Athena SCS

iEngine SSID Applet on Athena SCS IDProtect Duo for SLE78

FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.1

Date: December 10, 2015

Table of Contents

1 Introduction 3

1.1 Firmware and Logical Cryptographic Boundary 4
1.2 Mode of Operation and Versioning 4

2 Cryptographic Functionality 5

2.1 Critical Security Parameters 5

3 Roles, Authentication and Services 6

3.1 Assumption of Roles 6
3.1.1 Secure Channel Authentication 6
3.1.2 PIN Authentication 6
3.2 Services 7

4 Self-tests 9

5 Physical Security Policy 9

6 Mitigation of Other Attacks Policy 9

7 Security Rules and Guidance 10

8 References and Definitions 10

List of Tables

Table 1 – Security Level of Security Requirements 3
Table 2 – Ports and Interfaces 3
Table 3 – Content Identification and Approved Mode Indicator - OS 4
Table 4 – Content Identification and Approved Mode Indicator - Applet 4
Table 5 - CAVP Validated Approved Cryptographic Functions 5
Table 6 - Non-Approved but Allowed Cryptographic Functions 5
Table 7 - Critical Security Parameters (CSPs) 5
Table 8 - Public Keys 5
Table 9 – Roles and Authentication 6
Table 10 – Authenticated Services 7
Table 11 – Unauthenticated Services 7
Table 12 - CSP Access Rights within Services 8
Table 13 – Power-Up Self-tests 9
Table 14 – Conditional Self-tests 9
Table 15 – References 10
Table 16 – Acronyms and Definitions 10

List of Figures

Figure 1 – Module 3
Figure 2 – Module Block Diagram 4

1 Introduction

This document defines the Security Policy for the iEngine SSID Applet on Athena SCS IDProtect Duo for SLE78 module, hereafter denoted the Module. The Module is a single-chip embodiment smart card micro-controller validated to FIPS 140-2 overall Level 3 requirements.

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module does not support firmware updates.

The FIPS 140-2 security levels for the Module are as follows:

Table 1 – Security Level of Security Requirements

Area	Description	Level
1	Module Specification	3
2	Ports and Interfaces	3
3	Roles and Services	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Key Management	3
8	EMI/EMC	3
9	Self-test	3
10	Development	3
11	Mitigation of Other Attacks	3
	Overall	3

The Module is designed to be embedded into a smart card that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module relies on an external card reader to communicate with host systems and applications.

The Module uses standard passivation, packaged in an epoxy coating with metal antenna coil connections: the cryptographic boundary is the surfaces and edges of the epoxy and coil connections. The physical form of the Module is depicted in Figure 1. The Module's ports and interfaces are shown in Table 2.

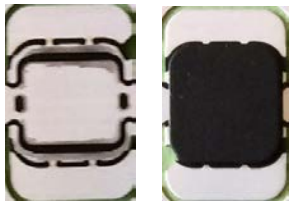

Figure 1 – Module

Table 2 – Ports and Interfaces

Port	Description	Logical Interface Type
LA, LB	ISO 14443 antenna coil connects	Control in, Data in, Data out, Status out, Power

1.1 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the major physical and logical components that comprise the Module.

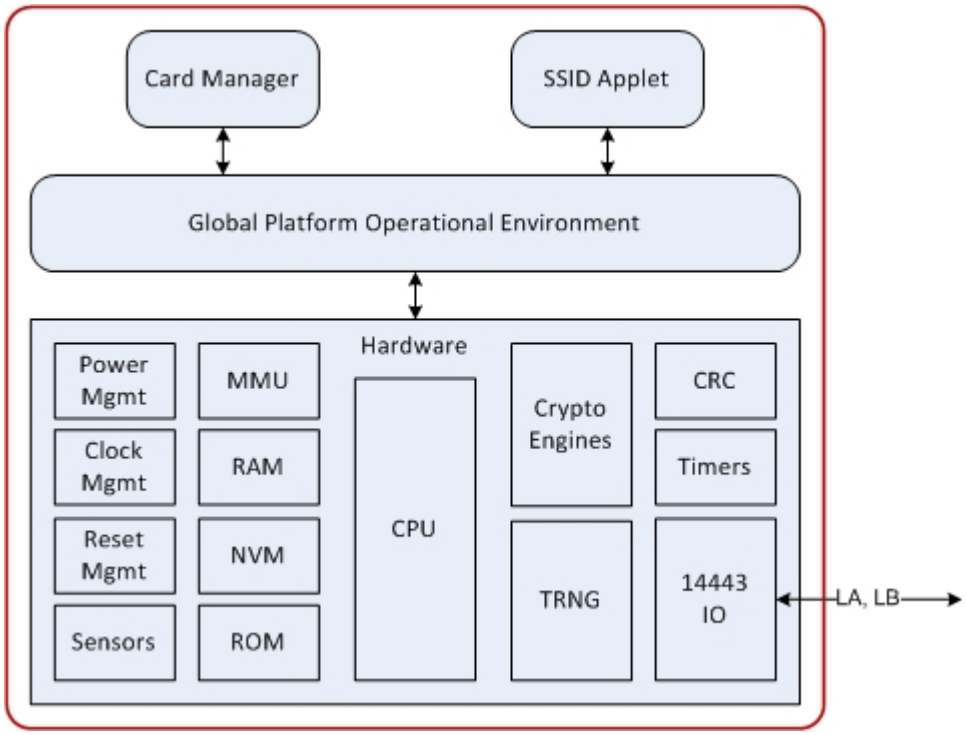

Figure 2 – Module Block Diagram

1.2 Mode of Operation and Versioning

The hardware and firmware version numbers for the Module are:

Hardware: Infineon SLE78CLFX4000P P-MCC8-2-6 package

Firmware: Athena IDProtect 0302.0306.0004 with iEngine SSID Applet V1.0.2

The Module is always in the Approved mode of operation. To verify that a module is in the Approved mode of operation, the *Manage Content* service is used to obtain the CPLC Data tag DF64 and DF65 and verify the following elements of the returned data:

Table 3 – Content Identification and Approved Mode Indicator - OS

Data Element	Length	Value	Associated Version
IC type	2	0302	Infineon SLE78CLFX4000P
Operating system release date	2	0306	Firmware Version Part 1
Operating system release level	2	0004	Firmware Version Part 2

Additionally, the operator may verify the package contents, using the *Manage Content* service to obtain tag 'DF65' and verify the following elements of the returned data:

Table 4 – Content Identification and Approved Mode Indicator - Applet

Data Element	Position	Value
Major Release	First nibble	1
Medium Release	Second nibble	0
Minor Release	Third nibble	2

2 Cryptographic Functionality

The Module implements the cryptographic functions listed in the tables below. Note that the Athena IDProtect OS contains additional cryptographic functionality that is unused in the module, so not included in Table 5.

Table 5 - CAVP Validated Approved Cryptographic Functions

Algorithm	Reference	Mode	Functions	Strength	Cert
AES	FIPS 197, SP 800-38A	CBC, ECB	Encrypt and decrypt	128	3435
AES CMAC	SP800-38C	CMAC	MAC Generation	128	3435
KDF	SP800-108	CTR KDF	Key Derivation	128	59
DRBG	SP 800-90A	Hash (SHA-256)	Random generation	256	836
ECDSA	FIPS 186-4	P-256	SigGen	128	690
SHA	FIPS 180-4	SHA-256	Digest generation for DRBG and SigGen	128 - 256	2835

Table 6 - Non-Approved but Allowed Cryptographic Functions

Algorithm	Reference
NDRNG	[Annex C] Hardware True RNG.

2.1 Critical Security Parameters

All CSPs used by the Module are listed in Table 7. The OS prefix denotes operating system, the SD prefix denotes the GlobalPlatform Security Domain and the SSID prefix denotes the SSID Applet.

Table 7 - Critical Security Parameters (CSPs)

Name	Description and usage
OS-DRBG_SEED	384 bit random value from HW RNG used to seed the DRBG.
OS-DRBG_STATE	880 bit value of current DRBG state.
OS-MKEK	AES-128 key used to encrypt all secret and private key data stored in NVM.
OS-PEK	AES-128 key used to encrypt all PINs stored in NVM.
SD-KENC	AES-128 key used to derive SD-SENC.
SD-KMAC	AES-128 key used to derive SD-SMAC and SD-SRMAC.
SD-SENC	AES-128 session encryption key used to decrypt secure channel data.
SD-SMAC	AES-128 MAC key used to verify inbound secure channel data integrity.
SSID-IAK	ECDSA P-256 internal authentication key for card authentication to the host.
SSID-PCHV1	8 byte PIN for cardholder authentication to the card (character space not restricted).
SSID-PCHV2	8 byte PIN for cardholder authentication to the card (character space not restricted).
SSID-PSO	8 byte PIN for Security Officer authentication to the card (character space not restricted).

Table 8 - Public Keys

Name	Description and usage
SSID-IAK-PUB	ECDSA P-256 internal authentication key.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Does not support GlobalPlatform SCP logical channels, so concurrent operations are not supported.

De-selection of the Card Manager or SSID applet, card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services. Authentication data is encrypted during entry (by SD-SENC), and is only accessible by authenticated services.

Table 9 lists all operator roles supported by the Module.

Table 9 – Roles and Authentication

Name	Description	Authentication
CO	Cryptographic Officer	SCP
SO	Security officer (the FIPS User role)	8 digit PIN
CH	Cardholder	8 digit PIN

3.1.1 Secure Channel Authentication

The Secure Channel Protocol authentication method is provided by the *Secure Channel* service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated.

The probability that a random attempt will succeed using this authentication method is 1/2^128 (2.9E-39) (based on the AES block size), which is less than 1/1,000,000.

The Module enforces a maximum of 7 failed SCP authentication attempts. After 7 failed authentication attempts, the module enters the terminate ISD error state. The probability that a random attempt will succeed over a one minute interval is 7/2^128 (2.1E-38), which is less than 1/100,000.

3.1.2 PIN Authentication

PIN authentication is performed using an 8 digit PIN. Each digit is a full byte; the card does not limit the character space.

The probability that a random attempt will succeed using this authentication method is 1/256^8 (5.4E-20), which is less than 1/1,000,000.

The Module enforces a maximum of 5 failed PIN authentication attempts. After 5 failed authentication attempts, the PIN is locked and must be unlocked by the CO. The probability that a random attempt will succeed over a one minute interval is 5/256^8 (2.7E-19), which is less than 1/100,000.

3.2 Services

All services implemented by the Module are listed in the tables below.

Table 10 – Authenticated Services

Service	Description	CO	SO	CH
Lifecycle	Modify the card or applet life cycle status.	x		
Secure Channel	Establish and use a secure communications channel.	x		
Manage Content	SSID applet cardholder information management.	x	x	x
Privileged info	Read module configuration or status information (privileged data objects).	x		
SSID Privileged info	Read SSID configuration or status information (privileged data objects) e.g. cardholder data.		x	x
SSID PIN Authenticate	Authenticate to the module using the SO or CH PIN.	x		

Table 11 – Unauthenticated Services

Service	Description
Context	Select an applet.
General info	Read unprivileged data objects, e.g. status information.
Reset	Power cycle or reset the Module. Includes Power-On Self-Test.
SSID Authenticate	Cardholder authentication to the external access control system.
SSID Context	Select SSID file node.
SSID Info	Read unprivileged data objects, e.g. cardholder data.

Table 12 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates or derives the CSP
- R = Read: The CSP is read from the module (CSP output)
- E = Execute: The module executes using the CSP
- W = Write: The CSP is written to the module (CSP entry)
- Z = Zeroize: The module destroys the CSP.
- -- = No access of the CSP by the service.

Table 12 - CSP Access Rights within Services

Service	CSPs											
	OS-DRBG_SEED	OS-DRBG_STATE	OS-MKEK	OS-PEK	SD-KENC	SD-KMAC	SD-SENC	SD-SMAC	SSID-IAK	SSID-PCHV1	SSID-PCHV2	SSID-PSO
LIFECYCLE	--	--	Z	Z	Z	Z	--	--	Z	Z	Z	Z
SECURE CHANNEL	E	E	E	--	E	E	G/E	G/E				
MANAGE CONTENT	--	--	--	--	--	--	E	E	--			
PRIVILEGED INFO	--	--	--	--	--	--	E	E	--			
SSID PRIVILEGED INFO				--			E	E				
SSID PIN AUTHENTICATE	--	--	--	E			E	E	--	E	E	E
CONTEXT	--	--	--	--	--	--	--	--	--			
GENERAL INFO	--	--	--	--	--	--	--	--	--			
RESET	Z	Z	--	--	--	--	Z	Z	--			
SSID AUTHENTICATE	--	--	--	--	--	--	--	--	E			
SSID CONTEXT	--	--	--	--	--	--	--	--	--			
SSID INFO	--	--	--	--	--	--	--	--	--			

4 Self-tests

On power up or reset, the Module performs the self-tests described in Table 13 below. Power-up self–tests are available on demand by power cycling the Module. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the "CM is mute" error state. Table 14 lists conditional self-tests performed by the Module, invoked when the listed condition occurs.

Table 13 – Power-Up Self-tests

Test Target	Description
FW Integrity	Firmware integrity test on all modifiable firmware code.
DRBG	Performs the DRBG KAT.
AES	Performs separate encrypt and decrypt KATs using an AES-128 in CBC mode.
AES CMAC	Performs a MAC generate/verify KAT.
ECDSA	Performs a signature generation and verification pair wise consistency test using P-256.
SHA 256	Performs a hash KAT.

Table 14 – Conditional Self-tests

Test Target	Description
DRBG	SP 800-90A health-test monitoring functions, invoked prior to first use of the DRBG.
DRBG	AS09.42 Continuous RNG Test, invoked each time the DRBG is used.

Note: The HW RNG is only called once per power cycle. Per IG 9.8, the NDRNG is not subject to the CRNGT.

5 Physical Security Policy

Physical inspection at the Module boundary is not practical after packaging. The Module also provides a transport key to protect against tampering during manufacturing and the protections listed in Section 6 next.

6 Mitigation of Other Attacks Policy

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 CSPs by monitoring the module power consumption and timing of operations or bypass sensitive operations.

This Module is protected against SPA, DPA, Timing Analysis and Fault Induction by combining State of the Art firmware and hardware counter-measures.

The 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. This chip is Common Criteria certified; more information is available at http://www.commoncriteriaportal.org/products/.

All cryptographic computations and sensitive operations provided by the Module are designed to be resistant to timing and power analysis. 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 Module does not operate in abnormal conditions such as extreme temperature, power and external clock, increasing its protection against fault induction.

7 Security Rules and Guidance

The Module implementation enforces the following security rules:

- The Module does not output CSPs (plaintext or encrypted).
- The Module does not support manual key entry.
- The Module does not output intermediate key values.
- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during self-tests, zeroization, key generation, and error states.
- There are no restrictions on which CSPs are zeroized by the zeroization service.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.

8 References and Definitions

Table 15 – References

Abbreviation	Full Specification Name
[FIPS113]	Computer Data Authentication
[FIPS140-2]	Security Requirements for Cryptographic Modules
[FIPS180-4]	Secure Hash Standard (SHS)
[FIPS186-2]	Digital Signature Standard (DSS)
[FIPS186-4]	Digital Signature Standard (DSS)
[FIPS197]	Advanced Encryption Standard (AES)
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard June 2002
[SP800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP800-90]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Table 16 – Acronyms and Definitions

Acronym	Definition
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter
DPA	Differential Power Analysis
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
LA and LB	Smartcard antenna connectors.
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis
SSID	Singapore Standards for Identification