DocuSign®

DocuSign QSCD Appliance

Hardware version 2.0.0.0
Firmware version 1.1.0.9

FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation

February 2023
Document Version 2.8

© Copyright 2023 DocuSign Ltd.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the DocuSign QSCD Appliance. This security policy describes how the DocuSign QSCD Appliance meets the security requirements of FIPS 140-2, and how to operate the appliance in a secure FIPS 140-2 mode.

This document was prepared as part of the FIPS 140-2 level 3 validation of the DocuSign QSCD Appliance.

The following table lists the module's FIPS 140-2 security level for each section.

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

Table 1 – FIPS 140-2 Section Security Level

1.2 Background

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 -- *Security Requirements for Cryptographic Modules*) details the requirements for cryptographic modules. More information on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP), the FIPS 140-2 validation process, and a list of validated cryptographic modules can be found on the CMVP website:
http://csrc.nist.gov/groups/STM/cmvp/index.html

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

1.3 Terminology

The following table prescribes a common understanding of the terms and abbreviations used throughout this document.

Term	Meaning
APT	Adaptive Proportion Test
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
COC	Certificate of Compliance
CKG	Cryptographic Key Generation
DTBS	Data To Be Signed
ESV	Entropy Source Validation
HSM	Hardware Security Module
IDP	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
KTS	Key-transport Scheme
LCD	Liquid Crystal Display
MAC	Message Authentication Code
NIC	Network Interface Controller
PBKDF	Password-Based Key Derivation Function
PCB	Printed Circuit Board
QSCD	Qualified Signature Creation Device
RCT	Repetition Count Test
REST	Representational state transfer
SAML	Security Assertion Markup Language
SHS	Secure Hash Standard
SSA	Server Signing Application
SSS	Shamir Secret Sharing
TLS	Transport Layer Security

Table 2 – Terminology

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 is organized as follows:

- **Section 1: Introduction** – Includes an overview of the DocuSign QSCD Appliance and explains the secure configuration and operation of the appliance.
- **Section 2: Module Overview** – Details each level of the FIPS 140-2 requirements section.
- **Section 3: Secure Operation** – Details the general features and functionality of the DocuSign QSCD Appliance.

The DocuSign QSCD Appliance is also referred to in this document as the appliance, cryptographic module, or the module.

2 Module Overview

The DocuSign QSCD Appliance is a highly secure, high capacity, network attached HSM. The device consists of COTS hardware, tamper resistance hardware, a hardened operating system, a database and server software.

The key features are:

- RSA digital signatures and verification
- AES encryption and decryption
- Authenticated and encrypted communication with the appliance
- REST protocol over HTTPS (HTTP over TLS)
- Tamper-responsive enclosure
- Secure backup capability

2.1 Cryptographic Module Specification

The DocuSign QSCD Appliance is a multi-chip standalone appliance. It has been designed to meet all FIPS 140-2 Level 3 requirements.

The cryptographic boundary, establishing a contiguous perimeter for the DocuSign QSCD Appliance, is defined as the components that are enclosed within the physical case of the module, save for the hot-swappable dual power supplies.

The module supports the TLS protocol version 1.2.

2.1.1 SSA (Server Signing Application)

The SSA is a Web Application that is deployed in the operational environment. It performs some of the operations on behalf of the user and is the application that interacts with the user while performing cryptographic operations, acting as a proxy between the user and the module.

The SSA has the following characteristics:

- It interacts directly with end users and thus does not expose the QSCD to attacks from external networks
- It conducts the whole lifecycle of creation of a user, key generation, certificate enrollment and the digital signature ceremony
- It enables the QSCD to be of a minimal functionality

To perform a signing operation, the SSA will:

- Create a new user
  Any cryptographic operation in the QSCD appliance starts with SSA user that creates a new user. The input for this command is the user ID and the user login name which uniquely identifies the entity that will use the key.
- Generate a key pair for the user
  A key is generated for the user. The output of this command is an encrypted key blob that will later be used by the user to perform the cryptographic operation. The module does not keep key storage for cryptographic keys used by the users.
- Get certificate
  Interact with the CA (Certificate Authority) to get a certificate for the user.
- Supply DTBS/R
  For Qualified digital signatures, upload the hash of the data will be signed by the user in advance and get as response a transaction ID.
- Ask the user to identify and authenticate according to the identity and authentication scheme.

The user then performs the following steps:

- Authenticate
  The user must authenticate to an external identity provider (IDP) and get a valid SAML ticket.
- Perform the cryptographic operation
  As the input of this command the user must supply the SAML ticket along with the encrypted key blob and the input data. Following the user authentication, a SAML token is passed through the SSA to the QSCD and triggers a signature operation.

The SSA then:

- Verify the SAML ticket
  Verify the validity of the SAML ticket and that it belongs to the key blob user and in that way ensure that each key is associated with the correct entity.
- Perform the cryptographic operation in the QSCD appliance.
- Collect the signature and return it to the signing application.
- Depending on the type of signature key (ephemeral or persistent) the SSA decides whether to delete the user and his/her key from the module and from the SSA.

2.2 Cryptographic Module Ports and Interfaces

The module is steel, rack mountable box. The physical ports in the front of the module include on/off power button with power indicator, a display, display keys and a USB connector. On the back of the module, there are two power connectors and two network connections (Ethernet Interfaces using TCP/IP).

The module is encased in a steel cover, with only the specified ports providing access to the module. All ports use standard connector interfaces.

Figure 1 – Front and Rear Interfaces

2.2.1 Logical and Physical Interfaces

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

FIPS 140-2 Logical Interfaces	Appliance's Physical Interfaces
Data Input Interface	Network ports USB slot for smartcard-based token[1] Display keys
Data Output Interface	Network ports USB slot for smartcard-based token[2]
Control Input Interface	Network ports Display keys
Status Output Interface	Network ports LCD LED indicators
Power Interface	DC power connector

Table 3 – Interfaces

Commands are packaged using a REST format and sent to the appliance over the TLS-secured sockets on ports 443, 9091 and 9092 (only in the tamper state). The TLS protocol is based on server authentication (One-way TLS).

The LCD shows instructions such as insert/remove the USB token, critical errors such as Tamper and general status information such as: host name, appliance status, software version, IP address, default gateway, etc.

The front of the module has several control buttons:

- On/off power button with power indicator
- Display keys (Up, Down, Left, Right, Back and OK) which are used to operate the appliance for example when performing comprehensive restore factory

Status and telemetry information is sent through the network ports to a cloud-based event monitoring system. This information can be used to collect performance figures, error reporting and to detect hardware, networking and performance issues as they occur. Additional status information is sent to an external audit log server. No CSPs or other sensitive information is sent to the external monitoring and audit systems.

2.2.2 Hardware Block Diagram

The following figure shows the module's hardware block diagram.

[1] Used only during module initialization, and reset tamper operation

[2] Used only while generating or copying Master Keys on the USB token

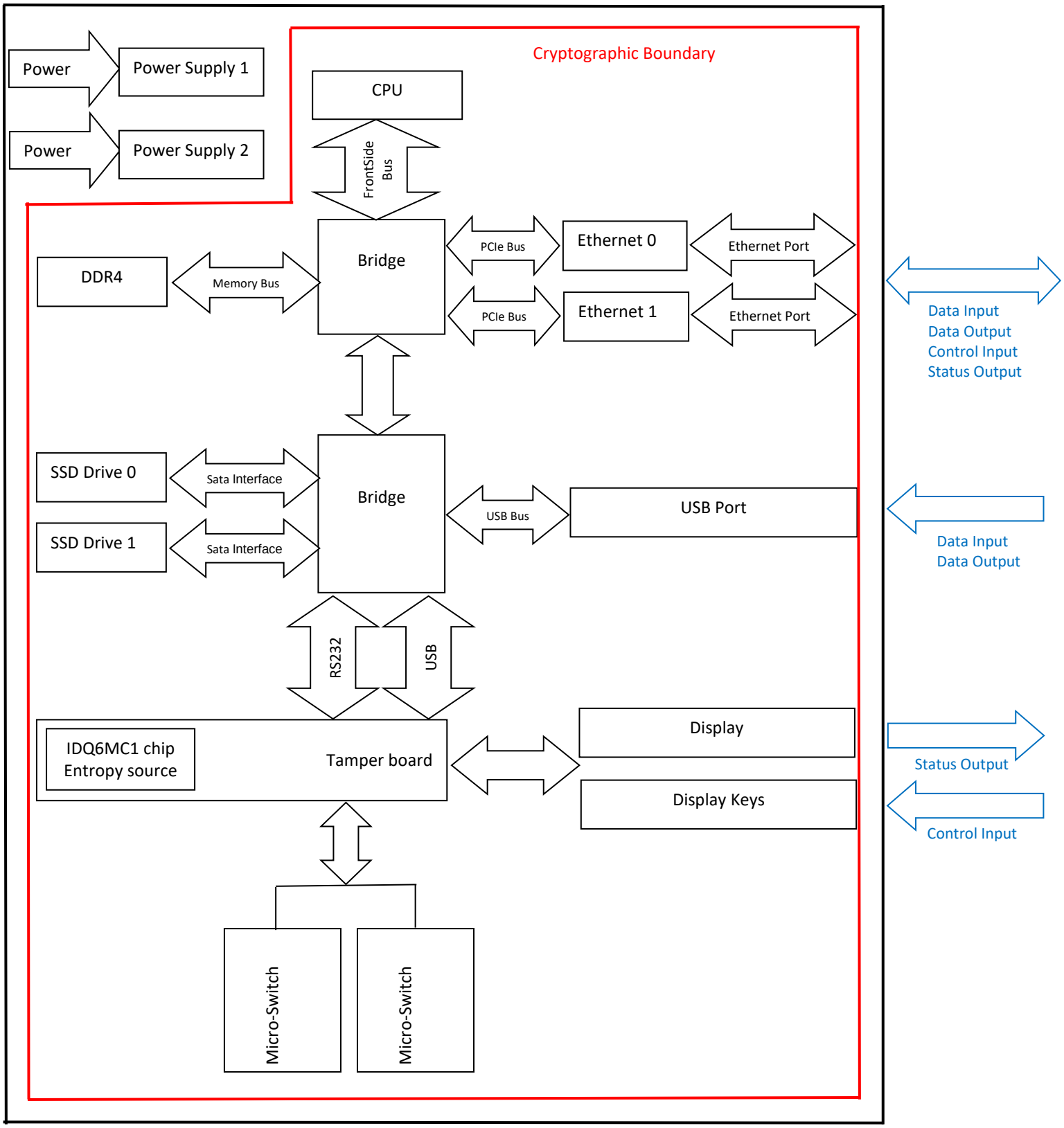

Figure 2 – DocuSign QSCD Appliance Hardware Block Diagram

2.3 Roles and Services

The module has two classes of roles: Crypto Officer (CO) and User. The module does not support role change, thus an operator that has been defined as a CO cannot change to the User role.

The module does not include a maintenance interface, nor does it include a maintenance role.

2.3.1 Crypto Officer Sub-Roles

There are three types of CO administrative sub-roles:

- **Appliance Administrator**
  This role is responsible for installing, configuring and maintaining the appliance, by performing the following operations:
  - Installing the appliance
  - View and modify system parameters
  - Backup/Restore the module's data
  - Shutdown/Hardware Restart the appliance
  - Upload software updates provided by DocuSign
  - Download technical log files from the appliance
  - Add/Update/Delete/View Trusted Anchors which are used to validate SAML tickets generated by an IDP
  - Configure networking parameters (IP address, default gateway, DHCP, etc.)
  - Configure time parameters (set current time, NTP server of the system)
  - Modify the debug level to control which information will be written to the technical log
  - Reset Tamper to set the appliance state back to Operational state after tamper event
  - Restore to factory settings to set the appliance back to Factory state

- **Users Administrator**
  This role is responsible for managing module accounts, and can perform the following operations:
  - Add a new Administrator
  - Delete an existing Administrator
  - Unlock an Administrator account that was locked after too many password failures
  - View Administrator user information

- **SSA (Server Signing Application) Administrator**
  This role is responsible for performing cryptographic operations on behalf of the user, by performing the following operations:
  - Create/delete a User entity
  - Generate key pair/key for the User
  - Perform cryptographic operation on behalf of the User

2.3.2 User Role

The user interacts with the QSCD via the SSA for the purpose of performing cryptographic operations such as digitally signing a document/data or performing AES encryption/decryption.

2.3.3 Services

The following table provides a high-level summary of the approved services provided by the module.

Category	Service	Information Summary	Role
Appliance Setup	Install appliance	Enter Operational state by installing the appliance; This service is available only when the appliance is in factory state	CO
	Write USB token	Write key part into the USB token	CO
	Read USB token	Read key part from the USB token	CO
	Reset tamper	Return to Operational State after Tamper event	CO
	Restore factory	Restore the appliance back to Factory State and erase all settings	CO
	Set time	Set module time using NTP protocol	CO
	Monitoring	Send system status and audit log to external monitoring servers	CO
Appliance Administration	Update network setting	Set network parameters for the Ethernet interfaces such as DHCP on/off, IP address, default gateway, DNS etc.	CO
	Update time setting	Set time or configure NTP server	CO
	Set system parameters	Set system parameters like password policy, RSA key generation parameters, logging etc.	CO
	Manage Trusted Anchors	Manage the Trusted Anchors which are used to validate SAML tickets	CO
	Perform software upgrade	Update the firmware	CO
	Perform backup	Backup system parameters and other settings into encrypted file	CO
	Restore from backup	Restore system parameters and other settings from backup file	CO
	Get technical log	Get the module's technical log files	CO
	Get server information	Get general information such as network information, time, status, etc.	Anonymous
	Restart	Perform hardware restart	CO
	Shutdown	Shutdown the module	CO
	Create Administrator user	Centralized storage and management functions of Administrator users and their passwords	CO
User Administration	Delete Administrator user	Centralized storage and management functions of Administrator users and their passwords	CO
	Get users list		CO
	Get user details		CO
	Change password		CO
	Unlock Administrator user		CO
User Authentication	Authenticate	Authenticate user using user ID/password or SAML ticket	CO, User
Cryptographic Operation	Digital signature	Enable client applications to use RSA keys for digital signatures signing operations in PKCS#1 v1.5 or PSS schemas	User
	Encryption/Decryption	Enable client applications to use AES keys for data encryption/decryption in CBC mode	User
	Get random	Get random data	Anonymous
SSA Administrator	Create User	Create a user	CO
	Delete User	Delete a user	CO

Category	Service	Information Summary	Role
	Generate User key pair/key	Generate RSA key pair/AES key on behalf of the user	CO
	Delete User key pair/key	Delete the user's RSA key pair	CO
	Supply DTBS	Supply data to be signed/encrypted	User
	Collect result	Collect the result of cryptographic operation	User

Table 4 – Approved Services

The following table shows each specific service, which role has access to it and which CSP and access type (Read, Write, eXecute) is used to provide the service. Refer to Table 10 for the description of the CSPs used by each operation.

Service	Role	Input	Output	CSP#	CSP Access (R/W/X)
Install appliance	CO	Master keys	Success code	1,2,3,4,5,6,7,13	R/W
Write USB token	CO	Master keys	Split Master Keys on USB token	1,2,3,4,5,6,7	R/W
Read USB token	CO	Split Master Keys from USB token	Master Keys in tamper	1,2,3,4,5,6,7	R/W
Reset tamper	CO	Split Master Keys from USB token	Master Keys in tamper	1,2,3,4,5,6,7,12	R
Restore factory	CO	None	None	7	X
				All	W
Monitoring	CO	None	Status and audit log	2,13	X
Update network setting	CO	Input data	Success code	3,7	X
Update time setting	CO	Input data	Success code	3,7	X
Set system parameters	CO	Input data	Success code	3,7	X
Manage Trusted Anchors	CO	Input data	Success code	3,7	X
				14	R/W
Perform software upgrade	CO	Signed software file	Success code	7,9,10	X
Perform backup	CO	None	Encrypted Backup File	5,6,7	X
Restore from backup	CO	Encrypted Backup File	Success code	5,6,7	X
Get technical log	CO	None	Log file	7	
Get appliance information	Anonymous	None	Appliance information		
Restart appliance	CO	None	None	7,15,16,18	W
Shutdown appliance	CO	None	None	7,15,16,18	W
Create Administrator user	CO	New Administrator User info	Success code	3,7	X
				17	W
Delete Administrator user	CO	User ID	Success code	7	X
				17	W
Get users list	CO	None	Users list	3,7	X
Get user details	CO	User ID	User information	3,7	X
Change password	CO	New password	Success code	3,7	X
				17	W

Service	Role	Input	Output	CSP#	CSP Access (R/W/X)
Unlock Administrator user	CO	User ID	Success code	7	X
Authenticate	CO, User	User ID, Authentication data	Success code	3,7	X
				14,17	R
Digital signature	User	Encrypted key blob, input buffer	Output buffer	1,3,4,7,8	X
Encryption/Decryption	User	Encrypted key blob, input buffer	Output buffer	1,3,4,7,9	X
Get random	Anonymous	None	Random data	18,19,20	R/W
Create User	CO	User information	Encrypted user blob	1,3,4,7	X
				8,9	W
Delete User	CO	User ID	Success code	7	X
Generate User key pair/key	CO	User ID	Encrypted key blob	1,3,4,7	X
				8,9	W
				18,19,20	R/W
Delete User key pair/key	CO	User ID	Success code	7	X
				8,9	W
Supply DTBS	CO	User ID, input buffer	Success code	4,7	X
Collect result	CO	User ID	Output buffer	3,7,8,9	X

Table 5 – Role Access to each Service

2.3.4 Authentication

Administrators use identity-based authentication with a user ID/password over the TLS session. After successful authentication, the module issues a JSON Web Token (JWT) ticket which is then used to verify the administrative user in all subsequent REST API commands.

Users also use identity-based authentication indirectly by authenticating to an external Identity Provider (IDP) which generates a SAML ticket. The SAML ticket is then used to verify the user in all subsequent REST API commands.

Each REST API command requires a specific administrator JWT or user SAML ticket. Thus, multiple concurrent operators are allowed, and each command is specifically tested to verify that the user is allowed to perform.

Authentication Mechanism	Rationale
User ID/Password	The module enforces a minimum password length of six Unicode characters. Each character may be numeric (0-9) or alphanumeric (a-z, A-Z) or Unicode. Based on an alphanumeric set of characters there are 62 possible characters and the password is at minimum 8 characters long. Therefore, the probability of a random attempt to succeed is: 1 in (62^8) = 1 in 218,340,105,584,896. This is significantly less than 1 in 1,000,000. It takes the module approximately 1msec to process a login attempt, for a maximum of 1,000 login attempts in 1 second and 60,000 login attempts in 1 minute. Therefore, the probability of a random attempt to succeed during a minute is: 1 in ((62^8) / 60,000) = 1 in (218,340,105,584,896 / 60,000) = 1 in 3,639,001,759. This too is significantly less than 1 in 100,000.
SAML Ticket	The SAML token is based on a 2048-bit digital signature which has security strength of 112 bit. The probability that random access will succeed is 1 / (2^112) which is far less than one in 1,000,000. The appliance cannot process more than 3000 SAML validations per second, thus the authentication provides a 1 in (2^112 / (3000*60)) probability of a successful random attempt during a one-minute period. This is exponentially less than 1 in 100,000.

Table 6 – Strength of Authentication

2.4 Physical Security

The module is encased within a steel box rigged with tamper-responsive micro-switches, and a tamper-evident can that covers a screw joining the top and bottom of the enclosure. 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 (CSPs) including the appliance Master Keys. All vents on the module are baffled to meet FIPS 140-2 physical security requirements for opacity and probing.

2.5 Operational Environment

The module operates in a non-modifiable operational environment under the FIPS 140-2 Section 4.6 definitions.

2.6 Cryptographic Key Management

The DocuSign QSCD 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:

2.6.1 Approved Cryptographic Algorithms

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Length	Use
Core Cryptographic Algorithms					
A2434	AES	FIPS 197	CBC	128, 192, 256 bits	Data Encryption
Vendor affirmed	CKG[1]	SP 800-133			Key Generation
A2434	HMAC	FIPS 198-1	HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	256 bits	Message Authentication
A2434	HMAC_DRBG	SP 800-90A	HMAC-SHA-256		Deterministic Random Number Generation
A2434	RSA	FIPS 186-4		2048, 3072, 4096 bits	Key Generation
A2434	RSA	PKCS#1 v1.5	SHA-256 SHA-384 SHA-512	2048, 3072, 4096 bits	Digital Signature Generation
A2434	RSA	PKCS#1 PSS	SHA-256 SHA-384 SHA-512	2048, 3072, 4096 bits	Digital Signature Generation
A2434	RSA	PKCS#1 v1.5	SHA-256 SHA-384 SHA-512	2048, 3072, 4096 bits	Digital Signature Verification
A2434	SHS	FIPS 180-4	SHA-256 SHA-384 SHA-512		Message Digest Hash for digital signature generation
E10	ESV	SP800-90B	N/A	N/A	Seeding/reseeding the DRBG
TLS (OpenSSL) Cryptographic Algorithms					
A2430	AES	FIPS 197	CBC	128, 256 bits	TLS Session Schema Session data encryption
A2430	CVL TLS 1.2	SP 800-135rev1	SHA-256		TLS Key Derivation[2]
A2430	HMAC	FIPS 198-1	HMAC-SHA-256	256 bits	TLS Session Scheme
A2430	KTS	FIPS 197 SP 800-38F	AES-CBC / HMAC	128, 256 bits	Key Transport[3]
A2430	PBKDF[4]	SP 800-132	Option 1a	256 bits	Password based key derivation
A2430	RSA	PKCS#1 v1.5	SHA-256 SHA-384 SHA-512	2048, 3072, 4096 bits	Digital Signature Generation
A2430	SHS	FIPS 180-4	SHA-256		TLS Session Schema

Table 7 – Implemented FIPS Approved Algorithms

[1] The unmodified output of the DRBG is used for symmetric key generation and as the seed for asymmetric key generation

[2] No parts of the TLS protocol, other than the KDF, have been tested by the CAVP and CMVP

[3] Key establishment methodology provides 128 or 256 bits of encryption strength

[4] The PBKDF algorithm parameters are: password length 32 bytes long, salt length 16 bytes long and the number of iterations is 2048. The resulting key material is only used for storage applications.

2.6.2 Allowed Cryptographic Algorithms

The module supports the following non-FIPS 140-2 Approved but allowed algorithms that may be used in the Approved mode of operation:

Algorithm	Usage
RSA Key Transport	Key establishment methodology using PKCS#1-v1.5 provides between 112 and 256 bits of encryption strength

Table 8 – Allowed Algorithms

2.6.3 Non-Approved Algorithms

The module supports the following non-approved algorithms which should not be used in the Approved mode of operation:

Algorithm	Usage
Elliptic Curve key generation Supported curves: P-256, P-384, P-521 (FIPS 186-4)	Ephemeral keys for TLS Key Establishment with security strength 128, 192, 256 bits
Elliptic Curve Diffie-Hellman Supported curves: P-256, P-384, P-521 (Sp800-56Ar3)	TLS Key Establishment with security strength 128, 192, 256 bits
AES GCM (SP 800-38D)	TLS Session Schema Session data encryption with security strength 128, 256 bits

Table 9 – Non-Approved Algorithms

2.6.4 Keys and CSPs

The module protects keys against unauthorized disclosure, modification, and submission as follows:

- The keys that are stored inside the module are used by their assigned entity only for specific processes or functions
- Access to functions that use keys is allowed only after the entity requesting access has been authenticated.
- TLS sessions between an operator's PC and the module are authenticated and encrypted.
- The module does not provide key storage for cryptographic keys used by an entity. After generating a key, it is exported in an encrypted and MACed blob to the entity for their use
- The variables that indicate the current sessions, the operators of sessions, and session keys are stored in RAM. When the module is powered off this information is erased as the RAM is powered off. Upon module restart, all entities must open new authenticated TLS sessions.
- The module provides no access to intermediate key generation values, and outputs no intermediate key generation information. All intermediate key generation values are zeroized when they are no longer needed.

The following table provides details on the CSPs used by the module.

CSP#	Key Type & Size	Name/Usage	Generation/Input/Output	Storage	Zeroization
Master Keys					
1.	AES-CBC 256 bits	MK-EXT-KEK Critical key for key value encryption of database keys			

CSP#	Key Type & Size	Name/Usage	Generation/Input/Output	Storage	Zeroization
2.	AES-CBC 256 bits	MK-INT-KEK Critical key for encryption of CSPs stored within the module	Internal[1]/External[2]/NA	Tamper device memory (plaintext[3])	Tamper event[4]
3.	AES 256 bits	MK-MAC Critical key for HMAC-SHA256 of database records			
4.	AES 256 bits	MK-JWS Critical key for HMAC-SHA256 of user blobs			
5.	AES-CBC 256 bits	MK-BKP-ENC Critical key for encryption of backup file			
6.	AES 256 bits	MK-BKP-MAC HMAC-256 of backup file			
7.	AES 256 bits	MK-JWT HMAC-256 of proof of Authenticating user			
User Keys					
8.	RSA 2048, 3072, 4096 bits	RSA-SIG User signing keys	Internal/Encrypted/Encrypted	User key blob (encrypted[5])	NA[6]
9.	AES 128, 192, 256 bits	USER-AES-KEY User encryption keys			
Other Module CSPs					
10.	RSA 3072 bits	FIRM-SIG RSA Public Key for validating the software and the upgrades file(s)	External/NA/NA	Disk (plaintext[7])	NA
11.	RSA 2048 bits	TLS-KEY Appliance's TLS RSA private/public key pair	External/NA/NA	Disk (encrypted[8])	NA
12.	RSA 2048 bits	TLS-KEY-TAMPER-STATE Appliance's TLS RSA public/private key pair for tamper state			
13.	RSA 3072 bits	AUDIT-LOG-KEY Audit log signature key	Internal/NA/NA	Disk (encrypted[9])	NA

[1] Generated inside the appliance during preliminary pre-installation procedure and split into two parts using SSS

[2] Two parts are recombined during installation using SSS and stored in tamper memory

[3] Stored in cleartext in tamper memory along with SHA256 hash for data integrity

[4] Any attempt to tamper the module results in tamper response, clearing the tamper memory

[5] User blobs are encrypted (AES-CBC) using MK-EXT-KEK and HMACed (HMAC-SHA256) using MK-JWS

[6] The module does not provide key storage for cryptographic keys used by an entity, therefore it cannot zeroize those keys

[7] The RSA public key used for firmware signature validation and firmware update validation is hardcoded in plaintext in the signed module firmware

[8] Used for establishment of TLS sessions with users and stored encrypted (AES-CBC) in password protected PFX file on the module SSD drive

[9] Stored encrypted (AES-CBC) using MK-INT-KEK in a file on the module SSD drive

CSP#	Key Type & Size	Name/Usage	Generation/Input/Output	Storage	Zeroization
14.	RSA 2048, 3072, 4096 bits	Trusted public keys and certificates	External/External/NA	Disk (plaintext[1])	NA
15.	AES-CBC 128, 256 bits	Session encryption / decryption keys	TLS key establishment/NA/NA	Memory (plaintext[2])	End of session or power cycle
16.	32 bytes secret key	Session HMAC keys			
17.	At least 8 alphanumeric characters long	User ID/Password Authentication	External/ Encrypted/NA	Disk (hashed[3])	User deletion
18.	HMAC_DRBG RNG Input	DRBG[4] state (Key and V)	Internal/NA/NA	Memory (plaintext)	Appliance service shutdown[5] or power cycle
19.	HMAC_DRBG RNG internal state	Entropy input string	Internal/NA/NA	Memory (plaintext)	NA
20.	DRBG seed from hardware chip	Entropy input	Internal/NA/NA	Memory (plaintext)	NA

Table 10 – Keys and CSPs

2.6.5 Random Number Generator

The module has an approved RNG:

- **Approved HMAC_DRBG**
  This RNG is used to generate random numbers from which the user's RSA and AES keys are generated.

- **Entropy Source**
  The module has a hardware-based entropy source ESV (Cert. #E10) that meets the requirements of NIST SP 800-90B. The Quantis IDQ6MC1 chip generates a seed that is input into the HMAC_DRBG RNG. A new seed is generated upon power-up, and later once every hour or when reseed is needed. The IDQ6MC1 is a quantum random number generator that generates entropy directly from a quantum process. The module is compliant with the ESV (Cert. #E10) and is configured according to section "Configuration Settings" in the public use document[6].
  The overall amount of generated entropy is 1.767981 bits per 2-bit sample and estimated amount of entropy per the sources output bit is.1.96 per 2-bit sample.

Note: The module generates cryptographic keys whose strengths are modified by available entropy.

The seed data output from the entropy source chip is continuously tested according to the requirements of NIST SP 800-90B. Two tests are being performed on the stream of random data produced by the chip: Repetition Count Test and Adaptive Proportion Test. These tests are also performed on the stream of random data output from HMAC_DRBG.

Random data produced by the RNG is used to generate random numbers and cryptographic keys.

[1] Stored in QSCD database in plaintext with integrity (HMAC-SHA256) using MK-MAC
[2] Negotiated during the establishment of the TLS connection, stored in volatile RAM and destroyed when the session is terminated
[3] Stored in the QSCD database with integrity (HMAC-SHA256) using MK-MAC
[4] DRBG Key of size 256 bits is based on a 512-bit random seed retrieved from an internal hardware entropy source (Quantis IDQ6MC1 chip)
[5] Upon shutdown, the HMAC_DRBG uninstantiate function zeroises the DRBG state
[6] https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E10_PublicUse.pdf

2.6.6 Key Establishment

The module uses TLS protocol for session key establishment. The cipher suites in use are TLS_RSA_WITH_AES_CBC_128_SHA256 and TLS_RSA_WITH_AES_CBC_256_SHA256.

2.6.7 Key Input/Output

Keys are input or output from the DocuSign QSCD Appliance in several processes:

- User keys are output from the appliance in encrypted and MACed key blobs.
- The CO can output/input CSPs from/to the appliance by performing backup and restore operations of the appliance's database (See 3.5).
- CSPs are output from the module to the USB port during Master Key generation. The server Master Keys are generated, split into two parts using the Shamir Secret Sharing (SSS) algorithm and then written on external password protected USB tokens connected to the USB port.
- Only during installation, restoration or reset tamper operations, CSPs are input to the module from the USB port. The key parts are read from two password protected USB tokens connected to the USB port. Then, the Master Keys are rebuilt using SSS.
- In regular operational mode there is no manual input or manual output of keys.

2.6.8 User Keys

There are two types of user keys that are managed by the SSA:

- **Ephemeral keys**
  Ephemeral keys can be used for signing for a very short time (several minutes). In many cases they are used for a single digital signature operation.

- **Persistent keys**
  Persistent keys can be used for a long period of time.

2.7 EMI/EMC

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

2.8 Self-Tests

The DocuSign QSCD Appliance monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-2. All tests run automatically without operator intervention.

The CO can initiate the power-up self-tests and the critical function tests by cycling the module's power and starting the QSCD firmware.

The module includes three types of self-tests: power-up self-tests, critical function tests and conditional tests. When the module is powering up and performing these tests, the display port shows the message "Starting…". Upon successful power-up self-tests and critical function tests, all QSCD services are started and the display shows the message "Installed". If an error occurred an appropriate error message is displayed, and the module enters the error state.

2.8.1 Power-Up Self Tests

The power-up self-tests are performed immediately after the module power is turned on. They include low-level hardware tests and cryptographic algorithm 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. The motherboard of the appliance performs an initial hardware check which is aimed to test the hardware components of the system such as the CPU, memory, network interfaces, SSD Drive and dual power supply. If there is any problem the appliance would not start, and the display will show the message (loading…). This low-level test is being performed prior to loading of the appliance operating system and running the QSCD services.

Cryptographic Algorithm Tests

Known Answer Tests (KATs) are run at power-up for all implementations of cryptographic algorithms used by the module. In a Known Answer Test, input values, values of keys and output values are all hardcoded, thus checking only the execution of the algorithm itself. If the execution of the algorithm yields a different output than the hardcoded expected ones, then the test fails and a corresponding error is displayed. Failure in the Core algorithm tests results in (CryptoError) and failure in the TLS library tests results in (SSLError).

The following Core cryptographic algorithms are tested:

- AES128, AES192, AES256 CBC Encrypt, Decrypt KATs
- SHA-256, SHA-384, SHA-512 KATs
- HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 Calculation, Verification KATs
- RSA 2048 Sign, Verify KATs
- HMAC_DRBG KAT

For the appliance's TLS, additional library (OpenSSL) with the following implemented algorithms is tested:

- AES128, AES192, AES256 ECB, CBC Encrypt, Decrypt KATs
- SHA-256, SHA-384, SHA-512 KATs
- HMAC-SHA256 Calculation, Verification KAT
- RSA 2048, 3072, 4096 Encrypt, Decrypt KATs
- PBKDF5 KAT using HMAC-SHA256

DRBG Tests

The DRBG tests are performed upon power-up and immediately following the cryptographic algorithm tests. Both the entropy source ESV (Cert. #E10) and the HMAC_DRBG are tested.

The entropy source ESV (Cert. #E10) power-up test follows the NIST SP 800-90B guidelines and include:

- Continuous health test on approximately 4000 random samples

The HMAC_DRBG power-up test follows the NIST SP 800-90A guidelines and include:

- Instantiate function KAT test
- Reseed function KAT test
- Generate function KAT test and reseed counter test

2.8.2 Critical Function Tests

The critical function tests are performed after the power-up self-tests.

Tamper Communication Test
Upon startup, the QSCD communicates with the tamper device to check if tamper event has occurred. Failure to communicate with the tamper board will result in tamper hardware error (TamperHWFailure).

Tamper Integrity Test
This test is designed to identify several problems that are related to the value of the critical keys stored in the tamper memory, for example:

- The appliance was installed from two USB tokens that are not a matching pair
- Due to hardware problem, the data in the tamper memory was changed and is now inconsistent
- A reset tamper operation was performed with wrong USB tokens, that do not match the database stored on the appliance

The test verifies the integrity of the critical Master Keys stored in the tamper device, by calculating the SHA256 hash of the data in the tamper memory and comparing it to the expected value. The hash is also compared to the hash value stored in the database of the appliance. If the test fails, the appliance would not start and a corresponding message (TamperMismatch) is displayed.

Firmware Integrity Test
After the hardware tests, the module performs RSA 3072-bit digital signature verification to ensure firmware has not been modified. All executable and shared object files of the software are digitally signed as part of the DocuSign development procedures. The public key for verification is hard coded into the firmware of the appliance. If the firmware failed the integrity test, the appliance would not start and a corresponding message (SWVerifyError) is displayed.

Database Access Test
A database connectivity check validates that the database is alive and can respond to requests. In the case of failure, the appliance's service will not start and thus will not provide service to clients. A corresponding message (DBError) is displayed.

Return Codes for DocuSign QSCD Appliance Initialization
As the various software subsystems are initialized, the return codes are checked for success to verify the subsystems were initialized successfully. In any case the above tests failed to execute a critical error message (CriticalError) is displayed.

2.8.3 Conditional Tests

RSA Key Generation Pairwise Sign/Verify Consistency Test

To ensure the correct operation of the RSA key generation, each newly generated RSA key pair is tested for pairwise consistency. The newly generated private key is used to sign test data, and the resulting signature is then verified by the corresponding public key.

Continuous RNG Tests for Entropy Source

The entropy source is a non-deterministic RNG seed that is generated by high quality internal hardware chip (Quantis IDQ6MC1 chip). The chip meets the requirements of NIST SP 800-90B standard. It produces 2-bit samples with estimated entropy of 1.767. The seed is updated every hour or when seed counter is read reached. The 2-bit outputs of the entropy source and checked by continuous random tests (RCT and APT) as defined in NIST SP 800-90B:

- Repetition Count Test (RCT) as defined in section 4.4.1, with the following values:
  $H = 1.5$, $\alpha = 2^{-30}$, $C = 21$

- Adaptive Proportion Test (APT) as defined in section 4.4.2, with the following values:
  W = 512, H = 1.5, $\alpha = 2^{-30}$, C = 248
  The cutoff value C meets the requirement C <= W.

If the continuous random tests fail, the appliance enters an error state with a corresponding error displayed.

Continuous RNG Tests for HMAC_DRBG

A Deterministic Random Bit Generator (DRBG) based on HMAC_DRBG algorithm as defined in NIST SP 800-90A. The output of the HMAC_DRBG algorithm is also continuously checked for statistical errors by running the continuous random tests (RCT and APT) as defined in NIST SP 800-90B:

- Repetition Count Test (RCT) as defined in section 4.4.1, with the following values:
  H = 6, $\alpha = 2^{-30}$, C = 6
- Adaptive Proportion Test (APT) as defined in section 4.4.2, with the following values:
  W = 512, H = 6, $\alpha = 2^{-30}$, C = 31
  The cutoff value C meets the requirement C <= W.

In addition, the HMAC_DRBG functions (instantiate, uninstantiate, reseed and generate) are continuously tested for correctness as required by NIST SP 800-90A.

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.

2.9 Mitigation of Other Attacks

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

3 Secure Operation

3.1 Product Delivery

At manufacturing both tamper device and tamper seal are assembled. The assembly of these components activates the tamper mechanism and tamper evidence of the module. The whole product is fully tested before delivery. The product is packaged and directly delivered to the customer. The product is in a Factory state when delivered to the customer. During delivery, the product is protected by a unique tamper seal on the case, the casing of the appliance, and is enclosed in a special plastic package protected with four distinct tamper evident security stickers similar to the following:

Figure 3 – Safety Sticker

Upon delivery, the CO must follow the instructions below:

- Verify that all the four stickers exist, have not been tampered with, and are attached to the plastic package.
- Verify that each tamper evident security sticker includes the word DocuSign and that its serial number matches the number listed in the QSCD delivery message sent from DocuSign.
- Check the appliance's case for any evidence of physical tampering.
- Check the tamper evident can on the back of the appliance and make sure it is not damaged.
- Verify that the serial numbers of the tamper evident stickers match the documentation COC (Certificate of Compliance) received with the appliance (for security reasons, the serial numbers of the package are sent in two separate ways: email and paper).
- Turn on the module, verify that tamper LED is not blinking and that it starts correctly without any error massage.

If any problems or suspicions arise, the CO must contact DocuSign Support via https://support.docusign.com/en/contactSupport or email security@docusign.com.

3.2 DocuSign QSCD Delivery Message

In addition to the module, the CO will also get an electronic DocuSign envelope from DocuSign Manufacturing. This envelope includes the following information about the DocuSign QSCD Appliance:

- DocuSign QSCD Appliance serial number (for example: QSCD0009)
- Serial numbers of all the tamper evident stickers
- Additional information related to the appliance

3.3 QSCD States

DocuSign QSCD Appliance can be in one of the three following states:

- **Factory Settings State**
  In this state the Appliance is not installed and does not contain any operational data such as Master Keys, Administrative Accounts or any other operational information in its database. All functionality of

creating administrative roles or performing cryptographic services is closed and cannot be performed. The appliance installation process changes the appliance's state from Factory state to FIPS approved Operational state. During installation, Master keys that were generated in pre-install procedure are read from two USB tokens. This sensitive operation should be done in a secure environment.

- **Operational State**
  In this state, it is possible to fully operate the appliance for its designated purpose as a QSCD.
  It is possible to turn the appliance back into factory state by performing the Reset Factory operation.
  Opening the appliance enclosure either when the power is on or off, will set the appliance to tamper state.

- **Tamper State**
  The appliance contains a tamper resistant mechanism which when activated erases the Master Keys data that are used to protect sensitive information.
  In the Tamper state the appliance does not serve any request beside an approval of an Appliance Administrator of the tamper condition called Reset Tamper.

Figure 2 below shows the transitions between the three states.

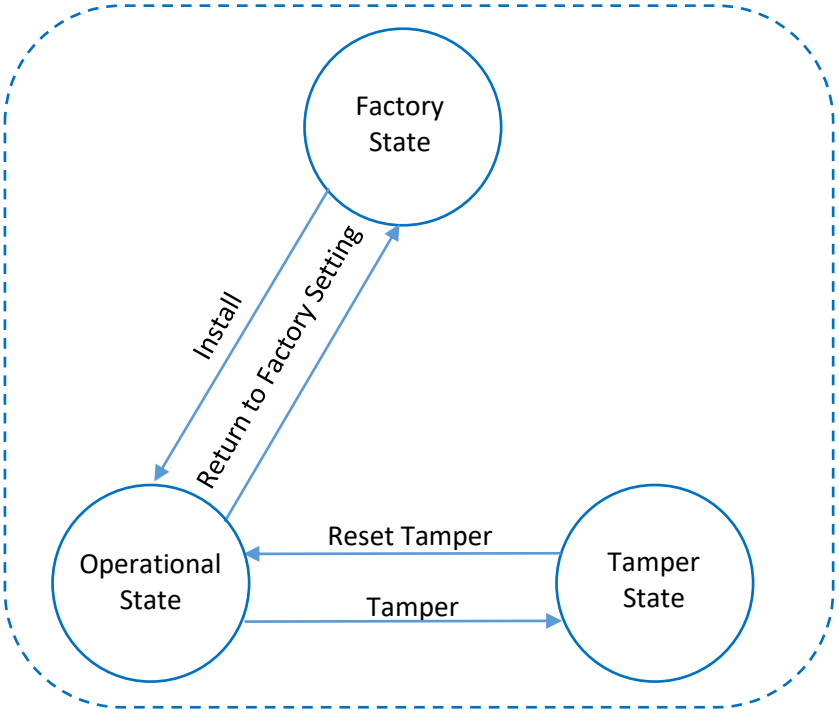

Figure 4 – QSCD States

3.4 Initialization

The appliance is delivered in the Factory Settings state. In this state it is not installed and does not contain any operational data. Once the CO starts performing the following operations to install and configure the Appliance to run, it is then operating in FIPS mode:

- **Generating Master Keys** – The Master Keys are generated prior to the appliance installation and contain secret information that is critical for the operation of the appliance. The Master Keys are generated inside the appliance, split into two parts and written on two password protected USB tokens; each belonging to a different CO.
- **Copying the USB Tokens** – It is possible to duplicate the set of USB tokens that contain the appliance Master Keys.

- **Installing the appliance** – This critical procedure must be performed in a secure environment. After the appliance installation, the administrator can modify the system parameters and start the cryptographic services of the appliance.
- **Setting the appliance to FIPS mode** – This final step sets the appliance to work in approved FIPS mode.

The Initialization operations can be performed by the Appliance Administrator, either by:

- **GUI Based Client Application** – This is a simple setup utility running on the Administrator Windows PC, which is connected to the appliance through Ethernet port NIC2 as it has a fixed IP address. Any operation from the GUI application requires physical access to the appliance by unplugging/plugging the USB token with Master Keys.

- **REST API Calls** – Administrators can connect to the appliance via the internal network and directly call the REST API functions.

3.4.1 Generating QSCD Master Keys

The generation of the Master Keys and optionally copying them onto the USB tokens are preliminary steps that must be performed prior to the installation of the module. These operations must be performed in a secure environment.

In this step, a GUI based client application running on a PC connected to the module is used to send commands to the appliance to generate the Master Keys, split them into two parts and store each part on a separate password protected USB token connected to the appliance.

The Master Keys are generated and split into the two parts using SSS algorithm. The USB tokens are formatted, their password set and the key parts are written into them. Each USB token is given to a different CO (Appliance Administrator). For a complete list of the master keys refer to section 2.6.3.

3.4.2 Installing the DocuSign QSCD Appliance

The appliance installation is performed by the Appliance Administrators using the GUI based client application. Installation commands are sent to the appliance over secure TLS 1.2 channel.

As explained in 3.4.1, two USB tokens with the split Master Keys are required for this operation. Each is password protected and belongs to a different CO. Thus, to complete the appliance installation, each CO must separately authenticate after inserting the token in their possession.

During installation, the CO performs the following security related actions:

- **Select Appliance Type** – The appliance type is selected: HSM mode, Advanced signatures or Qualified signatures.
- **Define Appliance Administrator** – The name and password of the Appliance Administrator is defined.
- **Define Users Administrator** – The name and password of the Users Administrator is defined.
- **Load Master Keys** – The Master Key components are read from the first and second USB tokens, rebuilt using SSS, and placed in the module's internal tamper device memory.

After installation, the CO (Appliance Admin) can set additional parameters like the appliance IP address, supported TLS cipher suites, default RSA key size, NTP servers and many more.

3.4.3 Setting the Appliance to FIPS Mode

To set the module in FIPS mode, the CO has to set the tls_mechanisms_mode parameter to value of 1. This will restrict the module to use only the RSA based TLS cipher suites (TLS_RSA_WITH_AES_128_CBC_SHA256 and TLS_RSA_WITH_AES_256_CBC_SHA256).

3.5 Backup and Restore of the DocuSign QSCD Appliance

The appliance offers a backup operation so that in the case of a technical failure, it will be possible to restore all the information of the database to a new appliance. The backup operation does not contain any key material such as pre-generated RSA keys, but it does contain the following information from inside the appliance:

- System Parameters
- Trusted Anchors (for example, public keys used to verify SAML/JWT tickets)
- Administrators account information

The restoration of an appliance is based on the following components:

- **Backup USB Tokens**
  A set of two backup USB tokens. From these tokens the whole set of Master Keys are rebuilt using SSS.
- **Backup File**
  An encrypted and MACed backup file that includes all the required information for a complete restore of the appliance. The information includes all entities in the database as well as some additional configuration information.

When the CO performs the backup operation using the dedicated REST API operation, a protected backup file is prepared by the appliance and downloaded to the Administrative workstation. The file must be accessible only to the COs that hold the USB tokens.

To restore an appliance, it first must be installed using the two backup USB tokens. Then, a restore database operation is performed with the provided backup file.

3.6 Reset Tamper

When an Appliance enters Tamper state, a blinking **Tamper** message appears on the appliance display. In this state, the appliance does not provide any service except the ability for the COs to perform the reset tamper operation. The two appliance administrators with the matching USB tokens are required to perform this process. Each CO has to insert his/her USB token and supply its password.

Warning: If you suspect the appliance has been tampered with, contact DocuSign Support via the following web page: https://support.docusign.com/en/contactSupport.

The reset tamper operation should be performed only if you are sure that the tamper event occurred as part of a maintenance operation or a controlled operation.

3.7 REST API

All commands to the DocuSign QSCD Appliance use the REST API, which is based on HTTPS (HTTP over TLS).

The module's REST API provides access to several categories of commands:

- Appliance setup
- Appliance admin
- User management
- Cryptographic operations

Most API calls require additional Administrator authentication or User authentication.

3.7.1 REST Command/Response

After a command is sent to the module, its input parameters are checked with improper or wrong parameters rejected with an error code returned. Correct commands are executed, with the reply sent back to the client over the secure channel.

The request is based on the following parameters:

- The operation's name
- Input parameters in JSON format

The response is based on the following parameters:

- Response return code (an integer)
- Output parameters in JSON format

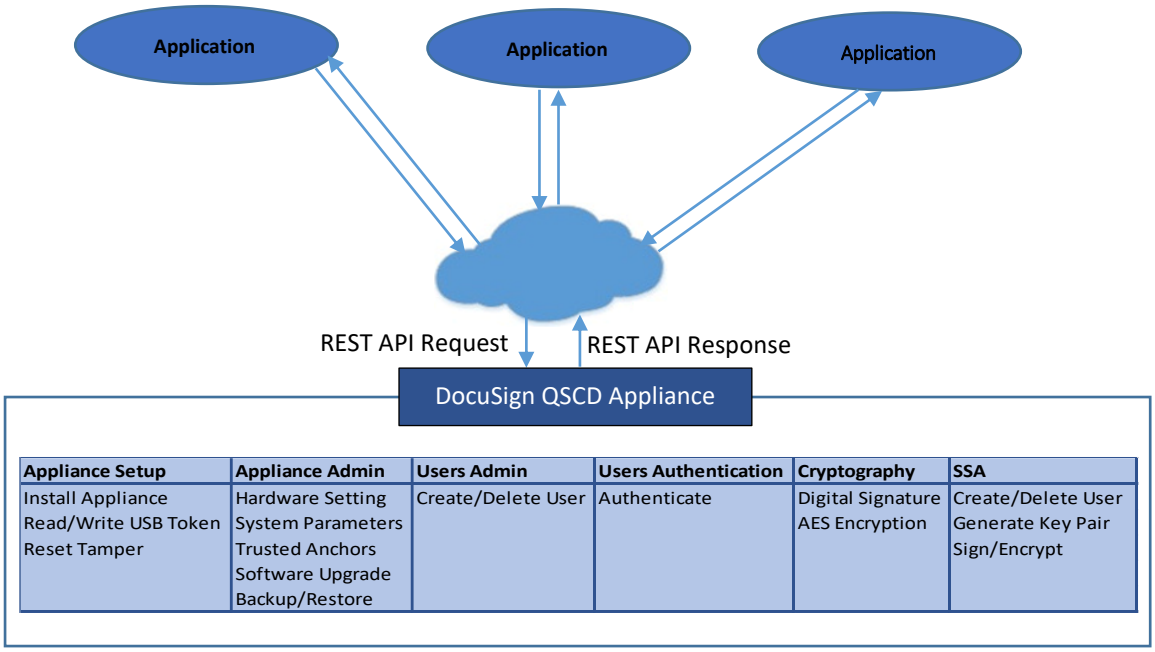

Figure 5 – DocuSign QSCD Appliance API Model

3.8 Error State

Failure in any of the power-up or the critical function tests results in entering error state. The QSCD appliance software terminates and the module does not provide any cryptographic services to the users. A corresponding message is written into the QSCD appliance log file. A short error message appears in the display in the front panel of the appliance that indicates the type of error.

Error	Meaning
CryptoError	Failed cryptographic KAT
SSLError	Failed cryptographic KAT of the TLS library
TamperHWFailure	Failed to communicate with the tamper board
TamperMismatch	The hash of the data in the tamper memory does not match the expected value or is not equal to the value stored in the QSCD appliance database
SWVerifyError	Failed to verify the firmware signature
DBError	Failed database connectivity check
CriticalError	Failed to execute any of the self-tests above

Table 11 – Error States

For more information about each error, refer to section 2.8.

3.9 Firmware Update

Firmware upgrades are sent to customers through DocuSign support channels. Each software upgrade is digitally signed using the private key corresponding to the FIRM-SIG key controlled by DocuSign engineering. Only CMVP validated versions are allowed to be uploaded.

Firmware upgrade can be performed only by the appliance administrator. Two REST API function calls are needed to perform this operation: Authenticate and Software Upload.

3.9.1 Authenticate Command

The Authenticate command is used to authenticate as the appliance administrator. It returns a JWT token that is later used to perform the Software Upload command.

Command	POST	https://{QSCD}:9091/api/v1/auth

Body	<pre>{
	"login_name" : "{ApplianceAdministrator}",
	"password" : "{ApplianceAdministratorPassword}"
	}</pre>	

Response	<pre>{
	"id": "a053d06c-4b67-cc6a-c745-8677bf3ab6e6",
	"login_name": "appliance_administrator",
	"type": "appliance_admin",
	"valid_thru": "2022-11-30T16:09:04.6736587Z",
	"appl_name": "QSCD0004",
	"jwt": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpX
	....
	tsdUnoX2AoC55XGHGhei-CPbaNL2I2aC"
	}</pre>	

Table 12 – Authenticate command

3.9.2 Software Upload Command

The Software Upload command loads the signed upgrade package. After the software is loaded into the module by the CO, the signature is verified using FIRM-SIG, which is embedded in the module's firmware. If the verification fails, the module returns an error code and the loaded software is discarded.

Command	POST	https://{QSCD}:9091/api/v1/software
Header: Authorization bearer	JWT ticket that was returned by the Authenticate command	
Body	Contents of software upgrade file	

Response	{
	"id":"bd6a5aac-b704-6f93-f6d8-2e5e30908170",
	"upgrade_progress_info": "upgrading",
	"code": 0,
	"file_name": "UpgradeVer_1_0_0_9.dsp",
	"install_time": "2022-05-25T04:36:16.3383505Z"
	}	

Table 13 – Software Upload command

3.10 Checking FIPS Mode

To verify that the module is operating in FIPS compliant mode, check the appliance display and call two REST API functions: Get Status and Get System Parameters.

3.10.1 Appliance Display

Verify that the appliance display shows a message that it has been installed.

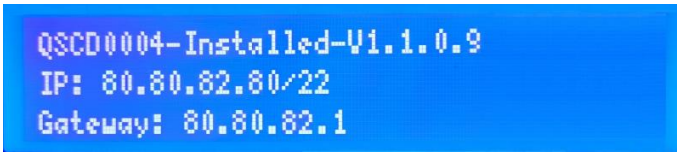

Figure 6 – DocuSign QSCD Appliance in FIPS mode (Installed State)

3.10.2 Get Status Command

The Get Status command queries the appliance's state. Verify the correct status (installed), hardware version (2.0.0.0) and software version (1.1.0.9).

Command	GET	https://{QSCD}:9091/api/v1/appliance

Response	<pre>{
	"name": "QSCD",
	"device_id": "eef8ebc4-f64d-a76c-5c65-6c18eef7ee4b",
	"sw_version": "1.1.0.9",
	"hw_version": "2.0.0.0",
	"md_version": "1.1.0.0",
	"time": {
	"use_ntp": false,
	"ntp_server": "0.0.0.0",
	"time": "2022-01-12T10:06:28.5442185Z"
	},
	"network": {
	"use_dhcp": false
	},
	"status": "installed",
	"kind": "key_gen_sign_hsm",
	"install_mode": "hsm",
	"cluster_id": "awhyIQJ2MXk=",
	"cluster_description": "Description",
	"state": "ok",
	"state_text": "On",
	"database_id": "dfac0fec-6876-4d68-8468-e2e4167e03e6",
	"debug_log_level": 0
	}</pre>	

Table 14 – Get Status command

3.10.3 Get System Parameters Command

The Get System Parameters command queries the supported TLS cipher suites. In FIPS mode, only RSA based cipher suites (TLS_RSA_WITH_AES_128_CBC_SHA256 and TLS_RSA_WITH_AES_256_CBC_SHA256) are enabled. Verify the that the value of the system parameter tls_mechanisms_mode is 1, meaning only RSA cipher suites are enabled.

Command	GET	https://{QSCD}:9091/api/v1/sysparams/tls_mechanisms_mode

Response	<pre>{
	"kind": "tls_mechanisms_mode",
	"name": "TLS Mechanisms Mode",
	"description": "0 - All mechanisms are available
	1 - RSA mechanisms only
	2 - ECDH mechanism only",
	"category": "general",
	"value_type": "int_type",
	"value": 1,
	"modifiable": true,
	"min_value": 0,
	"max_value": 2,
	"display": true,
	"display_order": 8
	}</pre>	

Table 15 – Get System Parameters command

3.11 Module Inspection

The CO must perform a scheduled inspection of the module to detect tamper evidence, by inspecting two areas for tamper evidence:

1. Check the module's front panel and physical interfaces
2. Check the Tamper Evident can, which is located on the back of the module