Entrust® Securing Digital Identities & Information

Title:	***FIPS 140-2 (level 2) Cryptographic Module Non-Proprietary Security Policy***
Product:	***Entrust Authority™ Security Kernel***
Date:	*July 6, 2021*
Revision:	*1.1.1*

Disclaimer

The information in this document is provided solely for informational purposes and is provided "as is" by Entrust without any representations, conditions and/or warranties of any kind, whether express, implied, statutory, by usage of trade, or otherwise. Entrust specifically disclaims any and all representations, conditions, and/or warranties of merchantability, satisfactory quality, and/or fitness for a particular purpose. To the maximum extent permitted by applicable law, in no event will Entrust be liable for any damages, losses or costs arising from your or any third-party actions or omissions in connection with this document.

The information in this document is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.

Export and/or import of cryptographic products may be restricted by various regulations in certain countries. Export and/or import permits may be required.

Table of Contents

1 About Entrust Corporation

Consumers, citizens, and employees increasingly expect anywhere-anytime experiences—whether they are making purchases, crossing borders, accessing e-government services or logging onto corporate networks. Entrust offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports, and ID cards to the digital realm of authentication, certificates and secure communications.

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: 1.0 and 1.1) 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 Operating System (OS).

1. HP Compaq Pro 6305 - AMD A4 with:

- Microsoft Windows Server 2016 Standard Edition
  - Security Policies:
    https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2936.pdf
  - Common Criteria Report:
    https://www.commoncriteriaportal.org/files/epfiles/2016-36-INF-1779.pdf

The BaseSK is also supported on the following platform for which full CMVP testing was not performed:

1. Lenovo ThinkCentre M910T with:

- Intel Core i7-7700 (3.60GHz, 8 MB), 64-bit running
- Microsoft Windows Server 2016 Standard Edition
  - Common Criteria Report:
    https://www.commoncriteriaportal.org/files/epfiles/2016-36-INF-1779.pdf

Note: The CMVP makes no claim as to the correct operation of the module on this operational environment

The GPC and OS were installed and configured to be Common Criteria (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 customer support portal: https://trustedcare.entrust.com/

> *"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 module is bound to FIPS 140-2 Cert. #2936 only for the purpose of the entropy source for the DRBG.

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 General Purpose Computer (GPC) in which it resides. See the following block diagrams for more detail.

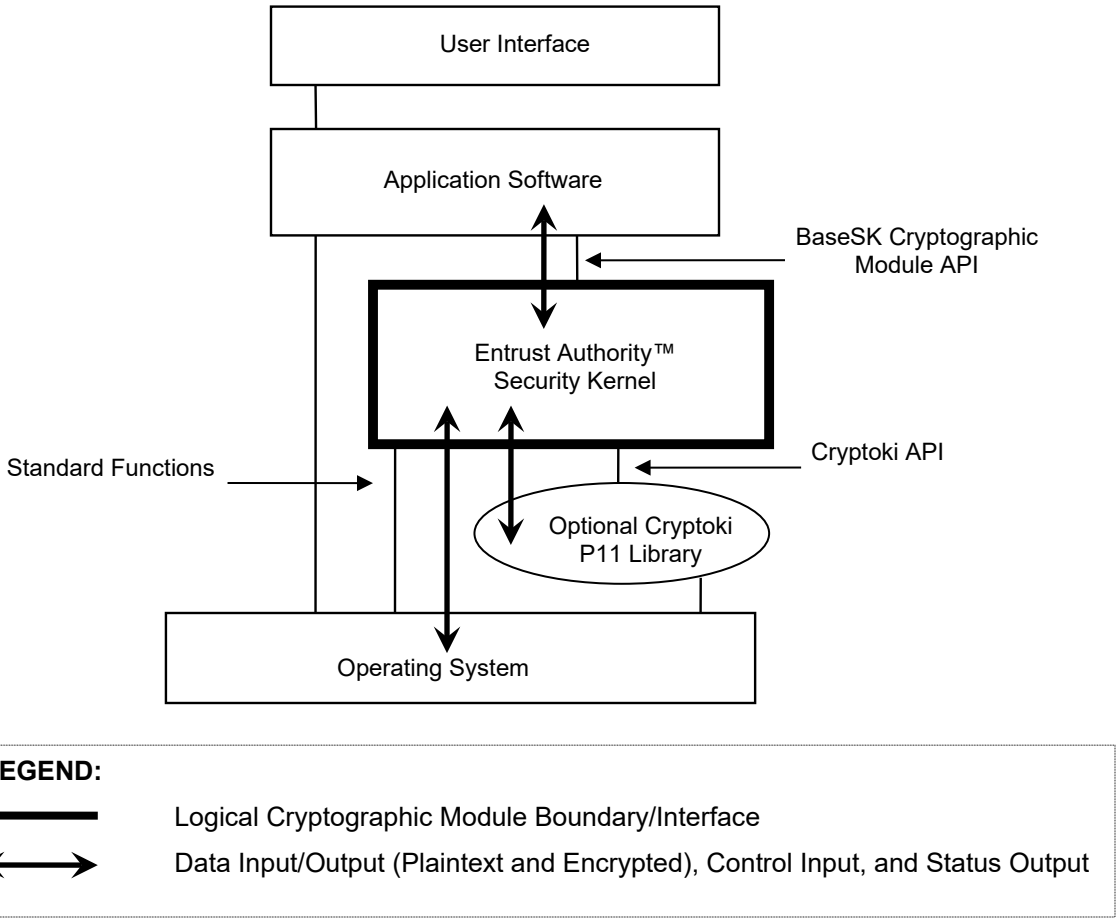

Figure 1: Cryptographic module block diagram for software (Logical)

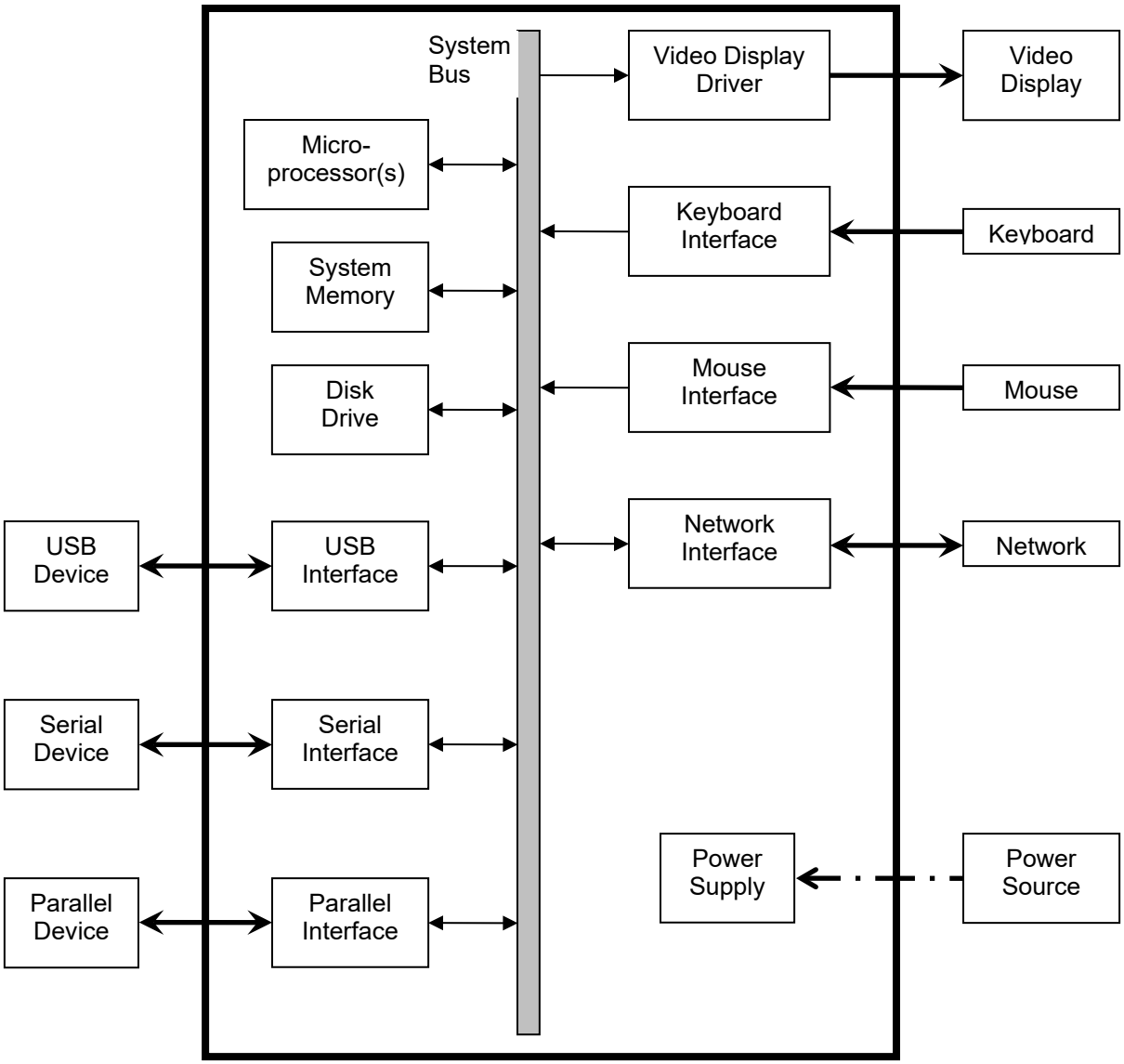

Figure 2: Cryptographic module block diagram for hardware (Physical)

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
Data Output Interface	Output parameters and/or return values of some APIs	Ethernet/Network Port, USB Port, Parallel Port, Serial Port
Control Input Interface	Input parameters of some APIs and all API calls themselves	Ethernet/Network Port, USB Port, Parallel Port, Serial 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
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. The probability that a random attempt will succeed, or a false acceptance will occur is $1/62^8$ which is less than $1/10^6$. 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 (input/output/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. The module supports an Approved and non-Approved mode of operation. When a service is called to use a non-Approved cryptographic algorithm listed in Table 13, then the non-Approved version of the service has been called and the module is in the non-Approved mode of operation.

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) • Key Derivation (primitive) Perform Regular Function • Key Input/Output (logical port) • Modify Object • Query Object • Non-Cryptographic Operation • Cryptographic Operation • Identity Management • Zeroization

Table 5: Services Authorized for Roles

Authorized Services	Approved Mode	Non-Approved Mode
Module Initialization	X	
Module Self-Tests	X	
Module Status	X	
Key Generation	X	X
Symmetric Cipher Encryption/Decryption	X	
Digital Signature Generation/Verification	X	X
Hash Generation	X	X
Random Number Generation	X	
MAC Generation/Verification	X	X
Key Transport (primitive)	X	
Key Agreement (scheme/primitive	X	X
Key Derivation (primitive)	X	X
Key Input/Output (logical port)	X	X
Modify Object	X	X
Query Object	X	
Non-Cryptographic Operation	X	X
Cryptographic Operation	X	
Identity Management	X	
Zeroization	X	X

Table 6: Authorized Services Available in Approved and non-Approved Mode

All Cryptographic Keys and CSPs used by the Module are described in Table 7 and Public Keys are described in Table 8.

Cryptographic Keys and CSPs	Description
AES enc/dec keys	AES (128/192/256 bits) encrypt / decrypt key
Triple-DES enc/dec keys	TDES (3-Key – 192 bits) encrypt / decrypt key
Triple-DES integrity keys	TDES (3-Key – 192 bits) integrity key
RSA signing keys	RSA (2048 to 8192 bits) signature generation key
RSA transport keys	RSA (2048 to 8192 bits) key decryption (private key transport) key
ECDSA signing keys	ECDSA (All NIST P curves except sizes 163 and 192 and non-NIST-Recommended elliptic curves with security strength above 112 bits) signature generation key
ECDH agreement keys	ECDH (All NIST defined P curves except sizes 163 and 192 and non-NIST-Recommended elliptic curves with security strength above 112 bits) private key agreement key.
HMAC keys	Keyed hash key (160/224/256/384/512 bits)
Entropy String	Entropy input string for HASH_DRBG (size)
Entropy Seed	DRBG seed coming from the NDRNG and HASH_DRBG (112 bits)
Entropy State	HASH_DRBG internal state of secret values V and C
Random value	DRBG output value (112 bits) used in key generation
Shared Secret	Used in key agreement

Table 7: Cryptographic Keys and CSPs Used by the Module

Cryptographic Public Keys	Description
RSA signing keys	RSA (1024 to 8192 bits) signature verification key
RSA transport keys	RSA (2048 or 3072 bits) key encryption key
DSA signing keys	DSA (1024 bits) signature verification key

ECDSA singing keys	ECDSA (All NIST P curves except sizes 163 and 192 and non-NIST-Recommended elliptic curves with security strength above 112 bits) signature verification key
ECDH agreement keys	ECDH (All NIST defined P curves except sizes 163 and 192 and non-NIST-Recommended elliptic curves with security strength above 112 bits) public key agreement key

Table 8: Cryptographic Public Keys Used

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

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

Service	Cryptographic Keys and CSPs	Type(s) of Access (e.g., IOGEZ)
Module Initialization	None	None
Module Self-Tests	None	None
Module Status	None	None
Key Generation	AES enc/dec keys	E
	Triple-DES enc/dec keys	E
	Triple-DES integrity keys	E
	RSA signing keys	E
	RSA transport keys	E
	DSA signing keys	E
	ECDSA signing keys	E
	ECDH agreement keys	E
	HMAC keys	E
Symmetric Cipher Encryption/Decryption	AES enc/dec keys	E
	Triple-DES enc/dec keys	E
Digital Signature Generation/Verification	RSA signing keys	E
	DSA signing keys	E
	ECDSA signing keys	E
Hash Generation	None	E
Random Number Generation	Entropy String	E
	Entropy Seed	E
	Entropy State	E
	Random value	O
MAC Generation/Verification	HMAC keys	E
Key Agreement (scheme/primitive)	ECDH agreement keys	E
	Shared Secret	O
Key Transport (primitive)	RSA transport keys	E
	AES enc/dec keys	E
Key Input/Output (logical port)	AES enc/dec keys	O,I
	Triple-DES enc/dec keys	O,I
	Triple-DES integrity keys	O,I
	RSA signing keys	O,I
	RSA transport keys	O,I
	DSA signing keys	O,I
	ECDSA signing keys	O,I

	ECDH agreement keys	O,I
	HMAC keys	O,I
Key Derivation (primitive)	Shared Secret	O,I
Modify Object	None	None
Query Object	None	None
Non-Cryptographic Operation	None	None
Cryptographic Operation	None	None
Identity Management	None	None
Zeroization	All CSPs	Z

Table 9: 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 10: 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 Approved mode.

Important: the overall bits of security of an algorithm depends on 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 60-bits of security strength against collisions and thus can only be used in legacy-use applications; any other use is non-Approved. SHA-1 can only be used in verification services for digital signature or message authentication code algorithms in approved mode.
** The same Triple-DES key shall not be used to encrypt more than 65535 64-bit data blocks. This means the same Triple-DES key shall not be used to encrypt a file that's size is bigger than 524k.
*** The minimum HMAC key size shall be bigger than 16 bytes.
**** AES GCM adheres to 140IG A.5 Key/IV Pair Uniqueness Requirements from SP 800-38D number two. The IV must be at least 96-bits in length.
*****The module generates cryptographic keys whose strengths are modified by available entropy.

Algorithm (Bits of Security)	Parameters (Bits of Security)	Function	Certificate Numbers
Random Number Generation Algorithms			
CKG from IG D.12 and SP800-133r2	N/A	Section 5.1 Key Pairs for Digital Signature Schemes Section 5.2 Key Pairs for Key Establishment Section 6.1 The "Direct Generation" of Symmetric Key	Vendor Affirmed

		Section 6.2.1 Symmetric Keys Generated Using Key-Agreement Schemes Section 6.2.2 Symmetric Keys Derived from Pre-existing Key Section 6.2.3 Symmetric Keys Derived from Passwords Section 6.3 Symmetric Keys Produced by Combining (Multiple) Keys and Other Data	
HASH_DRBG using SHA512 Hash from SP800-90A	112 bits*****	Deterministic Random Bit Generation	#C601
Hash Algorithms			
SHS from FIPS 180-4 • SHA1 (80*) ○ Legacy use only for Signature Verification • SHA224 (112) • SHA256 (128) • SHA384 (192) • SHA512 (256)	N/A	Message Digest Generation, Password Obfuscation	#C600
Symmetric Cipher Algorithms			
AES – ECB AES – CBC From FIPS 197	128 bit (128) 192 bit (192) 256 bit (256)	Encrypt, Decrypt	#C614
Triple-DES – ECB ** Triple-DES – CBC **	192 bit (112)	Encrypt, Decrypt	#C606
Digital Signature Algorithms			
FIPS 186-4 DSA • DSA-SHA1 (80*) Legacy use only for Signature Verification	DSA-1024	SigVer	#C602
FIPS 186-4 ECDSA • ECDSA-SHA1 (80*) ○ Legacy use only for Signature Verification • ECDSA-SHA224 (112) • ECDSA-SHA256 (128) • ECDSA-SHA384 (192) • ECDSA-SHA512 (256)	EC-P-192 (80* Legacy use only for Signature Verification) EC-P-224 (112) EC-P-256 (128) EC-P-384 (192) EC-P-521 (256)	SigGen SigVer KeyGen PKV	#C603
FIPS 186-4 RSA • RSA-SHA1 (80*) ○ Legacy use only for Signature Verification • RSA-SHA224 (112) • RSA-SHA256 (128) • RSA-SHA384 (192) • RSA-SHA512 (256) • RSAPSS-SHA1 (80*)	RSA-1024 (80* Legacy use only for Verification) RSA-2048 (112) RSA-3072 (128)	SigGen SigVer KeyGen	#C605

○ Legacy use only for Signature Verification • RSAPSS-SHA224 (112) • RSAPSS-SHA256 (128) • RSAPSS-SHA384 (192) • RSAPSS-SHA512 (256)			
FIPS 186-2 RSA • RSA-SHA224 (112) • RSA-SHA256 (128) • RSA-SHA384 (192) • RSA-SHA512 (256) • RSAPSS-SHA224 (112) • RSAPSS-SHA256 (128) • RSAPSS-SHA384 (192) • RSAPSS-SHA512 (256)	RSA-4096 (128)	SigGen	#C605
Key Agreement Schemes			
CVL - SP 800-135 KDF	X9.63 SHA-2 KDF	Key Derivation	#C607
KAS - ECDH from SP800-56Ar3 - 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)	EC-P-224 (112) EC-P-256 (128) EC-P-384 (192) EC-P-521 (256)	key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength	Vendor Affirmed
Message Authentication Code (MAC) Algorithms			
AES GCM**** from SP 800-38D	128 bit 192 bit 256 bit	Authenticated Encrypt, Authenticated Decrypt, Message Authentication	#C614
HMAC*** from FIPS 198-1 • HMAC-SHA1 (160) • HMAC-SHA224 (224) • HMAC-SHA256 (256) • HMAC-SHA384 (384) • HMAC-SHA512 (512)	80 bit (80* Legacy use only for Signature Verification) 112 bit (112) 128 bit (128) 192 bit (192) 256 bit (256)	Message Authentication, KDF Primitive, Password Obfuscation	#C604
Key Transport (Symmetric Cipher Algorithms)			
CVL – SP800-56B RSADP	RSA-2048 (112)	Key Transport	#C605
KTS - AES Key Wrap with padding (KWP) from SP 800-38F	128 bit 192 bit 256 bit	Key establishment methodology provides between 128 and 256 bits of encryption strength	#C614

Table 11: FIPS-Approved Algorithms

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

Algorithm	Parameters (Bits of Security)	Function
Random Number Generation Algorithm		
NDRNG	Minimum of 112-bits	seed for DRBG Note: *The module generates cryptographic keys whose strengths are modified by available entropy*.
Key Transport Primitives		
RSA not fully complaint with SP800-56B • PKCS1-v1.5 • PKCS1-v2 OAEP	RSA-2048 (112) RSA-3072 (128) RSA-4096 (128) (and sizes on the range 2048-8192 in 8-bit increments, except those listed here)	key wrapping; key establishment methodology provides between 112 and 202 bits of encryption strength
Digital Signature Algorithms		
FIPS 186-4 ECDSA • ECDSA-SHA1 (80*) ○ Legacy use only for Signature verification • ECDSA-SHA224 (112) • ECDSA-SHA256 (128) • ECDSA-SHA384 (192) • ECDSA-SHA512 (256)	EC-ansix9p224k1 (112) EC-brainpoolP224r1 (112) EC-brainpoolP224t1 (112) EC-ansix9p256k1 (128) EC-brainpoolP256r1 (128) EC-brainpoolP256t1 (128) EC-brainpoolP320r1 (128) EC-brainpoolP320t1 (128) EC-brainpoolP384r1 (192) EC-brainpoolP384t1 (192) EC-brainpoolP512r1 (256) EC-brainpoolP512t1 (256)	SigGen SigVer KeyGen PKV
FIPS 186-2 RSA with CVL Cert. #C605 • RSA-SHA224 (112) • RSA-SHA256 (128) • RSA-SHA384 (192) • RSA-SHA512 (256) • RSAPSS-SHA224 (112) • RSAPSS-SHA256 (128) • RSAPSS-SHA384 (192) • RSAPSS-SHA512 (256)	RSA-6144 (128) RSA-8092 (192) sizes on the range 4104-8192 in 8 bit increments	SigGen
FIPS 186-2 RSA with CVL Cert. #C605 - Legacy use only for Signature Verification • RSA-SHA1 (80) • RSA-SHA224 (112) • RSA-SHA256 (128) • RSA-SHA384 (192)	sizes on the range 1024-8192 in 8 bit increments	SigVer

• RSA-SHA512 (256) • RSAPSS-SHA1 (80) • RSAPSS-SHA224 (112) • RSAPSS-SHA256 (128) • RSAPSS-SHA384 (192) • RSAPSS-SHA512 (256)		
Key Agreement Primitives		
ECDH not fully complaint with SP800-56Ar3 • Standard primitive for the single pass scheme with X9.63 SHA-2 KDF. • Modified (aka: cofactor) primitive for the single pass scheme with X9.63 SHA-2 KDF	EC-ansix9p224k1 (112) EC-brainpoolP224r1 (112) EC-brainpoolP224t1 (112) EC-ansix9p256k1 (128) EC-brainpoolP256r1 (128) EC-brainpoolP256t1 (128) EC-brainpoolP320r1 (128) EC-brainpoolP320t1 (128) EC-brainpoolP384r1 (192) EC-brainpoolP384t1 (192) EC-brainpoolP512r1 (256) EC-brainpoolP512t1 (256)	key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength

Table 12: FIPS-Allowed Algorithms

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, the module will then transition to the non-Approved mode.

Algorithm	Parameters	Function	Service
Digital Signature Algorithms			
DSA • DSA-SHA1	DSA-512 (and sizes on the range 512-960 in 64-bit increments)	SigVer	Digital Signature Verification
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-ansix9p192k1 (80) EC-P-192 (80) EC-brainpoolP192r1 (80) EC-brainpoolP192t1 (80)	SigVer KeyGen PKV	Digital Signature Verification Key Agreement
RSA • RSA-SHA1 • RSA-SHA224 • RSA-SHA256 • RSA-SHA384 • RSA-SHA512 • RSAPSS-SHA1 • RSAPSS-SHA224 • RSAPSS-SHA256 • RSAPSS-SHA384 • RSAPSS-SHA512	sizes on the range 512-1016 in 8-bit increments for SigVer and sizes on the range 512-2040 for KeyGen	SigVer KeyGen	Digital Signature Verification Key Generation
Key Transport Primitives			

RSA • PKCS1-v1.5 • PKCS1-v2 OAEP	RSA-512 (and sizes on the range 512-2040 in 8-bit increments)	key transport; key establishment provides less than 112 bits of encryption strength	Key Generation Key Transport
Key Agreement			
DH	With sizes on the range 256-8192 in 8-bit increments.	key agreement; key establishment provides less than 80 bits to 202 bits of encryption strength	Key Input/Out Key Agreement
ECDH	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 provides less than 112 bits of encryption strength	Key Input/Out 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.	key agreement; key establishment provides less than 112 bits of encryption strength	Key Input/Out
Message Authentication Code (MAC) Algorithms			
AES-DAC	128, 192, 258 bits	Message Authentication, Password Obfuscation	MAC Generation/Verification
HMAC • 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.	Message Authentication, KDF Primitive, Password Obfuscation	MAC Generation/Verification
Triple-DES MAC (64)	192 bits (112)	Message Authentication	MAC Generation/Verification

Table 13: Non-FIPS-Approved Algorithms

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 HMAC256
- Memory Endianness test (Critical Function Test)
- Cryptographic algorithm known-answer tests
    - Random Number Generation Algorithms:
        - DRBG using SHA512 Hash
    - 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-2048, RSA-SHA256
        - RSA-2048, RSAPSS-SHA256
        - DSA-1024, DSA-SHA1
        - EC-P-256, ECDSA-SHA256
    - MAC Algorithms: (compute and compare to known value)
        - HMAC-SHA1
        - HMAC-SHA224
        - HMAC-SHA256
        - HMAC-SHA384
        - HMAC-SHA512
        - AES-128 GCM, AES-256 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)
        - ECDH (SP 800-56Ar3), standard X9.63 SHA-2 KDF, EC-P-256
    - AES Key Wrap with Padding:(KWP-AE-192, KWP-AD-192)
        - AES-192 with key data length 20 and 7 byte

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 health tests:(SP800-90A)
    - DRBG using SHA512 Hash

- 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 HMAC256 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://trustedcare.entrustdatacard.com/TrustedCare/MyProductsList (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 SP800-56Ar3 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.

7.5 Single Operator Mode of Operation

FIPS 140-2 states that when using a software cryptographic module, the operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). NIST has since provided further implementation guidance regarding this matter:

> *"Software cryptographic modules implemented in client/server architecture are intended to be used on both the client and the server. The cryptographic module will be used to provide cryptographic functions to the client and server applications. When a crypto module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients." [IG Section 6.1]*

This indicates that for an application built on the BaseSK cryptographic module, the application is always the single user of the cryptographic module even when multiple applications are running concurrently. This permits multiple concurrent BaseSK based applications to be running on the same machine in a FIPS 140-2 compliant manner.

7.6 Security Rules and Guidance

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module clears previous authentications on power cycle.
3. An operator does not have access to any cryptographic services prior to assuming an authorized role.
4. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module.
5. Power up self-tests do not require any operator action.

6. Data output are inhibited during key generation, self-tests, zeroization, and error states.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The module does not support concurrent operators.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any proprietary external input/output devices used for entry/output of data.
13. The module does not enter or output plaintext CSPs.
14. The module does not store any plaintext CSPs
15. The module does not output intermediate key values.
16. The module does not provide bypass services or ports/interfaces.

8 References

Author	Title
NIST	[FIPS 1] 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)
NIST	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000.
NIST	FIPS 186-4 Digital Signature Standard (DSS), July 2013 (https://csrc.nist.gov/publications/detail/fips/186/4/final)
NIST	FIPS 180-4 Secure Hash Standard (SHS), August 2015 (https://csrc.nist.gov/publications/detail/fips/180/4/final)
NIST	NIST Special Publication 800-131A Revision 2: Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf)
NIST	NIST Special Publication 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf)
NIST	NIST Special Publication 800-56A Revision 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf)
NIST	NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009
NIST	Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001 (https://csrc.nist.gov/publications/detail/fips/197/final)
NIST	NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 28, 2007 (https://csrc.nist.gov/publications/detail/sp/800-38d/final)
NIST	NIST Special Publication 800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012 (https://csrc.nist.gov/publications/detail/sp/800-38f/final)
NIST	FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008 (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf)
NIST	NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, June 2020
NIST	SP 800-135 Rev. 1 Recommendation for Existing Application-Specific Key Derivation Functions, December 2011 (https://csrc.nist.gov/publications/detail/sp/800-135/rev-1/final)
RFC	RFC-5639 Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010 (https://tools.ietf.org/html/rfc5639)
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 (https://www.commoncriteriaportal.org/files/epfiles/Windows%2010%20AU%20and%20Server%202016%20GP%20OS%20Security%20Target%20-%20Public.pdf http://www.commoncriteriaportal.org/files/epfiles/st_vid10390-st.pdf)