KACST / Parsec

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

HSID5000A

Version: 1.6

Date: 2016-11-28

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the KACST / Parsec, HSID5000A, hereafter denoted the Module. The Module is a hardware device which interfaces with a Personal Computer via a USB connector to provide secure cryptographic functionality to a specific entity identified by the presence of the particular Module, username, and a password. The Module meets FIPS 140-2 overall Level 3 requirements.

Table 1 – HSID5000A Configurations

	Module	HW P/N and Version	FW Version
1	HSID5000A	HSID5000A	v1.1.0

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Cryptographic Tokens. The Module is a multi-chip standalone embodiment; the cryptographic boundary is defined by the outer perimeter of the enclosure.

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

Table 2 – Security Level of Security Requirements

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

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The Module contains embedded electronic components which allow it to perform cryptographic operations using secrets and keys created and stored on the Module. All electronic components inside the Module enclosure are potted with a hard opaque material. The Module relies on a computer system as a power source and to serve as input/output devices.

Figure 1 – Module physical cryptographic boundary

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
USB	Universal Serial Bus	Power | Control in | Data in | Data out | Status out
LEDs	Four colour light emitting diodes	Status out (FIPS approved mode, FIPS non-approved mode, activity, power, errors and initialization)

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

The Module, represented as the Token subsystem, interface with the Computer subsystem via USB for power as well as data communication. The Reader component is responsible to manage and control the USB interface. Operational instructions are passed to the Module which will, depending on the command, perform a cryptographic operation using the Crypto component, read or write secrets or public information to the Storage component.

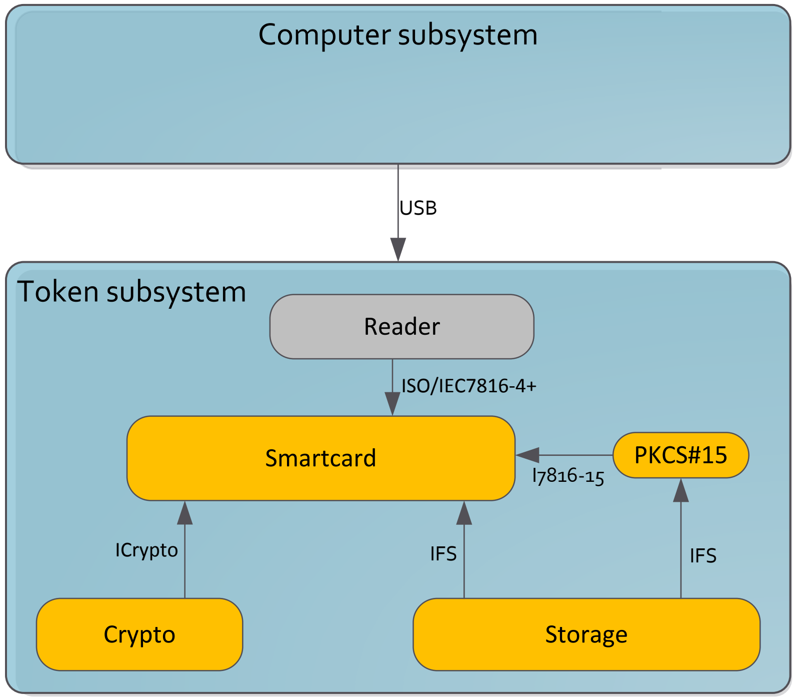

Figure 2 – Module Block Diagram

1.3 Modes of Operation

The Module has two modes of operation namely Approved and non-Approved. The Module is zeroized when switching between the modes.

In non-Approved mode all implemented cipher algorithm operations are allowed. In this mode, power and activity are indicated by the Module's red LED.

In Approved mode, only supported FIPS 140-2 "Approved" and "non-Approved, but allowed" cipher algorithm operations are allowed. In this mode power and activity are indicated by the Module's green LED.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, OFB, CFB8, CFB128, CTR Key sizes: 128, 192, 256 bits	3768
CCM	[SP 800-38C] Functions: Encryption, Decryption Key sizes: 128, 192, 256 bits	3768
GCM	[SP 800-38D] Functions: Encryption, Decryption Key sizes: 128, 192, 256 bits	3961
XTS-AES mode	[SP 800-38E] Functions: Encryption, Decryption Key sizes: 128, 256 bits	3768
DRBG	[SP 800-90A] Functions: Hash DRBG, HMAC DRBG, CTR DRBG Security Strengths: 128, 192, and 256 bits	1038
DSA	[FIPS 186-4] Functions: PQG Generation, PQG Verification, Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits	1048
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification, Public Key Validation Curves/Key sizes: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	811
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2468

Algorithm	Description	Cert #
SHA	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1 (not used for signature generation), SHA-224, SHA-256, SHA-384, SHA-512	3138
Triple-DES (TDES)	[SP 800-20, SP 800-67] Functions: Encryption, Decryption Modes: TECB, TCBC, TCFB64, TOFB Key sizes: 3-key	2096

Table 5 – Approved Cryptographic Functions Tested with Vendor Affirmation

Algorithm	Description	IG Ref.
KDF, Password-Based	[SP 800-132] Options: PBKDF with Option 1b Functions: HMAC-based KDF using SHA-1	Vendor Affirmed IG D.6
Key Extraction-then- Expansion	[SP 800-56C] Functions: HMAC-based KDF (with SHA-1 or higher)	Vendor Affirmed IG D.10

Table 6 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Non-SP 800-56A Compliant Diffie-Hellman	[IG D.8] Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
Non-SP 800-56A Compliant EC Diffie-Hellman	[IG D.8] EC Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
NDRNG	[Annex C] Hardware Non-Deterministic RNG. The NDRNG output is used to seed the FIPS Approved DRBGs.

Table 7 – Non-Approved Cryptographic Functions available in Non-Approved mode

Algorithm	Description
DSA	Functions: PQG Generation, PQG Verification, Key Pair Generation, Signature Generation, Signature Verification Key sizes: 1024 bits
MD5	Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications
RSA	Functions: Signature Generation, Signature Verification Key sizes: 2048 bits
SHA	Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1
Triple-DES (TDES)	Functions: Encryption, Decryption Modes: TECB, TCBC, TCFB, TOFB Key sizes: 2-key

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 8 – Critical Security Parameters (CSPs)

CSP	Description / Usage
Session private key	This is the private key of a 2048 bit Diffie-Hellman key pair created using the parameters defined as "group 14" in RFC3526.
Session key(s)	128 bit key(s) derived using Diffie-Hellman. These keys are used to en-/decrypt sensitive information per communication channel using AES-128-CCM (tag size 16 bytes). A maximum of 15 communication channels can exist, each with a unique session key.
Login Key	This is a PBKDF (HMAC_SHA1) derived key using the CO or User role name and password.
Passwords	Two strings of characters selected to authenticate the User or CO role.
User key	256 bit key internally generated using the DRBG. The key is used to en-/decrypt the user database using AES-256-CCM (tag size 16 bytes).
Asymmetric private key(s)	These keys are used to support DSA or EC algorithms. These keys can be generated internally or securely imported.
Diffie-Hellman	These keys are used to derive secret keys using the Diffie-Hellman algorithm. The size

CSP	Description / Usage
private key(s)	can be 2048-, 3072- or 4096 bit. These keys are generated internally.
Secret key(s)	128, 192 or 256 bit keys imported or derived from Diffie-Hellman or EC Diffie-Hellman. The keys are used to en-/decrypt data via any of the supported and applicable approved cipher algorithms.
DRBG Secrets	V, C, and Key

2.2 Public Keys

Table 9 – Public Keys

Key	Description / Usage
Upgrade public key	3072-bit DSA key used to verify Parsec firmware upgrades.
Session public key	Public key of 2048 bit Diffie-Hellman session key pair.
Asymmetric public key(s)	Public key of DSA or EC key pair(s).
Diffie-Hellman public key(s)	Public key Diffie-Hellman key pair(s). These keys are used to derive secret keys using the Diffie-Hellman algorithm.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two distinct operator roles, User and Cryptographic Officer (a.k.a. Administrator). The cryptographic module enforces the separation of roles allowing only one login at a time and enforcing re-authentication with every role change.

Table 10 lists all operator roles supported by the Module. The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators. Authentication data and other CSPs are protected during transmission over the boundary by a secret key derived per session.

Table 10 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
Cryptographic Officer (Administrator)	This role manages cryptographic algorithms and control user parameters / limits. There can only be one CO.	Identity-based	Name and password
User	This role can generate CSPs to use in cryptographic operations. There can only be one User.		

3.2 Authentication Methods

An operator is defined by the unique combination of the name and password.

To estimate the probability that a random guess of the password will succeed, we assume that the characters of the password are independent of each other. Since the password must be at least 5 lower case characters, the probability that a random guess of the password will succeed is therefore 1/26^5, which is less than the required 1/1,000,000.

The Module initially allows a maximum of three consecutive failed authentication attempts after which it prevents authentication for a configured timeout period of at least 60 seconds. Therefore, the probability of a successful random guess of the password during the initial timeout period is therefore a maximum of 3/(26^5), which is less than the required 1/100,000. Subsequent authentication attempts are only allowed at one attempt per configured timeout period.

Table 11 – Authentication Description

Authentication Method	Probability	Probability per Minute
Identity based	1/(26^5)	3/(26^5)

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.

Table 12 – Authenticated Services

Service	Description	CO	U
Zeroize	Destroys all **CSPs.**	X	
Create User	Create a User	X	
Delete User	Delete the User	X	
Personalize	Generate a personal **DSA, DH** or **EC key pairs.**		X
Change User role password	Update the User role **password**.		X
Change CO role password	Update the CO role **password**.	X	
Change mode of operation	Approved mode of operation is enabled or disabled in the configuration and the Module is **Zeroized**	X	
Restrict cryptographic algorithms	Enable or disable the selection of cryptographic algorithms in Approved and non-Approved mode. At least one algorithm must be enabled per mode.	X	
Set log severity level	Select the minimum log level to record	X	

Service	Description	CO	U
Change password configuration	Set minimum allowed User role password length	X	
	Set maximum allowed User role password length	X	
	Set/Remove password complexity requirements for User role password	X	
Authenticate	This service receives the CO or users name and password, passed encrypted by the **Session key** from the computer to the Module.	X	X
Export certificate signing request(s)	Export PKCS#10 formatted Certificate Signing Request (CSR) of newly generated **DSA or EC public key** so that it can be signed by a CA.		X
Import key pair(s)	Encrypted **DSA** or **EC private keys**, optionally with its matching public certificate and/or certificate authority certificate, can be imported and stored on the Module.		X
Export key pair(s)	**DSA** or **EC private keys**, together with a matching public X.509 certificate, can be exported from the Module.		X
Delete a key pair(s)	Remove a selected **DSA, DH** or **EC private key** and matching public key (and public certificate) from the non-volatile storage.		X
Import public key(s) and certificate(s)	PEM formatted DSA and EC Public certificates can be imported and stored on the Module.		X
Delete a public certificate(s)	Remove a public certificate with no matching private key (such as CA certificate) from the non-volatile storage.	X	X
Sign	Sign data using a **DSA** or **EC private key**		X
Verify	Verify signature of data using a **DSA** or **EC public key**		X
Derive	Derive a **Secret key** using specified **DH** or **EC key pair**.		X
Encrypt	Encrypt data using a **Secret key** on the Module		X
Decrypt	Decrypt data using a **Secret key** on the Module		X
Digest	Create a SHA1 or SHA2 digest of data		X
Upgrade firmware	Upgrade verified firmware modules. The firmware must be signed by a CA. Signatures are verified before the upgrade process start. The CA public certificate is programmed at the factory.	X	
Get Challenge	Generate a random value		X
Self-Tests	Perform the power-on self-tests	X	X

Table 13 – Unauthenticated Services

Service	Description
Status Information	Read and display the: • Mode of Operation • Module serial number(s) • Firmware version(s) and signature(s)
View/Export Public certificate(s) and Public Key(s)	View or export public certificates and keys from the Module

Table 13 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 the CSP.
- R = Read: The Module reads the CSP. The read access is typically performed before the Module uses the CSP.
- W = Write: The Module writes the CSP. The write access is typically performed after a CSP is imported into the Module, when the Module generates a CSP, or when the Module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 14 – CSP Access Rights within Services

Service	CSPs								
	Session private key	Session key(s)	User key	Login Keys	Asymmetric private key(s)	DH private key(s)	Passwords	Secret Key(s)	DRBG Secrets
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z
Create User	R	R	G	G			W		RW
Delete User			Z	Z	Z	Z		Z	
Personalize					G	G			RW
Change User role password		R	RW	W			R		
Change CO role password		R		W			R		
Change mode of operation	Z	Z	Z	Z	Z	Z	Z	Z	Z
Restrict cryptographic algorithms									
Set log severity level									
Change password configuration									

Service	CSPs								
	Session private key	Session key(s)	User key	Login Keys	Asymmetric private key(s)	DH private key(s)	Passwords	Secret Key(s)	DRBG Secrets
Authenticate	RW	G	R	R			R		RW
Export certificate signing request									
Import key pair(s)	R	R			W	W			
Export key pair(s)	R	R			R	R			
Delete key pair(s)					W	W	W		
Import public keys and certificate(s)									
Delete public certificate(s)									
Sign					R				
Verify									
Derive						R			
Encrypt								R	
Decrypt								R	
Digest									
Upgrade Firmware									
Get Challenge									RW
Self-tests									
Status Information									
View/Export public key or certificate(s)									

4 Self-tests

Each time the Module is powered up in the Approved mode it tests that the cryptographic algorithms still operate correctly. Power up self–test (POST) is initiated by power cycling.

On power up or reset, the Module perform self-tests described in Table 14 below. 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 error state.

Table 15 – Power Up Self-tests

Test Target	Description
HMAC	KATs: Per IG 9.3, this testing covers SHA POST requirements SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
AES	KATs: Encryption, Decryption Modes: ECB Key sizes: 128 bits
CCM	KATs: Encryption, Decryption Key sizes: 192 bits
GCM	KATs: Encryption, Decryption Key sizes: 256 bits
XTS-AES mode	KATs: Encryption, Decryption Key sizes: 128, 256 bits
TDES	KATs: Encryption, Decryption Modes: TECB, Key sizes: 3-key
DSA	PCT: Signature, Verification Key sizes: 2048 bits, SHA-384
ECDSA	PCT: Generation, Signature, Verification Key sizes: P-224 and K-233, SHA-256
DRBG	KATs: HASH (SHA256), HMAC (SHA256), CTR (AES 256 without derivation) Security Strengths: 256 bits
ECC CDH	KATs: Shared secret calculation per SP 800-56A §5.7.1.2, IG 9.6
Firmware integrity	KATs: Firmware SHA-1 digests

Table 16 – Conditional Self-tests

Test Target	Description
NDRNG	Continuous Random Number Generator test
DRBG	SP 800-90 Section 11.3 Health Tests. Required per IG C.1. FIPS 140-2 continuous test for stuck fault
DSA	DSA Pairwise Consistency Test performed on every DSA key pair generation.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation.
Firmware update	DSA 3072 signature verification performed when firmware is updated

5 Physical Security Policy

The Module is manufactured using an opaque white potting material poured and then hardened over all the components inside the enclosure and affixing to the inside wall of the enclosure. A transparent bezel seals the enclosure when placed over the USB connector onto the enclosure. Potting material also covers part of the USB connector on the PCB, making the enclosure splash proof.

The potting hardness test was performed at a single temperature (23.89°C / 75°F) and measured to be no less than 85 on the Shore D hardness scale. No assurance is provided for hardness conformance at any other temperature.

Any cuts to the bezel and or the enclosure which exposes the white potting material must be considered as tamper evidence. The potting will however prevent access to the CSP and the component should be destroyed before access is gained.

Table 17 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard opaque potting material	Before insertion into Computer subsystem	Inspect Module for physical damage which exposes a white material

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware update service to support necessary updates. New firmware versions must be validated against FIPS 140-2 to maintain compliance.

7 Mitigation of Other Attacks Policy

No claims of mitigation for attacks beyond the scope of FIPS 140-2 have been made.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The Module provides two distinct operator roles: User and Cryptographic Officer
2. The Module provides two modes of operation: Approved and non-Approved
3. The Module clears previous authentications on power cycle
4. When the Module has not been placed in a valid role, the operator does not have access to any cryptographic services
5. The operator is capable of commanding the Module to perform the power up self-tests
6. Power up self-tests do not require any operator action
7. Data output is inhibited during key generation, self-tests, zeroization, and in error states
8. Status information does not contain CSPs or sensitive data
9. The Module does not support concurrent operators
10. The Module does not support a maintenance interface or role
11. The Module does not have any external input/output devices used for entry/output of data
12. The Module does not enter or output plaintext CSPs
13. The Module does not output intermediate key values
14. The Module supports a maximum of 50 asymmetric key pairs

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 18 – References

Abbreviation	Full Specification Name
FIPS 140-2	FIPS Publication 140-2 Security Requirements for Cryptographic Modules; Dec 3, 2002
	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program; April 25, 2014
FIPS 186-4	Digital Signature Standard (DSS); July 2013
FIPS 180-3	Secure Hash Standard (SHS); October 2008
FIPS 197	Advanced Encryption Standard (AES); November 26, 2001
SP 800-38A	Recommendation for Block Cipher Modes of Operation (TDEA), Methods and Techniques; December 2001
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality - May 2004.
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC; November, 2007
SP 800-38E	Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices; January 2010
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007
SP 800-56B	Recommendation for Pair-Wise Key Establishment Using Integer Factorization, DRAFT, December 2008
SP 800-56C	Recommendation for Key Derivation through Extraction-then-Expansion
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher; May 2004
SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, March 2007
SP 800-131A	Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths; January 2011
X9.31	American National Standard (ANS) X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), Withdrawn, but available from X9.org
X9.62	American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)

Table 19 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
ANS	American National Standard
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CO	Cryptographic Officer
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EC	Elliptic Curve
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
KAT	Known answer test
KDF	Key derivation function
NIST	National Institute of Standards and Technology
PBKDF	Password based key derivation function
PCT	Pairwise consistency test
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard