DocuSign HSM Appliance

Hardware version 5.0
Firmware version 5.0.0

FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation

February 2017

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the DocuSign HSM Appliance. This security policy describes how the DocuSign HSM Appliance meets the security requirements of FIPS 140-2, and how to operate the appliance in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 level 3 validation of the DocuSign HSM Appliance.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 -- *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST web site at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with the operations and capabilities of DocuSign HSM Appliance in the technical terms of a FIPS 140-2 cryptographic module security policy. Additional information about DocuSign HSM Appliance and other DocuSign products is available at www.docusign.com.

1.3 Terminology

In this document the DocuSign HSM Appliance is referred to as the module or the appliance.

1.4 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Firmware Listing
- Other supporting documentation as additional references

This document provides an overview of the DocuSign HSM Appliance and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliance. Section 3 specifically addresses the required configuration for the FIPS 140-2-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is DocuSign proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact DocuSign.

2 FIPS 140-2 Security Level

DocuSign HSM Appliance is validated to meet the FIPS 140-2 security requirements for the levels shown below. The overall module is validated to FIPS 140-2 security level 3.

FIPS 140-2 Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Port and Interfaces	3
Role, Services and Authentication	3
Finite State Model	3
Physical Security (Multi-Chip Standalone)	3
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A
Operational Environment	N/A

Table 1 - FIPS 140-2 Security Requirement Level

3 Security Rules

The DocuSign HSM Appliance is a high-performance cryptographic service provider. Contained within a secure, tamper-responsive steel case, the appliance performs high-speed cryptographic operations while protecting sensitive data. All keys and critical security parameters are protected within the cryptographic boundary by the physical security mechanisms of the module.

The DocuSign HSM Appliance supports various cryptographic algorithms including AES for encryption and SHA-256 for hashing. It can be used to securely store secret/private keys and has the ability to maintain an internal public key database. The appliance performs all cryptographic operations internally, and through self-tests it ensures that these operations are functioning correctly. There is no room for error when protecting mission critical data.

Whether performing the backend cryptography for a high-volume e-Commerce site or just providing authentication services for a small company, the appliance satisfies the need with its wide-range of cryptographic functionality. It includes the following features:

- Cryptography using Triple-DES, AES, Triple-DES-MAC, HMAC, Triple-DES-CMAC, AES-CMAC, AES-CCM, AES-CTR, AES-GMAC, RSA, ECDSA, SHA-1, SHA-256, SHA-384 and SHA-512.
- Public key database and certificate support
- Authenticated and encrypted communication with the module
- Secure storage of secret/private keys
- Software key medium and smart card support
- Tamper-responsive enclosure
- High level API requiring no cryptographic expertise
- In-depth logging, auditing and secure auditing
- Secure backup capabilities

3.1 Secure by Design

The DocuSign HSM Appliance is a multi-chip standalone module. The hardware version 5.0 with firmware version 5.0.0 has been designed to meet all of the Level 3 FIPS 140-2 requirements. This means that the module provides strong security both inside and out. Encased within a tamper-responsive and tamper-evident steel box, the module both protects against and reacts to attacks.
Access to DocuSign HSM Appliance is only permitted through specific, well-defined interfaces detailed in Well-Defined Interfaces section.
All vents on the module are baffled to meet the FIPS 140-2 opacity requirements for physical security.
DocuSign HSM Appliance hardware version 5.0 includes a hot removable and replaceable dual power supply. The removable power supply units are external components of the module. The power supply bays, internal power wires, power connectors, internal power circuit and fan are excluded components.

The security features of the module ensure that access to sensitive information is granted only to an authorized operator. Tamper Evident cans provide evidence of any attempt to tamper with module cover. The Tamper Evident cans are placed over a screw that joins the top cover and bottom enclosure.
The Tamper Evident cans are applied at manufacturing stage.
The Tamper Evident cans are shown in Figure 1.

Figure 1 – Tamper Evident cans

The units are encased in a solid metal case rigged with micro-switches and only the specified physical interfaces permit access to the module. Intrusion attempts cause power to be instantly cut off, preventing access to any useful information by zeroizing all plaintext critical security parameters including the appliance's critical keys.

Four smart cards (Master, Init, Startup and Root) are used for the purpose of initializing the module. The initialization must be done in a secure environment.
The Master smart card serves as a logical key of a specific appliance. It is required to be able to start the appliance's database initialization process.

The above appliance's critical keys are split between the Init and Startup smart cards. Thus it is mandatory to insert all smart cards for a successful initialization of the module.
During initialization of the module, a part of the appliance's critical keys is kept inside the internal Tamper Device. Therefore, for a normal startup of the module, it is only required to insert the Startup smart card.
After a detected tamper, the DocuSign HSM Appliance must be re-initialized with both Init and Startup smart cards.

Remark: It is possible to configure DocuSign HSM Appliance such that there is no need to enter the Startup smart card as part of starting the module. In this configuration all the appliance's critical keys content is kept inside the internal tamper device and erased upon a tamper event.
This can be done using the appliance's console.
Use the *Unattended Mode* option in the appliance's console to configure this option. You will need to insert the Startup smart card as well as enter the Startup smart card password. This will enable the unattended startup configuration.
The same console option can be used to clear the attended startup configuration.

The module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (Class B). It is labeled in accordance with FCC requirements.

3.2 Product Delivery

When the Crypto Officer receives the appliance, the Crypto Officer must check the appliance's case for any evidence of physical tampering. The Crypto Officer should verify that the Tamper Evident cans are attached to the appliance and that they are not damaged. If you think the appliance has been tampered with during delivery, contact DocuSign.

3.3 Well-Defined Ports

The module is a hard, rack mountable box. The physical ports include the power connector, network connections (Ethernet Interfaces using TCP/IP), power switches, indicators, a touch screen and one smart card reader. The module is encased in a steel cover, with only the specified ports providing access to the module. All ports use standard PC pin outs.

The ports are shown in Figure 2. On the front of the module there is a smart card reader and touch screen. Below that, from left to right, there are three indicator lights and on/off button. On the back of the module, on the bottom left, there are two power connectors and on the top left there are two network connections. These ports are all listed in table 2.

Figure 2 – Front and Rear Interfaces

For FIPS 140-2 purposes, both network ports are treated the same. Through the network ports either an encrypted and RSA based authenticated sessions (Two-way TLS 1.2, using TLS_RSA_WITH_AES_256_CBC_SHA256), or a user ID/password authenticated sessions are permitted over either ports when operating in a FIPS 140-2 compliant manner. In a non-FIPS 140-2 compliant manner, the module could be configured so that traffic over the trusted Ethernet port was plaintext while traffic over the non-trusted network was encrypted and authenticated or user-ID/password authenticated.

Table 2 shows the mapping of the FIPS 140-2 logical interfaces to the module's physical interfaces.

FIPS 140-2 Logical Interfaces	Adapter physical interfaces
Data Input Interface	Network ports, touch screen port smart card reader
Data Output Interface	Network ports
Control Input Interface	Network ports, touch screen port
Status Output Interface	Network ports, indicators, touch screen port
Power Interface	DC power connector

Table 2 Interfaces

Figure 3 below, shows the module's hardware block diagram.

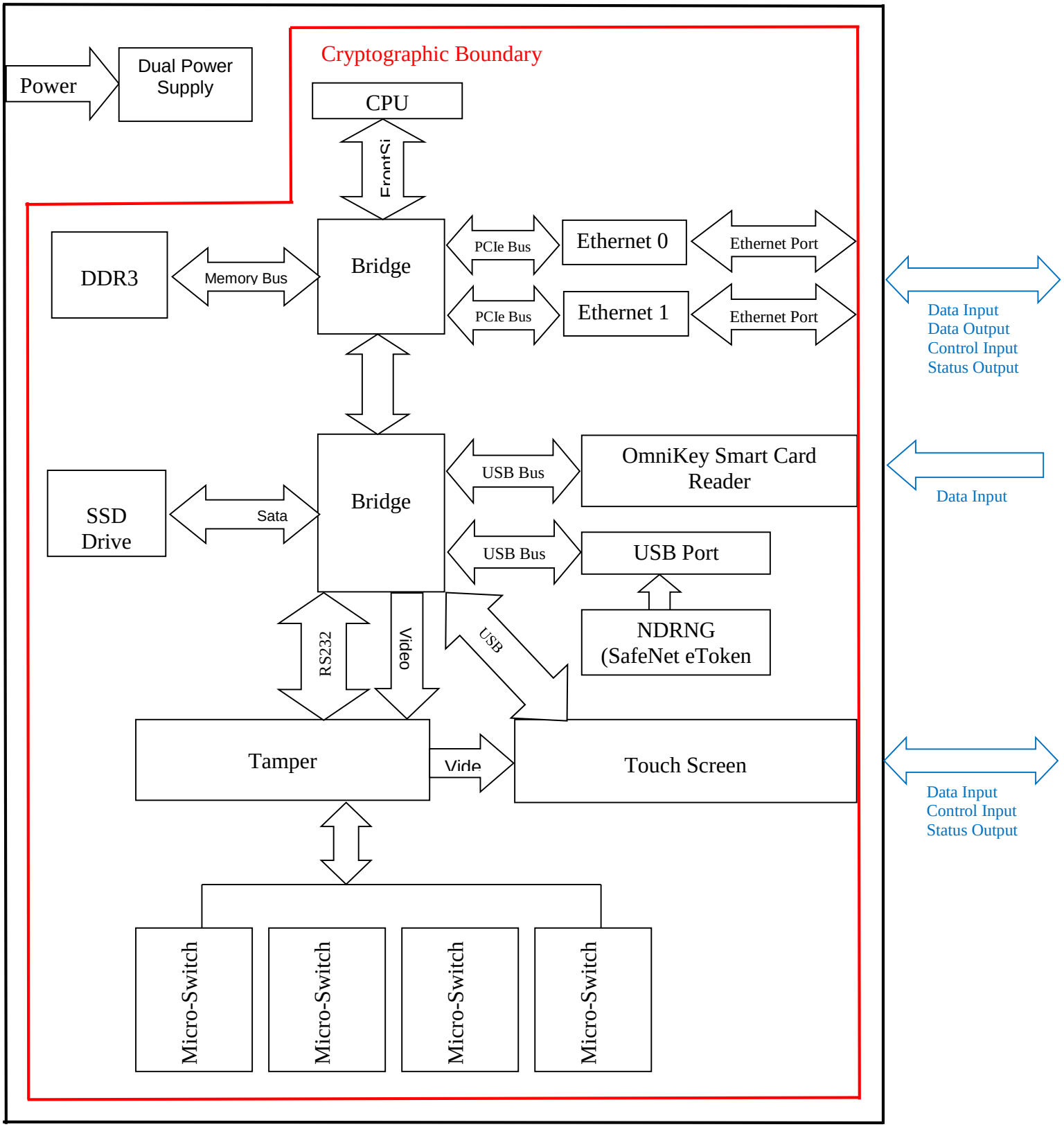

Figure 3 – DocuSign HSM Appliance Hardware Block Diagram

3.4 DocuSign HSM API

All requests for cryptographic services are done through the DocuSign HSM Appliance API. This API, written primarily in C and based on RPC (Remote Procedure Calls), provides a high-level interface to the cryptographic services provided by the module, thus masking many of the complexities of cryptography from the developer. Figure 4 depicts this API model.

Status information can also be sent via syslog protocol to a syslog server or via SNMPv2 traps to an SNMP server. This status information is sent using the network ports of the module.

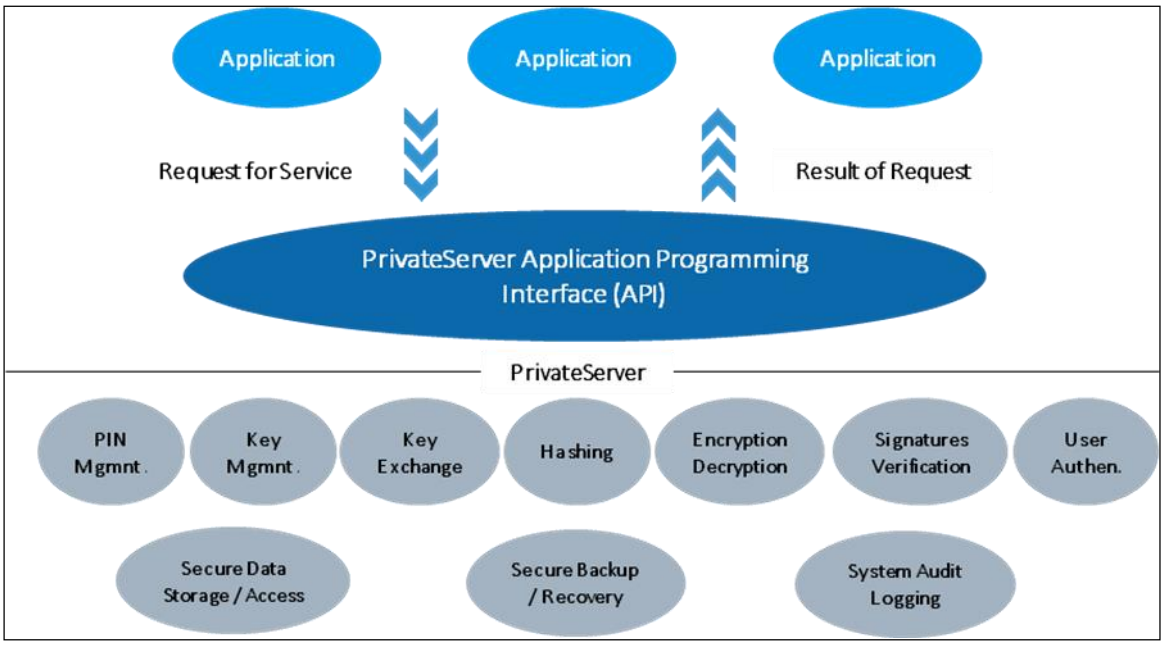

Figure 4 - DocuSign HSM Appliance API Model

3.5 Database Replication

The database replication is an automatic mechanism that synchronizes all information among appliances that operate in load balancing/high availability environment. The mechanism establishes an encrypted session using one way TLS 1.2 protocol between the two servers. Then, a challenge-response using the critical key for symmetric authentication for database replication is performed to authenticate the server and confirm it was initialized with the same key. Only then, the encrypted and MACed database records with the corresponding Critical database keys, are sent over this secure channel.

3.6 Code Printing

A special license can enable DocuSign HSM Appliance printing codes to a network printer. A client application will interface the appliance through the normal data input interface. The application will either send the code encrypted or direct the appliance's service to calculate a new code for the given user. The code will be sent non-encrypted to the network printer that will use a special paper for concealing the code.

The code printing is not available without special request because it is disabled in the manufacturing process. Only if client wants code printing it is enabled during manufacturing and the appliance will operate in non-FIPS mode.

3.7 Roles and Services

The DocuSign HSM Appliance supports multiple, simultaneous operators. A database record entry is created by the appliance for each operator and contains the operator name, authorization bits, quotas for operator temporary keys created by the operator, the certifier (CA) of the operator, and the minimum access level. The authorization mask controls the operator's permissions. Additional optional attributes are user password for password based authentication and X.509 certificate for RSA based authentication.

There are two primary roles an operator can hold, User/Application and Supervisor (Crypto-Officer):

3.7.1 Supervisor (Crypto-Officer) Role

The Supervisor is responsible for operator and key management, module initialization and startup, and the module's configuration. All authorization bits are turned on (i.e., 0xFFFFFFFF) for the Supervisor.

There can be only one individual holding the role of Supervisor. Only the Supervisor may possess the smart cards and passwords necessary to initialize and startup the module. This must be done locally, using the appliance's smart card reader. No other operator that can authenticate using this local interface. By connecting directly through the appliance, the Supervisor has the ability to access certain management operations of the module, including:

- Initializing the module and it's databases
- Starting the module
- Configuring the module's IP information
- Resetting a tamper condition

3.7.2 User/Application Role

The User/Application is for accessing the cryptographic services provided by the module. The User logs into the module remotely from a device that communicates with the appliance's application program interface using the RSA challenge-response protocol or uid/password. None of the authorization bits (see table 5 for the functionality listing of those bits) are turned on (i.e., 0x00000000) for the User.

A User must first authenticate to the module, there are two authentication schemes:

- **RSA based Authentication scheme**
  In this scheme, after a successful authentication, an encrypted session is created. The RSA challenge-response protocol used by the module is standard two-way TLS 1.2 session using TLS_RSA_WITH_AES_256_CBC_SHA256 mechanism. It is used to authenticate the operator and to establish a temporary session key (that is destroyed at the close of the session). Through this session, the operator may perform the cryptographic services for which they have permissions.

The session keys (MAC and encryption/decryption) are negotiated during authentication of a user when creating a session. The appliance creates these keys during the opening of an encrypted session, and they are destroyed when the session is terminated. These keys are temporary and are only stored in volatile memory.

- **User ID / Password authentication scheme**
  This authentication method can be established over one-way TLS 1.2 encrypted session or over a non-encrypted session.
  Through this session, the operator may perform the cryptographic services for which they have permissions.
  Any operation that either imports a key or exports a key from the module is restricted when the authentication is over non-encrypted session, Also, any change password or set password operation must be done over encrypted session.

3.7.3 Authentication

The DocuSign HSM Appliance employs identity-based authentication of operators through either the RSA challenge-response mechanism or the User ID/Password authentication mechanism.

RSA challenge-response Authentication
The RSA challenge-response mechanism requires the exchange and verification of the operator's private key over standard two-way TLS 1.2 authentication protocol. All keys used for authentication are private keys generated externally and certified by a CA signature. The challenge is signed using a 2048 bit RSA key which has security strength of 112 bits. Therefore, the probability that random access will succeed is far less than one in 1,000,000 attempts since the probability of getting the same result is 2^112. Since there is a single server's RSA decrypt involved in every authentication attempt, and the appliance is capable of performing a maximum of 1000 RSA 2048 sign operations per second, the probability of a successful random attempt during a one-minute period is 1 in 2^112/(1000*60), (equal to 1 in 8.65*10^28) which is far less than one in 100,000 attempts.

User ID/Password Authentication
In the case that the user ID/Password authentication scheme is used, the minimal password length is 6 alphanumeric characters so the number of combinations is 72^6 = 139*10^9. This means that the probability a random access will succeed is far less than one in 1,000,000 attempts using this authentication mechanism. In addition, upon a failed authentication attempt, a delay of 500ms will occur before the failure response is returned to the client. Since only up to 1000 sessions can be opened simultaneously the probability of a successful random attempt during a one-minute period is 1 in 72^6/(1000*60*2), (equal to 1 in 1.1*10^6) which is far less than one in 100,000 attempts.
There is no limitation to the maximum password length.

Direct Authentication from Console
The Supervisor possesses the smart cards and passwords necessary to initialize and startup the appliance. The Supervisor can log into the module locally using the smart cards or remotely using the RSA challenge-response protocol. A Supervisor attempting to

authenticate directly to the module through the touch screen port must use the Startup smart card and password. The smart card password must be at least 6 alphanumeric characters. This yields a minimum of 64^6=6.87*10^10 (over 1,000,000,000) possible combinations. Therefore, the probability a random access will succeed is far less than one in 1,000,000 attempts using this authentication mechanism. After twelve failed authentication attempts the Startup smart card is locked. Therefore, a successful random attempt during a one-minute period is 1 in 64^6/12, (equal to 1 in 5.72*10^9) which is far less than one in 100,000 attempts.
The module also suppresses feedback of authentication data being entered by returning '*' characters. The maximum password length is 50 characters long.

Remark: It is possible to configure DocuSign HSM Appliance such that there is no need to enter the Startup smart card as part of starting the module. In this configuration all critical keys are loaded from the tamper device into the volatile memory upon startup.

3.7.4 Services

Table 3 provides a high-level summary of the approved services provided by the module.

Category	Service	Information Summary
Server Management	Perform backups	Backup the HSM database in encrypted file
	Restore backups	Restore encrypted database
	Configure database replication	Configure database replication between several appliances operating in load balancing / high availability environment
	Retrieve log file	Retrieve the audit log file. The audit log can be signed.
	Reset the log file	Clear the HSM audit log file
	Monitoring	SNMPv2 and Syslog services
	Perform firmware update	Update the firmware of the appliance
	Perform shutdown	Shutdown the HSM
	Get appliance details	Retrieve the appliance's Identity and public key
	Self-tests	Perform internal self-tests
	Retrieve FIPS mode	Retrieve the HSM FIPS mode status
User Management	Create user	Centralized storage and management of users allows creation, modification, delete or query user records.
	Retrieve user information	
	Update user record	
	Revoke user	
	Create a non-authenticated user	

Category	Service	Information Summary
	User authentication	Two-way user authentication using the RSA challenge-response key distribution mechanism. A smart card or software token can be used. Also, for local access by the Supervisor a smart card can be used. A user ID /password authentication mechanism can also be used.
	Update user password	Set, reset or change user password. These operations can be done only over encrypted session.
Session Management	Retrieve session information	Retrieve information about all active sessions
	Terminate a session	Terminate a session
Key Management	Retrieve non-sensitive key information	Secure storage and management of cryptographic keys (Triple-DES/AES keys, RSA public and private keys, ECDSA public and private keys, Diffie-Hellman public and private keys, HMAC secret data, Special-purpose keys). In the case of user ID/password authentication over non-encrypted session, keys cannot be imported or exported in clear format to/from the HSM.
	Update Key record	
	Generate or import key	
	Export non-read locked key	
	Delete any key	
Cryptography	Data encryption and decryption	Enable client applications use keys kept in DocuSign HSM Appliance for data encryption and decryption operations. Symmetric [Triple-DES ECB, CBC, AES ECB, CBC, CTR] and Asymmetric cryptography [RSA]. The RSA encryption supports the following schemes: PKCS#1 v1.5, OAEP.
	Digital signatures	Enable client applications use keys kept in DocuSign HSM Appliance for digital signatures signing and verification operations. Generate and verify digital signatures (RSA and ECDSA). The RSA digital signature generation supports the following schemes: PKCS#1 v1.5, PSS and ANSI X9.31. Also, digital signature verification service is supported based on the above algorithms.

Category	Service	Information Summary
	Data hashing and data integrity	Enable client applications use keys kept in DocuSign HSM Appliance for hashing and data integrity operations. Generate message digests [SHA-1, SHA-256, SHA-384 and SHA-512 (FIPS 180-4)], HMAC, Triple-DES-CMAC, AES-CMAC, AES-CCM, AES-GMAC
	Key exchange	Enable client applications use keys kept in DocuSign HSM Appliance for key exchange operations. Key transport over TLS Generate keys [Diffie-Hellman and EC Diffie-Hellman] RSA based key exchange

Table 3 – Approved Services

Table 4 provides a high-level summary of the non-approved services provided by the module.

Service	Information Summary
Data encryption and decryption	Symmetric [DES, DES Stream, FF3]
Digital signatures	Generate and verify digital signatures [RSA ISO9796]
Data hashing	Generate message digests [ARDFP, MD5]
Data integrity	Generate message MAC [DES MAC]
Data encryption-signature and verification-decryption	Encrypt and sign [AES-GMAC_GCM]
Code printing	Print user code on a network printer

Table 4 – Non-Approved Services

Table 5 shows each specific service, which role has access to it and which CSP is used and in which access control (Read, Write, Execute). Refer to table 6 for the description of the CSP used by each operation.

Category	Services	Role	Input	Output	CSP#	CSP Access (R/W/X)
Server Management	Perform backups	CO	None	Encrypted Backup File	2, 5	X
	Restore backups	CO	Encrypted Backup File	Success code	2, 5	X

Category	Services	Role	Input	Output	CSP#	CSP Access (R/W/X)
	Configure database replication	CO	Encrypted Backup File	Success code	4	X
	Retrieve log file	CO	None	Log File	5	X
	Reset the log file	CO	None	Success code		
	Monitoring	CO	None	HSM status and audit log		
	Perform firmware update	CO	Updated Firmware	Success code	8	X
	Perform shutdown	CO	None	None	5, 9, 10, 11	W
	Get appliance details	CO/User	None	Appliance information	6, 7	R
	Self-tests	CO	None	Success code		
	Retrieve FIPS mode	CO	None	FIPS status		
User Management	Create user	CO	New User Information	Success code	3	X
	Retrieve user information	CO	User ID	User information	3	X
					13	R
	Update user record	CO	User ID	Success code	3	X
					13	W
	Revoke user	CO	User ID	Success code		
	Create a non-authenticated user	CO	User ID	Success code	3	X
	User authentication	CO/User	User ID, authentication data	Success code	3, 6, 7, 14	X
					15	R
	Update user password	CO/User	User ID, user password	Success code	3	X
					15	W
Session Management	Retrieve session information	CO	None	Information about active sessions		
	Terminate a session	CO	Session ID	Success code	5, 9, 10, 11	W
Key Management	Retrieve non-sensitive key information	CO/User	Key ID	Key information	3	X
	Update Key record	CO	Key ID	Success code	3	X
		CO/User	Key ID	Success code	1, 3	X

Category	Services	Role	Input	Output	CSP#	CSP Access (R/W/X)
	Generate or import key				12	W
	Export non-read locked key	CO/User	Key ID	Success code	1, 3	X
					12	R
	Delete any key	CO	Key-ID	Success code	1, 3	X
					12	W
Cryptography	Data encryption and decryption	CO/User	Key ID, input buffer	Key ID, output buffer	1, 3, 5, 12	X
	Digital signatures	CO/User	Key ID, input buffer	Key ID, output buffer	1, 3, 5, 12	X
	Data hashing and data integrity	CO/User	Key ID, input buffer	Key ID, output buffer	1, 3, 5, 12	X
	Key Exchange	CO/User	Key ID, input buffer	Key ID, output buffer	1, 3, 12	X

Table 5 - Role Access to each Service

1. X means that the key is used for executing cryptographic operation.
2. W or R is relevant to User keys that can be imported or exported via encrypted session, depending on the key definitions.
3. The temporary session keys, CSPs 9, 10 and 11, are used for executing encryption and MAC operations on the session information.
4. The DRBG CSPs, 16, 17 and 18 are used for executing cryptographic operations to generate random numbers.

3.8 Cryptographic Algorithms and Secure Key Management

The DocuSign HSM Appliance supports a variety of cryptographic algorithms, and implements these algorithms based on the cryptographic standards. It provides the following FIPS 140-2 approved algorithms:

3.8.1 Approved Algorithms

Data Encryption

- Triple-DES (ANSI X9.52) in ECB and CBC modes – 192 bits; Cert. #2207
- AES (FIPS PUB 197) in ECB, CBC and CTR modes – 128 bits, 192 bits and 256 bits; Cert. #4031

Data Packet Integrity

- Triple-DES-MAC; Cert. #2207; Vendor affirmed
- HMAC-SHA1/SHA256/SHA384/SHA512, key size 16 – 511 bytes; Cert. #2632
- AES-CMAC 128/192/256 bits; Cert. #4031
- Triple-DES-CMAC; Cert. #2207
- AES-CCM 128/192/256 bits; Cert. #4031

Message Digest

- SHA1, SHA256, SHA384, SHA512; Cert. #3326
- Triple-DES-MAC; Cert. #2207; Vendor affirmed
- AES GMAC 128/192/256 bits; Cert. #4031

Random Number Generator

- HMAC_Based DRBG (NIST SP800-90A); Cert. #1205

TLS V1.2 (OpenSSL)

- CVL (KDF); Cert #857
- HMAC-SHA256, key size 32 bytes; Cert. #2630
- AES (FIPS PUB 197) in CBC modes – 128 bits, 192 bits and 256 bits; Cert. #4029
- SHA256; Cert #3325
- KTS (AES Cert. #4029 and HMAC Cert. #2630)

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

RSA Key Generation

- FIPS 186-4 2048/3072 bits; Cert. #2069

Digital Signature Generation Algorithms (RSA Based)

- PKCS#1 v1.5 2048/3072 bits; Cert. #2069
- PSS 2048/3072; Cert. #2069
- ANSI X9.31 2048/3072 bits; Cert. #2069

Digital Signature Verification Algorithms (RSA Based)

- PKCS#1 v1.5 1024/2048/3072 bits; Cert. #2069

- PSS 1024/2048/3072; Cert. #2069
- ANSI X9.31 1024/2048/3072 bits; Cert. #2069

Digital Signature Generation Algorithms (ECDSA Based)
- ECDSA P-256/P-384/P-521; CVL Cert. #1039

Digital Signature Verification Algorithms (ECDSA Based)
- ECDSA P-256/P-384/P-521; Cert. #900

3.8.2 Non Approved Algorithms

The module supports the following algorithms that are allowed in FIPS mode for key agreement and key establishment:
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength).
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)

The following algorithms cannot be used when module is operated in FIPS mode:

Message Digest
- MD5
- DES MAC
- ARDFP (a proprietary hashing algorithm)

Digital Signature Generation Algorithms
- RSA cipher only with ISO9796 padding

Data Encryption
- DES Stream
- DES (FIPS 46-3) in ECB and CBC modes – 64 bits

Data Encryption-Signature and Verification-Decryption
- AES GMAC GCM

Format Preserving Encryption
- FF3 (non-compliant) radix 10 or 61 (NIST SP 800-38G)

The DocuSign HSM Appliance stores all non-volatile keys in the database. The database is stored encrypted (with AES-128) on the appliance's internal hard drive. Within the database, keys have properties associated with them. These properties determine which operations may be performed on a particular key and establish which users are authorized to carry out these operations.

There are two levels of access to the keys stored on the module, Owner and User. Each key maintains a list of Owner IDs and User IDs. This should not be confused with the User Role

as both levels of access are applicable to the User or Supervisor Role. The Owner of a key can perform all operations on the key and can grant or revoke key access rights to other entities. The User of a key may access it for cryptographic operations only and is not able to read the key or perform administrative functions on it.
When a user is authenticated to the DocuSign HSM Appliance, his/her user identity is defined. When accessing a key for the purpose of management or usage, this user identity is checked against the owner IDs list or user IDs list depending on the required operation.

User Keys are keys that are generated upon request or input by the user for various key operations. User keys consist of two types of keys: User Normal Keys, and User Temporary keys. Users choose what type of key they want to create or input. Users can generate or input any of the following key types: Triple-DES keys, AES 128, 192 and 256 bit keys, RSA 2048 or 3072 bit keys, ECDSA P-256, P-384, P-521 curves and HMAC secret data. The only difference is that a User Normal key can be reused whereas a User Temporary key cannot. User Normal keys are stored in memory and then written to the database before the close of a user session. User Normal keys can be reloaded by the user for a new user session. User Temporary keys are only stored in memory and are erased upon close of a user session.

3.8.3 Initial Configuration

The DocuSign HSM Appliance has four AES-128 critical keys which are generated using an external smart card reader. One half of each of the critical keys is stored on the Startup smart card and the other halves are stored on the Init smart card. During the initial configuration, the first half of the critical keys is read from the Init smart card and stored inside the internal tamper device. The second half of the keys is read from the Startup smart card into the module's volatile memory. The critical keys are then created by XORing the split keys from the Startup smart card and Init smart card and loading the result into the appliance's volatile memory. When the appliance is on, the critical keys are only stored in volatile memory.
When the module is powered off, only the volatile memory is erased. Only the Startup smart card is required to start the appliance.
In case of tamper event, both the module's volatile memory and the tamper device memory are erased. Thus, both the Init and Startup smart cards are required to reset the tamper event and start the appliance again.
It is possible to configure DocuSign HSM Appliance such that there is no need to enter the Startup smart card as part of starting the module. In this configuration (Unattended mode) all the appliance's critical keys content is kept inside the internal tamper device and erased upon a tamper event.

The four critical keys are used for the following internal operations:

- Encrypting key values in the keys database
- Encrypting the database during a backup operation
- Checking the integrity of database records using a MAC key
- Symmetric authentication for database replication

The Special-Purpose keys are only used for internal operations on the appliance. These keys include the customer's organization-wide root public key, appliance's RSA private/public key

pair, the appliance's critical keys, and the appliance's key for continuous operations context encryption.

Public keys and certificates stored in the public key database are inaccessible through the anonymous services (anonymous services are enabled when operating in non-FIPS 140-2 compliant mode). Certificates loaded onto the module must be signed by the organization's private key and this signature is verified before addition to the public key database.

In the FIPS 140-2 compliant mode of operation, all operator sessions are authenticated and encrypted so that no secret or private keys are passed in or out of the module unprotected. In the case of a User ID/Password authenticated session is over non-encrypted session, no key can be imported or export from the module in non-encrypted format. Also any change password or set password operations can be done over an authenticated and encrypted session.
The module also provides the ability to back up the key database in encrypted form.

Table 6 provides a list of all keys and their types.

CSP#	Cryptographic Keys and CSPs	Key Type	Key Generation/Establishment
1.	Critical key for key value encryption of database keys	AES 128	Imported to the appliance during Module Initialization from Init smart card and Startup smart card
2.	Critical key for Backup encryption	AES 128	Imported to the appliance during Module Initialization from Init smart card and Startup smart card
3.	Critical key for database Record MAC calculation	AES 128	Imported to the appliance during Module Initialization from Init smart card and Startup smart card
4.	Critical key for symmetric authentication for database replication	AES 128	Imported to the appliance during Module Initialization from Init smart card and Startup 5smart card
5.	Key for continuous operations context encryption	AES 128	Generated during session initialization
6.	Appliance's RSA Public/private key pair	RSA 2048 bit key	Generated during Module initialization
7.	Organization Root Public Key	RSA 2048 bit key	Generated during Module initialization
8.	DocuSign RSA public key used to verify firmware signature	RSA 2048 bit key	Hard coded in the firmware

CSP#	Cryptographic Keys and CSPs	Key Type	Key Generation/Establishment
9.	Session encryption/decryption keys	AES 256	Temporary key, generated during session initiation
10.	Session HMAC keys	HMAC key 32 bytes	Temporary key, generated during session initiation
11.	Session MAC keys	AES 256	Temporary key, generated during session initiation
12.	User keys – (Two types: user Normal keys and user Temporary keys.)	Multiple key types: Triple-DES CBC\ECB\CMAC\MAC keys, AES CBC\ECB\CCM\CMAC\GMAC 128, 192 and 256 bit keys, RSA Private Key 2048 and 3072 bit keys, RSA Public Key 1024, 1536, 2048, 3072 and 4096 bit keys, HMAC secret data 16 – 511 byte keys, ECDSA P-256, P-384 and P-521 private and public keys, Diffie-Hellman 2048 bit (N=256) private and public keys	Generated by the appliance or imported from the appliance's client API (uploaded securely via the appliance's secure connection).
13.	Public key certificates	RSA 2048 bit public keys stored in certificates	Uploaded in first connection attempt of the user and later used to verify that only this user media is used
14.	RSA based User Authentication	Authentication of operators uses RSA challenge-response mechanism. Authentication provides 1 in 2^112/(1000*60) probability of a successful random attempt during a one-minute period.	Used by user's key media during session initiation
15.	UID/Password Authentication	At least 6 alphanumeric characters long. Yields a minimum of 72^6 (over 1,000,000,000) possible combinations.	Used during session initiation
16.	DRBG Key	HMAC-DRBG RNG Input	Internally generated by DRBG

CSP#	Cryptographic Keys and CSPs	Key Type	Key Generation/Establishment
17.	DRBG seed	DRBG seed in SafeNet eToken 5105	Internally generated by SafeNet eToken 5105
18.	DRBG state	DRBG state in SafeNet eToken 5105	Internally generated by SafeNet eToken 5105

Table 6 - Keys, Key Types, and Access

Remark: The DRBG Key, which is of size 256bit is based on a 256bit random seed that is retrieved from an internal SafeNet eToken 5105 (FIPS 140-2 validation #1883).
The estimated entropy is at least 5.74/8, which means that a random seed of 256bit, will produce minimum entropy of 184bit. This estimate is based on initial assumption of full entropy received from eToken modified by own estimation over conditioned samples output from eToken's DRBG to the remark.
This assumes a residual security risk results from the incomplete testing of a third-party entropy source.

3.9 Self-Testing

The DocuSign HSM Appliance monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-2. The module includes the following self-tests:

3.9.1 Critical Function Tests

Low-Level Hardware Tests
When power is first applied to the module, the hardware performs a series of checks to ensure it is functioning properly.

Firmware Integrity Test
After the hardware tests, the module performs RSA digital signature verification to ensure firmware has not been modified.

Statistical Random Number Generator test
Perform statistical tests on the output of the Random Number Generator.

Return codes for DocuSign HSM Appliance initialization
As the various software subsystems are initialized, the return codes are checked for success to verify the subsystems were initialized successfully.

Find key database and open key database test
Check whether the key database path is properly set in the environmental variables and whether the key database can be opened.

3.9.2 Power-Up Self Tests

Cryptographic Algorithm KATs
Known Answer Tests (KATs) are run at power-up for the Triple DES and AES encryption/decryption, Message Authentication Codes and Hash Algorithms.

- DES Encrypt KATs
- DES Decrypt KATs
- Triple-DES-CBC and Triple-DES-ECB Encrypt KATs
- Triple-DES-CBC and Triple-DES-ECB Decrypt KATs
- AES128, AES192, AES256 CBC and ECB Encrypt KATs
- AES128, AES192, AES256 CBC and ECB Decrypt KATs
- DES-MAC KATs
- Triple-DES-MAC KATs
- SHA-1 KATs
- SHA-256 KATs
- SHA-384 KATs
- SHA-512 KATs
- HMAC-SHA1/SHA256/SHA384/SHA512 KATs
- Triple-DES-CMAC KATs
- AES-CMAC KATs
- AES-CCM KATs
- AES_CTR KATs
- HMAC_DRBG KATs
- AES128_OpenSSL Encrypt KATs
- AES128_OpenSSL Decrypt KATs
- AES192_OpenSSL Encrypt KATs
- AES192_OpenSSL Decrypt KATs
- AES256_OpenSSL Encrypt KATs
- AES256_OpenSSL Decrypt KATs
- SHA-256_OpenSSL KATs
- HMAC-SHA-256_OpenSSL KATs
- TLS_PRF_OpenSSL KATs

Startup RSA Pairwise Consistency Test
Test RSA encrypt/decrypt operation

Startup RSA Digital Signature Test
- RSA Sign KATs
- RSA Verify KATs

Startup ECDSA Pairwise Consistency Test
Test sign/verify using ECDSA to ensure the correct operation.

3.9.3 Conditional Tests

RSA Key Generation Pairwise Consistency Test
All RSA operations are tested to ensure the correct operation of the RSA key generation, encryption/decryption, and signatures.

ECDSA Key Generation Pairwise Consistency Test
All ECDSA operations are tested to ensure the correct operation of the ECDSA key generation, and signatures.

Continuous RNG test (for HMAC_DRBG)
DocuSign HSM Appliance random is based on a non-deterministic seed that is generated by the approved DRBG (Cert. #98) of internal SafeNet eToken 5105 (FIPS 140-2 validation #1883).
The seed is updated every minute and checked for continuous test based on comparison errors.
The output of the HMAC_DRBG algorithm is checked for continuous test and statistical errors.
If any of the tests fails, the module enters the error state.
Continuous RNG test for DRBG output (for DRBG Cert. #98)

Firmware Update Test
Module firmware can only be remotely upgraded from the management system with proper authentication to the module. However, in order to strictly control the loading of new firmware to the appliance, the new firmware must be digitally signed by DocuSign. The load of a firmware update takes place using RSA signatures. The successful load of this update would render the module non FIPS validated unless the update has also been validated.

3.10 Mitigation of Other Attacks

The DocuSign HSM Appliance does not include any mechanisms to prevent against special attacks.

4 FIPS 140-2 Level 3 Approved Mode

In FIPS approved mode of operation an authenticated session must be used. The supervisor role can define for every user whether to use the RSA based authentication scheme or the User ID/Password authentication scheme.
The supervisor role must use the four smart cards (Master, Init, Startup and Root smart card) during pre-operational initialization of the module. The Master smart card is shipped with each DocuSign HSM Appliance and belongs to the specific appliance. It serves as a logical key to access sensitive operations such as performing the pre-operational initialization.

The module is then configured to require the Startup smart card during standard initialization. It is possible to configure DocuSign HSM Appliance such that there is no need to enter the Startup smart card during the initialization of the module. In this configuration all appliance's critical keys content is kept inside the internal tamper device and erased upon a tamper event. This can be configured by using the Unattended Mode option in the appliance's console. When configuring the module to require no Startup smart card, the supervisor will be prompted to insert the Startup smart card as well as enter the Startup smart card password. Upon success, this will enable the unattended startup configuration. The Unattended Mode option in the appliance's console can also be disabled following the same procedures.

The module is shipped with either a FIPS 140-2 approved or non-approved mode. This is as requested by the customer at the time of purchase.
In order to switch a module to a FIPS 140-2 approved mode, set the FIPS Mode to On, in the DocuSign HSM Appliance management utility, Server->Settings dialog box. Once this configuration is accepted, the module is shutdown and restarts using that configuration file. These instructions can be used to put the module back into the FIPS approved mode of operations if the module is placed into a non-approved mode of operations.

When operating in an approved mode, certain functionality is unavailable. The anonymous functions, non-FIPS 140-2 compliant certificates, and non-FIPS 140-2 compliant challenge-response mechanism are all disabled.

For FIPS 140-2 compliance, the session type for both Users and the Supervisor must be set to 3 (i.e., ACC_AUTHEN - authenticated and encrypted session) as depicted in Table 7. This can be set using the DocuSign HSM Appliance management utility. The CO's authorization mask is 0xFFFFFFFF, and the User's authorization mask is 0x00000000. These can be set using the management utility provided or API calls.

Session / Role	Non-Authenticated Session	Encrypted and Authenticated Session
User / Application	No	Yes
Supervisor (Crypto-Officer)	No	Yes

Table 7 - Roles vs. Session Type

When in FIPS mode Cryptographic services shall only use FIPS 140-2-approved algorithms. A list of these algorithms can be found in section 2.4. The module also supports RSA key wrapping in FIPS mode for key establishment and key agreement.

The FIPS mode is displayed in the title either the Users view, Keys view or Sessions views when using the DocuSign HSM Appliance Management utility. It is also displayed in the server -> Properties dialog of the management utility.

4.1 Module Inspection

The cryptographic officer must perform a scheduled inspection of the module to detect tamper evidence. The cryptographic officer shall inspect three areas for tamper evidence:

1. The cryptographic officer shall inspect both of the Tamper Evident cans, which are located on the back of the module.
2. The cryptographic officer shall check the module's front physical interfaces that are located behind the module's front door.
3. The cryptographic officer shall remove the front ventilation cover to check for tamper evidence behind it.