KONA N41M0

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Document Version: 1.1.6

Date: 10/13/2015

CHANGE RECORD

Revision	***Date***	***Author***	***Description of Change***
1.1.0			
1.1.1	Jan 6, 2015	KONA I	Reordering of table 10, table 11, and table 12 Removing useless CSPs(SD-SDEK, and DAP-SYM)
1.1.2	Feb 11, 2015	KONA I	Removing triple DES keys in operation system CSPs.
1.1.3	Feb 23, 2015	KONA I	Updates during final review.
1.1.4	April 29, 2015	KONA I	Update misprint in Figure 3 and PKI Applet version number.
1.1.5	Sep 23, 2015	KONA I	Update regarding DRBG HEALTH CHECK functionality
1.1.6	Oct 13, 2015	KONA I	Update regarding description of AES in Table 6

Table of Contents

List of Tables

List of Figures

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1,*Jan 2011, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2*AmendmentD, Sept 2009
[ISO 7816]	ISO/IEC 7816-1: 1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[JavaCard]	*Java Card 3.0.4 Runtime Environment (JCRE) Specification* *Java Card 3.0.4Virtual Machine (JCVM) Specification* *Java Card 3.0.4Application Programming Interface* Published by Sun Microsystems, March 2006
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[SP 800-90A]	NIST Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25July 2013
[ETSI TS 102 613]	Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics
[ETSI TS 102 622]	Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)
[ETSI TS 102 705]	Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications

Table 1: References

Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DF	Dedicated File
DPA	Differential Power Analysis
EF	Elementary File
GP	GlobalPlatform
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NFC	Near Field Communication
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
OP	Open Platform (predecessor to GlobalPlatform)
PCT	Pair-wise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis
SWP	Single Wire Protocol
TPDU	Transaction Protocol Data Unit, see [ISO 7816]

Table 2: Acronyms and Definitions

1 Overview

This document defines the Security Policy for the KONA I Co., Ltd. KONA N41M0 cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 3, is a single chip module implementing the Global Platform operational environment, with Card Manager and a PKI Applet.

The PKI Applet is available for any Cryptographic solution the card may give. The term *platform* herein is used to describe the chip and operational environment, not inclusive of the PKI Applet.

The Module is a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

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

Security Requirement	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	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 3: Security Level of Security Requirements

The Module and the PKI Applet implementation are compliant with:

- [ISO 7816] Parts 1-4 (the Module)
- [ISO 7816] Parts 4, 8 and 9 (PKI Applet)
- [ETSI TS 102 613]

- [ETSI TS 102 622]
- [JavaCard]
- [GlobalPlatform]

1.1 Versions, Configurations and Modes of Operation

Hardware: Infineon SLE97CNFX1M00PEA22 (supports Contact ISO 7816 and ETSI TS 102 613)

Firmware: KONA N41M0 v2.01 and PKI Applet v1.3.3

The module is always in an Approved mode of operation. The module does not support a non-Approved mode of operation. To determine if this is a FIPS certified module operating in the Approved mode of operation, call the Module Info and Applet Info services and compare the Hardware/Firmware versions to the versions on the FIPS certificate.

1.2 Hardware and Physical Cryptographic Boundary

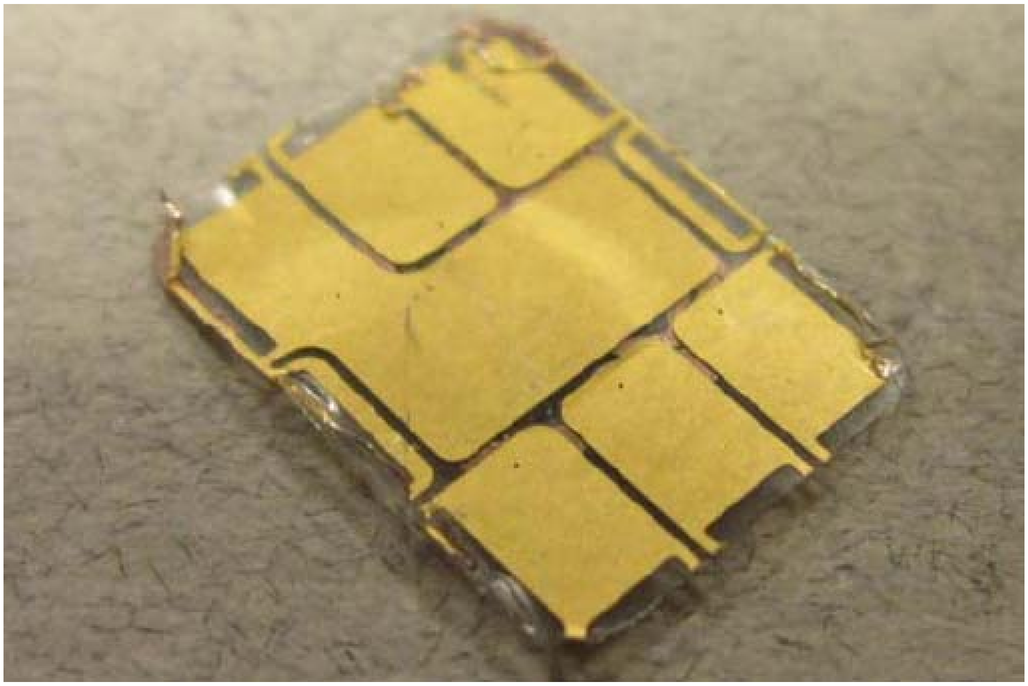

Figure 1: KONA N41M0 Chip (Front)

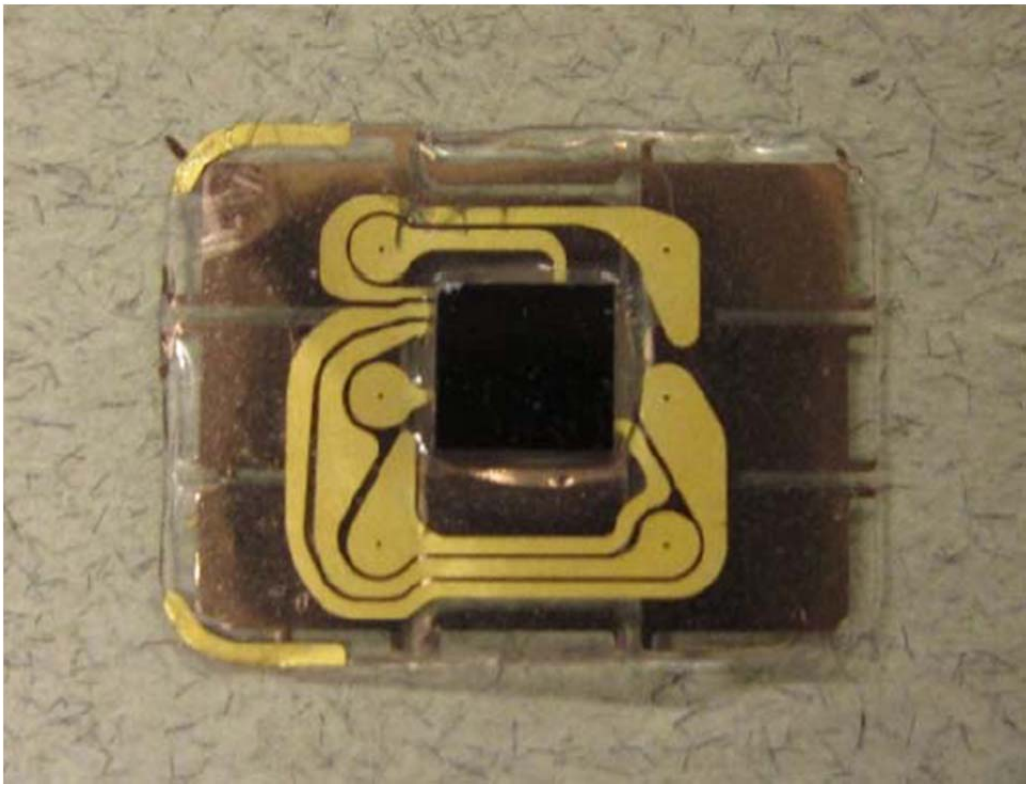

Figure 2: KONA N41M0 Chip (Back)

The Module is designed to be embedded into six (6) form factors: plastic card bodies, USB tokens, key FOBs, secure SD cards, embedded secure elements, and (U) SIMs. The physical form of the Module is depicted in Figure 1 and 2; this shows the physical cryptographic boundary, representing the surface of the chip and the bond pads. In production use, the Module is delivered to either vendors or end user customers in the following various forms:

- As bare die in wafer form for direct chip assembly by wire bonding or flip chip assembly
- Wire bonded and encapsulated by epoxy with additional packaging (e.g., Dual Interface Modules; Contact only Modules; Contactless Modules; SMD packages)
- For plastic card bodies and secure SD cards form factor, the Module relies on [ISO7816] card readers as input/output devices.
- For key FOBs form factor, the Module relies on [ETSI 102 613] card readers as input/output devices.
- For USB token, embedded secure elements and (U) SIM form factors, the Module relies on [ISO7816] and [ETSI 102 613] card readers as input/output devices.

Port	Description	Logical Interface Type
V_{CC}, GND	ISO 7816: Supply voltage	Power
RST	ISO 7816: Reset	Control in
CLK	ISO 7816: Clock	Control in
I/O	ISO 7816: Input/output	Control in, Data in, Data out, Status out

Port	Description	Logical Interface Type
V_{pp}	ETSI 102 613: SWP	Control in, Data in, Data out, Status out

Table 4: Ports and Interfaces

1.3 Firmware and Logical Cryptographic Boundary

Figure 3 depicts the Module operational environment.

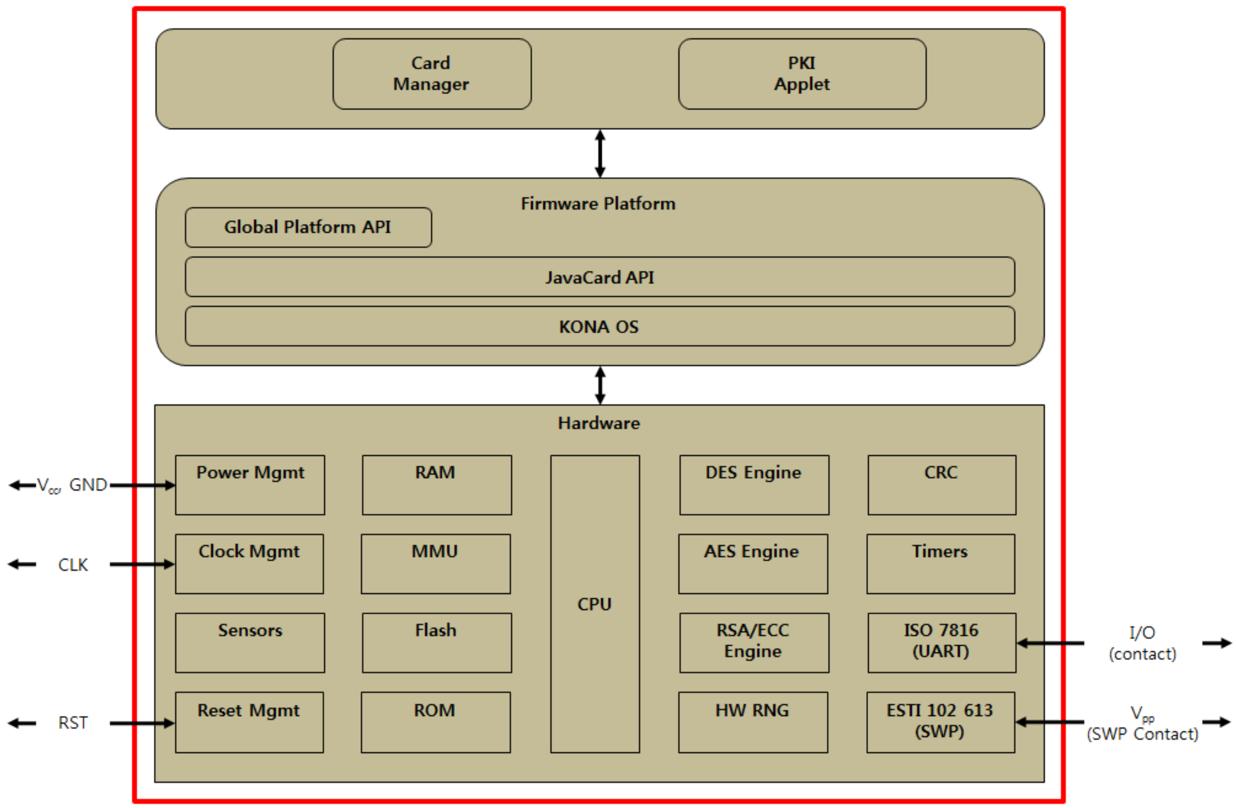

Figure 3: Module Block Diagram

- The ISO 7816 UART supports the T=0 and T=1 communications protocol variants

  The entire logical interfaces (data I/O, control, status) path through the ISO 7816 port
- The ETSI 102 613 SWP supports Single Wire communication protocol variants
- 1016 KB FLASH; 32 KB RAM

Section 3 describes applet functionality in greater detail. The JavaCard and Global Platform APIs are internal interfaces available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

2 Cryptographic Functionality

The Module implements the Approved and non-Approved but allowed cryptographic functions listed below in Table 5: Approved Cryptographic Functions and Table 6: Non-Approved but Allowed Cryptographic Functions Table.

Algorithm	Description	Cert. #
DRBG	[SP 800-90A] CTR_DRBG with security strength 128,192 and 256.	884
Triple-DES	[SP 800-67] Triple Data Encryption Standard (TDES) algorithm. The module supports the 2-Key[1] and 3-Key options; CBC and ECB modes.	1979
Triple-DES MAC	[FIPS113] Triple-DES MAC (Triple-DES Cert. #1979)	Vendor Affirmed
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports 128, 192, and 256-bit key lengths and ECB and CBC modes.	3525
AES CMAC	[SP800-38B] AES-256 CMAC	3525
HMAC	[FIPS 198-1] The module supports generation and verification with SHA-1, SHA-256, and SHA-512; key lengths >= 112 bits.	2253
SHA-1, SHA-2	[FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms; SHA-1, SHA-256, SHA-384, and SHA-512.	2907
RSA	[FIPS 186-4] RSA key generation, signature generation, and signature verification. The module supports 2048-bit RSA keys with SHA-2 for key generation, signature generation, and signature verification. For legacy use, the module supports 1024-bit RSA keys and SHA-1 for signature verification.	1811
RSA CRT	[PKCS#1] RSA key generation, signature generation, and signature verification. The module supports 2048-bit RSA keys with SHA-2 for key generation, signature generation, and signature verification. For legacy use, the module supports 1024-bit RSA keys and SHA-1 for signature verification.	1812
ECDSA	[FIPS 186-4] EllipticCurve Digital Signature Algorithmes. The module supports the NIST defined P-256, P-384, and P-521 curves for key pair generation, signature generation, and signature verification. For legacy use, the module supports P-192 and P-224 curves and SHA-1 for signature verification.	718

Table 5: Approved Cryptographic Functions

[1] 2-Key TDES Encryption is Restricted per SP 800-131A to limit the total number of blocks of data encrypted with the same cryptographic key to be no greater than 2^20. This restriction is implemented in the module's firmware.

Algorithm	Description
NDRNG	Hardware RNG. The HW RNG output used to seed the FIPS approved DRBG with entropy depending on DRBG's instantiated security strength. *Note*: The NDRNG only produces about 98% min-entropy. This will still initialize the Approved DRBG with the required >=112 bits of security. More specifically, it lowers the DRBG's security strength to 125 bits of security for AES-128 CTR_DRBG, 188 bits of security for AES-192 CTR_DRBG, and 250 bits of security for AES-256 CTR_DRBG.
Symmetric Key Wrap	AES (Cert. #3525, key wrapping)
Non-SP 800-56A Compliant ECDH	[IG D.8] EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)

Table 6: Non-Approved but Allowed Cryptographic Functions

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs is described in the services detailed in Section 4. In the tables below, the following prefixes are used:

- OS prefix denotes operating system.
- SD prefix denotes the GlobalPlatform Security Domain.
- DAP prefix denotes the GlobalPlatform Data Authentication Protocol.
- PKI prefix denotes a PKI Applet CSP.

CSP	Description/Usage
OS-RNG-SEED	256, 320, 384bits seed (entropy input) to AES-128/192/256 based CTR_DRBG.
OS-RNG-STATE	The current DRBG state. CSPs as described in FIPS IG 14.5.
OS-MKEK	3-Key Triple-DES master key used to encrypt all keys stored in NVM.
SD-KENC	AES-128 master key used to generate SD-SENC.
SD-KMAC	AES-128 master key used to generate SD-SMAC.
SD-KDEK	AES-128 sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES-128 session encryption key used to encrypt/decrypt secure channel data.
SD-SMAC	AES-128 session CMAC key used to verify inbound secure channel data integrity.
PKI-AUTH	Only one (1) AES-128 (SCP03) Key used by the *Authenticate* service.
PKI-KAP-PRI	Only one (1) EC P-256/384/521 private key of temporarily generated EC key-pair used by the EC DH Key Agreement.
PKI-MAC	0 to 15 Triple-DES (2/3-Key)/AES-256 CMAC or HMAC (16-32 bytes) keys are used by the *Message Authentication* service.
PKI-SGV-PRI	0 to 20 (10 for RSA and 10 for EC) RSA/RSA-CRT 2048-bit or EC P-256/384/521 private keys are used by the *Key Pair Generation* and *Digital Signature* services.
PKI-CSP-WRAP	Only one (1) AES-256 key used for wrap/unwrap other CSPs and Random Output by *Update CSPs, Get Data, PIN Verify, Reset Retry Counter and Random Number Generation services*. At the Very beginning this container initialized with AES-256 key by ECDH Key Agreement Service.
PKI-CON-SECRET	0 to 20 Triple-DES (2/3-Key) or AES-128/192/256 keys are used by the *Confidentiality* service.
PKI-SO-PIN	4 to 8-byte hex-string for unblocking USER-PIN. The PKI Applet has only one (1) instance for storing the Security Officer (SO) PIN.
PKI-USER-PIN	4 to 8-byte hex-string for user authentication to access files that require PIN Authentication. The PKI Applet has only one (1) instance for storing the User PIN.

Table 7: Critical Security Parameters

2.2 Public Keys

Key	Description/Usage
DAP-PUB	RSA 2048-bit new firmware signature verification key.
PKI-KAP-PUB	Only one (1) container to store P-256, P-384, and P-521 public keys of temporarily generated EC key-pair at ECDH Key Agreement Service.
PKI-SGV-PUB	0 to 20 (10 for RSA and 10 for EC) RSA/RSA-CRT 2048-bit or EC P-256/384/521 public keys are used by the *Key Pair Generation, Get Data* and *Digital Signature* services.
PKI-3P-PUB	0 to 15 3rd party public key containers is available in PKI-Applet. RSA-1024/2048 bits public key, EC P-192, P-224, P-256, P-384 and P-521 public keys are used for Digital Signature Verification. PKI-3P-PUB container can also be used in Get Data service.

Table 8: Public Keys

3 Roles, Authentication and Services

The Module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage.

- Only one operator at a time is permitted on a channel.
- Applet de-selection (including Card Manager), 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-KDEK), is stored in plaintext and is only accessible by authenticated services.
- Context service (SELECT) enables operator role change. Because SELECT procedure contains applet de-selection in it, re-authentication is required.

Lists of all operator roles supported by the Module.

Role ID	Role Description	Authentication Type	Authentication Method
CO	Cryptographic Officer – manages Module content and configuration, including issuance and management of Module data via the ISD.	Identity-based	*Secure Channel Protocol Authentication*
User	User – can run PKI Applet services.	Identity-based	*PKI Applet Authentication*

Table 9: Roles Supported by the Module

3.1 Secure Channel Protocol Authentication Method

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 external entity is authenticated to the Module in the CO role).

The probability that a random attempt will succeed is 1/2^128 = 2.9E-39 (assuming a 128-bit block).

The maximum number of consecutive authentication attempts before a card error occurs is 300. So the corresponding conservative upper bound for the number of authentication attempts in a one-minute period is 300. Therefore, the probability that a random attempt at authentication will succeed in a one-minute period is 300/2^128 = 8.8E-37.

3.2 PKI Applet Authentication Method

The PKI Applet uses a predetermined datum (PKI-AUTH) and AES-128 (SCP03) to authenticate the User operator. The probability that a random attempt at authentication will succeed is determined by the message size (128 bits for SCP03), chosen to correspond to the algorithm block size.

The probability that a random attempt at authentication will succeed is 1/2^128=2.9E-39.

The maximum number of consecutive authentication attempts before a card error occurs is 2^24. So the corresponding conservative upper bound for the number of authentication attempts in a one-minute period is 2^24. Therefore, the probability that a random attempt at authentication will succeed in a one-minute period is (2^24)/(2^128) = 4.9E-32.

3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

All services which allow user access to the secret keys, private keys, and CSPs are authenticated service, so unauthorized user can't read or edit the secret keys, private keys, and CSPs.

Service	Description	CO	User
Secure Channel	Establish and use a secure communications channel (INITIALIZE UPDATE; EXTERNAL AUTHENTICATE).	X	
Context	Select an Applet or manage logical channels (APDU: SELECT, MANAGE CHANNEL).	X	
Module Info (Unauthenticated)	Read unprivileged data objects or module information, e.g. Module configuration or status information (APDU: GET DATA, GET STATUS).	X	
Applet Info (Unauthenticated)	Read Applets Information (APDU: GET DATA) of PKI-Applet by User Role.		X
Authenticate	PKI Applet authentication service (SCP-03).		X
Module Reset	Power cycle or reset the Module. Includes Power-On Self-Test.	X	

Table 10: Unauthenticated Services

Service	Description	CO	User
Lifecycle	Modify the card or applet life cycle status (SET STATUS). By calling SET STATUS (TERMINATE) APDU, the status of applet become TERMINATE, and applet CSPs zeroization is performed.	X	
Manage Content	Load and install application packages and associated keys and data (APDU: DELETE; LOAD; INSTALL; PUT KEY; STORE DATA). Zeroize can be performed by calling DELETE APDU, used to delete the PKI Applet and CSPs.	X	
Activation	Activates PKI-Applet, DF/EFs. And also Deactivate EFs (APDU: ACTIVATE APPLET, ACTIVATE FILE and DEACTIVATE FILE).		X
File Management Service	Creates and Selects EF's and DF's (APDU: CREATE FILE, SELECT FILE).		X
Data File Operation	Updates, reads or erase binary into Transparent EFs (APDU: UPDATE BINARY, READ BINARY and ERASE BINARY).		X
Update CSPs	Update Secret keys, Public Keys and initialized PIN reference data.		X
Reset Retry Counter	Resets the reference data (PIN) retry counter to its initial value, or changes/updates reference data on completion of the reference data retry counter to its initial value for both SO_PIN and USER_PIN.		X
PIN Verify	Authenticate the user by comparing the verification data (PIN) with the reference data stored in the applet internally.		X
Random Number Generation	Generates Random Number by NDRBG/DRBG and return a random number.		X
Key Pair Generation	Generates RSA and ECDSA key-pair.		X
Get Data	Retrieves Public keys in plain form and secret keys in encrypted form.		X
Manage Security Environment	Manage the security environment for performing security operations with key and algorithm.		X
Digital Signature	Signature generation and signature verification with RSA and ECDSA.		X
Message Authentication	Generates and verifies MAC by Triple-DES MAC, AES CMAC, and HMAC.		X
Message Digest	Generates Digest using SHA-1 and SHA-2.		X
Confidentiality	Encrypt/Decrypt plain text with AES-128/192/256 Keys or TDES-2/3 keys.		X
Key Agreement	Creates shared secret by allowed EC DH.		X
Destroy PKI Applet CSPs	Destroys (Zeroizes) all PKI Applet CSPs and delete Profile.		X

Table 11: Authenticated Services

Service	CSPs and Public Keys																			
	OS-RNG-SEED	OS-RNG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	PKI-AUTH	PKI-KAP-PRI	PKI-MAC	PKI-SGV-PRI	PKI-CSP-WRAP	PKI-CON-SECRET	PKI-SO-PIN	PKI-USER-PIN	DAP-PUB	PKI-KAP-PUB	PKI-SGV-PUB	PKI-3P-PUB
Secure Channel	--	E W	E	E	E	E	G E W	G E W	--	--	--	--	--	--	--	--	--	--	--	--
Context	--	--	--	--	--	--	Z	Z	--	--	--	--	--	--	--	--	--	--	--	--
Module Info (Unauth)	--	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--	--
Applet Info (UnAuth)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Authenticate	--	--	E	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--
Module Reset	G E W Z	G E W Z	W I	--	--	--	Z	Z	--	--	--	--	--	--	--	--	--	--	--	--
Lifecycle	Z	Z	Z	Z	Z	Z	E	E	Z	Z	Z	Z	Z	--	Z	Z	--	--	--	--

Service	CSPs and Public Keys																			
	OS-RNG-SEED	OS-RNG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	PKI-AUTH	PKI-KAP-PRI	PKI-MAC	PKI-SGV-PRI	PKI-CSP-WRAP	PKI-CON-SECRET	PKI-SO-PIN	PKI-USER-PIN	DAP-PUB	PKI-KAP-PUB	PKI-SGV-PUB	PKI-3P-PUB
Manage Content	--	--	E	W I Z	W I Z	W I Z	E Z	E Z	W Z	Z	Z	Z	Z	Z	Z	Z	E W I	--	--	--
Activation	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
File Management Service	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Data File Operation	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Update CSPs	--	--	E	--	--	--	--	--	W I	--	W I	--	E W I	W I	W I	W I	--	--	--	W I
Reset Retry Counter	--	--	E	--	--	--	--	--	--	--	--	--	E	--	E W I	E W I	--	--	--	--
PIN Verify	--	--	E	--	--	--	--	--	--	--	--	--	E	--	E	E	--	--	--	--
Random Number Generation	G E W I Z	G E W Z	E	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--

Service	CSPs and Public Keys																			
	OS-RNG-SEED	OS-RNG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	PKI-AUTH	PKI-KAP-PRI	PKI-MAC	PKI-SGV-PRI	PKI-CSP-WRAP	PKI-CON-SECRET	PKI-SO-PIN	PKI-USER-PIN	DAP-PUB	PKI-KAP-PUB	PKI-SGV-PUB	PKI-3P-PUB
Key Pair Generation	G E W Z	G E W Z	E	--	--	--	--	--	--	--	--	G W	--	--	--	--	--	--	G W	--
Get Data	--	--	E	--	--	--	--	--	--	--	O	--	E	O	--	--	--	--	O	O
Manage Security Environment	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Digital Signature	--	E W	E	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	E	E
Message Authentication	--	--	E	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--
Message Digest	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Confidentiality	--	--	E	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	
Key Agreement	--	--	E	--	--	--	--	--	--	G E W Z	--	--	G W	--	--	--	--	G E W O Z	--	--

Service	CSPs and Public Keys																			
	OS-RNG-SEED	OS-RNG-STATE	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	PKI-AUTH	PKI-KAP-PRI	PKI-MAC	PKI-SGV-PRI	PKI-CSP-WRAP	PKI-CON-SECRET	PKI-SO-PIN	PKI-USER-PIN	DAP-PUB	PKI-KAP-PUB	PKI-SGV-PUB	PKI-3P-PUB
Destroy PKI Applet CSPs	--	--	E	--	--	--	--	--	W	-	Z	Z	Z	Z	Z	Z	--	--	--	--

Table 12: CSP and Public Key Access within Services

- G = Generate: The Module generates the CSP.
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP.
- O = Output: The Module outputs the CSP.
- I = Input: The Module receives the CSP. (i.e., it enters the module).
- Z = Zeroize: The module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure).
- -- = Not accessed by the service.

4 Self-test

4.1 Power-On Self-tests

On power-on or reset, the Module performs self-tests as described in Table 13: Power-On Self-Test below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the system is halted and will start again after a reset.

Test Target	Description
Firmware Integrity	32-bit XOR checksum performed over all code located in NVM. This integrity test is not required or performed for code stored in masked ROM code memory. The module calculates a 32-bit XOR checksum over the whole program memory area. The OS and the loaded applet are also covered by the 32-bit XOR checksum.
DRBG	Performs a fixed input KAT on AES-128 bits CTR DRBG.
Triple-DES	Performs encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
Triple-DES MAC	Performs Triple-DES MAC generate and verify KATs using a3-key Triple-DES key.
AES	Performs AES-128 key in ECB mode for decrypt KAT. Encrypt KAT is tested by AES CMAC.
AES CMAC	Performs AES CMAC generate and verify KATs using an AES-128 key.
HMAC	Performs HMAC generate and verify KATs using only SHA-384 (okay per IG 9.4).
SHA-1, SHA-2	Performs SHA-1 and SHA-512 KATs. SHA-256 is tested by the RSA sign/verify KAT, SHA-224 is tested by the ECDSA sign/verify KAT (even though it is not used by the module), and SHA-384 is tested by the HMAC-SHA-384 KAT.
RSA	Performs separate RSA signature generation and verification KATs using an RSA 2048-bit key with SHA-256.
RSA CRT	Performs separate RSA CRT signature generation and verification KATs using an RSA 2048-bit key with SHA-2.
ECDSA	Performs separate ECDSA signature generation and verification KAT using the P-224 curve with SHA-224.
Symmetric Key Wrap	Performs separate key wrap and unwrap KATs using an AES-128 key and 2-key Triple-DES key.
Non-SP 800-56A Compliant ECDH	Self-tests as described in FIPS IG 9.9 using EC P-224.

Table 13: Power-On Self-Test

4.2 Conditional Self-Tests

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
DRBG	SP 800-90A Section 11.3 DRBG Health Checks
ECDSA	ECDSA Pair wise Consistency Test performed on every ECDSA key pair generation. The test performs a calculation and a verification of a digital signature.
RSA	RSA Pair wise Consistency Test performed on every RSA key pair generation. The encrypt/decrypt function is always used for the pairwise consistency check because it is unknown what the key pair will be used for at the time of generation.
RSA CRT	RSA CRT Pair wise Consistency Test performed on every RSA key pair generation. The encrypt/decrypt function is always used for the pairwise consistency check because it is unknown what the key pair will be used for at the time of generation.
Firmware Load	RSA 2048 with SHA-256 signature verification performed when firmware is loaded. When new firmware is loaded into the Module using the *Manage Content* service, the Module verifies the integrity of the new firmware (applet) using MAC verification with the SD-SMAC key. Optionally, the Module may also verify a signature of the new firmware (applet) using the DAP-PUB public key; the signature block in this scenario is generated by an external entity using the private key corresponding to DAP- PUB.

Table 14: Conditional Self-Test

5 Physical Security Policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and is protected by passive shielding (metal layer coverings opaque to the circuitry below) and active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield places the Module permanently into the SYSTEM HALTED error state(POWER OFF state in [FSM], but never transits to POWER ON INITIALIZATION state).

The Module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process.

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Electromagnetic Interference and Compatibility (EMI/EMC)

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

8 Mitigation of Other Attacks Policy

The Module implements defenses against:

- Light attacks
- Invasive fault attacks
- Side-channel attacks (SPA/DPA)
- Timing analysis
- Differential fault analysis (DFA)

9 Security Rules and Guidance

The Module implementation also enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry.
- The module does not output plaintext CSPs or intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- Security Domains support security services such as key handling, encryption, decryption, digital signature generation and verification for their providers' (Card Issuer, Application Provider or Controlling Authority) applications. For the security services, secure channel should be initiated, and the **crypto-officer** can initiate the secure channel by authentication.
- Identity based authentication is used by **PKI-Applet** through Secure Channel Protocol 3 (SCP-03). Selecting and authenticating **PKI-Applet** using an authentication key (internally stored) will implicitly select an operator in “**user**” role. The role performs general security services, including cryptographic operations and other approved security functions. Prior to invoke any **PKI-Applet** service by **user-role**, authentication should be done with GP SCP03 specified in Global Platform Card Specification v2.2Amendment D and also by PIN verification if the resource required.
-

10 Appendix

Physical form factor Figures using KONA N41M0 module

Figure 4: KONA I KONA N41M0 – Plastic Body: Physical Form

Figure 5: KONA I KONA N41M0 – Secure SD Cards: Physical Form

Figure 6: KONA I KONA N41M0 – Key FOBs : Physical Form

Figure 7: KONA I KONA N41M0 – USB Token: Physical Form

Figure 8: KONA I KONA N41M0 – (U)SIM : Physical Form