Entrust® Securing Digital Identities & Information

Title: ***FIPS 140-2 (level 2) Cryptographic Module Security Policy***

Product: ***Entrust Authority™ Security Kernel***

Date: July 11, 2016

Revision: *1.6*

Table of Contents

1 About Entrust

Entrust provides trusted solutions that secure digital identities and information for enterprises and governments in more than 2,000 organizations spanning 60 countries. Offering trusted security for less, Entrust solutions represent the right balance between affordability, expertise and service. These include SSL, strong authentication, fraud detection, digital certificates and PKI. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

2 Introduction

This document describes the Entrust Authority™ Security Kernel (BaseSK) cryptographic module nonproprietary security policy. This document is required for FIPS 140-2 validation. It describes the capabilities, protection, and access rights provided by the BaseSK. It contains a specification of the rules under which the BaseSK must operate. These rules were derived from the requirements in [FIPS]. This document helps individuals and organizations to determine whether the BaseSK will meet their security requirements.

3 Cryptographic Module

3.1 Validation

The BaseSK validation is at FIPS 140-2 (level 2) overall.

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

Table 1: Security Level By FIPS 140-2 Section

3.2 Definition

The BaseSK (Software versions: 8.1sp1, 8.1sp1R2 and 8.1sp1R3) in FIPS 140-2 terminology is defined as a multi-chip standalone cryptographic module.

The BaseSK was tested on the following hardware computing platform and OS.

1. Dell Optiplex 755 with:
   - Intel Core 2 Duo E8400 (64-bit, 3.0 GHz)
2. Microsoft Windows Server 2008 R2 Enterprise Edition
   - Common Criteria Report: http://www.commoncriteriaportal.org/files/epfiles/st_vid10390-vr.pdf

The GPC and OS were installed and configured to be CC EAL2 compliant as specified in [OS]. For details on the platforms on which products that use the BaseSK are supported, refer to the Entrust Platform Support and Integration Center.

"For Level 2 Operational Environment, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any GPC provided that the GPC incorporates the specified CC evaluated EAL2 (or equivalent) operating system/mode/operational settings or another compatible CC evaluated EAL2 (or equivalent) operating system with like mode and operational settings." [IG Section G.5]

The logical boundary of the cryptographic module is the API into which application software may call. The physical boundary of the cryptographic module is the physical case of the GPC in which it resides. See the following block diagrams for more detail.

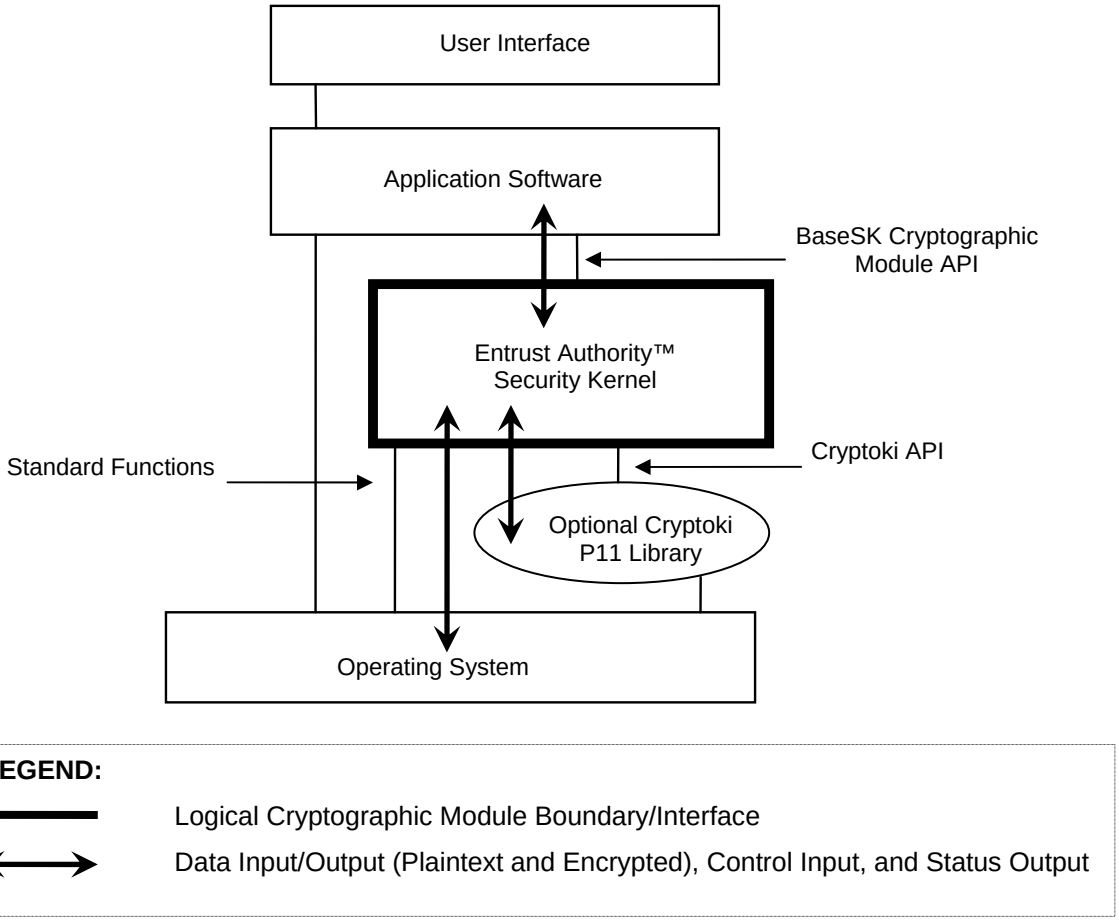

Figure 1: Cryptographic module block diagram for software (Logical).

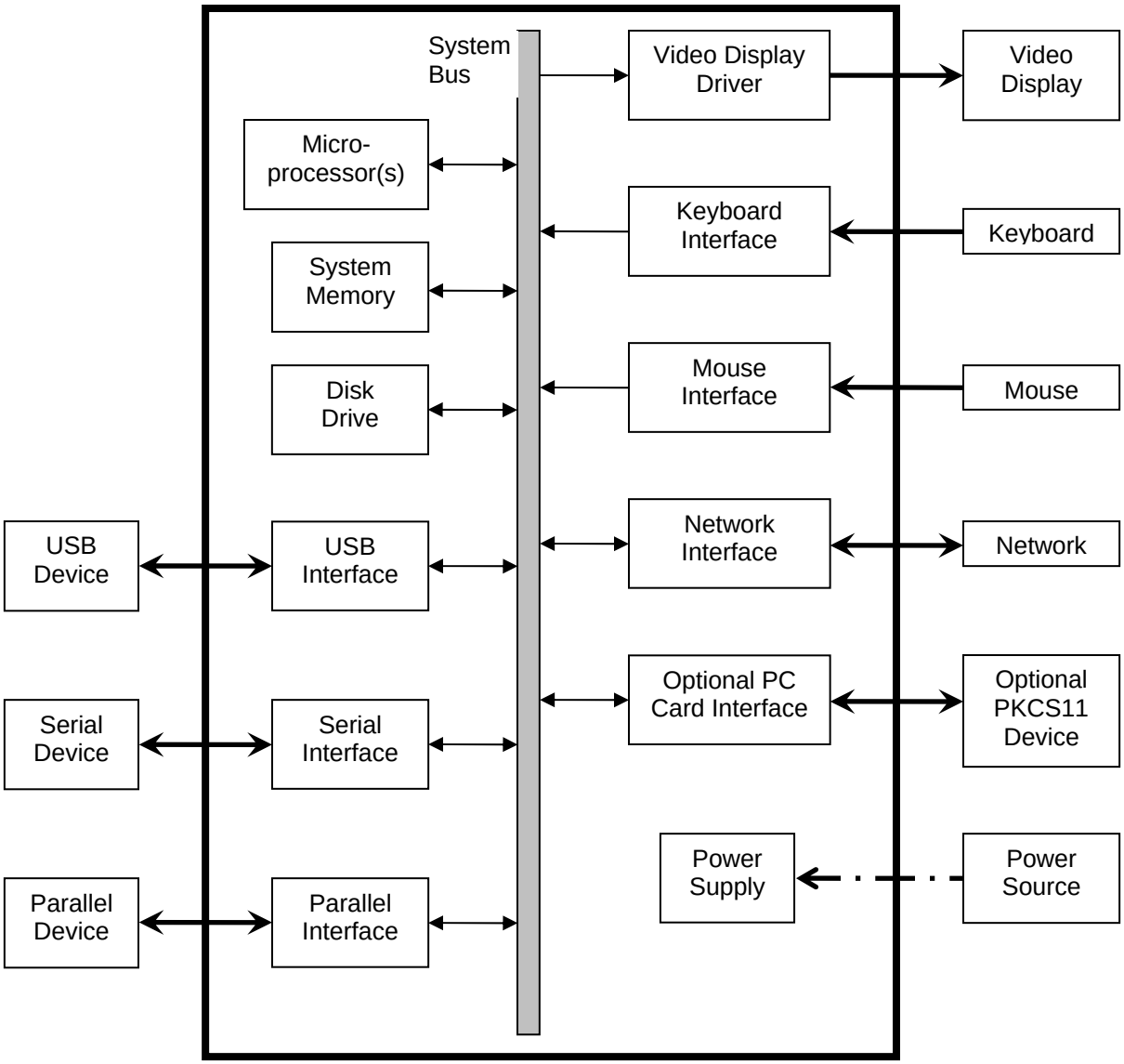

Figure 2: Cryptographic module block diagram for hardware (Physical).

3.3 Security Kernel

The BaseSK implements cryptographic algorithms and provides cryptographic services through an application programming interface (API) that allows developers to integrate security into the applications they design. This API is the logical interface to the cryptographic module and is described in detail in the BaseSK documentation [API].

3.4 Ports and Interfaces

The BaseSK has the following mapping of logical interfaces to physical ports.

FIPS 140-2 Interface	Logical Interface	Physical Interface
Data Input Interface	Input parameters of some APIs	Ethernet/Network Port, USB Port, Parallel Port, Serial Port, PKCS 11 Port
Data Output Interface	Output parameters and/or return values of some APIs	Ethernet/Network Port, USB Port, Parallel Port, Serial Port, PKCS 11 Port
Control Input Interface	Input parameters of some APIs and all API calls themselves	Ethernet/Network Port, USB Port, Parallel Port,, Serial Port, PKCS 11 Port, Keyboard and Mouse
Status Output Interface	Output parameters and/or return values of some APIs	Ethernet/Network Port, USB Port, Parallel Port, Monitor, Serial Port, PKCS 11 Port
Power Interface	Initialization function	Power Interface

Table 2: Mapping Logical Interfaces to Physical Ports

4 Policies

4.1 Identification and Authentication Policy

FIPS 140-2 requires that roles be defined for operators of the cryptographic module. In order to perform a service using the cryptographic module the operator must first assume a role. The following mandatory roles from [FIPS] are implicitly supported by the BaseSK:

> **User**: "*The role assumed to perform general security services, including cryptographic operations and other Approved security functions.*"
>
> **Crypto Officer**: "*The role assumed to perform a set of cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit functions).*"

This cryptographic module uses role based authentication. Both the User and Crypto Officer roles are authenticated via password when the operator logs into the OS. As described in Section 4.2 Access Control Policy, the operator implicitly assumes either the User or Crypto Officer role for each call to a BaseSK API.

Role	Type of Authentication	Authentication Data
User	Password	Minimum 8 characters on the range [a-z,A-Z,0-9]
Crypto Officer	Password	Minimum 8 characters on the range [a-z,A-Z,0-9]

Table 3: Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Password	The strength of the password authentication mechanism depends on the range from which the password is selected. When the OS is configured to require a minimum 8 character password on the range [a-z,A-Z,0-9] this mechanism provides 62^8 possibilities. During a one minute period, $62^8/10^5$ attempts are required for a one in 100,000 probability that one of the attempts will succeed. That would require more than 36 million operations per second and is not feasible on the GPC. (motivated by AS03.25, AS03.26, AS03.21)

Table 4: Strengths of Authentication Mechanisms

4.2 Access Control Policy

Each service offered by the cryptographic module has been assigned a role. To perform a service, the operator calls a cryptographic module API and by doing so implicitly assumes the assigned role. The operator can input/output data including cryptographic keys and critical security parameters (CSP) only through the parameters and the return value provided by the API. The access the operator has to cryptographic keys and CSPs (read/write/execute) is restricted by the API and how it operates on each value.

The services that are provided to each authorized role are listed in the table below. The module does not support any unauthenticated services.

Role	Authorized Services
Crypto Officer	Module Initialization Module Self-Tests Module Status Key Generation
User	Perform Approved Security Function • Symmetric Cipher Encryption/Decryption • Digital Signature Generation/Verification • Hash Generation • Random Number Generation • MAC Generation/Verification • Key Transport (primitive) • Key Agreement (scheme/primitive) Perform Regular Function • Key Input/Output (logical port) • Key Derivation (primitive) • Modify Object • Query Object • Non-Cryptographic Operation • Cryptographic Operation • Identity Management • Zeroization

Table 5: Services Authorized for Roles

The access that each service provides to security-related information (keys and CSPs) is listed in the table below.

Service	Cryptographic Keys and CSPs	Type(s) of Access (e.g., RWE)
Module Initialization	None	None
Module Self-Tests	None	None
Module Status	None	None
Key Generation	AES enc/dec keys Triple-DES enc/dec keys Triple-DES integrity keys RSA signing keys RSA transport keys DSA signing keys ECDSA signing keys ECDH agreement keys DH agreement keys HMAC keys	Execute Execute Execute Execute Execute Execute Execute Execute Execute Execute Execute
Symmetric Cipher Encryption/Decryption	AES enc/dec keys Triple-DES enc/dec keys	Execute Execute
Digital Signature Generation/Verification	RSA signing keys DSA signing keys ECDSA signing keys	Execute Execute Execute
Hash Generation	None	None
Random Number Generation	Entropy String Random value	Execute Read
MAC Generation/Verification	Triple-DES integrity keys HMAC keys	Execute Execute Execute
Key Agreement (scheme/primitive)	ECDH agreement keys DH agreement keys Shared Secret	Execute Execute Read
Key Transport (primitive)	RSA transport keys	Execute
Key Input/Output (logical port)	AES enc/dec keys Triple-DES enc/dec keys Triple-DES integrity keys RSA signing keys RSA transport keys DSA signing keys ECDSA signing keys ECDH agreement keys DH agreement keys HMAC keys	Read, Write Read, Write Read, Write Read, Write Read, Write Read, Write Read, Write Read, Write Read, Write Read, Write Read, Write
Key Derivation (primitive)	Secret	Read, Write
Modify Object	None	None
Query Object	None	None
Non-Cryptographic Operation	None	None
Cryptographic Operation	None	None
Identity Management	None	None
Zeroization	All CSPs	Write

Table 6: Access Rights to CSPs within Services

4.3 Physical Security Policy

The cryptographic module is software-based and does not provide any physical security mechanisms.

4.4 Mitigation of Other Attacks Policy

The cryptographic module is not designed to mitigate against attacks outside of the scope of FIPS 140-2..

Other Attacks	Mitigation Mechanism	Specific Limitations
None	N/A	N/A

Table 7: Mitigation of Other Attacks

5 Cryptographic Algorithm Support

The following table contains the set of validated FIPS Approved algorithms (including appropriate algorithm validation certificates) that can be used in FIPS mode.

Important: the overall bits of security of an algorithm depends both bits of security offered by the algorithm itself and bits of security by the key it is used with; the overall bits of security of the algorithm is always the lower of the two.

* SHA-1 provides less than 80-bits of security when used in a digital signature algorithm; it provides only 69-bits of security strength against collisions and is thus not recommended for use in new applications.

Table 8: FIPS-Approved Algorithms		
Algorithm (Bits of Security)	**Parameters (Bits of Security)**	**Certificate Numbers**
Random Number Generation Algorithms		
DRBG using SHA512	N/A	#167 and #405
Hash Algorithms		
SHS • SHA1 (80*) • SHA224 (112) • SHA256 (128) • SHA384 (192) • SHA512 (256)	N/A	#1689 and #2206
Symmetric Cipher Algorithms		
AES	128 bit (128) 192 bit (192) 256 bit (256)	#1923 and #2631
Triple-DES	192 bit (112)	#1253 and #1580
Digital Signature Algorithms		
FIPS 186-2 DSA • DSA-SHA1 (80*)	DSA-1024	#610 and #794
FIPS 186-3 ECDSA	EC-ansix9p192k1 (80) EC-P-192 (80)	#275 and

• ECDSA-SHA1 (80*) • ECDSA-SHA224 (112) • ECDSA-SHA256 (128) • ECDSA-SHA384 (192) • ECDSA-SHA512 (256)	EC-brainpoolP192r1 (80) EC-brainpoolP192t1 (80) EC-ansix9p224k1 (112) EC-P-224 (112) EC-brainpoolP224r1 (112) EC-brainpoolP224r1 (112) EC-ansix9p256k1 (128) EC-P-256 (128) EC-brainpoolP256r1 (128) EC-brainpoolP256t1 (128) EC-P-384 (192) EC-brainpoolP384r1 (192) EC-brainpoolP384t1 (192) EC-P-521 (256)	#454
FIPS 186-3 RSA • RSA-SHA1 (80*) • RSA-SHA224 (112) • RSA-SHA256 (128) • RSA-SHA384 (192) • RSA-SHA512 (256) • RSAPSS-SHA1 (80*) • RSAPSS-SHA224 (112) • RSAPSS-SHA256 (128) • RSAPSS-SHA384 (192) • RSAPSS-SHA512 (256)	RSA-1024 (80) RSA-2048 (112) RSA-3072 (128)	#992 and #1345
Key Agreement Schemes		
ECDH from SP800-56A - 6.1.2.2 Ephemeral Unified Model, C(2, 0, ECC CDH) - 6.2.2.2 One-Pass Diffie-Hellman, C(1, 1, ECC CDH) - 6.3.2 Static Unified Model, C(0, 2, ECC CDH) - (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)	EC-ansix9p192k1 (80) EC-P-192 (80) EC-brainpoolP192r1 (80) EC-brainpoolP192t1 (80) EC-ansix9p224k1 (112) EC-P-224 (112) EC-brainpoolP224r1 (112) EC-brainpoolP224r1 (112) EC-ansix9p256k1 (128) EC-P-256 (128) EC-brainpoolP256r1 (128) EC-brainpoolP256t1 (128) EC-P-384 (192) EC-brainpoolP384r1 (192) EC-brainpoolP384t1 (192) EC-P-521 (256)	#15 and #111
SP 800-135 KDF	X9.63 SHA-1 KDF	Vendor Affirmed
Message Authentication Code (MAC) Algorithms		
HMAC • HMAC-SHA1 (160) • HMAC-SHA224 (224) • HMAC-SHA256 (256) • HMAC-SHA384 (384)	80 bit (80) 112 bit (112) 128 bit (128) 192 bit (192)	#1158 and 1628

• HMAC-SHA512 (512)	256 bit (256)	
Triple-DES MAC (64)	192 bit (112)	Triple-DES Cert. #1253, vendor affirmed
AES GCM	128 bit 192 bit 256 bit	#1923 and #2631

The following table contains the set of FIPS Allowed algorithms (including appropriate key sizes) that can also be used in FIPS mode.

Table 9: FIPS-Allowed Algorithms	
Algorithm	**Parameters (Bits of Security)**
Key Transport Primitives	
RSA • PKCS1-v1.5 • PKCS1-v2 OAEP • (key transport; key establishment methodology provides between 80 and 128 bits of encryption strength)	RSA-1024 (80) RSA-2048 (112) RSA-3072 (128)
Digital Signature Algorithms	
FIPS 186-3 ECDSA • ECDSA-SHA1 (80*) • ECDSA-SHA224 (112) • ECDSA-SHA256 (128) • ECDSA-SHA384 (192) • ECDSA-SHA512 (256)	EC-ansix9p160k1 (80) EC-ansix9p160r1 (80) EC-ansix9p160r2 (80) EC-brainpoolP160r1 (80) EC-brainpoolP160t1 (80) EC-brainpoolP320r1 (128) EC-brainpoolP320t1 (128) EC-brainpoolP512r1 (256) EC-brainpoolP512t1 (256)
Key Agreement Primitives	
DH • (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength)	DH-1024 DH-1536
ECDH • standard primitive for the single pass scheme with X9.63 SHA-1 KDF. • modified (aka: cofactor) primitive for the single pass scheme with X9.63 SHA-1 KDF.	EC-ansix9p160k1 (80) EC-ansix9p160r1 (80) EC-ansix9p160r2 (80) EC-brainpoolP160r1 (80) EC-brainpoolP160t1 (80) EC-ansix9p192k1 (80) EC-P-192 (80) EC-brainpoolP192r1 (80) EC-brainpoolP192t1 (80)

• (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)	EC-ansix9p224k1 (112) EC-P-224 (112) EC-brainpoolP224r1 (112) EC-brainpoolP224r1 (112) EC-ansix9p256k1 (128) EC-P-256 (128) EC-brainpoolP256r1 (128) EC-brainpoolP256t1 (128) EC-brainpoolP320r1 (128) EC-brainpoolP320t1 (128) EC-P-384 (192) EC-brainpoolP384r1 (192) EC-brainpoolP384t1 (192) EC-brainpoolP512r1 (256) EC-brainpoolP512t1 (256) EC-P-521 (256)

The following table contains the set of non-FIPS Approved algorithms that are implemented but **must not** be used when operating in FIPS mode, or if used, must not be considered to provide any security.

Table 10: Non-FIPS-Approved Algorithms

Algorithm	Parameters
Random Number Generation Algorithms	
FIPS 186-2 using SHA1	N/A
Hash Algorithms	
MD2	N/A
MD5	N/A
RMD-160	N/A
Symmetric Cipher Algorithms	
CAST	40 bit 48 bit 56 bit 64 bit
CAST3	40 bit 48 bit 56 bit 64 bit
CAST5	80 bit 128 bit (and sizes on the range 40-128 in 8 bit increments)
DES	64 bit
IDEA (compatible)	128 bit
RC2 (compatible)	128 bit (and sizes on the range 40-128 in 8 bit increments)

RC4	128 bit (and sizes on the range 40-128 in 8 bit increments)
Digital Signature Algorithms	
DSA • DSA-SHA1	DSA-512 (and sizes on the range 512-960 in 64 bit increments)
RSA • RSA-MD2 • RSA-MD5 • RSA-RMD160	RSA-512 (and sizes on the range 512-8192 in 8 bit increments)
RSA • RSA-SHA1 • RSA-SHA224 • RSA-SHA256 • RSA-SHA384 • RSA-SHA512 • RSAPSS-SHA1 • RSAPSS-SHA224 • RSAPSS-SHA256 • RSAPSS-SHA384 • RSAPSS-SHA512	RSA-512 RSA-4096 RSA-6144 (and sizes on the range 512-8192 in 8 bit increments, except those listed in the Approved/Allowed section above)
Key Transport Primitives	
RSA • PKCS1-v1.5 • PKCS1-v2 OAEP	RSA-512 (and sizes on the range 512-8192 in 8 bit increments, except those listed in the Approved/Allowed section above)
Key Agreement	
PAKE (password authenticated key exchange) with SPEKE (simple password exponential key exchange) as the underlying protocol.	Using X963 KDF with SHA1 and supporting all symmetric keys ranging from 40 to 256 bit.
DH	With sizes on the range 256-1536 in 8 bit increments.
Message Authentication Code (MAC) Algorithms	
HMAC • HMAC-MD5 • HMAC-RMD160 • HMAC-SHA1 • HMAC-SHA224 • HMAC-SHA256 • HMAC-SHA384 • HMAC-SHA512	HMAC is supported with all symmetric keys ranging from 40 to 256 bit. HMAC-SHA-X is only non-Approved when used with a non-Approved key size.

AES-DAC	128 bit 192 bit 256 bit
CAST-DAC	40 bit 48 bit 56 bit 64 bit
CAST3-DAC	40 bit 48 bit 56 bit 64 bit
CAST5-DAC	80 bit 128 bit (and sizes on the range 40-128 in 8 bit increments)
DES-DAC	64 bit
IDEA-DAC (compatible)	128 bit
RC2-DAC (compatible)	128 bit (and sizes on the range 40-128 in 8 bit increments)

6 Self Tests

The cryptographic module contains the following self-tests to verify its correct operation; these tests are automatically run during initialization in the FIPS Approved Mode of operation.

Power-On Self-Tests:

- Software integrity test using Triple-DES-MAC
- Cryptographic algorithm known-answer tests
  - Random Number Generation Algorithms:
    - DRBG using SHA512
  - Hash Algorithms: (compute digest and compare to known value)
    - SHA1
    - SHA224
    - SHA256
    - SHA384
    - SHA512
  - Symmetric Cipher Algorithms: (encrypt/decrypt and compare to known value)
    - AES-128
    - AES-192
    - AES-256
    - Triple-DES
  - Digital Signature Algorithms: (with known public key, confirm that known signature verifies; with known private key, confirm known signature is computed)
    - RSA-1024, RSA-SHA1
    - RSA-1024, RSAPSS-SHA1
    - DSA-1024, DSA-SHA1
    - EC-P-192, ECDSA-SHA1
  - MAC Algorithms: (compute and compare to known value)
    - HMAC-SHA1
    - HMAC-SHA224

        - HMAC-SHA256
        - HMAC-SHA384
        - HMAC-SHA512
        - AES GCM
        - Note: Triple-DES-MAC is not separately tested as permitted by [IG Section 9.1].
    - Key Agreement: (with two known key-pairs, confirm that a known secret is derived)
        - DH-1024
        - ECDH (SP 800-56A), standard X9.63 SHA-1 KDF, EC-P-192

Note: Non-mandatory tests on Non-FIPS-Approved algorithms are also performed.

Note: Known answer tests for the RSA Key Transport primitive are not required because these operations are tested during RSA conditional pair-wise consistency tests (permitted by AS09.18).

Conditional Tests:

- Random Number Generation Algorithm continuous tests:
    - DRBG using SHA512
    - FIPS 186-2 using SHA1
- Key Pair Generation pair-wise consistency tests
    - DSA-SHA1 digital signature sign/verify
    - ECDSA-SHA1 digital signature sign/verify
    - RSA digital signature sign/verify
    - RSA key transport encrypt/decrypt

  Note:
    - Digital signature algorithm pair-wise consistency tests are only required using one message digest algorithm; permitted by [IG Section 9.4].

7 Operator Guidance

7.1 Assumptions

The following assumptions are made about the operating environment of the cryptographic module:

- Unauthorized reading, writing, or modification of the module's memory space (code and data) by an intruder (human or machine) is not possible; this is prevented by the process memory management of the OS.
- Replacement or modification of the legitimate cryptographic module code by an intruder (human or machine) is not feasible.
- The module is initialized to the FIPS 140-2 mode of operation.

7.2 Delivery, Installation and Initialization

The following steps must be performed in order to securely deliver, install and initialize the BaseSK cryptographic module in the FIPS 140-2 Approved mode of operation:

- All BaseSK versioned source files [SRC] must be built and linked into a target application.
- The target application must be designed such that when loaded into memory, without input from the operator, it automatically calls `SK_Initialize(true)` and then uses the `SK_SoftwareAuthenticator` object to verify its software integrity from a pre-

computed MAC value stored in an ini file. Note that the `SK_SoftwareAuthenticator` is designed to internally call `SK_RunAllSelfTests()` as its last step.

- The operator must acquire the target application and associated MAC value ini file through a medium at least as secure as download from https://secure.entrust.com (i.e. a trusted SSL download).
- The OS on which the target application resides must enforce that passwords contain a minimum of 8 characters on the range [a-z,A-Z,0-9] and must enforce that login is required after each power-on of the GPC (motivated by AS03.25, AS03.26, AS03.21).
- The target application must be launched (and as stated above will automatically perform software authentication and self tests). The BaseSK cryptographic module is now in the approved mode of operation and all cryptographic services are available.

7.3 Operator Responsibilities

The operator must continually fulfill the following responsibilities to maintain the BaseSK cryptographic module in the FIPS 140-2 approved mode of operation:

- Input and output of plaintext private keys, plaintext secret keys, or plaintext CSPs via any physical port of the module is prohibited.
- Input and output of encrypted private keys, encrypted secret keys, or encrypted CSPs via any physical port of the module is only permitted when encrypted using an approved algorithm.
- Non-FIPS-Approved Algorithms (see Table 10) must not be requested from the BaseSK cryptographic module.
- No key generated by the cryptographic module shall be considered to offer more than 256-bits of security, regardless of its size. (motivated by VE07.13.01)
- When performing ECDH
    - The bits of security of the EC key shall be at least as large as the bits of security of the key being agreed upon.
    - Ephemeral private keys shall be securely destroyed after a single use.
    - Static public keys shall
        - Be received over a trusted channel that asserts:
          The sender is the entity with whom ECDH should be performed.
          The sender possesses the matching private key.
          The sender does not use this key for other purposes.
        - Or a corresponding certificate shall be verified to confirm:
          The sender is the entity with whom ECDH should be performed, because their name is in the certificate.
          The sender possesses the matching private key, because the certification authority performed proof-of-possession when the cert was issued.
          The sender does not use this key for other purposes, because the keyUsage does not contain digitalSignature.
- When performing "Static Unified Model" ECDH, the $Nonce_U$, ID_U, ID_V from SP800-56A shall be achieved by SK_KeyAgreeParams and the SK_Key::KeyAgree API.

7.4 Module Interfaces

All physical ports are available to all operators of the module. Each BaseSK API that is part of the cryptographic module's logical interface is included in [API] and labeled either "FIPS Role: User" or "FIPS Role: Crypto Officer" depending on the role that is implicitly assumed by calling it. All API arguments and return values are labeled as Data Input, Data Output, Control Input, or Status Output. The documentation for each API includes details on any relevant security events and/or parameters and which "FIPS Service" is being performed.

8 References

Author	Title
NIST	[FIPS] FIPS PUB 140-2: Security Requirements For Cryptographic Modules, December 2002 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
NIST	[IG] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, August 2010 (http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf)
Entrust	[API] FIPS 140-2 (level 2) Cryptographic Module API Documentation for the Entrust Authority™ Security Kernel
Entrust	[SRC] FIPS 140-2 (level 2) Cryptographic Module Source Distribution for the Entrust Authority™ Security Kernel
Microsoft	[OS] Microsoft Windows Common Criteria Evaluation (http://www.commoncriteriaportal.org/files/epfiles/st_vid10390-st.pdf)