Engage Communication, Inc.

BlackVault HSM

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.15

Date: June 13, 2018

Contents

List of Tables

List of Figures

Introduction

This document specifies the Security Policy for the Engage Communication BlackVault Hardware Security Module (HSM) module, hereafter denoted the Module. The Module is an embedded Ethernet attached HSM that combines a cryptographically advanced HSM with a smart card reader, integrated touch screen display and USB port. The Module meets FIPS 140-2 overall Level 3 requirements.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version	OE (if applicable)
1	BlackVault HSM	007-BVES-01	7.0.10.2	N/A

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated cryptographic products. The Module is a multi-chip embodiment; the cryptographic boundary is the outer perimeter of the printed circuit board (PCB) with all components outside of the metal enclosure being excluded. The metal enclosure protects the security area containing the processor, memory, CPLD and other components.

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 the figures below; the red outline depicts the security region, which is contained within a metal enclosure, but the physical boundary is defined as the outer perimeter of the PCB. Figures 1 and 2 are photos top and bottom of the multi-chip embodiment with a red outline indicating the security region. The Module relies on physical smart card, Ethernet, USB interfaces, and a touch screen display as input/output devices.

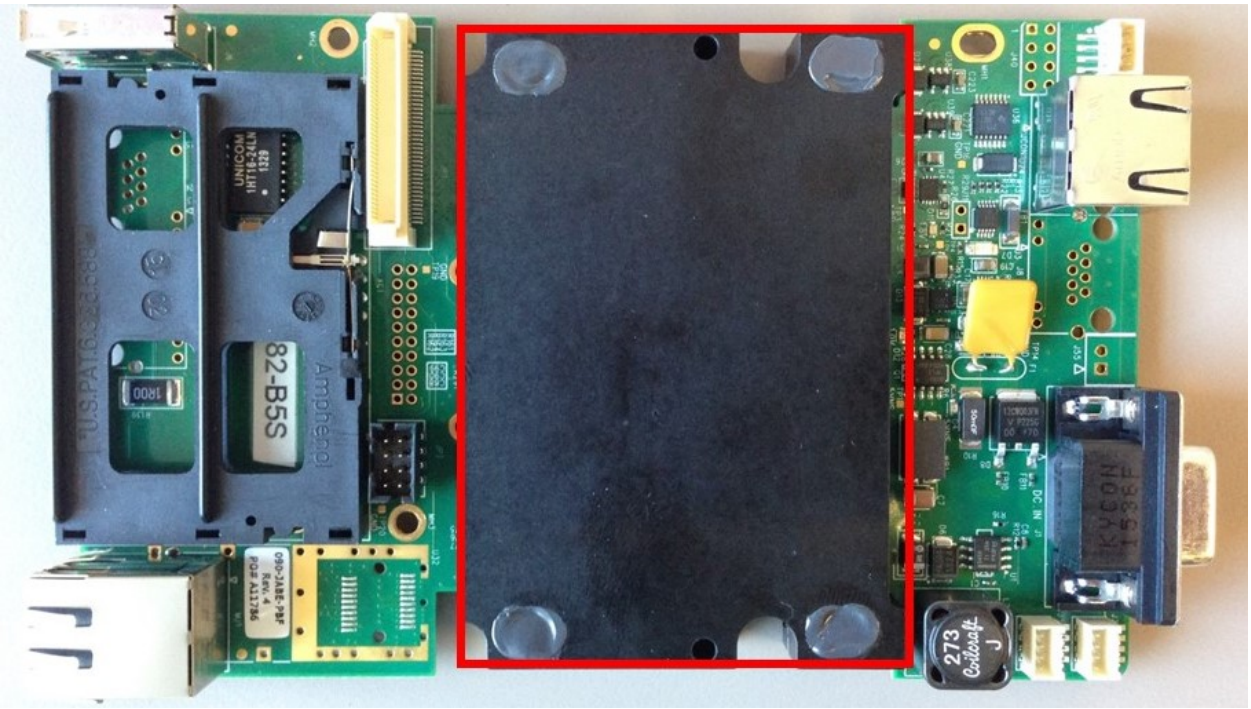

Figure 1 – Module Top

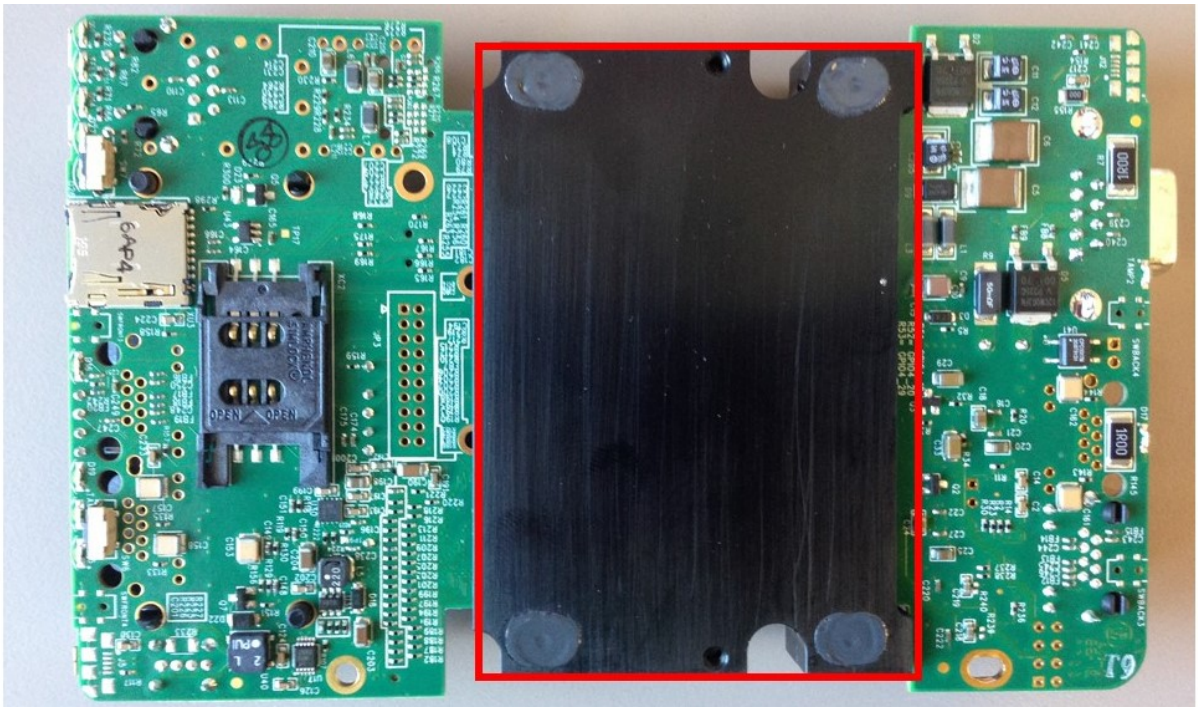

Figure 2 - Module Bottom

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Smart Card Interface	Communicates with smart cards. Authentication for Crypto Officer and User. Holds split key shares for key backup/restore and smart card database export/import.	Data in | Data out
USB Host	Interface for key backup/restore and smart card database export/import.	Data in | Data out
Ethernet	Main interface providing module services	Control in | Data in | Data out | Status out
Touch Screen Display Interface	HSM management interface for connecting an external touch screen display	Control in | Status out
LEDS	Provides operational status	Status out
Power	Power Input	Power in
Serial Connector	Bootloader Firmware load status	Status out
External Sensor	Cover removal tamper detect	Control in
Serial Interface 2, USB1 Peripheral, Keypad, SD Memory Card, SPI3, and USB LAN PHY	Disabled	Disabled

1.2 Logical Cryptographic Boundary

Figure 3 depicts the Module's operational environment.

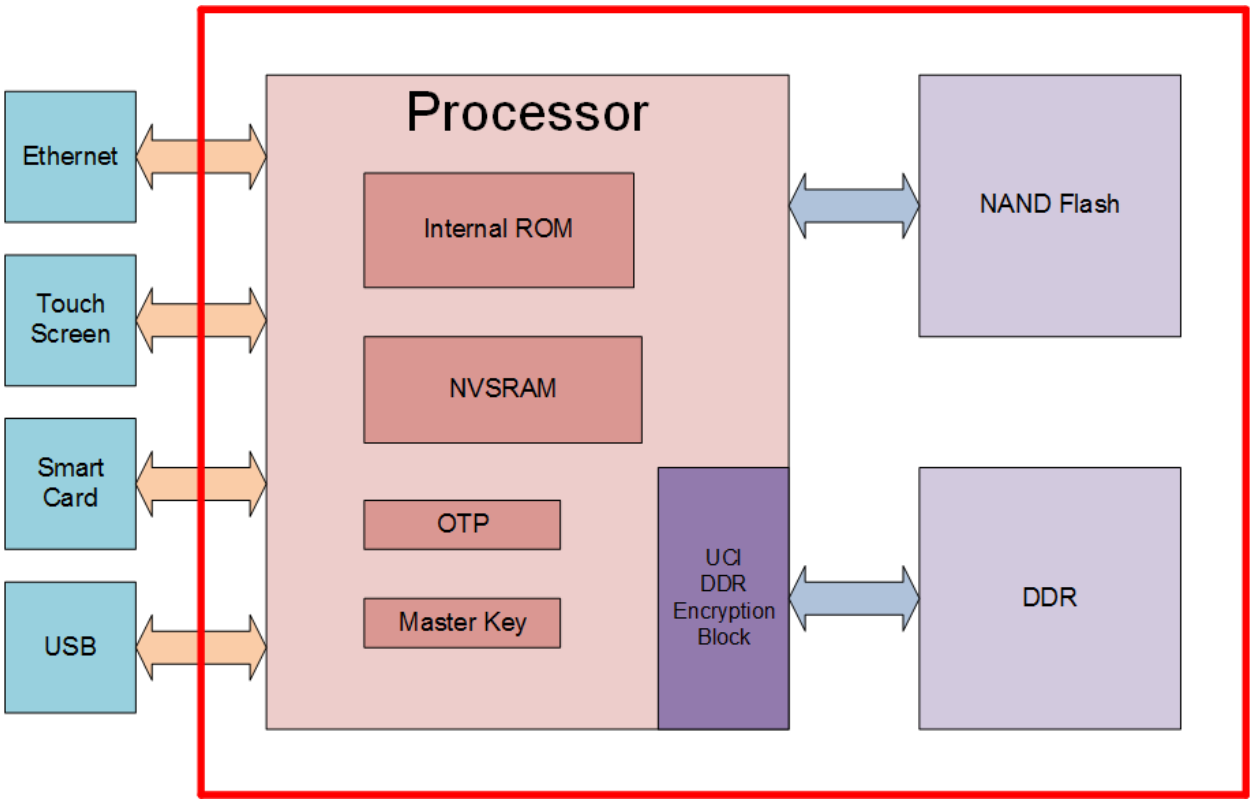

Figure 3 – Module Block Diagram

The Module includes a processor with external NAND Flash and DDR memory.

The firmware components are signed and stored persistently in NAND Flash. Internal ROM securely boots the Bootloader firmware with authentication utilizing an RSA public key stored in the OTP memory.

The Bootloader firmware securely boots the HSM Firmware with authentication utilizing an RSA public key embedded in the Second Level Boot firmware code. The HSM Firmware is loaded and run from the DDR memory.

The DDR Encryption Block encrypts data in the external DDR. It is referred to in this document as the Universal Cryptographic Interface or UCI.

There are active Ethernet, Touch Screen Display, Smart Card, and USB interfaces.

User Critical Security Parameters (CSP) are kept persistently in the NAND flash. While in use they are kept in the DDR and encrypted by the DDR Encryption Block. The Master Key protects the User CSPs in NAND Flash. It is battery backed and zeroized on a tamper event. The NVSRAM is also battery backed and holds system CSPs.

1.3 Modes of Operation

The module has an Approved and non-Approved mode of operation. The module is configured to operate in one of these two modes during initialization and requires re-initialization to change modes. To verify the module is in the Approved mode of operation, the touch screen interface indicates which mode the module is operating in. The sole difference between the Approved mode and the non-Approved mode is that some Non-Approved cryptographic functions are allowed in the non-Approved mode (see Section 2 for a list). All CSPs are automatically zeroized when switching between modes of operation.

Module initialization consists of creating a Crypto Officer card set and a User Card Set. In general, the Crypto Officer creates and destroys Users, while the User has access to the cryptographic functions of the module. A set of cards is created with n (up to 20) being the number of cards and m being the number of cards out of the set required to authenticate. The role is assumed and ready for services under that role only when m of n cards are authenticated.

Initialization consists of creating the Crypto Officer card set, the User card set, and determining whether the module will operate in FIPS mode. Once initialization is completed, the module is in the operational state.

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	Employed	Cert #
Hardware MEMC-AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB Key sizes: 128 bits	Yes	AES #2767
Firmware AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, OFB, CFB1, CFB8, CFB128, CTR Key sizes: 128, 192, 256 bits	Yes	AES #2768
CMAC	[SP 800-38B] Functions: Generation, Verification Key sizes: AES with 128, 192, 256 bits	Yes	AES #2768
CCM	[SP 800-38C] Functions: Generation, Verification Key sizes: 128, 192, 256 bits	No. Tested but not used.	AES #2768
GCM	[SP 800-38D] Functions: Generation, Verification Key sizes: 128, 192, 256 bits For TLS, IV is generated in compliance with SP800-52 and is compatible with TLS1.2. Otherwise, the IV is randomly generated internally using the Approved SP800-90A DRBG in accordance with IG A.5, Scenario #2. If power is lost and then restored, a new key for use with AES GCM is established.	Yes	AES #2768
XTS-AES mode	[SP 800-38E] Functions: Encryption, Decryption Key sizes: 128, 256 bits	No. Tested but not used.	AES #2768

Hardware GP-AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: OFB Key sizes: 256 bits	Yes	AES #2801
KTS	[SP 800-38F] Functions: KW Key sizes: 128, 192, 256 bits	Yes	AES #4038
CVL	[SP 800-56A Section 5.7.1.2 ECC CDH Primitive] Parameter sets/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	Yes	CVL #295
KDF	[SP 800-135] Functions: TLS v1.0/1.1 KDF, TLS 1.2 KDF, ANSI X9.63 (SHA-224, SHA-256, SHA-384, SHA-512)	Yes, TLS v1.2 only. TLS v1.0/1.1 are not used.	CVL #864, 1200
RSADP	[SP 800-56B Section 7.1.2] Functions: RSA Decryption Key size: 2048	Yes	CVL #865
DRBG	[SP 800-90A] Functions: Hash DRBG, HMAC DRBG, CTR DRBG, which provides 256 bits of encryption strength	Yes, CTR DRBG only	DRBG #468
DSA	[FIPS 186-4] Functions: PQG Generation, PQG Verification, Key Pair Generation, Signature Generation, Signature Verification Key sizes: 1024 SigVer Only, 2048, 3072 bits	Yes. SigGen with SHA-1 affirmed for use with protocols only but not used.	DSA #1093
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification, Public Key Generation, Public Key Validation Curves/Key sizes: P-192 SigVer Only, P-224, P-256, P-384, P-521, K-163 SigVer Only, K-233, K-283, K-409, K-571, B-163 SigVer Only, B-233, B-283, B-409, B-571	Yes. SigGen with SHA-1 affirmed for use with protocols only but not used.	ECDSA #904
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Yes	HMAC #1732
RSA	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1	Yes. SigGen with SHA-1 affirmed for use	RSA #2073

	(PSS and PKCS1.5)] Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: 1024 and 1536 Legacy Use SigVer Only, 2048, 3072, 4096 bits	with protocols only but not used.	
UCL RSA	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 PSS Functions: Signature Verification Key size: 2048 bits	Yes	RSA #2366
SHA	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Yes	SHS #2327
UCL SHA256	[FIPS 180-4] Function: Digital Signature Verification SHA sizes: SHA-256	Yes	SHS #3606
Hardware GP-SHA256	[FIPS 180-4] Function: Digital Signature Verification SHA sizes: SHA-256	Yes	SHS #3607

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
EC Diffie-Hellman	Key agreement, key establishment methodology provides between 112 and 256 bits of encryption strength; CVL Cert. #295.
EC Diffie-Hellman	Key agreement, key establishment methodology provides between 112 and 256 bits of encryption strength
MD5	MD5 usage within the TLS key derivation function
NDRNG	[Annex C] Hardware Non-Deterministic RNG. The NDRNG output is used to seed the FIPS Approved DRBG and provides 256 bits of security strength.
Non-SP800-56B Compliant RSA Key Transport	Key Wrapping; key establishment methodology provides 112 or 128 bits of encryption strength

Table 6 – Protocols Allowed in FIPS Mode

Protocol	Description
TLS 1.2	AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256 AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256

Note: The TLS protocol has not been reviewed or tested by the CAVP and CMVP.

Table 7 – Non-Approved Cryptographic Functions for use in non-FIPS mode only

Algorithm	Description
DSA	Functions: PQG Generation, Key Pair Generation, Signature Generation with SHA-1 and SHA-2, Signature Verification Key sizes: 1024 bits
ECDSA	Functions: Signature Generation Component, Key Pair Generation, Signature Generation with SHA-1 and SHA-2 Curves/Key sizes: P-192, K-163, B-163
MD5	Message Digest
RSA	Functions: Key Pair Generation, Signature Generation with SHA-1 and SHA-2 Key sizes: 1024, 1536

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
Km	Master Key. Protects user keys Ku. AES 256 OFB. Generated internally. Stored in battery backed processor memory. Never input or output. Destroyed via the Zeroize service.
Kuci	UCI Key. Protects DDR using the DDR Encryption Block. AES 128 ECB. Generated internally. Stored in NVSRAM. Never input or output. Destroyed via the Zeroize service.
Kursapr	RSA Private User Key. Generated internally. Kept in NAND flash protected by Km. Protected by Kuci in DDR. Input and output in encrypted format during Wrap/Unwrap and Backup/Restore services. Zeroized via the Zeroize RSA Key service.
Kudsapr	DSA Private User Key. Generated internally. Kept in NAND flash protected by Km. Protected by Kuci in DDR. Input and output in encrypted format during Wrap/Unwrap and Backup/Restore services. Zeroized via the Zeroize DSA Key service.
Kuecdsapr	ECDSA Private User Key. Generated internally. Kept in NAND flash protected by Km. Protected by Kuci in DDR. Input and output in encrypted format during Wrap/Unwrap and Backup/Restore services. Zeroized via the Zeroize EC Key service.
Kuaes	AES User Key. Modes ECB, CFB8, CFB128, OFB, CBC, and GCM. Generated internally. Kept in NAND flash protected by Km. Protected by Kuci in DDR. Input and output in encrypted format during Wrap/Unwrap and Backup/Restore services. Zeroized via the Zeroize AES Key service.
Kugeneric	User Generic Key. Generated explicitly or the result of shared secret output from a Derive Key operation. Used in HMAC only. Generated internally. Kept in NAND flash protected by Km. Protected by Kuci in DDR. Input and output in encrypted format during Wrap/Unwrap and Backup/Restore services. Zeroized via the Zeroize Generic Key service.
Kwmac	Key Wrapping MAC Key. Used to generate CMAC for wrapped key MAC. Generated internally. Never input. Output in encrypted format during the Wrap/Unwrap service. Protected by Kuci in DDR. Zeroized after use and by power cycle.
Sdrbg	System DRBG CTR state. Used in generation of User Keys. State CSPs V (128 bits) and Key (AES 256). Entropy input from NDRNG. Generated internally on Module Reset. Protected by Kuci in DDR. Never input or output. Zeroized upon power cycle.
Udrbg	User DRBG CTR state. User Service Random Number Generation. State CSPs V (128 bits) and Key (AES 256). Entropy input from NDRNG. Generated internally on Module Reset. Protected by Kuci in DDR. Never input or output. Zeroized upon power cycle.
Kmbk	Master Backup Key. Encrypts Backup Key and Export Key before splitting shares on Smart Cards using AES 256 OFB. Installed during manufacturing. Protected by Km in NVSRAM. Never input or output. Volatile copy of the key is zeroized via power cycle.
Kbk	Backup Key. AES 256 CBC key encrypts User Keys for Backup service. Generated internally. Input and output in encrypted format and split using Shamir's Algorithm on

CSP	Description / Usage
	Smart Card shares. Zeroized after use.
Kex	Export Key. AES 256 CBC key encrypts smart card database for Export service. Generated internally. Input and output in encrypted format and split using Shamir's Algorithm on Smart Card shares. Zeroized after use.
Ktlspr	TLS private key. RSA 2048. Used for Module TLS certificate. Generated internally. Kept in NAND flash protected by Km. Protected by Kuci in DDR. Never input or output. Destroyed via the Zeroize service.
Ktlss	TLS session key. Established during the TLS handshake. Protected by Kuci in DDR. Never input or output. Zeroized after session termination.
Ktlsi	TLS integrity key. Established during the TLS handshake. Protected by Kuci in DDR. Never input or output. Zeroized after session termination.
Ktlsp	TLS RSA pre-master secret. Established during the TLS handshake. Protected by Kuci in DDR. Input in encrypted format during the TLS handshake. Never output. Zeroized after use.

2.2 Public Keys

Table 9 – Public Keys

Key	Description / Usage
Kblver	Bootloader Verification Key. Stored in the OTP, used to verify the Bootloader code stored in NAND Flash on hardware boot. 2048 bit RSA.
Kfver	HSM Firmware Verification Key. Embedded in the bootloader code. Verifies the HSM Firmware loaded by the Bootloader. 2048 bit RSA.
Kaco	Crypto Officer Authentication Key. Authenticates Crypto Officer. 2048 bit RSA.
Kau	User Authentication Key. Authenticates User. 2048 bit RSA.
Kabkex	Backup Export Authentication Key. Authenticates Smart Card shares used in Backup, Restore, Export, and Import services. 2048 bit RSA.
Kursapu	RSA Public User Key. Kept in NAND flash protected by Km. Protected by Kuci in DDR.
Kudsapu	DSA Public User Key. Kept in NAND flash protected by Km. Protected by Kuci in DDR.
Kuecdsapu	ECDSA Public User Key. Kept in NAND flash protected by Km. Protected by Kuci in DDR.
Ktlspu	TLS public key. RSA 2048. Used for Module TLS certificate. Kept in NAND flash protected by Km. Protected by Kuci in DDR.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Crypto Officer (CO). The cryptographic module enforces the separation of roles using a separate RSA public key for each operator.

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 is not persistent across a power cycle.

A role is authenticated by smart cards. At module initialization time, N cards are created with M cards required for authentication. M can be a subset of N.

Table 10 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Crypto Officer – Creates User.	Identity-based	Digital Signature Verification
User	User – Has access to module cryptographic services.	Identity-based	Digital Signature Verification

3.2 Authentication Methods

2048-bit RSA Signature Verification

The authentication method is 2048 bit RSA signature verification. The security strength of an RSA 2048 bit key is 112 bits. The authentication process takes no less than 5 seconds. This allows 12 incorrect authentication attempts in one minute. The probability of incorrect authentication attempts succeeding in one minute is 12/2^112 or 2.31 x 10^-33.

Table 11 – Authentication Description

Authentication Method	Probability	Justification
RSA Signature Verification	1/2^112	2.31 x 10^-33

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. Both the Approved and non-Approved modes of operation have access to all services listed in this section; the only distinction is that the Approved mode restricts access to non-Approved algorithms and non-Approved key sizes, whereas the non-Approved mode can employ both Approved and non-Approved algorithms and key sizes.

Table 12 – Authenticated Services

Service	Description	CO	U
Zeroize	Destroys Km (Master Key); the Km is used to encrypt all persistently stored operator keys. This service will also destroy the Crypto Officer role and User role and requires reinitialization of the module.	X	
Module Reset (Power Up Self-Test)	Reset the Module via Touch Screen Display.	X	X
Firmware Upgrade	Upgrades Firmware.	X	
Settings	Set date and time, network configuration, and Manufacturing/User firmware selection.	X	
Export Logs	Plaintext HSM logs are moved to USB drive.	X	
Shut Down	Unit is shut down (but not restarted) via Touch Screen Display.	X	X
Export/Import	Encrypted smart card database is exported or imported.	X	
Backup/Restore	Encrypted User Keys are backed up or restored from backup.		X
Info: Date/Time, Network	View date, time, and network configuration on Touch Screen Display.	X	X
Info: Firmware	View firmware version on Touch Screen Display.	X	X
Info: List Keys	List Keys and view copyrights on Touch Screen Display.		X
Generate RSA Key	Key Generate ANSI 9.31 RSA key pairs with key size 2048, 3072, 4096 bits.		X
Generate DSA Key	Key Generate DSA key pairs with key size 2048, 3072 bits.		X
Generate ECDSA KEY	Key Generate ECDSA key pairs P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571.		X
Generate Generic Key	Key Generate Generic keys. 128, 192, and 256 bit keys.		X
Generate AES Key	Key Generate AES 128, 192, and 256 bit keys.		X
Zeroize RSA Key	Zeroize RSA key pairs.		X

Service	Description	CO	U
Zeroize DSA Key	Zeroize DSA key pairs.		X
Zeroize ECDSA KEY	Zeroize ECDSA key pairs.		X
Zeroize Generic Key	Zeroize Generic keys.		X
Zeroize AES Key	Zeroize AES keys.		X
Encrypt/Decrypt AES	AES encrypt/decrypt with modes ECB, CBC, OFB, CFB1, CFB8, CFB128, and GCM.		X
Encrypt/Decrypt RSA	RSA Encrypt/Decrypt for key transport.		X
RSA Sign/Verify	RSA signature generation/verification ANSI X9.31, PSS, and PKCS1.5. Signature generation 2048, 3072 and 4096, no SHA-1. Signature verification 1024, 2048, 3072 and 4096.		X
DSA Sign/Verify	DSA signature generation/verification. Signature generation 2048 and 3072, no SHA-1. Signature verification 1024, 2048, and 3072.		X
ECDSA Sign/Verify	ECDSA signature generation/verification. Signature generation no SHA-1 (SHA-1 verification allowed).		X
HMAC Sign/Verify	HMAC generation/verification with Generic Key.		X
CMAC Sign/Verify	CMAC signature generation/verification with AES key.		X
Derive Key	Produces Generic Key or AES key		X
Message Digest	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.		X
Wrap/Unwrap Key	Key Import/Export with AES or RSA key wrap.		X
Copy Key	Makes a copy of a key within the HSM		X
Random	Retrieve random bytes from User DRBG		X
Logout	After Logout, only Unauthenticated Services are allowed	X	X

Table 13 – Unauthenticated Services

Service	Description
Module Initialize	Master Key Km is generated. Crypto Officer and User cards sets are created. Kaco and Kau are input from the Smart Card Interface. TLS certificate is created, Ktlspr and Ktlspu keys are generated. Can be done only if module is in the Uninitialized state.
Authenticate Crypto Officer	Authenticates the Crypto Officer. Services allowed to the Crypto Officer are available.
Authenticate User	Authenticates User. User allowed Services are available.

Service	Description
Show Status	View FIPS mode of operation and Module State on Touch Screen Display .
Module Reset (Power Up Self-Test)	Reset the Module by power cycle.

Table 14 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 exports the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module imports the CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 14 – CSP Access Rights within Services

	Km	Kuci	Kursapr	Kudsapr	Kuecdsapr	Kuaes	Kugeneric	Kwmac	Sdrbg	Udrbg	Kmbk	Kbk	Kex	Ktlspr	Ktlss	Ktlsi	Ktlsp
Zeroize	Z	Z															
Module Reset (Self-test)	E	Z G E							G E	G				G			
Firmware Upgrade, Settings, Export Log, Clear Error State, Shut Down, Info, Logout, Show Status		E															
Import	E	E									E		E W				
Export		E									E		G E R				
Backup		E	R	R	R	R	R		E		E	G E R					

	Km	Kuci	Kursapr	Kudsapr	Kuecdsapr	Kuaes	Kugeneric	Kwmac	Sdrbg	Udrbg	Kmbk	Kbk	Kex	Ktlspr	Ktlss	Ktlsi	Ktlsp
Restore	E	E	W	W	W	W	W				E	W E					
Generate RSA Key	E	E	G						E					E	E	E	E
Destroy RSA Key		E	Z											E	E	E	E
Generate DSA Key	E	E		G					E					E	E	E	E
Destroy DSA Key		E		Z										E	E	E	E
Generate ECDSA Key	E	E			G				E					E	E	E	E
Destroy ECDSA Key		E			Z									E	E	E	E
Generate Generic Key	E	E					G		E					E	E	E	E
Destroy Generic Key		E					Z							E	E	E	E
Generate AES Key	E	E				G			E					E	E	E	E
Destroy AES Key		E				Z								E	E	E	E
Encrypt Decrypt AES		E				E								E	E	E	E
Encrypt Decrypt RSA		E	E											E	E	E	E
RSA Sign/Verify		E	E											E	E	E	E
DSA Sign/Verify		E		E										E	E	E	E
ECDSA Sign/Verify		E			E									E	E	E	E
HMAC Sign/Verify		E					E							E	E	E	E
CMAC Sign/Verify		E				E								E	E	E	E
Derive Key	E	E			E	G	G							E	E	E	E
Message Digest		E												E	E	E	E
Wrap Key		E	R	R	R	R E	R	G E R						E	E	E	E

	Km	Kuci	Kursapr	Kudsapr	Kuecdsapr	Kuaes	Kugeneric	Kwmac	Sdrbg	Udrbg	Kmbk	Kbk	Kex	Ktlspr	Ktlss	Ktlsi	Ktlsp
Unwrap Key	E	E	W E	W	W	W E	W							E	E	E	E
Copy Key	E	E												E	E	E	E
Random		E								E				E	E	E	E
Module Initialize	G E	G E												G			
Authenticate Crypto Officer		E															
Authenticate User		E												E	E	E	E

Table 14 continued – CSP Access Rights within Services Public Keys

	Kblver	Kfver	Kaco	Kau	Kabkex	Kursapu	Kudsapu	Kuecdsapu	Ktlspu
Zeroize									
Module Reset (Self-test)	E	E							
Firmware Upgrade, Settings, Export Log, Clear Error State, Shut Down, Info, Logout, Show Status									
Import					W E				
Export					W E				
Backup					W E	R	R	R	
Restore					W E	W	W	W	
Generate RSA Key						G			E
Destroy RSA Key						Z			E
Generate DSA Key							G		E
Destroy DSA Key							Z		E
Generate ECDSA Key								G	E
Destroy ECDSA Key								Z	E
Generate Generic Key									E
Destroy Generic Key									E

	Kblver	Kfver	Kaco	Kau	Kabkex	Kursapu	Kudsapu	Kuecdsapu	Ktlspu
Generate AES Key									E
Destroy AES Key									E
Encrypt Decrypt AES									E
Encrypt Decrypt RSA						E			E
RSA Sign/Verify						E			E
DSA Sign/Verify							E		E
ECDSA Sign/Verify								E	E
HMAC Sign/Verify									E
CMAC Sign/Verify									E
Derive Key								E	E
Message Digest									E
Wrap Key						R W E	R	R	E
Unwrap Key						W	W	W	E
Copy Key									E
Random									E
Module Initialize			R	R					G
Authenticate Crypto Officer			E						
Authenticate User				E					E

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module. The self-tests do not require operator action. Success is indicated by the Module remaining in the Operational state.

On power up or reset, the Module performs the self-tests described in Table 15 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.

While in operation, the Module performs the conditional tests described in Table 16. If any of the conditional tests fails, the Module enters the Error state. If the firmware load tests fail, the Module will fail to boot.

The critical functions tests executed on power up or reset are listed in Table 17. If a critical function test fails the Module enters the Error State.

Table 15 – Power Up Self-tests

Test Target	Description
AES (Cert. #2768)	KATs: Encryption, Decryption Modes: ECB Key sizes: 128 bits
GP-AES (Cert. #2801)	KATS: Encryption, Decryption Modes: OFB Key sizes: 256
UCI AES (Cert. #2767)	KATs: Encryption, Decryption Modes: ECB Key sizes: 128 bits
DRBG (Cert. #468)	KATs: HASH DRBG, HMAC DRBG, CTR DRBG Security Strengths: 256 bits
DSA (Cert. #1093)	PCT: Signature Generation, Signature Verification Modes: SHA-384 Key sizes: 2048 bits
GCM (Cert. #2768)	KATs: Encryption, Decryption Key sizes: 256 bits
AES CMAC (Cert. #2768)	KATS: Generation, Verification Modes: CBC Key Sizes: 128, 192, 256
HMAC (Cert. #1732)	KATs: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
RSA (Cert. #2073)	KAT: Signature Generation, Signature Verification Modes: SHA-256, PSS Key sizes: 2048 bits
ECDSA (Cert. #904)	PCT: Signature Generation, Signature Verification Modes: SHA-512 Keys sizes: P-224, K233
ECC CDH (Cert. #295)	KATS: Shared Secret Calculation Key sizes: P-224

Test Target	Description
SHA (Cert. #2327)	KATs: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
AES-KW (Cert. #4038)	KATs: Wrap, Unwrap Key Sizes: AES 256
AES CCM (Cert. #2768)	KATs: Encryption, Decryption Key Sizes: AES 192 CCM
AES XTS (Cert. #2768)	KATs: Encryption, Decryption Key Sizes: AES 128 and 256 XTS
GP-SHA256 (Cert. #3607)	KAT: SHA256
UCL SHA256 (Cert. #3606)	KAT: SHA256
UCL RSA (Cert. #2366)	KAT: Signature Verification Modes: SHA-256, PSS Key sizes: 2048 bits

Table 16 – Conditional Self-tests

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
NDRNG	NDRNG Continuous Test performed when the DRBG requests seed material
DSA	DSA Pairwise Consistency Test performed on every DSA key pair generation.
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation.
Firmware Boot Loader Load	RSA 2048 signature verification performed when firmware boot loader is loaded using Kblver.
Manufacturing Image Firmware Load	RSA 2048 signature verification performed when manufacturing image firmware is loaded using Kfver.
User Image Firmware Load	RSA 2048 signature verification performed when user image firmware is loaded.
DRBG Health Checks	Performed conditionally per SP 800-90 Section 11.3. Required per IG C.1.

Table 17 – Critical Function Tests

Test Target	Description
Policy Manager	Tests matrix of roles and services for allowed services given role.
State Manager	Consistency test for setting and retrieval of BlackVault State and FIPS Mode state.

5 Physical Security Policy

The BlackVault is tamper responsive. A Tamper event may be caused by lifting of the security region's metal enclosure or separation of the top or bottom parts of the security region metal enclosure. When a Tamper event occurs, the unit is zeroized and cannot be returned to an operational state. The rivets used to fasten the metal enclosure are non-reusable, and their removal must be considered as evidence of tamper.

Table 18 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Physical Damage	Visual inspection every three months.	The operator shall inspect the module for signs of tamper. Which may include scratches, scrapes, drill holes, chips in the plastic molding, etc.

6 Operational Environment

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

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 19 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001

Table 20 – Acronyms and Definitions

Acronym	Definition
CAVP	NIST Cryptographic Algorithm Validation Program.
CSP	Critical Security Parameter.
GP	General purpose hardware cryptography engine.
OTP	One Time Programming.
UCI	Universal Cryptographic Interface, the DDR encryption block.
UCL	Universal Cryptographic Library.