Hydra PC Personal Edition FIPS Module Security Policy

Revision Document No. 1.4

5 August, 2009

SPYRUS, Inc.
info@spyrus.com>
<http://www.spyrus.com>

SPYRUS Document No. 550-070001-05

SPYRUS Document No. 550-070001-05

Contents

1 Introduction

This Security Policy specifies the security rules under which the HYDRA PC PERSONAL EDITION FIPS Module operates. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by SPYRUS, Inc. These rules, in total, define the interrelationship between the modules:

1. Operators,
2. Services, and
3. Critical Security Parameters (CSPs).

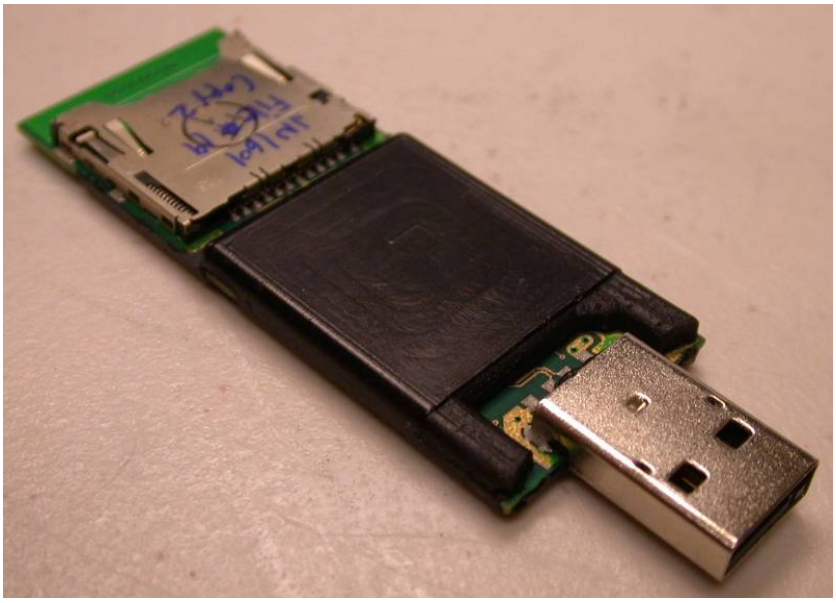

Figure 1 Hydra PC Personal Edition FIPS Module (Top View)

Figure 2 Hydra PC Personal Edition FIPS Module (Bottom View)

1.1 Overview

The Hydra PC Personal Edition FIPS Module enables security critical capabilities such as user authentication, message privacy and integrity, authentication, and secure storage in rugged, tamper-evident hardware. The Hydra PC Personal Edition FIPS Module communicates with a host computer via the USB interface.

The Hydra PC Personal Edition FIPS Module is a strong encryption solution providing FIPS-validated NSA Suite B encryption algorithms. Hydra PC protects data for government, large enterprises, small organizations, and home users. Key features include:

- Encryption technology uses the Suite B algorithms approved by the U.S. government for protecting both Unclassified and Classified data
- Encrypted file storage on removable miniSD/miniSDHC/microSD/microSDHC flash cards or PC hard drive for unlimited capacity.
- Strong protection against intruder attack.
- Exclusive feature restricts use to only the PCs that you designate. Even with the user's PIN, Hydra PC will not work on an unauthorized PC.

Access protection is as important as encryption strength. Data encrypted with Hydra PC cannot be decrypted until the authorized user gains access to the device.

1.2 Implementation

The HYDRA PC PERSONAL EDITION FIPS Module is implemented as a multi-chip standalone module as defined by FIPS 140-2. The FIPS 140-2 module identification data for the HYDRA PC PERSONAL EDITION FIPS Module is shown in the table below:

Hardware P/N	Hardware Version	Firmware Version
880070103F	01.00.01	01.02.12
880070104F	01.00.01	01.02.13

The HYDRA PC PERSONAL EDITION FIPS Module is available with a USB interface compliant to the *Universal Serial Bus Specification*, Revision 2.0, dated 23 September 1998. All Interfaces have been tested and are compliant with FIPS 140-2.

1.3 Cryptographic Boundary

The Cryptographic Boundary of the HYDRA PC PERSONAL EDITION FIPS Module is defined to be the physical perimeter of the printed circuit board. Please see Figure 3 for a schematic view with the PCB, epoxy coating and interfaces shown.

The following non-security relevant hardware components of the HYDRA PC PERSONAL EDITION FIPS Module are excluded from the cryptographic boundary:

- USB connector
- SD Memory connector
- Two LEDs
- Three capacitors near the edge of the epoxy-protected area on the PCB
- Secure PIN entry and fingerprint scanner interface (disabled)

1.4 Ports and Interfaces

See Figure 3 and Tables 1-1, 1-2 for the ports and interfaces of the module.

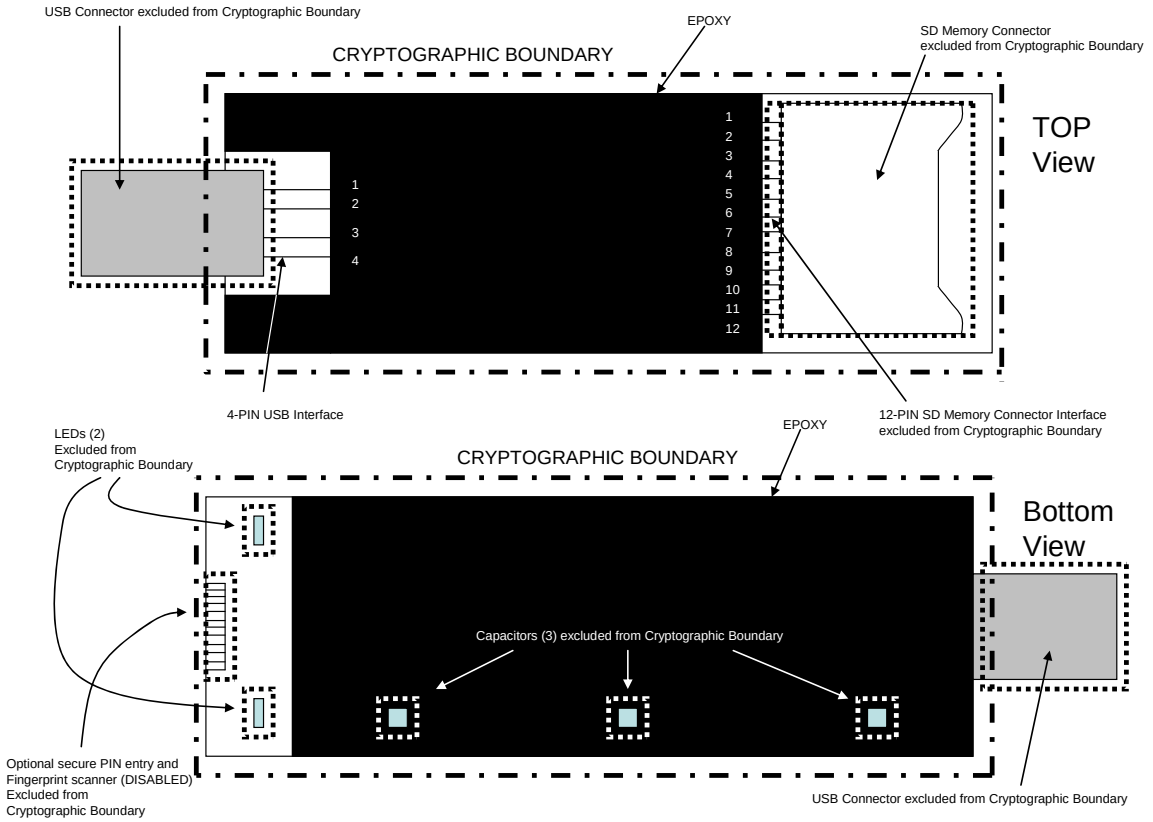

Figure 3 – Ports and interfaces of HYDRA PC PERSONAL EDITION FIPS Module (Top and Bottom Views)

Table 1-1 – USB Interface

PIN	Category
1	Power
2	Data Input, Data Output, Control Input, Status Output
3	Data Input, Data Output, Control Input, Status Output
4	Power

Table 1-2 – SD Interface

PIN	Category
1	Data Input/Data Output
2	Data Input/Data Output
3	Data Input
4	Power

PIN	Category
5	Not connected
6	Not connected
7	Power
8	Data Input,
9	Power
10	Data Input/Data Output
11	Data Input/Data Output
12	Power

1.5 Approved Mode of Operation

The HYDRA PC PERSONAL EDITION FIPS Module has one mode of operation, the Approved mode of operation. All commands that use FIPS 140-2 Approved security functions (e.g. algorithms) are defined to be in the "Approved mode of operation."

The HYDRA PC PERSONAL EDITION FIPS Module supports the FIPS 140-2 algorithms in the tables below.

Table 1-3 Approved Algorithms supported by HYDRA PC PERSONAL EDITION FIPS Module

Encryption & Decryption
AES Certificates #858, #846, #850
Digital Signatures
ECDSA Certificates #97, #96
Hash
SHA-224, SHA-256, SHA-384, SHA-512 Certificates #852, #837
RNG
FIPS 186-2 RNG Certificate #486 HASH_DRBG (SP 800-90) Certificate #3

Table 1-4 Non-Approved Algorithms allowed for use in HYDRA PC PERSONAL EDITION FIPS Module

AES Key Wrapping per the NIST AES Key Wrapping Specification
AES-256 Certificate #846
Key Transport / Key Agreement
EC-Diffie-Hellman per SP 800-56A (key establishment methodology provides 128 bits of encryption strength)
RNG
Hardware RNG for seeding Approved DRNG

2 FIPS 140-2 Security Levels

The HYDRA PC PERSONAL EDITION FIPS Module cryptographic module complies with the requirements for FIPS 140-2 validation to the levels defined in Table 2.1. The FIPS 140-2 overall rating of the HYDRA PC PERSONAL EDITION FIPS Module is Level 3

Table 2-1
FIPS 140-2 Validation Levels

FIPS 140-2 Category	Level
1. Cryptographic Module Specification	3
2. Cryptographic Module Ports and Interfaces	3
3. Roles, Services, and Authentication	3
4. Finite State Model	3
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	3
8. EMI/EMC	3
9. Self-tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A

3 Security Rules

The HYDRA PC PERSONAL EDITION FIPS Module enforces the following security rules. These rules are separated into two categories: 1) those imposed by FIPS 140-2, and 2) those imposed by SPYRUS.

3.1 FIPS 140-2 Imposed Security Rules

Table 3-1 FIPS 140-2 Policies and Rule Statements

Policy	Rule Statement
Authentication Feedback	The HYDRA PC PERSONAL EDITION FIPS Module shall obscure feedback of authentication data to an operator during authentication (e.g., no visible display of characters result when entering a password).
Authentication Mechanism	The HYDRA PC PERSONAL EDITION FIPS Module shall enforce Identity-Based authentication.
Authentication Strength (1)	The HYDRA PC PERSONAL EDITION FIPS Module shall ensure that feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism
Authentication Strength (2)	The HYDRA PC PERSONAL EDITION FIPS Module shall satisfy the requirement for a single–attempt false acceptance rate of no more than one in 1,000,000 authentications
Authentication Strength (3)	The HYDRA PC PERSONAL EDITION FIPS Module shall satisfy the requirement for a false acceptance rate of no more than one in 100,000 for multiple authentication attempts during a one minute interval
Configuration Management	The HYDRA PC PERSONAL EDITION FIPS Module shall be under a configuration management system and each configuration item shall be assigned a unique identification number.

Policy	Rule Statement
CSP Protection	The HYDRA PC PERSONAL EDITION FIPS Module shall protect all CSPs from unauthorized disclosure, modification, and substitution.
Emissions Security	The HYDRA PC PERSONAL EDITION FIPS Module shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart B, Class B.
Error State (1)	The HYDRA PC PERSONAL EDITION FIPS Module shall inhibit all data output via the data output interface whenever an error state exists and during self-tests.
Error State (2)	The HYDRA PC PERSONAL EDITION FIPS Module shall not perform any cryptographic functions while in an Error State.
Guidance Documentation	The HYDRA PC PERSONAL EDITION FIPS Module documentation shall provide Administrator and User Guidance per FIPS 140-2, Section 4.10.4.
Hardware Quality	The HYDRA PC PERSONAL EDITION FIPS Module shall contain production quality ICs with standard passivation.
Interfaces (1)	The HYDRA PC PERSONAL EDITION FIPS Module interfaces shall be logically distinct from each other.
Interfaces (2)	The HYDRA PC PERSONAL EDITION FIPS Module shall support the following five (5) interfaces: • data input (PIN 2, 3 – USB interface and PIN 1, 2, 3, 8,10,11 – SD Interface) • data output (PIN 2,3 – USB interface and PIN 1, 2,10,11– SD Interface) • control input (PIN 2, 3 – USB interface

Policy	Rule Statement
	and No Pins – SD Interface) • status output (PIN 2, 3 – USB interface and No Pins – SD Interface) • power interface (PIN 1, 4 – USB interface and PIN 4, 7, 9,12 – SD Interface)
Key Association	The HYDRA PC PERSONAL EDITION FIPS Module shall provide that: a key entered into, stored within, or output from the HYDRA PC PERSONAL EDITION FIPS Module is associated with the correct entity to which the key is assigned.
Logical Separation	The HYDRA PC PERSONAL EDITION FIPS Module shall logically disconnect the output data path from the circuitry and processes performing the following key functions: • key generation, • key zeroization
Mode of Operation	The HYDRA PC PERSONAL EDITION FIPS Module services shall indicate that the module is in an approved mode of operation with a standard success return code and the output of the Get Capabilities command.
Public Key Protection	The HYDRA PC PERSONAL EDITION FIPS Module shall protect public keys against unauthorized modification and substitution.
Re-authentication	The HYDRA PC PERSONAL EDITION FIPS Module shall re-authenticate an identity when it is powered-up after being powered-off.
RNG Strength	The HYDRA PC PERSONAL EDITION FIPS Module shall use a 'seed input' into the deterministic random number generator of sufficient length that ensures at least the same amount of operations are required to determine the value of the generated key.
Secure Development (1)	The HYDRA PC PERSONAL EDITION FIPS Module source code shall be annotated.

Policy	Rule Statement
Secure Development (2)	The HYDRA PC PERSONAL EDITION FIPS Module software shall be implemented using a high-level language except that limited use of a low-level language is used to enhance the performance of the module.
Secure Distribution	The HYDRA PC PERSONAL EDITION FIPS Module documentation shall include procedures for maintaining security while distributing and delivering the module.
Self-tests (1)	The power-up tests shall not require operator intervention in order to run.
Self-tests (2)	The HYDRA PC PERSONAL EDITION FIPS Module shall perform the self-tests listed in Section 7.
Self-tests (3)	The HYDRA PC PERSONAL EDITION FIPS Module shall enter an Error State and output an error indicator via the status interface whenever self-test is failed.
Services	The HYDRA PC PERSONAL EDITION FIPS Module shall provide the following services: (see Reference Table 4.2).
Software Integrity	The HYDRA PC PERSONAL EDITION FIPS Module shall apply a 16-bit EDC software integrity check to all firmware components.
Status Output	The HYDRA PC PERSONAL EDITION FIPS Module shall provide an indication via the "status output" interface if all of the power-up tests are passed successfully.
Strength of Key Establishment	The HYDRA PC PERSONAL EDITION FIPS Module shall use a key establishment methodology that ensures at least the same amount of operations are required to determine

Policy	Rule Statement
	the value of the transported/agreed upon key.
Unauthorized Disclosure	The HYDRA PC PERSONAL EDITION FIPS Module shall protect the following keys from unauthorized disclosure, modification and substitution: • secret keys • private keys.
Zeroization (1)	The HYDRA PC PERSONAL EDITION FIPS Module shall provide a zeroization mechanism that can be performed either procedurally by the operator *or* automatically by the HYDRA PC PERSONAL EDITION FIPS Module interface software on the connected host platform.
Zeroization (2)	The HYDRA PC PERSONAL EDITION FIPS Module shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the HYDRA PC PERSONAL EDITION FIPS Module.

3.2 SPRYUS Imposed Security Rules

Table 3-2 SPYRUS Imposed Policies and Rule Statements

Policy	Rule Statement
Single User Session	The HYDRA PC PERSONAL EDITION FIPS Module shall not support multiple concurrent operators.
No Maintenance Interface	The HYDRA PC PERSONAL EDITION FIPS Module shall not provide a maintenance role/interface.
No Bypass Mode	The HYDRA PC PERSONAL EDITION FIPS Module shall not support a bypass mode.
Health-Tests	The HYDRA PC PERSONAL EDITION FIPS Module shall conduct extensive health tests,

Policy	Rule Statement
	including verification of the correctness of the AES and ECC key establishment functions, before and after every series of file encryption operations.

3.3 Identification and Authentication Policy

The table below describes the type of authentication and the authentication data to be used by operators, by role. For a description of the roles, see section 4.1.

Table 3-3 Identification and Authentication Roles and Data

Role	Type of Authentication	Authentication Data
Administrator (Crypto-Officer)	Manual Login	SSO PIN (min 7 to 128 characters) + Host Authentication Code (min 14 to 262 characters)
User	Manual Login	USER PIN (min 7 to 128 characters) + Host Authentication Code (min 14 to 262 characters)

4 Roles and Services

4.1 Roles

The HYDRA PC PERSONAL EDITION FIPS Module supports two roles, Administrator and User, and enforces the separation of these roles by restricting the services available to each one. Each role is associated with a single user identity, namely the user in sole knowledge of the PIN associated with the role.

Table 4-1 Roles and Responsibilities

Role	Responsibilities
Administrator	The Administrator is responsible for initializing the HYDRA PC PERSONAL EDITION FIPS Module. Before issuing a HYDRA PC PERSONAL EDITION FIPS Module to an end user, the Administrator initializes the HYDRA PC PERSONAL EDITION FIPS Module with private keying material. The Administrator cannot use critical security parameters loaded on the module. The HYDRA PC PERSONAL EDITION FIPS Module validates the Administrator identity before accepting any initialization commands. The Administrator is also referred to as the Site Security Officer (SSO).
User	The User role is available after the HYDRA PC PERSONAL EDITION FIPS Module has been initialized. The user can load, generate and use secret keys for encryption services.

4.2 Services

The following table describes the services provided by the HYDRA PC PERSONAL EDITION FIPS Module.

Table 4-2
HYDRA PC PERSONAL EDITION FIPS Module Services

Service	Description
Cancel File Session	Cancel the current file session and remain logged on.
Change Secrets	Forces Hydra PC to change the authorization factor used for authorizing a user and host to access the module

Service	Description
Delete Hydra Keys	Delete and zeroize Hydra PC file transport and signature keys
End File Decrypt	Validates the completion of decrypt or Verify Session
End File Encrypt	Completes the encrypted file stream format.
File Encrypt And Hash	Encrypt (AES-256) and Hash (SHA-384) a block of data.
File Hash And Decrypt	(SHA-384) Hash and Decrypt (AES-256) a file.
Generate Single User	Generates Single User Transport data.
Get Capabilities	Returns the current capabilities of the HYDRA PC token including: Global Information File, Firmware Version, Hardware Version, storage size of the mini SD memory installed, the product name, and module state (Failure/Operational). This service provides a response that indicates the approved mode of operation (see Section 3.1).
Get Public	Get Public Key Data (ECDSA) from HYDRA PC.
Get State	Returns the current state information from the HYDRA PC token: HYDRA state, Mini SD Media status, current lock state of the mass storage drive.
Hash File	Hash (SHA-384) a block of data.
Load Secret	Forces Hydra PC to load cached authorization factors for operator and host authorization.
Log Off	Performs logoff on Hydra PC.
Log On	Performs logon for user
Make Ready	Generates the Hydra keys enabling signing of encrypted user files and generation of encryption and decryption keys for each encrypted file.
Set Drive Lock	Set drive lock command locks and

Service	Description
	unlocks the miniSD mass storage device.
Signed Firmware Update	Perform a signed firmware update of the Hydra PC Firmware using a signed firmware update block.
Start File Decrypt	Performs the file decrypt and verify session or verify only session. The command can also just verify encrypted file header information without starting a session.
Start File Encrypt	Starts a file encrypt session. Initializes a file session with the requested AES Key Size, AES Block Mode and hash mode.
Setup Basic Secure Channel	Generates a non-authenticated secure channel using a new ephemeral key pair (ECDH P256) and a host ephemeral public.
Get User State	Returns the current HYDRA PC State, Time remaining (in ms) after invalid logon; Size of Data Out Block; Number of Attempts remaining after invalid logon; and Total critical errors
Initialize	Initializes the Hydra PC by invocation from the Admin Tools software.
Zeroize	Zeroizes all encryption keys by invocation from the Admin Tools software.

5 Identification and Authentication

5.1 Initialization Overview

The initialization procedure is as follows:

1. The module is powered (plugged in an available USB port on the host PC), the operator starts the host software used to allow the operator to send the default SSO PIN Phrase - set at the factory.

2. Next, the operator who has logged in with the default SSO PIN Phrase, loads the USER ID, USER PIN Phrase, Host Authentication Code (HAC) (which identifies the machine from which operators are allowed to send USER PIN Phrase or SSO PIN Phrase) and generates an ECC Public/Private key that is going to be used to establish a SP800-56A key between the host software and Hydra module to provide UserID+User PIN Phrase+HAC or SSO PIN Phrase+HAC confidentiality when entered into the module.

3. Next, the operator changes the default SSO PIN Phrase, which completes the initialization procedure. From this point on, the User or SSO must enter the appropriate PIN Phrase from an authorized machine (which sends the HAC) to authenticate.

5.2 Operator Authentication

Operator Authentication is accomplished by 1) HAC transfer from Host to the module following power-on; and 2) PIN entry by the user. After receiving the Host HAC, the HYDRA PC PERSONAL EDITION FIPS Module waits for authentication of the user by entry of a PIN phrase. Once a valid PIN phrase has been accepted the HYDRA PC PERSONAL EDITION FIPS Module is ready for cryptographic commands.

The HYDRA PC PERSONAL EDITION FIPS Module stores the number of logon attempts in non-volatile memory. The count is reset after every successful entry

of a User PIN Phrase by a user and after every successful entry of the SSO PIN Phrase by the SSO.

If an incorrect User PIN or Host Authorization Code is loaded during the authentication process, a delay of 4 seconds is imposed. If a second incorrect attempt occurs, the delay is increased to 8 seconds, etc., doubling for every failed attempt.

If the User fails to logon to the HYDRA PC PERSONAL EDITION FIPS Module in 10 consecutive attempts, the HYDRA PC PERSONAL EDITION FIPS Module will block access to the User's personality directory, and then transitions to a state that is initialized only for the Adminiatrator to perform restorative actions. To restore operation to the HYDRA PC PERSONAL EDITION FIPS Module, the User or will have to reload the initialization parameters and User PIN phrase. If the User fails to logon to the HYDRA PC PERSONAL EDITION FIPS Module in 10 consecutive attempts, the HYDRA PC PERSONAL EDITION FIPS Module will block all of the Private or Secret Components, Key Registers and disallow User access. When the HYDRA PC PERSONAL EDITION FIPS Module is inserted after a zeroize, it will power up and transition to the Zeroized State, where it will only accept the Zeroize Default PIN phrase. After the Zeroize Default PIN phrase has been accepted, the HYDRA PC PERSONAL EDITION FIPS Module transitions to the Uninitialized State and must be reinitialized, as described in section 5.1.

5.3 Generation of Random Numbers

The Random Number Generators are not invoked directly by the User. The Random Number output is generated by the FIPS 186-2 algorithm in the case of static private keys and associated key wrapping keys, or the HASH_DRBG algorithm specified in SP 800-90 in the case of ephemeral keys, nonces, and symmetric keys. These calls are internal and their output is not exported to the user.

5.4 Strength of Authentication

The strength of authentication mechanism is stated in Table 5-1 below.

Table 5-1Strength of Authentication

Authentication Mechanism	Strength of Mechanism
Single PIN-entry attempt / False Acceptance Rate	The probability that a random PIN-entry attempt will succeed or a false acceptance will occur is 1.66×10^{-14}. The requirement for a single–attempt / false acceptance rate

Authentication Mechanism	Strength of Mechanism
	of no more than 1 in 1,000,000 (i.e. less than a probability of 10^{-6}) is therefore met.
Multiple PIN-entry attempt in one minute	Hydra PC authentication mechanism has a feature that doubles the time of authentication with each successive failed attempt. There is also a maximum bound of 10 successive failed authentication attempts before zeroization occurs. The probability of a successful attack of multiple attempts in a one minute period is 1.66×10^{-13} due to the 10 failed attempt maximum. This is less than one in 100,000 (i.e., 1×10^{-5}), as required.

6 Access Control

6.1 Critical Security Parameters (CSPs)

Table 6-1
HYDRA PC PERSONAL EDITION FIPS Module CSPs

Key	Algorithm(s) Standards	Symbolic Form	Description/Usage
ECDSA Private key	ANSI X9.62	d_{ECDSA}	The ECDSA P-384 Private Key of the User employed in Elliptic Curve digital signing operations to Sign File Header data during file encryption
SMS Key Encrypting Key	FIPS-197	KEK	An AES-256 key wrap key (AKA a Transport Encryption Key) used for wrapping the SMS File Encryption Key
SMS File Encrypting Key	FIPS-197	FEK	File Encrypting Key (FEK) used to encrypt or decrypt a particular file or message.
ECC Ephemeral Private Key	SP 800-56A	$d_{e,U}$	A user ECDH ephemeral private key.
Host Secure Session Key	SP 800-56A	Z	AES-256 (CBC) secure session key. It is used to encrypt the Host Authorization code and the SSO or User PIN.
RNG Seed Key	FIPS 186-2	XKEY	FIPS 186-2 XKEY variable
Dual_EC_DRBG Seed	SP 800-90	s	SP 800-90 Hash_DRBG s variable
Hash_DRBG Seed	SP 800-90	V	SP 800-90 Hash_DRBG V variable
User PIN	N/A	USER PIN	User authentication using a 7 to 128 character PIN entered by Host during logon.
SSO PIN	N/A	SSO PIN	SSO's authentication using a 7 to 128 character PIN entered by Host during logon.

6.2 Public Keys

Table 6-2 - HYDRA PC PERSONAL EDITION FIPS Module Public Keys

Key	Algorithm(s) Standards	**Description/Usage**
Firmware authentication key	ANSI X9.62	Used for signature verification of a firmware update block. Each block is signed using an ECDSA P384 firmware signature key. A block is loaded only if the signature is valid.
ECDSA Public key	ANSI X9.62	The ECDSA P-384 Public Key of the User employed in Elliptic Curve digital signing operations to verify File Header data during file decryption
ECDH Public Key	SP 800-56A	The responder static public key in SP800-56A ECC CDH One-Pass Diffie-Hellman key establishment protocol. Used to set up a secure channel between the module firmware and the host software for transmission of critical security parameters.
ECC Ephemeral Public Key	SP 800-56A	The initiator ephemeral public key in SP800-56A ECC CDH One-Pass Diffie-Hellman key establishment process.
ECC Static Public Key	SP 800-56A	An ECDH static Public key.

6.3 CSP Access Modes

Table 6-3
HYDRA PC PERSONAL EDITION FIPS Module Access Modes

Access Type	Description
Generate (G)	"Generate" is defined as the creation of a CSP
Delete (D)	"Delete" is defined as the zeroization of a CSP
Use (U)	"Use" is defined as the process in which a CSP is employed. This can be in the form of loading, encryption, decryption, signature verification, or key wrapping.

6.4 Access Matrix

The following table shows the services (see section 4.2) of the HYDRA PC PERSONAL EDITION FIPS Module, the roles (see section 4.1) capable of performing the service, the CSPs (see section 6.1) that are accessed by the service and the mode of access (see section 6.3) required for each CSP. The following convention is used: if the role column has an 'X', then that role may execute the command.

Table 6-4
HYDRA PC PERSONAL EDITION FIPS Module Access Matrix

Service Name	Roles			Access to Critical Security Parameters	
	Unauth-enticated	Admin	User	CSPs	Access Mode
Cancel File Session			X		
Change Secrets		X		USER/SSO PIN	D,G
Change Secrets			X	USER PIN	D,G
Delete Hydra Keys			X	d_{ECDSA}, $d_{e,U}$	D
End File Decrypt			X	FEK, d_{ECDSA}, $d_{e,U}$, Z	U,D
End File Encrypt			X	FEK, d_{ECDSA}, $d_{e,U}$, Z	U,D
File Encrypt And Hash			X	FEK, d_{ECDSA}, $d_{e,U}$, V, Z	U G,U
File Hash And Decrypt			X	FEK, d_{ECDSA}, $d_{e,U}$, V, Z	U G,U
Generate Single User			X	FEK, KEK	G,U
Get Capabilities	X				
Get Public	X				
Get State	X				
Hash File			X		
Load Secret			X	USER PIN	U
Log Off			X		
Log On			X	USER PIN Z, d_{ECDSA}	U G
Log On		X		SSO PIN Z, d_{ECDSA}	U G
Make Ready			X	Z, d_{ECDSA}	G
Set Drive Lock			X		

Service Name	Roles			Access to Critical Security Parameters	
	Unauth-enticated	Admin	User	CSPs	Access Mode
Signed Firmware Update			X		
Start File Decrypt			X	FEK,KEK, $d_{e,U}$, KEK	G,U D
Start File Encrypt			X	FEK,KEK, $d_{e,U}$, V, KEK	G,U U D
Setup Basic Secure Channel			X	Z	G,U
Get User State			X		
Initialize			X	USER PIN, s, V	G
Zeroize	X			FEK, KEK, Z, d_{ECDSA} $d_{e,U}$	D

7 Self-Tests

The HYDRA PC PERSONAL EDITION FIPS Module executes the following self-tests:

1. Power Up Self-Tests:
 - ECDSA KAT (includes SP800-90 HASH-DRBG (512) KAT)
 - DH KAT (public key check, KDF, modular exponentiation)
 - AES KAT1 (Encrypt/Decrypt - Certificate #858)
 - AES KAT2 (Encrypt/Decrypt – Certificate #846)
 - AES KAT3 (Encrypt/Decrypt – Certificate #850)
 - SHA 256 KAT
 - SHA 512 KAT
 - FIPS186-2 DRNG KAT
 - Firmware Integrity Test (SHA-384 hash)

2. Conditional Self-Tests
 - Continuous RNG Test (FIPS186-2 DRNG)
 - Continuous RNG Test (SP800-90 DRNG)
 - Continuous RNG Test (Hardware RNG)
 - ECDSA Pairwise consistency test
 - EC-DH Pairwise consistency test
 - Firmware load test (ECDSA signature verification)

Self-tests can be initiated by the operator of the module by executing a power-off to the module immediately followed by a power-on operation. If the module fails any of the self-tests, transition to the Failure state is immediate.

8 Mitigation of Other Attacks

No claims of mitigation of other attacks listed in Section 4.11 of FIPS 140-2 by the HYDRA PC PERSONAL EDITION FIPS Module are made or implied in this document.

Acronyms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
DPA	Differential Power Analysis
DRBG	Digital Random Bit Generator
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interface
FEK	File Encryption Key
FIPS	Federal Information Processing Standard
HAC	Host Authentication Code
KAT	Known Answer Test
MKEK	Master Key Encryption Key
NDRNG	Non-deterministic Random Number Generator
PC	Privacy Card, Personal Computer
PCB	Printed Circuit Board
PIN	Personal Identification Number
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SD	Secure Digital (flash memory card)
SDHC	Secure Digital High-capacity
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
SSD	Solid-state Drive
USB	Universal Serial Bus

References

AES-Keywrap National Institute of Standards and Technology (NIST) **AES Key Wrap Specification,** 16 November 2001 1

FIPS 140-2 FIPS PUB 140-2, Change Notice, Federal Information Processing Standards Publication (Supersedes FIPS PUB 140-1, 1994 January 11) **Security Requirements For Cryptographic Modules,** Information Technology Laboratory, National Institute of Standards and Technology (NIST), Gaithersburg, MD, Issued May 25, 2001.

FIPS 180-3 FIPS PUB 180-3 Federal Information Processing Standards Publication **Secure Hash Standard (SHS)**, October 2008

FIPS 186-2 FIPS PUB 186-2, with Change Notice, Federal Information Processing Standards Publication U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology **DIGITAL SIGNATURE STANDARD (DSS),** 2000 January 27

FIPS 197 FIPS PUB 197 **ADVANCED ENCRYPTION STANDARD (AES),** November 26, 2001

SP 800-56A NIST Special Publication 800-56A **Recommendation for Pairwise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised),** Barker, E., Johnson, D., Smid, M., Computer Security Division, NIST, March 2007.

SP 800-90 NIST Special Publication 800-90 **Recommendation for Random Number Generation Using Deterministic Random Bit Generators,** Barker, E., Kelsey, J., Computer Security Division, Information Technology Laboratory, NIST, June 2006.