is able to execute the services provided by the application in a Secure Channel Session (see [GP] for more details).
No Roles	
Public Operator	No-role operator who does not know any secrets related to the ISD. This non-authenticated operator can only access non-security relevant services provided by the ISD that do not require any prior authentication.
Maintenance Roles	
None	This CM does not support any maintenance role.

Table 5 - Roles description

Concurrent operators are not supported by this CM: only one logical data in/out interface is available to external operators.

5.2 IDENTIFICATION

This Cryptographic Module performs identity based authentication using cryptographic keys. A unique ID and version number are associated with each cryptographic key to uniquely identify the off-card entity performing the authentication.

Identity Authentication	
CA ISD Key Set	KVN, KID (see [GP])
AP SD Key Set	KVN, KID (see [GP])

Table 6 – Identity Authentication

5.3 ROLE AUTHENTICATION

This Cryptographic Module supports identity based authentication of the Card Administrator and Application Provider. For this mechanism, the two following properties stand:

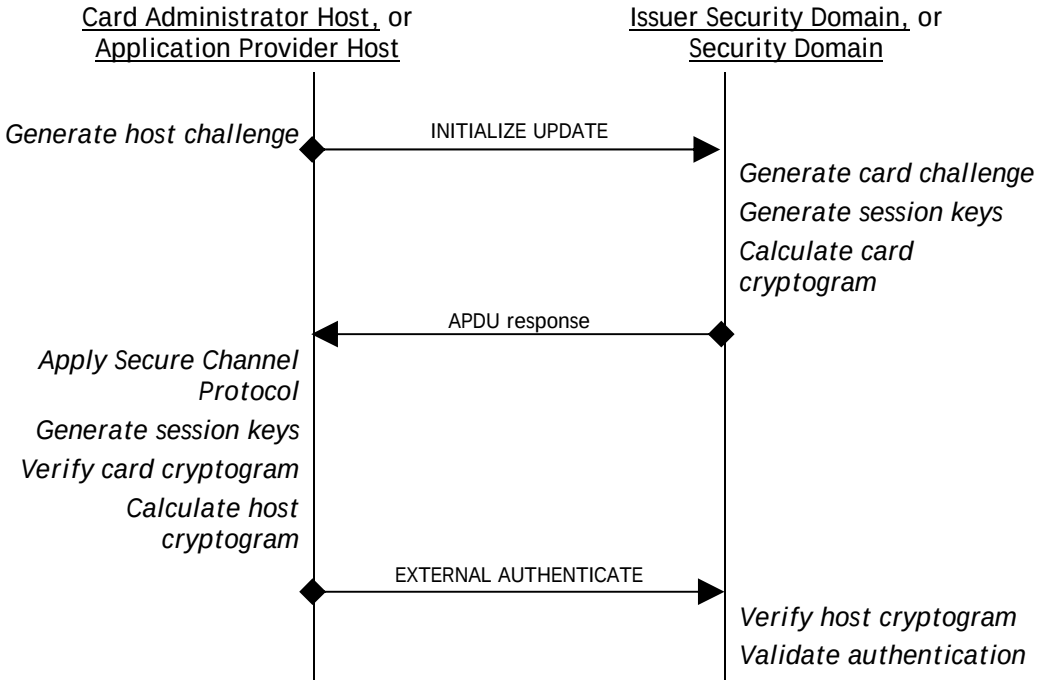
- the probability is less than one in 1,000,000 that a random attempt at authentication will succeed
- during any one minute period, the probability is less than 1 in 100,000 that a random authentication attempt will succeed

This mechanism includes a counter of failed authentication and a blocking mechanism. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The authentication mechanism is blocked when the associated counter reaches zero. The counter threshold is in the range one to 255 with default value 80. This mechanism is called velocity checking (see [GP]).

If the authentication mechanism of the ISD is blocked the CM is irreversibly terminated (the KSSK and PSSK are zeroized and the CM enters the GlobalPlatform TERMINATED state in which only the GET DATA service is available).

5.3.1 Card Administrator and Application Provider Authentication

The Card Administrator and Application Provider authenticate by opening a GlobalPlatform Secure Channel Session with the ISD and Security Domain respectively. This Secure Channel Session establishment involves two APDU commands as follows:



5.4 SERVICES

5.4.1 Card Administrator Services

This role can only be active when the ISD is currently selected.

Authentication	
INITIALIZE UPDATE	CA can initiate a GlobalPlatform Secure Channel Session, setting key set version and index.
EXTERNAL AUTHENTICATE	CA can open a GlobalPlatform Secure Channel Session with the ISD in order to communicate with it in a secure and confidential way.
Card Content Management	
INSTALL	CA can initiate or perform the various steps required for CM content management.
LOAD	CA can transfer a Load File to the CM.
DELETE (card content)	CA can delete a uniquely identifiable object such as an Executable Load File (package) or an Application (applet) or an Executable Load File and its related Applications.
PUT KEY	Regarding ISD keys, CA 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
DELETE (key)	CA can delete an ISD key uniquely identified by the KID and KVN.
SET STATUS	CA can modify the Card Life Cycle State or an Application Life Cycle State.
GET STATUS	CA 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.
STORE DATA	CA can transfer data to the ISD.
Public Commands	
SELECT	Operator can select an Application. This command also logs out the current role.
Public ISD Commands	
GET DATA	Operator can retrieve public data from the ISD. No CSPs can be read using this service.

5.4.2 Application Provider Services

This role can be active when a Security Domain is currently selected.

Authentication	
INITIALIZE UPDATE	AP can initiate a GlobalPlatform Secure Channel Session, setting key set version and index.
EXTERNAL AUTHENTICATE	AP can open a GlobalPlatform Secure Channel Session with the SD in order to communicate with it in a secure and confidential way.
Card Content Management	
INSTALL	AP can initiate or perform the various steps required for CM content management.
LOAD	AP can transfer a Load File to the CM.
DELETE (card content)	AP can delete a uniquely identifiable object such as an Executable Load File (package) or an Application (applet) or an Executable Load File and its related Applications.
PUT KEY	Regarding SD keys, AP can either: • Replace an existing SD key with a new key • Replace multiple existing SD keys with new keys • Add a single new SD key • Add multiple new SD keys
DELETE (key)	AP can delete a SD key uniquely identified by the KID and KVN.
SET STATUS	AP can modify the SD Life Cycle State or an associated Application Life Cycle State.
GET STATUS	AP can retrieve Life Cycle status information of the SD, Executable Load File, Executable Module, Application or Security Domain. No CSPs can be read using this service.
STORE DATA	AP can transfer data to the SD.
Public Commands	
SELECT	Operator can select an Application. This command also logs out the current role.
Public ISD Commands	
GET DATA	Operator can retrieve public data from the ISD. No CSPs can be read using this service.

5.4.3 Public User Services

Public Commands	
SELECT	Operator can select an Application.
Public ISD Commands	
GET DATA	Operator can retrieve public data from the ISD. No CSPs can be read using this service.

5.4.4 Relationship between services and roles

	Card Administrator	Application Provider	Public Operator
DELETE	X	X	
EXTERNAL AUTHENTICATE	X	X	
GET DATA	X	X	X
GET STATUS	X	X	
INITIALIZE UPDATE	X	X	
INSTALL	X	X	
LOAD	X	X	
PUT KEY	X	X	
SELECT	X	X	X
SET STATUS	X	X	
STORE DATA	X	X	

Table 7 - Services and associated roles

5.4.5 Relationship between services and CSPs

Relationship can be:

- Create (creation of the CSP object)
- Write
- Generate
- Execute (computation involving the CSP)
- Delete
- Zeroize

Key Secure Storage Key

Service	Type of access
First Card reset	Generate
INITIALIZE UPDATE	Execute
EXTERNAL AUTHENTICATE	Execute
LOAD	Execute
PUT KEY	Execute
SET STATUS (TERMINATED)	Zeroize

PIN Secure Storage Key

Service	Type of access
First Card reset	Generate
SET STATUS (TERMINATED)	Zeroize

The PSSK will be used only if the Global PIN is used by a loaded application.

CA ISD Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Execute	CA-Kenc, CA-Kmac
EXTERNAL AUTHENTICATE	Execute	CA-Kenc, CA-Kmac
PUT KEY	Execute/Write	CA-Kenc, CA-Kmac, CA-Kkek
DELETE (key)	Delete	CA-Kenc, CA-Kmac, CA-Kkek

CA Session Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Generate	CA-Senc, CA-Smac
Card reset	Delete	CA-Senc, CA-Smac

In a Secure Channel Session with Security Level C-MAC:

Service	Type of access	Key
DELETE	Execute	AP-Smac
EXTERNAL AUTHENTICATE	Execute	AP-Smac
GET DATA	Execute	AP-Smac
GET STATUS	Execute	AP-Smac
INSTALL	Execute	AP-Smac
LOAD	Execute	AP-Smac
PUT KEY	Execute	AP-Smac
SET STATUS	Execute	AP-Smac
STORE DATA	Execute	AP-Smac

In a Secure Channel Session with Security Level C-DECRYPTION and C-MAC:

Service	Type of access	Key
DELETE	Execute	AP-Senc, AP-Smac
EXTERNAL AUTHENTICATE	Execute	AP-Senc, AP-Smac
GET DATA	Execute	AP-Senc, AP-Smac
GET STATUS	Execute	AP-Senc, AP-Smac
INSTALL	Execute	AP-Senc, AP-Smac
LOAD	Execute	AP-Senc, AP-Smac
PUT KEY	Execute	AP-Senc, AP-Smac
SET STATUS	Execute	AP-Senc, AP-Smac
STORE DATA	Execute	AP-Senc, AP-Smac

AP SD Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Execute	AP-Kenc, AP-Kmac
EXTERNAL AUTHENTICATE	Execute	AP-Kenc, AP-Kmac
PUT KEY	Execute/Write	AP-Kenc, AP-Kmac, AP-Kkek
DELETE (key)	Delete	AP-Kenc, AP-Kmac, AP-Kkek

AP Session Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Generate	AP-Senc, AP-Smac
Card reset	Delete	AP-Senc, AP-Smac

In a Secure Channel Session with Security Level C-MAC:

Service	Type of access	Key
DELETE	Execute	AP-Smac
EXTERNAL AUTHENTICATE	Execute	AP-Smac
GET DATA	Execute	AP-Smac
GET STATUS	Execute	AP-Smac
INSTALL	Execute	AP-Smac
LOAD	Execute	AP-Smac
PUT KEY	Execute	AP-Smac
SET STATUS	Execute	AP-Smac
STORE DATA	Execute	AP-Smac

In a Secure Channel Session with Security Level C-DECRYPTION and C-MAC:

Service	Type of access	Key
DELETE	Execute	AP-Senc, AP-Smac
EXTERNAL AUTHENTICATE	Execute	AP-Senc, AP-Smac
GET DATA	Execute	AP-Senc, AP-Smac
GET STATUS	Execute	AP-Senc, AP-Smac
INSTALL	Execute	AP-Senc, AP-Smac
LOAD	Execute	AP-Senc, AP-Smac
PUT KEY	Execute	AP-Senc, AP-Smac
SET STATUS	Execute	AP-Senc, AP-Smac
STORE DATA	Execute	AP-Senc, AP-Smac

Global PIN

Service	Type of access
First Card reset	Create
SET STATUS (TERMINATED)	Zeroize

The Global PIN is only used by a loaded application.

5.5 SETTING MODULE IN APPROVED MODE OF OPERATION

The module is always in the approved mode of operation.

5.6 VERIFYING MODULE IS IN APPROVED MODE OF OPERATION

It is possible to verify that a module is in the approved mode of operation.

The Card Administrator must:

1. SELECT the ISD and send a GET DATA command with the CPLC Data tag '9F7F' and verify that the returned data contains fields as follows (other fields are not relevant here). This verifies the version of the operating system.

Data Element	Length	Value	Version
IC type	2	'010B'	AT90SC28872RCU Revision G
Operating system release date	2	'9288'	Firmware Version Part 1
Operating system release level	2	'0303'	Firmware Version Part 2

6 SELF-TESTS

6.1 POWER-ON SELF-TESTS

Each time this cryptographic module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged.

Cryptographic algorithm testing:

Known Answer Tests (KATs) are conducted for each cryptographic algorithm in one mode of operation. Known input data and answers are stored in EEPROM. The following KATs are performed in random order:

- ANSI X9.31 DRNG,
- SHA-1,
- SHA-256,
- TDES (encrypt and decrypt with 112-bit key in CBC mode),
- AES (encrypt and decrypt with 128-bit key in CBC mode),
- RSA PKCS#1 (sign and verify with 1024-bit private and public key),

KATs are performed prior to the dispatch of the first APDU command for processing. If one of the KATs fails the card goes mute (performs no further data or status input or output and must be reset). When the KATs are successfully completed an Answer To Reset (ATR) status message is output from the module indicating that all self-tests passed.

Firmware integrity testing:

A standard CRC16 checksum is used to verify that no 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 firmware integrity verification. If a test fails the card is irreversibly terminated (the KSSK and PSSK are zeroized and the CM enters the GlobalPlatform TERMINATED state in which only the GET DATA service is available).

6.2 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 generation/verification and encryption/decryption are tested). If the test fails the card goes mute (performs no further data or status input or output and must be reset).

Continuous RNG Tests:

The hardware RNG and DRNG are tested for repetition of serially output 64-bit values. If the test fails the card goes mute.

Firmware Load Test:

Application loading follows the GlobalPlatform 2.1.1 specifications: GlobalPlatform Secure Channel Session with TDES MAC (see [GP]). Note that a failed application load rolls back to the state prior to the load starting.

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

7 SECURITY RULES

This section details the rules that form the policy of the Cryptographic Module.

7.1 PHYSICAL SECURITY

The Cryptographic Module (CM) is a single-chip implementation which Cryptographic boundaries encompass the chip. The physical component of the CM is protected by a hard opaque tamper-evident metal active shield.

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 and state-of-the-art physical security features:
    - Dedicated Hardware for Protection Against SPA/DPA/DEMA Attacks
    - Advanced Protection Against Physical Attack, Including Active Shield
    - Environmental Protection Systems
    - Voltage Monitor
    - Frequency Monitor
    - Temperature Monitor
    - Light Protection
    - Secure Memory Management/Access Protection
- 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 metal cover), with high probability of causing serious damage to the chip while attempting to probe it or remove it from the module.

This IC is designed to meet Common Criteria EAL4+

7.2 AUTHENTICATION SECURITY RULES

This CM implements identical authentication mechanisms for each role. Each authentication mechanism includes the verification of the knowledge of a secret shared between the CM and the external operator, and, for each restricted service, verification that the authentication security status is granted.

Each of these secrets has a unique object reference that is used by the external operator to identify them:

- The CA ISD Key Set represents the role of the Card Administrator
- The AP SD Key Set represents the role of the Application Provider

7.3 APPLICATION LIFECYCLE SECURITY RULES

Additional applications can be loaded in the module after card issuance as specified in GlobalPlatform. However, these additional applications must be FIPS 140-2 validated before being loaded.

- Application loading is one of the services provided by the operating system that is restricted to the Card Administrator or Application Provider: a Secure Channel Session must be open between the external operator (more precisely the middleware the CA or AP is using to manage card content) and the ISD. Application loading is protected by a TDES MAC on every block of data.
- The application loading service is available before and after card issuance.
- The AP is responsible for application personalization and lifecycle management following GlobalPlatform.
- The AP is responsible for creating as many instances of loaded applets as required, according to card resources.

7.4 ACCESS CONTROL SECURITY RULES

This module manages sensitive data and services whose access is controlled by the following rules:

- CA ISD Key Set must be loaded through a GlobalPlatform Secure Channel Session ensuring their integrity and confidentiality (112-bit TDES encryption and a TDES based integrity checksum).
- AP SD Key Set must be loaded through a GlobalPlatform Secure Channel Session ensuring their integrity and confidentiality (112-bit TDES encryption and a TDES based integrity checksum).

7.5 KEY AND PIN MANAGEMENT SECURITY RULES

Key and PIN Material

This card supports the following CSPs:

Key name (CSP)	Type	Length	Strength
Key Secure Storage Key	TDES	112-bits	80-bits
PIN Secure Storage Key			
CA ISD Key Set			
AP SD Key Set			
CA Session Key Set	TDES session key	112-bits	80-bits
AP Session Key Set			
Global PIN	PIN	64- to 2048-bits	
DRNG Seed concatenated with DRNG Seed Key	TDES	112-bits	80-bits

This card can also support a range of symmetric and asymmetric keys:

Key name (CSP)	Type	Length	Strength
TDES keys	TDES	168-bits	112-bits
AES keys	AES	128-, 192- and 256-bits	128-, 192- and 256-bits
RSA keys	RSA	1024- and 2048-bits	80- and 112-bits

Key Generation

Key Secure Storage Key

The KSSK is generated at first reset of the card using the DRNG.

PIN Secure Storage Key

The PSSK is generated at first reset of the card using the DRNG.

Key Derivation

CA Session Key Set, AP Session Key Set

[GP] ISD Session keys are derived by the operating system upon opening a Secure Channel Session (successful mutual-authentication):

- CA-Smac Session Key: generated from CA-Kmac, used for protecting data integrity in GlobalPlatform Secure Channel Session secure mode (MAC).
- CA-Senc Session Key: generated from CA-Kenc, used for protection data confidentiality in GlobalPlatform Secure Channel Session mode (Encryption).
- AP-Smac Session Key: generated from AP-Kmac, used for protecting data integrity in GlobalPlatform Secure Channel Session secure mode (MAC).
- AP-Senc Session Key: generated from AP-Kenc, used for protection data confidentiality in GlobalPlatform Secure Channel Session mode (Encryption).

Key Entry

CA ISD Key Set, AP SD Key Set

These Keys are entered in the module using the PUT KEY APDU command for:

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

The CM enforces confidentiality while entering Security Domain secret keys using key encryption following [GP] (FIPS approved algorithms and operation mode). The CM provides no Security Domain secret key output. All secret values of these keys are entered encrypted with the TDES CA-Kkek or AP-Kkek identified during the GlobalPlatform Secure Channel Session initialization, when one of the Security Domain key sets is selected.

Key and PIN Storage

Key Secure Storage Key (KSSK)

PIN Secure Storage Key (PSSK)

These two keys are stored plaintext in EEPROM.

CA ISD Key Set, AP SD Key Set

These keys are stored encrypted with the TDES key KSSK in EEPROM. The CM also applies an integrity checksum to these Keys.

Global PIN

This PIN is stored encrypted with the TDES key PSSK in EEPROM. The CM also applies an integrity checksum to this PIN.

Key and PIN Output

No keys or PINs can be output from the module.

Key and PIN Zeroization

The CM offers services to zeroize all the persistent keys and PINs:

- The KSSK and PSSK are zeroized when Card lifecycle state is set to TERMINATED. The Card Administrator or Application Provider can achieve this explicitly using the SET STATUS command, or a severe security event may occur (failure of an integrity check on patches, EEPROM code, PINs or Keys). By zeroizing the KSSK and the PSSK, all other Keys and PINs stored in the module are made irreversibly unusable.

The CM offers services to zeroize all the session keys:

- When a Secure Channel Session is closed for any reason other than power-off, the CM overwrites the session keys with random data from the DRNG. When a Secure Channel Session is closed due to a power-off, the session keys are lost as they are stored in RAM. The RAM is actively cleared to zero on the next power-on.

RNG Seed Values

The CM offers services to randomize and overwrite all DRNG seed values and keys:

- During power up initialization, the CM computes new DRNG Seed and DRNG Seed Key values using the HRNG. Any old seed values (which were randomized) are then overwritten with the new computed values.

7.6 ELECTROMAGNETIC INTERFERENCE/COMPATIBILITY (EMI/EMC)

The Cryptographic Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

8 MITIGATION OF OTHER ATTACKS

Typical smart card attacks are Simple Power Analysis, Differential Power Analysis, Timing Analysis and 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.

This Cryptographic Module is protected against SPA, DPA, Timing Analysis and Fault Induction by combining State of the Art firmware 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. For more information see specification AT90SC Vulnerability Analysis Lite, General Business Use, AT90SC_EVA_Lite_V1.0 (17 Jul 06).

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.

9 SECURITY POLICY CHECK LIST

9.1 ROLES AND REQUIRED AUTHENTICATION

Role	Type of Authentication	Authentication Data
Card Administrator	TDES authentication	CA ISD Key Set
Application Provider	TDES authentication	AP SD Key Set

Table 8 - Roles and Required Identification and Authentication

9.2 STRENGTH OF AUTHENTICATION MECHANISM

Authentication Mechanism	Strength of Mechanism
TDES authentication with CA ISD Key Set	2^{80}
TDES authentication with AP SD Key Set	2^{80}

Table 9 - Strengths of Authentication Mechanisms

All these authentication objects implement a limited retry counter.

9.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Administrator	Section 5.4.1 lists authorized services for this role
Application Provider	Section 5.4.2 lists authorized services for this role

Table 10 - Services Authorized for Roles

9.4 MITIGATION OF ATTACKS

Other Attacks	Mitigation Mechanism	Specific Limitations
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Timing Attacks	Counter Measures against TA	N/A
Fault Induction	Counter Measures against FI	N/A

Table 11 - Mitigation of Other Attacks

10 REFERENCES

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	FIPS 140-2 Security Requirements for Cryptographic modules, May 25, 2001
[JCRE]	Runtime Environment Specification, Java Card Platform, Version 2.2.2, March, 2006
[JCAPI]	Application Programming Interface, Java Card Platform, Version 2.2.2, March, 2006
[JCVM]	Virtual Machine Specification, Java Card Platform, Version 2.2.2, March, 2006
[GP]	GlobalPlatform Card Specification, Version 2.1.1, March 2003
[7816-3]	ISO/IEC 7816-3, Third edition 2006-11-01, Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols
[7816-4]	ISO/IEC 7816-4, Second edition 2005-01-15, Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange

Table 12 - References

11 ACRONYMS AND DEFINITIONS

Acronym	Definition
AdvX	Advance Crypto
AP	Application Provider
API	Application Programming Interface
AVR	Automatic Voltage Regulation
CA	Card Administrator
CM	Cryptographic Module
CSP	Critical Security Parameter
DRNG	Deterministic Random Number Generator
GP	GlobalPlatform
HRNG	Hardware Random Number Generator
ISD	Issuer Security Domain
KSSK	Key Secure Storage Key
KID	Key Identifier, see [GP]
KVN	Key Version Number, see [GP]
PKCS	Public Key Cryptography Standard
PSSK	PIN Secure Storage Key
RNG	Random Number Generator
SD	Security Domain
SSD	Supplementary Security Domain

Table 13 – Acronyms and Definitions

[END OF THE DOCUMENT]