DocuSign®

DocuSign QSCD Appliance

Hardware version 2.0.0.0
Firmware version 1.2.0.7

FIPS 140-3 Non-Proprietary
Security Policy

Level 3 Validation

August 2024
Document Version 1.7

Table of Contents

List of Tables

List of Figures

1 General

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 140-3, and how to operate the appliance in a secure FIPS 140-3 compliant mode.

This document was prepared as part of the FIPS 140-3 level 3 validation of the DocuSign QSCD Appliance. It fulfils the security policy requirements as specified in ISO/IEC 19790:2012, B.2.1 to B.2.12 and in NIST Special Publication 800-140B, CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B.

The following table lists the module's FIPS 140-3 security level for each individual area.

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services and authentication	3
5	Software/Firmware security	3
6	Operational Environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameters management	3
10	Self-Tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A

Table 1 – FIPS 140-3 Section Security Level

1.1 Background

FIPS 140-3 (Federal Information Processing Standards Publication 140-3 -- *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 140-3 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 140-3 cryptographic module security policy. Additional information about DocuSign QSCD Appliance and other DocuSign products is available at www.docusign.com.

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

1.2 Terminology

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

Term	Meaning
API	Application Programming Interface
APT	Adaptive Proportion Test
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
COC	Certificate of Compliance
COTS	Commercial Off The Shelf
CRC16	Cyclic Redundancy Check (16 bit)
CSP	Critical Security Parameters
DTBS	Data To Be Signed
ECDHE	Ephemeral Elliptic Curve Diffie-Hellman
EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
ESV	Entropy Source Validation
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware Security Module
IDP	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
KAT	Known Answer Test
KDF	Key Derivation Function
KTS	Key-Transport Scheme
LCD	Liquid Crystal Display
MAC	Message Authentication Code
NIC	Network Interface Controller
NTP	Network Time Protocol
PBKDF	Password-Based Key Derivation Function
PCB	Printed Circuit Board

Term	Meaning
PSP	Public Security Parameters
QSCD	Qualified Signature Creation Device
RCT	Repetition Count Test
REST	Representational state transfer
SAML	Security Assertion Markup Language
SCA	Signature Creation Application
SHS	Secure Hash Standard
SSA	Server Signing Application
SSD	Solid State Drive
SSP	Sensitive Security Parameter
SSS	Shamir Secret Sharing
TLS	Transport Layer Security
TSP	Trust Service Provider

Table 2 – Terminology

2 Cryptographic Module Specification

2.1 Module Overview

The DocuSign QSCD Appliance is a digital signature product intended to be used as a Qualified Signature Creation Device (QSCD) in a secure operational environment. It is a highly secure, high capacity network attached HSM. The device consists of COTS hardware, tamper resistance hardware, a hardened operating system, an internal database and server software.

The key features of the appliance are:

- RSA digital signatures and verification
- AES encryption and decryption
- Authenticated and encrypted communication with the appliance
- REST protocol over HTTPS (HTTP over TLS 1.2)
- Tamper-responsive enclosure
- Secure backup capability

Figure 1 – The Module's Front and Rear View

2.2 Module Identification

Model	Hardware version	Firmware version	Distinguishing Features
DocuSign QSCD Appliance	2.0.0.0	1.2.0.7	Module type: hardware Embodiment: multi-chip standalone appliance The module is operating in FIPS compliant mode: • It is in the installed state • Only ECDHE_RSA_AES_GCM cipher suites are enabled

Table 3 – Cryptographic Module Tested Configuration

2.3 Hardware Architecture

2.3.1 Cryptographic Boundary

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.

2.3.2 Hardware Block Diagram

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

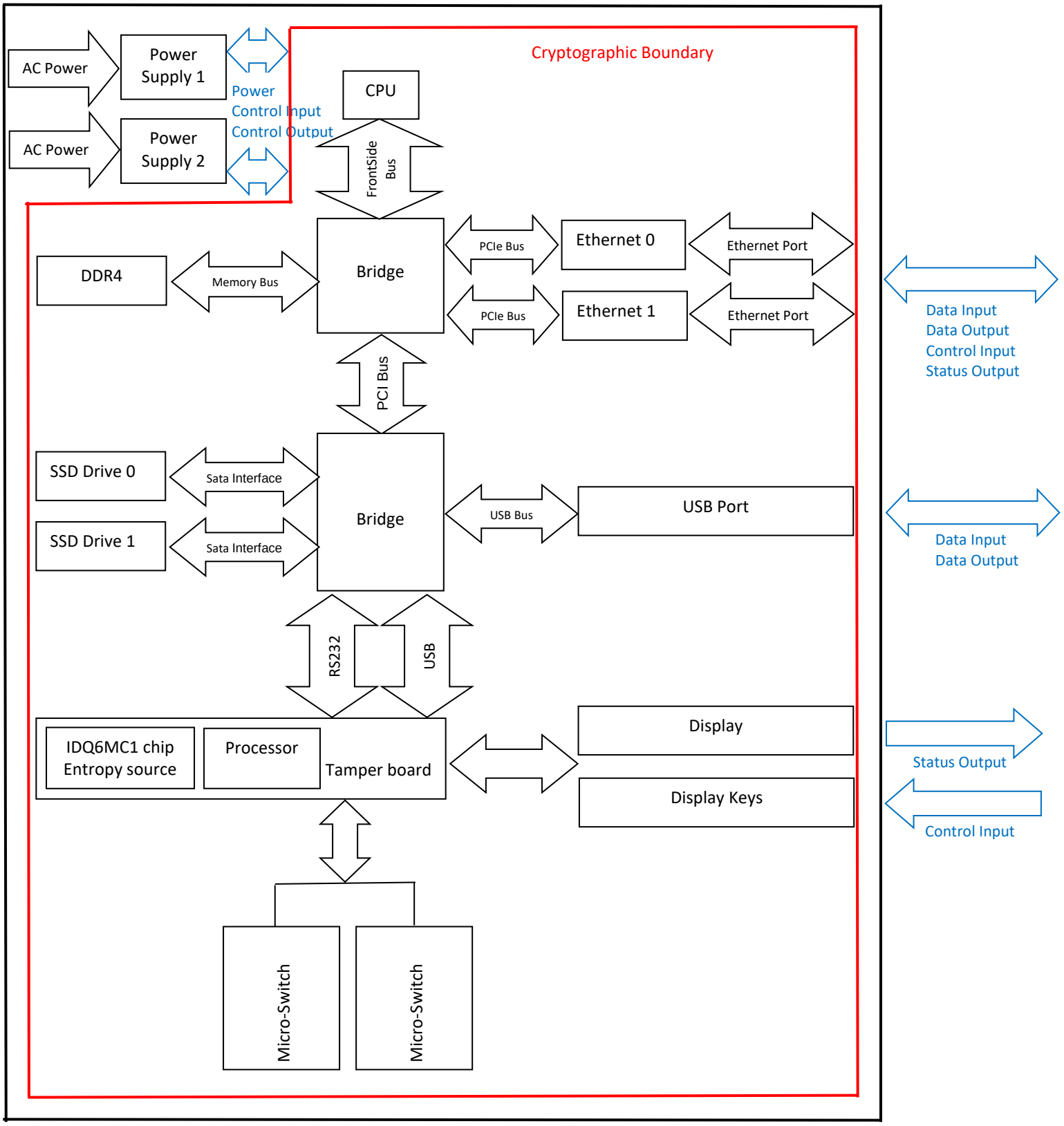

Figure 2 – DocuSign QSCD Appliance Hardware Block Diagram

2.3.3 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.

2.4 System Architecture

DocuSign QSCD Appliance is installed in a secure operational environment and interacts with other software components and services.

2.4.1 Components of QSCD Secure Environment

The following figures illustrates the secure environment architecture of a TSP (Trust Service Provider).

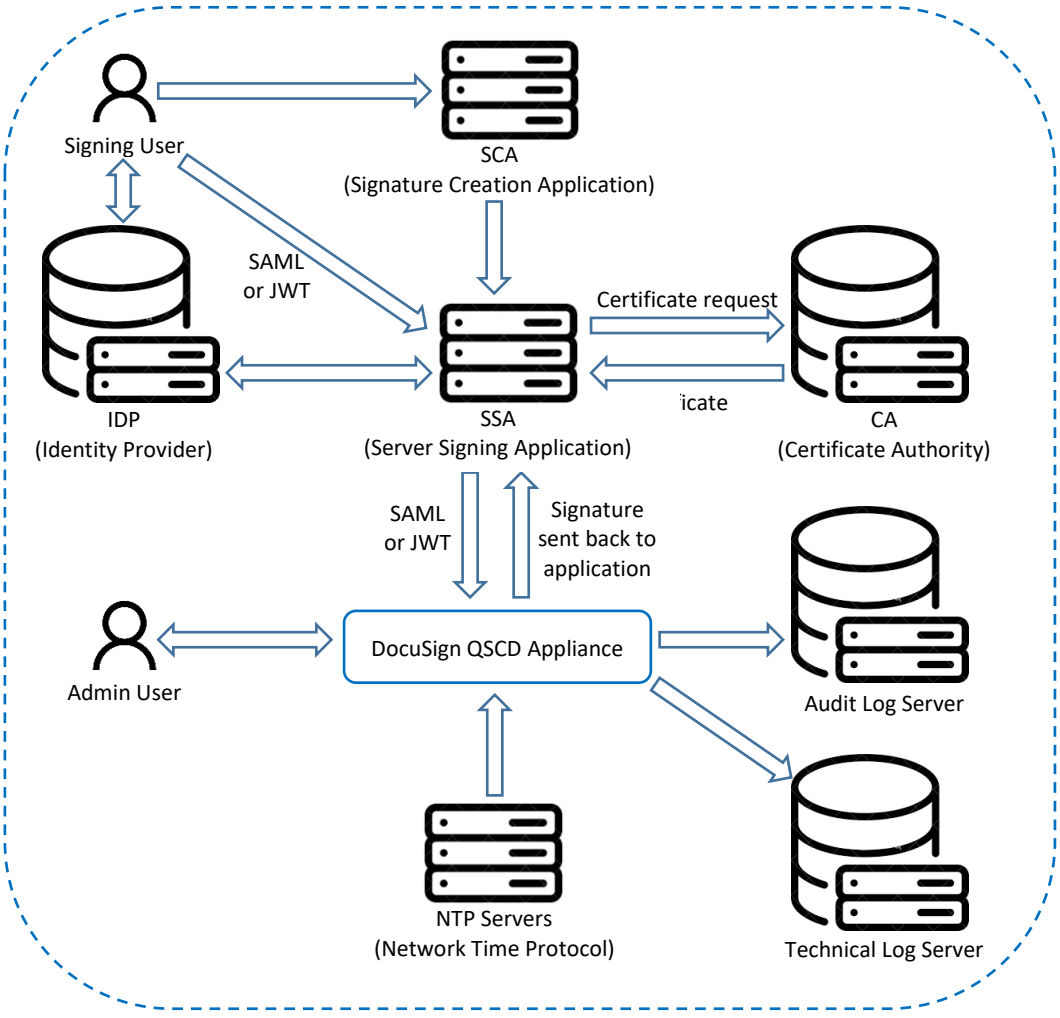

Figure 3 – DocuSign QSCD Secure Operational Environment

The DocuSign QSCD operational environment includes the following components:

- **SSA (Server Signing Application)**
  The SSA is a Web application that enables the signer to perform digital signatures through a web interface. For detailed explanation about the signing process performed by the SSA, refer to section 2.4.2.
- **IDP (Identity Provider)**
  The IDP authenticates the signer and provides a proof of authentication in the format of a signed

SAML or JWT token. The DocuSign QSCD validates the SAML token and enables the signer to access his/her signature key.

- **SCA (Signature Creation Application)**
  The SCA is an application that is executed in the user's PC or in a web application. Prior to the signature process, the SCA presents the data to be signed (DTBS) for review by the signer in order to obtain the signer's decision. The SCA interacts with the SSA for the purpose of digital signature creation. The SSA replies to the SCA with a digital signature, and the SCA incorporates the digital signature in the document.
- **CA (Certificate Authority)**
  The CA generates certificates for signers based on the signature key generated in the Appliance. The SSA interfaces with the CA; it sends the certificate request to the CA and the CA replies with a certificate.
- **Audit Logs Server**
  All audit information is sent to an external audit log server.
- **Technical Logs Server**
  Some technical logs information is sent to an external server.
- **NTP Server**
  The DocuSign QSCD is synchronized with the NTP servers to ensure it has accurate time.
- **Administrator Machine**
  Administrators can connect remotely to the Appliance using TLS protocol and perform administrative operations.

2.4.2 SSA (Server Signing Application)

The SSA is a Web Application that is deployed in the operational environment and enables the signer to perform digital signatures through a web interface. It is the application that interacts with the user while performing cryptographic operations, acting as a proxy between the user and the module, so some of the operations it performs are on behalf of the user.

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.

2.5 Software Architecture

2.5.1 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.

2.5.2 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

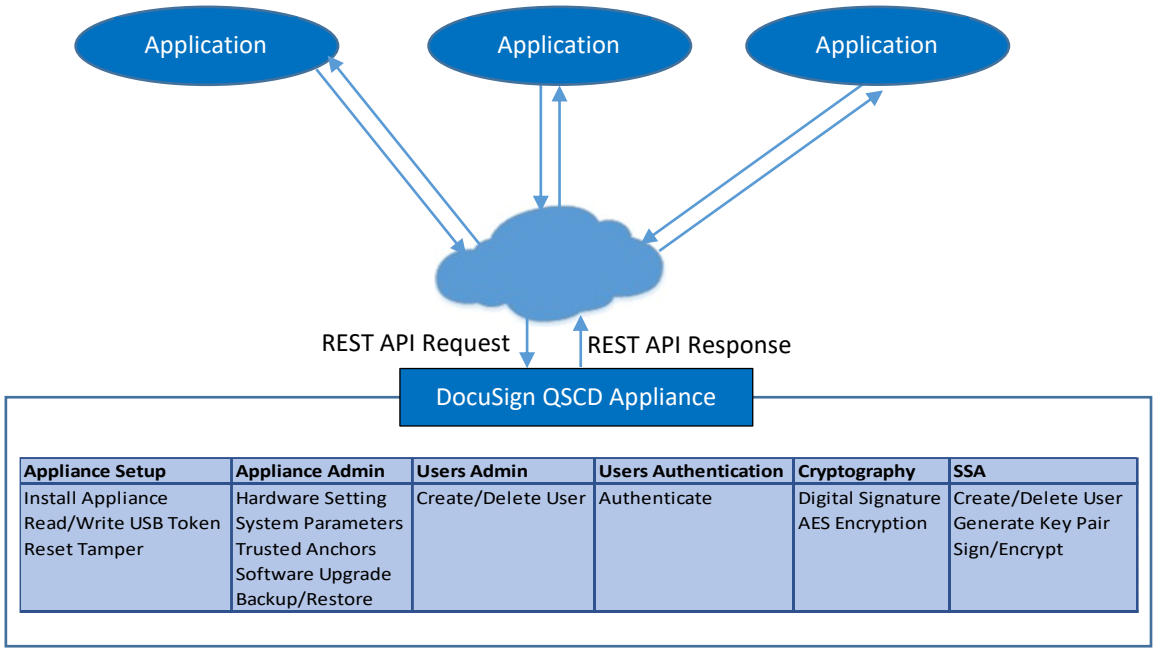

Figure 4 – DocuSign QSCD Appliance API Model

2.6 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 or more 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. The transition to Tamper state will happen in any case the appliance has been tampered with, regardless of the appliance being in Factory or Operational state.

Figure 5 below shows the transitions between the three states.

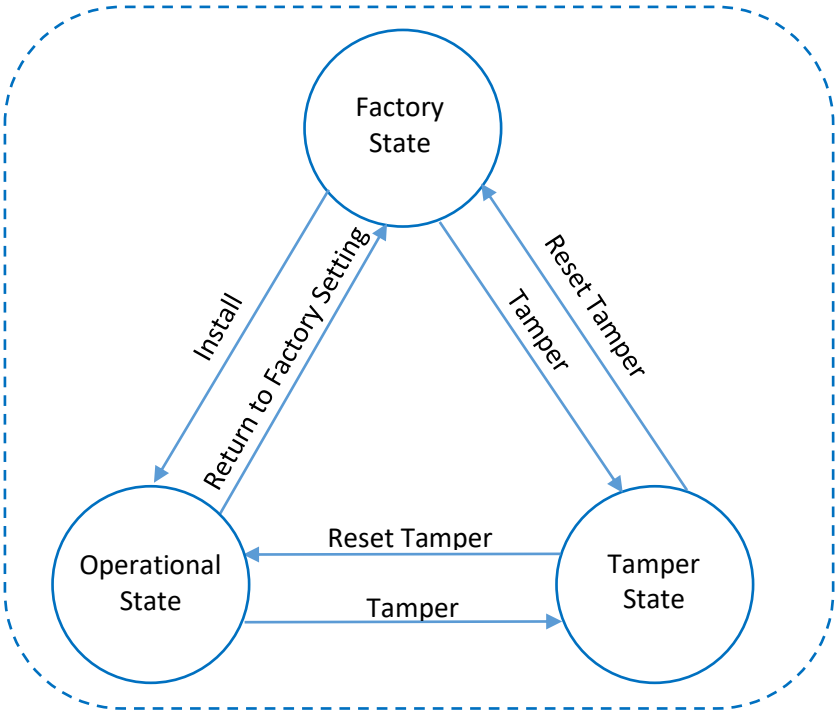

Figure 5 – QSCD States

2.7 Modes of Operation

While the QSCD is in Operational state, it can be in either FIPS or non-FIPS mode. The distinction between these two modes depends on the selected TLS cipher suite. When operating in FIPS mode the QSCD must use only the ECDHE_RSA_AES_GCM based cipher suites. Refer to section 2.12 for instructions how to check if the module is operating in FIPS compliant mode.

2.8 Error States

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
TamperCrcError	Failed to validate the tamper firmware CRC16
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
Tamper	A tamper event occurred
SWVerifyError	Failed to verify the firmware signature
DBError	Failed database connectivity check
CriticalError	Failed to execute any of the self-tests above

Table 4 – QSCD Error States

For more information about each error, refer to section 10.

2.9 Cryptographic Algorithms

The DocuSign QSCD Appliance supports a variety of cryptographic algorithms, and implements these algorithms based on the different cryptographic standards.

2.9.1 Approved Cryptographic Algorithms

The module supports the following approved algorithms:

CAVP Cert.	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/Function
Core Cryptographic Algorithms				
A4400	AES FIPS 197	CBC	AES / 128, 192, 256 bits / 128, 192, 256 bits	Data Encryption
Vendor affirmed	CKG[1] SP 800-133		DRBG Key / 256 bits / 256 bits	Key Generation
A4400	HMAC FIPS 198-1	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	HMAC / 256, 256, 256 bits / 256, 256, 256 bits	Message Authentication
A4400	HMAC_DRBG SP 800-90A	HMAC-SHA-256	HMAC / 256 bits / 256 bits	Deterministic Random Number Generation
A4400	RSA FIPS 186-5	Appendix A.1.6 Table B.1 (2^{-100})	RSA Key Generation/ 2048, 3072, 4096 bits / 112, 128, 128 bits	Key Generation
A4400	RSA PKCS#1 v1.5	SHA-256, SHA-384, SHA-512	RSA-PKCS#1 2048, 3072, 4096 bits / 112, 128, 128 bits	Digital Signature Generation
A4400	RSA PKCS#1 v2.1	PSS-SHA-256, PSS-SHA-384, PSS-SHA-512	RSA-PSS 2048, 3072, 4096 bits / 112, 128, 128 bits	Digital Signature Generation
A4400	RSA PKCS#1 v1.5	SHA-256, SHA-384, SHA-512	RSA-PKCS#1 2048, 3072, 4096 bits / 112, 128, 128 bits	Digital Signature Verification
A4400	SHS FIPS 180-4	SHA-256, SHA-384, SHA-512	SHA2 / None / 128, 192, 256	Message Digest Hash for digital signature Generation
E10	ESV SP 800-90B	N/A		Seeding/reseeding the DRBG

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

CAVP Cert.	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/Function
TLS (OpenSSL) Cryptographic Algorithms				
A4404	AES FIPS 197	CBC	AES / 128, 256 bits / 128, 256 bits	TLS Session Schema Session data encryption
A4404	AES FIPS 197	GCM[1]	AES / 128, 192, 256 bits / 128, 192, 256 bits	TLS Session Schema Session data encryption
A4404	CVL TLS 1.2 SP 800-135rev1	SHA-256, SHA-384	SHA2 / None / 128, 192 bits	TLS Key Derivation[2]
A4404	HMAC FIPS 198-1	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	HMAC / 256, 256, 256 bits / 256, 256, 256 bits	TLS Session Scheme
A4404	SHS FIPS 180-4	SHA-256, SHA-384, SHA-512	SHA2 / None / 128, 192, 256	TLS Session Schema
A4404	Elliptic Curve FIPS 186-5	Appendix A.2.2	P-256, P-384, P-521 / 256, 384, 521 bits / 128, 192, 256 bits	Elliptic Curve Key Generation
A4404	KAS-ECC-SSC Sp800-56Ar3	ECC Ephemeral Unified Scheme	P-256, P-384, P-521 / 256, 384, 521 bits / 128, 192, 256 bits	Key Exchange[3]
A4404	PBKDF[4] SP 800-132	Option 1a	256 bits	Password based key derivation
A4404	RSA PKCS#1 v1.5	SHA-256, SHA-384, SHA-512	RSA-PKCS#1 / 2048, 3072, 4096 bits / 112, 128, 128 bits	Digital Signature Generation
A4404	Elliptic Curve FIPS 186-5	ECDSA	P-256, P-384, P-521 / 256, 384, 521 bits / 128, 192, 256 bits	Digital Signature Generation[5]
A4404	Elliptic Curve FIPS 186-5	ECDSA	P-256, P-384, P-521 / 256, 384, 521 bits / 128, 192, 256 bits	Digital Signature Verification[1]

Table 5 – Approved Algorithms

[1] Implementation of AES-GCM complies to NIST SP 800-56Ar3 guidelines. IV is generated internally using the approved DRBG. A 64-bit counter is used, to assure that no two encryptions will use the same counter value.

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

[3] As per IG D.F Scenario 2 path (2), the CAVP testing is performed in which case it is split into (i) testing the computation of the shared secret, (ii) testing the key derivation function used in deriving the keying material as per SP800-135 Rev 1

[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.

[5] This algorithm, mode, and key/moduli sizes have been CAVP-tested but are not used by any approved service of the module

2.9.2 Non-Approved Algorithms

The module supports the following non-approved algorithms which are not allowed in the approved mode of operation:

Algorithm/Function	Use/Function
RSA Key Transport (KTS)	Key establishment methodology using PKCS#1-v1.5 provides between 112 and 256 bits of encryption strength

Table 6 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.10 Module 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 or more parts and written on password protected USB tokens; each belonging to a different CO.
- **Copying the USB Tokens** – It is possible to duplicate a USB token that contains appliance Master Key part.
- **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.

2.10.1 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 parts and store each part on a separate password protected USB token connected to the appliance.

The QSCD Appliance Master keys are protected using M of N protection measure, which requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high-security tasks such as QSCD installation. The Master Keys are split into N parts, but during installation, only M out of N parts will be required to successfully build the Master Keys and install the appliance. The minimum number of N parts is 2 and the maximum is 9. The value of M has to be smaller or equal to N.

After the Master Keys are generated they are split into N 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). Later, during installation, the Master Keys are built using M parts out of N using the SSS algorithm. For a complete list of the master keys refer to section 9.1.

2.10.2 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 2.10.1, M out of N 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 N out of M 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.

2.11 Setting the Appliance to FIPS Mode

To set the module in FIPS mode, the CO has to set the appliance to use only the ECDH based TLS cipher suites

(TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384). Use the Set System Parameters command to set the value of the system parameter tls_mechanisms_mode to 2, meaning only the ECDH cipher suites are enabled.

Command	PUT	https://{QSCD}:9091/api/v1/sysparams/tls_mechanisms_mode
Header	Content-Type: application/json	
Header	Authorization: Bearer JWT ticket that was returned by the Authenticate command	

Body	{
	"value":"2"
	}	

Response	204 No Content	

Table 7 – Set System Parameters command

2.12 Checking FIPS Mode

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

2.12.1 Appliance Display

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

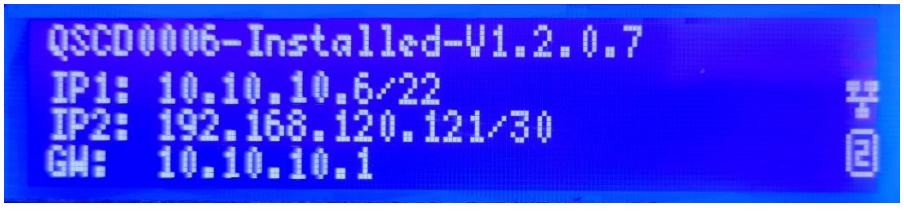

Figure 6 – DocuSign QSCD Appliance in FIPS mode (Installed State)

2.12.2 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 (1.2.0.7).

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

Response	{
	"name": "QSCD",
	"device_id": "eef8ebc4-f64d-a76c-5c65-6c18eef7ee4b",
	"sw_version": "1.2.0.7",
	"hw_version": "2.0.0.0",
	"md_version": "1.2.0.0",
	"time": {
	"use_ntp": false,
	"ntp_server": "0.0.0.0",
	"time": "2023-07-12T10:06:28.5442185Z"
	},
	"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
	}	

Table 8 – Get Status command

2.12.3 Get System Parameters Command

The Get System Parameters command queries the supported TLS cipher suites. In FIPS mode, only ECDH based cipher suites should be enabled (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384). Verify the that the value of the system parameter tls_mechanisms_mode is 2, meaning only the ECDH cipher suites are enabled.

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

Response	{
	"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": 2,
	"modifiable": true,
	"min_value": 0,
	"max_value": 2,
	"display": true,
	"display_order": 8
	}	

Table 9 – Get System Parameters command

2.13 Backup and Restore

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 M out of N 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 M out of N backup USB tokens. Then, a restore database operation is performed with the provided backup file.

2.14 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. M out of N appliance administrators with the matching USB tokens are required to perform this process. Each administrator 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.

2.15 Firmware Update

Firmware upgrades are sent to customers through DocuSign support channels. Each software upgrade package is digitally signed using 3072-bit RSA private key controlled by DocuSign engineering corresponding to the public key FIRM-SIG. If the signature verification fails, the module returns an error code and the loaded software is discarded. 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.

2.15.1 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
Header	Content-Type: application/json	

Body	{
	"login_name" : "{ApplianceAdministrator}",
	"password" : "{ApplianceAdministratorPassword}"
	}	

Response	{
	"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"
	}	

Table 10 – Authenticate command

2.15.2 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	Content-Type: multipart/form-data	
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 11 – Software Upload command

3 Cryptographic Module 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.

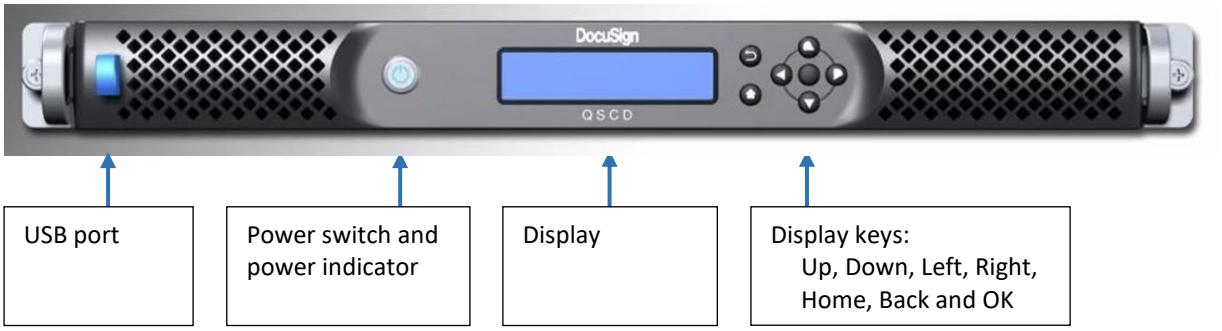

Figure 7 – The Module's Front View

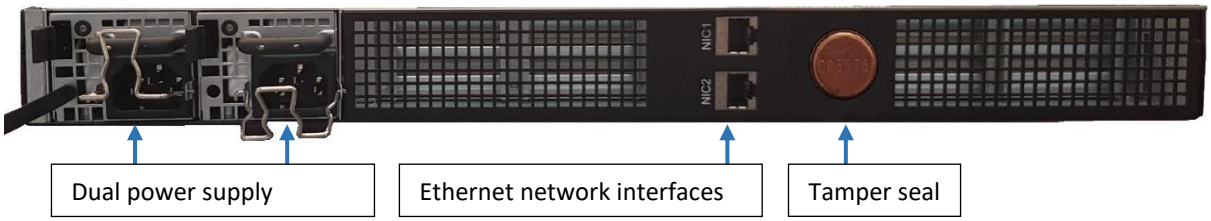

Figure 8 – The Module's Rear View

3.1 Logical and Physical Interfaces

The following table shows the mapping of the FIPS 140-3 logical interfaces to the module's physical interfaces.

Logical Interface	Physical Port	Data that passes over port/interface
Data Input Interface	Ethernet Network ports	Ciphertext data, ciphered cryptographic keys, device management data, device configuration data, ciphered authentication data, status information, and other key management data
	USB port for smartcard-based token[1]	Cryptographic keys
Data Output Interface	Ethernet Network ports	Ciphertext data, ciphered cryptographic keys, device management data, device configuration data, ciphered authentication data, status information, and other key management data
	USB port for smartcard-based token[2]	Cryptographic keys

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

[2] Used only during pre-installation when generating or copying Master Keys on the USB token

Logical Interface	Physical Port	Data that passes over port/interface
Control Input Interface	Ethernet Network ports	Input commands, input data
	Display keys	Input commands
	On/Off Power switch	Input commands
	Power connectors	Input signals
Control Output Interface	Power connectors	Output signals
Status Output Interface	Ethernet Network ports	Status output data
	LCD display	Status output data
	LED indicators	Output indicators
Power Interface	Power connectors	Power

Table 12 – Ports and Interfaces

Commands sent through the network port 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 power connector has control input and control output signals between the external power supplies and the cryptographic boundary of the module. The signals only control the power mechanism of the module and are not inhibited whenever the module is in error state.

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.

3.2 LEDs and Indicators

The front of the module has several indicators and control buttons:

- The LCD display 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 display also shows different error messages (see sections 2.8 and 10).
- On/off power button with power indicator. The power switch has a dual-colored LED:
  - A steady blue indicates that the device is running normally
  - A flashing red indicates a malfunction, such as bad memory, stopped fan, loss of one of the two power sources, etc.
- Display keys (Up, Down, Left, Right, Home Back and OK) which are used to operate the appliance for example when performing comprehensive restore factory

The rear of the module has two field replaceable power supplies. Each power supply unit is connected to a power network and includes a status LED whose color indicates the unit's power status:

- A steady green indicates that power is applied (110-220V)
- A blinking red and a continuous audible alert indicate that power is not applied to this unit but applied to the other unit

4 Roles, Services, and Authentication

4.1 Roles

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.

4.1.1 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:
  - Install 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)
  - 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
  - Modify the debug level to control which information will be written to the technical log

- **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

4.1.2 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.

4.2 Services

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

Category	Role	Service	Input	Output
TLS Session[1]	CO, User, Anonymous	TLS Session establishment	QSCD and client random data, QSCD certificate	TLS session and ephemeral keys
	CO, User, Anonymous	Close TLS session	None	None
Appliance Setup	CO	Install appliance	Master keys	Success code
	CO	Write USB token	Master keys	Split Master Keys on USB token
	CO	Read USB token	Split Master Keys from USB token	Master Keys in tamper memory
	Anonymous	Reset tamper	Split Master Keys from USB token	Master Keys in tamper memory
	CO	Restore factory	None	None
Appliance Administration	CO	Set time from NTP	NTP input	None
	CO	Monitoring	None	Status and audit log
	CO	Update network setting	Input data	Success code
	CO	Update time setting	Input data	Success code
	CO	Set system parameters	Input data	Success code
	CO	Manage Trusted Anchors	Input data	Success code
	CO	Perform software upgrade	Signed software file	Success code
	CO	Perform backup	None	Encrypted backup file
	CO	Restore from backup	Encrypted backup file	Success code
	CO	Get technical log	None	Log file
	CO, Anonymous	Get appliance information	None	Appliance information
	CO	Restart	None	None
	CO	Shutdown	None	None
User Administration	CO	Create Administrator user	New Administrator User info	Success code
	CO	Delete Administrator user	User ID	Success code

[1] The TLS session service is used by all other QSCD services as it establishes the basic communication channel with the module, on which the REST API functions are sent.

Category	Role	Service	Input	Output
	CO	Get users list	None	Users list
	CO	Get user details	User ID	User information
	CO	Change password	New password	Success code
	CO	Unlock Administrator user	User ID	Success code
Authentication	CO, User	Authenticate	User ID, Authentication data	Success code
Cryptographic Operations	User	Digital signature	Encrypted key blob, input buffer	Output buffer
	User	Encryption/Decryption	Encrypted key blob, input buffer	Output buffer
	User, Anonymous	Get random	Required length of random data	Random data
SSA Administrator	CO	Create User	User information	Encrypted user blob
	CO	Delete User	User ID	Success code
	CO	Generate User key pair/key	User ID	Encrypted key blob
	CO	Delete User key pair/key	User ID	Success code
	CO	Supply DTBS	User ID, input buffer	Success code
	CO	Collect result	User ID	Output buffer

Table 13 – Roles, Service, Input and Output

4.3 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. In this case, the JWT ticket is protected by AES 256 bit key (MK-JWT) and HMAC-SHA-256 algorithm.

Users also use identity-based authentication indirectly by authenticating to an external Identity Provider (IDP) which generates a SAML or JWT ticket. The SAML/JWT ticket is then used to verify the user in all subsequent REST API commands. In this case the SAML/JWT ticket is protected by RSA private key whose public key is stored in the appliance trusted anchors (TRUSTED-ANCHORS).

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

Role	Authentication Method	Authentication Strength
CO	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.
CO	SAML/JWT ticket protected by RSA 2048 bit key[1]	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 x 60)) probability of a successful random attempt during a one-minute period. This is exponentially less than 1 in 100,000.

[1] The calculation is performed for the smallest supported RSA key size (2048 bit). When using larger RSA keys (3072 and 4096 bit), the probabilities are even smaller.

Role	Authentication Method	Authentication Strength
CO	JWT ticket protected by AES-256 bit key	The JWT token is based on a HMAC-SHA-256 with AES 256 bit key which has security strength of 256 bit. The probability that random access will succeed is 1 / (2^{256}) which is far less than one in 1,000,000. The appliance cannot process more than 10000 JWT validations per second, thus the authentication provides a 1 in (2^{256} / (10000 x 60)) probability of a successful random attempt during a one-minute period. This is exponentially less than 1 in 100,000.

Table 14 – Roles and Authentication

4.4 Approved Services

The following table shows for specific service, which role has access to it and which SSP and access type is used to provide the service. Refer to section 9.1 for the description of the SSPs used by each operation.

The convention below applies to the following table when specifying the access permissions (types) that the service has for each SSP:

- **G = Generate** The module generates or derives the SSP
- **R = Read** The SSP is read from the module (e.g. the SSP is output)
- **W = Write** The SSP is updated, imported, or written to the module
- **E = Execute** The module uses the SSP in performing a cryptographic operation
- **Z = Zeroise** The module zeroises the SSP

Service	Description	Roles	Approved Security Functions	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
TLS session establishment	Open TLS connection between QSCD and client machine	CO, User, Anonymous	EC Key Generation FIPS 186-5	17	G	
				20	R,W,Z	
			HMAC-DRBG	18,19	G	
			HMAC-SHA-256	21,22,23	R,W	
Close TLS session	Close TLS connection between QSCD and client machine	CO, User, Anonymous	HMAC-DRBG	17,18,19	Z	
Install appliance	Enter Operational state by installing the appliance; This service is available only when the appliance is in factory state	CO	SSS, HMAC-SHA-256	1,2,3,4,5, 6,7	R,W	Message on front panel display
			RSA Generate FIPS 186-5	13	G	
Write USB token	Write key part into the USB token	CO	SSS, HMAC-SHA-256	1,2,3,4,5, 6,7	R,W	Message on front panel display

Service	Description	Roles	Approved Security Functions	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
Read USB token	Read key part from the USB token	CO	SSS, HMAC-SHA-256	1,2,3,4,5, 6,7	R,W	Message on front panel display
Reset tamper	Return to Operational state after Tamper event	CO	SSS, HMAC-SHA-256	1,2,3,4,5, 6,7,16	R,W	Message on front panel display
Restore factory	Restore the appliance back to Factory State and erase all settings	CO	AES-CBC	7	E	Message on front panel display
				All	Z	
Set time from NTP	Set module time using NTP protocol	Anonymous				
Monitoring	Send system status and audit log to external monitoring servers	CO	AES-CBC	2	E	
			Sign PKCS#1 v1.5	13	E	
Update network setting	Set network parameters for the Ethernet interfaces such as DHCP on/off, IP address, default gateway, DNS, routing table etc.	CO	AES-CBC	3,7	E	Message on front panel display
Update time setting	Set time or configure NTP server	CO	AES-CBC	3,7	E	
Set system parameters	Set system parameters like password policy, RSA key generation parameters, logging etc.	CO	AES-CBC	3,7	E	
Manage Trusted Anchors	Manage the Trusted Anchors which are used to validate SAML tickets	CO	AES-CBC	3,7	E	
				14	R,W	
Perform software upgrade	Update the firmware	CO	AES-CBC	7,9	E	
			Verify PKCS#1 v1.5, HMAC-SHA-256	12	E	
Perform backup	Backup system parameters and other settings into encrypted file	CO	AES-CBC	5,6,7	E	
Restore from backup	Restore system parameters and other settings from backup file	CO	AES-CBC	5,6,7	E	
Get technical log	Get the module's technical log files	CO	AES-CBC	7	E	
Get appliance information	Get general information such as network information, time, status, etc.	CO, Anonymous				

Service	Description	Roles	Approved Security Functions	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
Restart	Perform hardware restart	CO		7,17,18, 19,20	Z	Message on front panel display
Shutdown	Shutdown the module	CO		7,17,18, 19,20	Z	
Create Administrator user	Create administrator user	CO	AES-CBC	3,7	E	
				10	W	
Delete Administrator user	Delete administrator user	CO	AES-CBC	7	E	
				10	Z	
Get users list	Get list of users	CO	AES-CBC	3,7	E	
Get user details	Get user details	CO	AES-CBC	3,7	E	
Change password	Change password of administrator user	CO	AES-CBC	3,7	E	
				10	W	
Unlock Administrator user		CO	AES-CBC	7	E	
Authenticate	Authenticate user using user ID/password or SAML ticket	CO, User	AES-CBC	3,7	E	
				10,14	R	
Digital signature	Enable client applications to use RSA keys for digital signatures signing operations in PKCS#1 v1.5 or PSS schemas	User	AES-CBC	1,3,4,7	E	
			Sign PKCS#1 v1.5, RSA-PSS	8	E	
Encryption/ Decryption	Enable client applications to use AES keys for data encryption/decryption in CBC mode	User	AES-CBC	1,3,4,7,9	E	
Get random	Get random data	Anonymous	HMAC-SHA-256	21,22,23	R,W	
Create User	Create a user	CO	AES-CBC	1,3,4,7	E	
				8,9	W	
Delete User	Delete a user	CO	AES-CBC	7	E	
Generate User key pair/key	Generate RSA key pair/AES key on behalf of the user	CO	AES-CBC	1,3,4,7	E	
			FIPS 186-5	8,9	W	
			RSA key gen	11	R,W,Z	
			HMAC-SHA-256	21,22,23	R,W	
Delete User key pair/key	Delete the user's RSA key pair	CO	AES-CBC	7	E	
				8,9	Z	

Service	Description	Roles	Approved Security Functions	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
Supply DTBS	Supply data to be signed/encrypted	CO	AES-CBC	4,7	E	
Collect result	Collect the result of cryptographic operation	CO	AES-CBC	3,7, 9	E	
			Sign PKCS#1 v1.5, RSA-PSS	8	E	

Table 15 – Approved Services

5 Software/Firmware Security

The module performs two software and firmware integrity tests:

- **Software Integrity Test**
  The QSCD appliance's firmware is signed with an RSA 3072-bit digital signature. This signature is verified using the corresponding RSA public key (FIRM-SIG) to ensure the integrity of the software.
- **Tamper Firmware Test**
  The tamper controller firmware is embedded in an EPROM on the tamper board. The EDC used to ensure the tamper firmware integrity is CRC16.

Both tests are performed during the module power-up to ensure the software and firmware haven't been modified. The tests are run before any other service has started. If the integrity tests succeed, then all other services are started. If any of the test fail, the QSCD services will not start and the module will enter error state.

Later, those integrity tests are performed once a day as part of the periodic self-tests of the module. The CO can initiate those integrity tests on demand by requesting to restart the module by calling the restart REST API function.

6 Operational Environment

This section is not applicable for FIPS 140-3 Level 3.

7 Physical Security

7.1 Physical Security Mechanisms

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

The module is encased within a steel box rigged with a tamper-evident seal (see photo in section 3) and tamper-responsive micro-switches. Only the specified physical interfaces permit access to the module. Any intrusion attempt cause power to instantly cut off, preventing access to any useful information by zeroizing all plaintext Critical Security Parameters (CSPs) including the appliance Master Keys stored in the tamper board.

The external tamper-evident seal provides physical evidence of any attempt to tamper with the module cover. The seal, installed at the manufacturing stage, is placed over the screw that joins the top cover and the bottom enclosure. Both the seal and screw must be removed in order to open the cover of the module. If the screw is even partially removed the micro-switches are tripped and the tamper response is triggered.

There are two micro-switches, which are connected to the tamper board. One micro-switch is used for tamper detection regardless if the power is on or off and triggers zeroization of the appliance Master keys. The other micro-switch is used for tamper detection while power is on and it immediately turns off the appliance and, in that way, stops all services and zeroizes all CSPs.

Any attempt to restart the Appliance, automatically displays tamper alerts on the physical display. Only a Reset Tamper operation performed by an CO (Appliance Administrator) can set the QSCD Appliance back to an Operational state. During the Reset Tamper Operation, the COs must physically insert the M out of N USB tokens.

All vents on the module are baffled to meet FIPS 140-3 physical security requirements for opacity and probing.

7.2 Module Inspection

The CO should perform a scheduled inspection of the module to verify no physical tampering has occurred. This includes inspecting the enclosure of the appliance as well as the tamper seal and the physical interfaces as listed in the following table.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Appliance enclosure	1 year	• Inspect the appliance cover for any bent metal • Inspect the appliance external cover for any holes or drilling • Verify it is not possible to see the inner parts of the appliance and that the whole box is intact
Tamper-evident seal	1 year	• Verify that the tamper evident seal at the back of the appliance is not damaged • Verify the seal serial number matches the registered number of that appliance
USB port	1 year	• Verify no USB device is connected to the USB port
Network	1 year	• Verify that no hardware is attached to the network interfaces of the Appliance except for the cables you expect to be attached

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Environment	1 year	• Verify that there is no additional hardware or software component in the operational environment of the Appliance (such as a network sniffer, a router, etc.) that may compromise the security of the operational environment

Table 16 – Physical Security Inspection Guidelines

Figure 9 – QSCD Appliance Tamper Seal Location

If there is any suspicion that the appliance has been tampered with, contact DocuSign Support via https://support.docusign.com/en/contactSupport or email security@docusign.com.

7.3 Environment Temperature and Voltage

The following table shows the QSCD appliance response to minimum and maximum temperature and voltage values. The temperature measurement is on the air inlet into the appliance. An additional protection on the module monitors the CPU temperature and if it exceeds, the appliance will shut down to prevent possible damage to the hardware.

	Temperature or voltage measurement	EFP or EFT	Shutdown or Zeroisation
Low Temperature	+5°C	EFP	Shutdown
High Temperature	+45°C	EFP	Shutdown
Low Voltage	10.75V	EFT	Shutdown
High Voltage	12.9V	EFT	Shutdown

Table 17 – EFP / EFT

8 Non-invasive Security

No additional non-invasive mitigation techniques are employed by the module.

9 Sensitive Security Parameters Management

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

- The SSPs 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.

9.1 Sensitive Security Parameters (SSPs)

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

SSP#	SSP Name / Type	Strength (bits)	Security Function and Cert. Number	Gener-ation	Import / Export	Establish-ment	Storage	Zero-isation	Use / related keys
Master Keys									
1.	MK-EXT-KEK AES-256 bits	256	AES-CBC A4400	Internal[1]	External[2] / NA		Tamper device memory (plaintext[3])	Tamper event[4]	Critical key for key value encryption of database keys
2.	MK-INT-KEK AES-256 bits	256	AES-CBC A4400						Critical key for encryption of CSPs stored within the module
3.	MK-MAC AES-256 bits	256	HMAC-SHA-256 A4400						Critical key for HMAC-SHA-256 of database records
4.	MK-JWS AES-256 bits	256	HMAC-SHA-256 A4400						Critical key for HMAC-SHA-256 of user blobs
5.	MK-BKP-ENC AES-256 bits	256	AES-CBC A4400						Critical key for encryption of backup file
6.	MK-BKP-MAC AES-256 bits	256	HMAC-SHA-256 A4400						HMAC-256 of backup file

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

[2] M out of N 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

SSP#	SSP Name / Type	Strength (bits)	Security Function and Cert. Number	Gener-ation	Import / Export	Establish-ment	Storage	Zero-isation	Use / related keys
7.	MK-JWT AES-256 bits	256	HMAC-SHA-256 A4400						HMAC-SHA-256 of proof of Authenticating user
User Keys and CSPs									
8.	USER-RSA-SIG RSA 2048, 3072, 4096 bits	112, 128, 128	PKCS#1 v1.5 Sign/ Verify PKCS#1 PSS Sign A4400	Internal	Encrypted / Encrypted		User key blob (encrypted[1])	NA[2]	User signing keys
9.	USER-AES-KEY AES 128, 192, 256 bits	128, 192, 256	AES-CBC A4400						User encryption keys
10.	ADMIN-PASS At least 8 alphanumeric characters long			External	Encrypted / NA		Disk (hashed[3])	User deletion	User ID/Password Authentication
11.	INTER-RSA-GEN	112, 128, 128	FIPS 186-5 RSA key gen A4400	Internal	NA/NA		Memory	Key generation ended	Intermediate RSA key generation values
Module SSPs									
12.	FIRM-SIG RSA 3072 bits	128	PKCS#1 v1.5 Verify A4400	External	NA/NA		Disk (plaintext[4])	NA	RSA Public Key for validating the software and the upgrades file(s)
13.	AUDIT-LOG-KEY RSA 3072 bits	128	PKCS#1 v1.5 Sign A4400	Internal	NA/NA		Disk (encrypted[5])	NA	Audit log signature RSA private key
14.	TRUSTED-ANCHORS RSA 2048, 3072, 4096 bits	112, 128, 128	PKCS#1 v1.5 Verify A4400	External	External / NA		Disk (plaintext[6])	NA	Trusted PSPs (public keys and certificates)

[1] User blobs are encrypted (AES-CBC) using MK-EXT-KEK and HMACed (HMAC-SHA-256) using MK-JWS

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

[3] Stored in the QSCD database with integrity (HMAC-SHA-256) using MK-MAC

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

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

[6] Stored in QSCD database in plaintext with integrity (HMAC-SHA-256) using MK-MAC

SSP#	SSP Name / Type	Strength (bits)	Security Function and Cert. Number	Gener-ation	Import / Export	Establish-ment	Storage	Zero-isation	Use / related keys
TLS Session Keys									
15.	TLS-KEY RSA 2048, 3072, 4096 bits	112	PKCS#1 v1.5 Sign A4400	External	NA / NA		Disk (encrypted[1])	NA	Appliance's TLS RSA private/public key pair
16.	TLS-KEY-TAMPER-STATE RSA 2048, 3072, 4096 bits	112	PKCS#1 v1.5 Sign A4400						Appliance's TLS RSA public/private key pair for tamper state
17.	SESSION-EXCHANGE Elliptic Curve, P-256, P-384, P-521	128, 192, 256	ECDH A4404	Internal	NA/NA	TLS 1.2 KDF	Memory (plaintext[2])	End of session or power cycle	TLS session key for key exchange
18.	SESSION-ENC 128, 256 bits	128, 256	AES-GCM A4404						TLS session key for data encryption
19.	SESSION-HMAC 32 bytes secret key	256	HMAC-SHA-256 HMAC-SHA-384 A4404						TLS session for HMAC data integrity
20.	INTER-EC-GEN	128, 192, 256	FIPS 186-5 EC key gen A4404	Internal	NA/NA		Memory	Key generation ended	Intermediate EC key generation values
DRBG Keys									
21.	HMAC_DRBG RNG Input		HMAC-SHA-256 A4400	Internal	NA/NA		Memory (plaintext)	Appliance service shutdown[3] or power cycle	DRBG[4] state (Key and V)
22.	HMAC_DRBG RNG internal state			Internal	NA/NA		Memory (plaintext)	NA	Entropy input string
23.	DRBG seed from hardware chip			Internal	NA/NA		Memory (plaintext)	NA	Entropy input

Table 18 – SSPs

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

[2] Negotiated during the establishment of the TLS connection, stored in volatile RAM and destroyed when the session is terminated

[3] Upon shutdown, the HMAC_DRBG uninstantiate function zeroises the DRBG state

[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)

9.2 Random Number Generator

Entropy sources	Minimum number of bits of entropy	Details
ESV (Cert. #10)	Produce 2-bit samples with estimated entropy of 1.760755	A hardware-based entropy source ESV (Cert. #10) that meets the requirements of NIST SP 800-90B (Recommendation for the Entropy Sources Used for Random Bit Generation). The entropy source is based on Quantis IDQ6MC1 chip that generates entropy directly from a quantum process. The entropy source is used as a seed input to the HMAC_DRBG RNG. It generates a new seed every hour or when the reseed counter has reached the value of 100,000 requests. The module is compliant with the ESV (Cert. #E10) and is configured according to section "Configuration Settings" in the public use document[1]. The overall amount of generated entropy is 1.760755 bits per 2-bit sample and estimated amount of entropy per the sources output bit is.1.96 per 2-bit sample.
HMAC_DRBG		A Deterministic Random Bit Generator (DRBG) based on HMAC_DRBG algorithm as defined in NIST SP 800-90A rev 1 (Recommendation for Random Number Generation Using Deterministic Random Bit Generators). The algorithm uses HMAC-SHA-256 as its hash algorithm. The output of this DRBG is used to generate random data for key generation (RSA, EC, AES keys), TLS session establishment, digital signature and more.

Table 19 – Non-Deterministic Random Number Generation Specification

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

9.3 Key Establishment

The module uses TLS protocol version 1.2 for session key establishment. The cipher suites in use are TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.

9.4 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 2.12).
- CSPs are output from the module to the USB port during Master Key generation. The server Master Keys are generated, split into N 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 M out of N 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.

[1] https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E10_PublicUse.pdf

9.5 Split Knowledge Procedures

Split knowledge procedures for key import and export are used during pre-installation, installation and reset tamper. Those procedures use USB tokens on which the master keys are split using the Shamir Secret Sharing algorithm.

Those procedures use M of N scheme. The Master Keys are split into N USB tokens where ($2 \leq N \leq 9$). Then, it is possible to reconstruct the Master Keys from any subset of M USB tokens where ($2 \leq M \leq N$). This means that the minimum is ($N = M = 2$) meaning the Master keys are split into two parts and must be constructed from the same two parts. The higher supported limit is ($N = M = 9$), meaning the Master keys are split into nine parts and must be constructed from the same nine parts.

The SSS algorithm well-known and proven to provide the requirement that the knowledge of any ($M – 1$) components provides no information about the original CSP other than the length.

9.6 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.

10 Self-Tests

The DocuSign QSCD Appliance monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-3. 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.

The order in which the self-tests are performed makes sure that any test that relies on another function will be performed only after that function was tested successfully. For example, the firmware integrity test is being performed only after the relevant cryptographic functions were tested.

10.1 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.

10.1.1 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.

10.2 Critical Function Tests

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

10.2.1 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 results in tamper hardware error (TamperHWFailure).

10.2.2 Tamper CRC Test

This test calculates the CRC16 of the tamper firmware. Failure to calculate the expected CRC value results in tamper CRC error (TamperCrcError).

10.2.3 Tamper Integrity Test

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

- The appliance was installed from USB tokens that are not from the same set
- 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.

10.2.4 DRBG Tests

The DRBG tests are performed upon power-up and immediately following the cryptographic algorithm tests. Both the entropy source ESV (Cert. #10) and the HMAC_DRBG are tested.

The entropy source ESV (Cert. #10) power-up test follows the NIST SP 800-90B guidelines and include:

- Continuous health test on approximately 4000 random samples as described in 10.3.3.

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

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

10.2.5 Firmware Integrity Test

As part of the DocuSign development procedures, all executable and shared object files of the firmware are digitally signed using 3072-bit RSA private key controlled by DocuSign engineering. The signature of each file is produced using PKCS#1 v1.5-SHA-256 algorithm.

When the module starts, after the hardware tests, it performs the firmware integrity test. The module verifies the signatures using the corresponding RSA public key (FIRM-SIG) which is embedded in the module's code. If the signature verification fails, the appliance does not start and a corresponding message (SWVerifyError) is displayed.

10.2.6 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.

10.2.7 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.

10.3 Conditional Tests

10.3.1 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-SHA-256, HMAC-SHA-384, HMAC-SHA-512 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, GCM Encrypt, Decrypt KATs
- SHA-256, SHA-384, SHA-512 KATs
- HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 Calculation, Verification KAT

- RSA 2048, 3072, 4096 Encrypt, Decrypt KATs
- ECDSA P-256, P-384, P-521 Sign, Verify Test
- ECDH P-256, P-384, P-521 Key exchange KATs
- PBKDF5 using HMAC-SHA-256 KAT

10.3.2 RSA/EC Key Generation Pairwise Sign/Verify Consistency Test

To ensure the correct operation of the RSA/EC key generation, each newly generated RSA/EC 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.

10.3.3 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 1.760755. The seed is updated every hour or when reseed counter is reached. The 2-bit outputs of the entropy source are 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.

10.3.4 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 are continuously tested for correctness as required by NIST SP 800-90A:

- Instantiate function KAT
- Reseed function KAT
- Generate function KAT
- Reseed counter test
- Uninstantiate KAT

10.3.5 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.

10.4 Periodic Self-Tests

Once a day, the module performs periodic self-tests, which include the power-up self-tests (except low-level hardware tests) and the critical function tests listed above.

10.5 On Demand Self-Tests

The CO can initiate the self-tests on demand by requesting to restart the module by calling the restart REST API function.

11 Life-Cycle Assurance

11.1 Secure Module 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 and the casing of the appliance. It is also enclosed in a special plastic package protected with four distinct tamper evident security stickers similar to the following:

Figure 10 – 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.
- Open the plastic package and check the appliance's case for any evidence of physical tampering.
- Check the tamper evident seal on the back of the appliance and make sure it is not damaged.
- Verify that the serial numbers of the tamper evident stickers and the tamper seal, 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 error message does not appear on the display in the front panel 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.

11.1.1 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: QSCD0004)
- Serial numbers of all the tamper evident stickers
- Additional information related to the appliance

11.2 Deploying the QSCD Appliance

Installation of QSCD appliance should follow these general guidelines:

The key features of the appliance are:

- The Appliance should be installed as part of the organizational IT infrastructure.

- The Appliance should be placed in a physically secure location in the IT infrastructure, which allows very limited physical access and a minimal number of IT personnel.
- The secure environment should be frequently inspected for any suspicious activity.
- A firewall should be employed to control and monitor all incoming and outgoing communication with the Appliance.
- No external access to the Appliance is allowed. All communication with the Appliance can be done only within the TSP (Trust Service Provider) operational environment. This means that:
    - Any administrative access for the purpose of managing the Appliance (performed by an Appliance Administrator) or for managing Administrative accounts (performed be a User's Administrator), must be performed from within the internal network of the Appliance infrastructure.
    - All Administrative software shall be deployed only in the internal operational environment of the TSP.
    - The SSA (Secure Signing Application) must also be deployed in the internal infrastructure of the TSP and can access the Appliance using the SSA Administrator credentials. Only the SSA can be accessible by signers from the external network of the TSP.

11.3 Installation

Refer to section 2.10 for general instructions on installing the QSCD appliance. For detailed instructions refer to the QSCD admin guide.

11.4 Maintenance

A scheduled inspection of the module should be performed to verify no physical tampering has occurred (see 7.2).

11.5 Secure Destruction

The procedures required for the secure destruction of the module are described in a proprietary document, which will be provided upon request.

12 Mitigation of Other Attacks

The DocuSign QSCD Appliance does not include any mechanisms to mitigate other attacks.