DocuSign Signature Appliance
Hardware version 8.0
with Firmware version 8.5/8.51.9.0

FIPS 140-2 Non-Proprietary
Security Policy
Level 3 Validation

May 2018

Table of Contents

1 INTRODUCTION

1.1 Purpose

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

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

1.2 References

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

1.3 Terminology

In this document, the DocuSign Signature Appliance is referred to as *the Appliance*.

1.4 Document Organization

This document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains the following documents:

- Vendor Evidence
- 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 Signature Appliance and explains the secure configuration and operation of the Appliance.
- **Section 2: FIPS 140-2 security level** – Details each level of the FIPS 140-2 requirements section.
- **Section 3: Appliance Security Rules** – Details the general features and functionality of the DocuSign Signature Appliance.

- **Section 4: FIPS 140-2 Level 3 Compliant Mode** – Addresses the required configuration for the FIPS 140-2 mode of operation.

With the exception of this non-proprietary Security Policy, the FIPS 140-2 Validation submission documentation is DocuSign-proprietary and may only be released under appropriate non-disclosure agreements.

This document may be reproduced and distributed providing such a reproduction is complete and unmodified.

For access to the FIPS 140-2 Validation Submission documents, contact DocuSign.

2 FIPS 140-2 security level

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

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

Table 1 - FIPS 140-2 Security Requirements Level

3 Security Rules

The DocuSign Signature Appliance is a digital signature appliance that enables users within an organization to digitally sign documents and data. Contained within a secure, tamper-responsive steel case, the Appliance performs the actual digital signature operation using an asymmetric key of the user. All keys and critical security parameters are protected within the cryptographic boundary by the physical security mechanisms of the Appliance.

The Appliance provides the basic RSA digital signature operation. Additional cryptographic algorithms are used in support of this main functionality. These are used to encrypt: the session between the user's PC and the Appliance; the asymmetric keys that are kept in the internal database; and the backup of the Appliance's database. They are also used to provide data integrity. The Appliance performs all cryptographic operations internally and, through self-tests, it ensures that these operations function correctly.

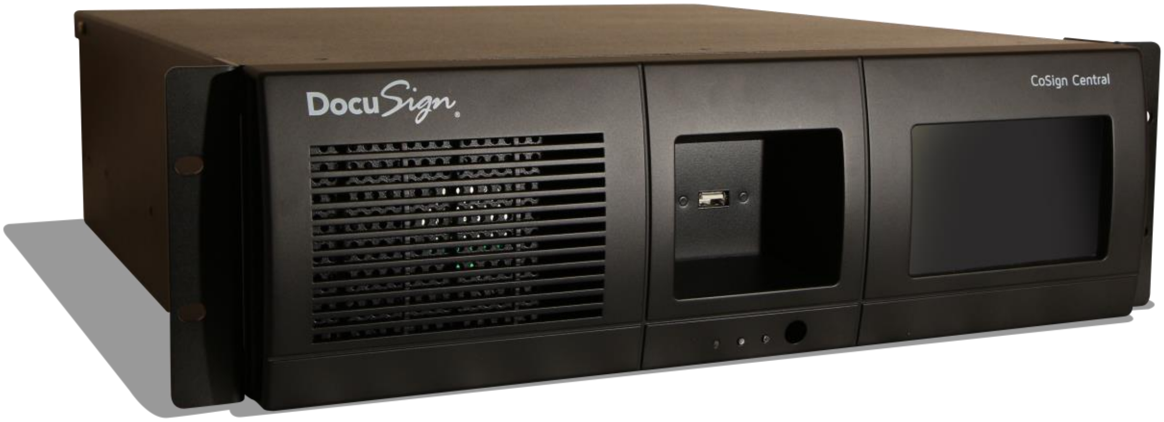

Figure 1 - DocuSign Signature Appliance

3.1 Secure by Design

The DocuSign Signature Appliance is a multi-chip standalone appliance. It has been designed to meet all of the Level 3 FIPS 140-2 requirements. Encased within a tamper-responsive and tamper-evident steel box, the Appliance both protects against and reacts to attacks. Access to the Appliance is only permitted through specific, well-defined interfaces detailed in Well-Defined Interfaces section.

All vents on the module are baffled meet the FIPS 140-2 opacity requirements for physical security.

The Appliance includes a dual power supply, where the power supply can be removable and replaceable.

The dual-power supply, containing two power supply units, is an external component of the module and outside the physical cryptographic boundary of the module.
Tamper Evident cans provide evidence of any attempt to tamper with module cover. The Tamper Evident cans are placed over a screw that joins the top cover and bottom enclosure.
The Tamper Evident cans are applied at manufacturing stage.
The Tamper Evident cans are shown in Figure 2.

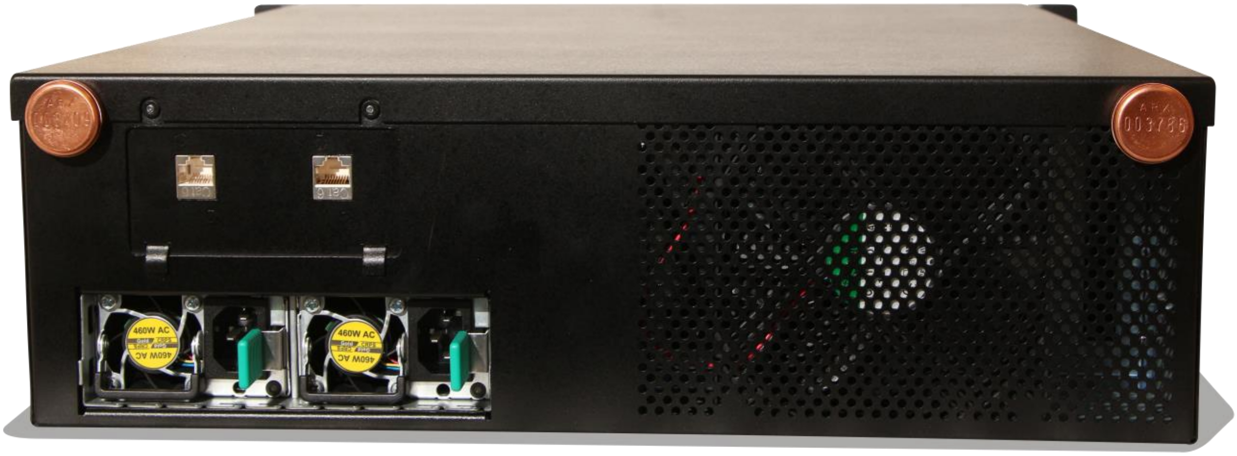

Figure 2 - Tamper Evident cans

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

3.2 Product Delivery

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

3.3 Initialization

The Appliance is delivered to you in the *Factory Settings* state. In this state it is not yet a FIPS module and only the following options are relevant:

- **Setting network parameters** – The Cryptographic Officer can set the IP address of the Appliance, define that the IP address is retrieved using a DHCP protocol and set other networking related parameters. This operation is performed through Appliance's console.
- **Time adjustments** – The Cryptographic Officer can define the current time of the Appliance or retrieve time from an NTP server. This operation is performed through the Appliance's console.
- **Installation** – This critical procedure must be performed in a secure environment. Only after the Appliance is installed it can begin to provide its digital signature services.
  For additional details related to appliance initialization, see *Installing the DocuSign Signature Appliance* section.
- **Restoration** – This critical procedure must be performed in a secure environment. Restoration is similar to installation. This procedure uses the backup file of the internal database.
  For additional details related to appliance restoration, see *Restoring the DocuSign Signature Appliance* from backup on following section.

Remark:

A web based console is used. The web based console is accessed through a dedicated LAN interface (labeled as LAN0) of the Appliance to IP address 10.0.0.2 on port 8088.
Also, any operation from the web based console requires physical access to the Appliance by unplugging/plugging the license token as part of approving the operation.

3.3.1 Installing the DocuSign Signature Appliance

The Appliance installation is performed using the administrative DocuSign SA Client. The Cryptographic Officer uses the administrative DocuSign SA Client to send installation commands to the Appliance. The installation commands are sent using the regular client/appliance secure protocol (see *Secure Operation – DocuSign SA Client* section).
During installation, the following security related issues are handled:

- The first Crypto Officer User ID and password are provided. The Crypto Officer is defined in the users database with the required permissions to manage users, groups and the Appliance.
  Assigning users to groups is relevant only for when the Appliance is installed in Directory Independent mode.

- A set of four Server critical Triple-DES keys and IPSEC shared secret are randomly generated inside the Appliance and are placed inside the internal tamper device. The keys and shared secret are also loaded into the two blue USB tokens. These tokens must be stored on the Crypto Officer's premises and are only used during the:
    - Reset tamper operation performed by the Crypto Officer.
    - Restoration of the Appliance.
    - Installing an alternate appliance for High Availability purpose.
- In the case that it is configured to use an internal CA, A RSA key pair is generated for the internal CA (Certificate Authority) of the Appliance. This key is used for generating X.509-based Certificates for users. The RSA private key is encrypted and stored in the Appliance's database.

During normal appliance operation, a USB-based license plug is plugged into the Appliance's USB port. The USB token controls the number of possible existing users in the Appliance's database and expiration date for the Appliance's service.

DocuSign manufactures the Appliance based on firmware versions 8.0, 8.1, 8.4, 8.5 or 8.51.9.0.
Also, it is possible to upgrade to Appliance firmware version 8.4 upgrade to Appliance firmware version 8.5 and then upgrade to Appliance firmware 8.51.9.0.
Appliance firmware version 8.4 is not FIPS approved.
For more information of how to perform a firmware upgrade, refer to Chapter 5.

3.3.2 Restoring the DocuSign Signature Appliance from backup

If the Appliance was physically damaged, reset to factory settings, or damaged in some other way, a backup of the Appliance's database must be restored to a new or existing appliance. The restore operation is very similar to the installation of a new appliance and must be performed in a secure environment. In addition, the Appliance must be in the *Factory Settings* state to perform the restore operation.

A restoration differs from an installation in the following ways:

- A valid backup file of an operational appliance must be available.
- The Crypto Officer must have a valid backup token that includes the critical keys and the IPSEC shared secret of that operational appliance.

During restoration:

- The Crypto Officer provides the backup file and plugs the backup token into the Appliance's USB token slot.
- All users and their relevant data, such as their private keys, are restored to the Appliance's database.

After restoration, all users can sign their documents and data using the Appliance.

After restoration, the product is a FIPS module and begins serving user requests and Crypto Officer requests.

3.4 Users Directories

The DocuSign Signature Appliance supports installation in environments where a user directory already exists. Currently the following Users Directory environments are supported:

- Microsoft Active Directory
- LDAP based environment such as: IBM Tivoli, SUN Directory Server and Oracle Internet Directory.

The Appliance provides two additional functionalities when using these environments:

- **Synchronization with the Users Directory of the environment** – The Appliance is synchronized with the users directory of the environment. Every user in the users directory who is classified as a signer is also defined in the Appliance and is able to sign documents.
- **Authentication using Kerberos Ticketing mechanism** – When a user attempts to securely connect to the Appliance for any operation, such as signing a document, the login operation is done using the Kerberos Ticketing mechanism. The Appliance authenticates users from Active Directory relying on the Kerberos Ticketing mechanism.
- Besides the above directories, the Appliance supports the Directory Independent environment where users are defined by the administrator of the organization and the login operation is performed internally by the Appliance.

Note: Only the Directory Independent environment and module interface to Microsoft Active Directory are submitted for FIPS 140-2 validation.

Also, it is possible to authenticate a user based on a SAML or JWT ticket provided by a trusted Identity Provider.

3.5 Managing the DocuSign Signature Appliance

3.5.1 Cryptographic Officer

The Crypto Officer performs both appliance and users/groups management of the Appliance.
In the case of Active Directory based environment, users are managed in the directory and all changes that are made in the directory sync with the list of users in the Appliance.
The Crypto Officer connects securely to the Appliance (see *Secure Operation – DocuSign SA Client* section). The following sections describe in detail all operations that can be performed by the Crypto Officer.
The Crypto Officer creates users and groups according to the organization's policy. For each user, a User-ID and a Password is provided. This operation is relevant only when the Appliance is installed in Directory Independent environment. In Active Directory environment, a user is created in the Appliance when the Crypto Officer creates the user in Active Directory and defines the user as a member of the Signers User Group.

By default, after a user is created, the Appliance automatically generates a new RSA key pair and a Certificate for the user.

The Crypto Officer can delete users. When a user is deleted, all the user's keys, certificates, and graphical images are also deleted. This operation is relevant only when the Appliance is installed in Directory Independent Environment. In Active Directory Environment users are deleted from the Appliance when the Crypto Officer deletes the user in Active Directory or removes the user from the Signers User Group.

3.5.2 User

In the case of Directory Independent environment, the user can change the password. The password length must be greater than six Unicode characters and less than twenty eight Unicode characters.

In the case of Active directory environment, the user's password is managed by the directory.

The user can also direct the Appliance to generate additional RSA keys. It is possible to store several graphical signature images in the user account in the Appliance. These images are stored in the Appliance's database, retrieved by the DocuSign SA (Signature Appliance) Client, and can be incorporated into the signed document in the user's PC.

A user can only use keys that are owned by that user.

Remark: it is possible to configure the Appliance to use an RSA key pool when the Appliance's internal CA is used. The implementation is based on a process which is executed within the Cryptographic module and writes the newly generated keys to the database, encrypted with *appliance Critical Key 1*.

These keys will be assigned to user when it is required to assign a signature key for the user. A certain key from the key pool can only belong to a certain user.

3.6 Secure Operation – DocuSign SA Client

Any operator who wishes to use the Appliance's services can connect via a secure protocol using the DocuSign SA Client. The secure networking protocol is a standard TLS (Transport Layer Security) protocol with the following parameters:

- The TLS protocol is based on a Server RSA key. The TLS Server RSA key is externally generated during manufacturing. Each individual appliance includes a different TLS Server RSA key.
- The TLS session is based on AES CBC/Triple-DES-CBC encryption and HMAC-SHA-1/HMAC-SHA-256 data integrity.
- Upon session creation, the only operation that can be performed is an authentication command. The authentication is based on User ID and Password authentication, which are verified by the Appliance or using a Kerberos ticket when the Appliance is installed in Active Directory environment.

Also, it is possible to authenticate a user based on validating a SAML or JWT Token that was created by a trusted Identity provider.

- Only after the user is authenticated, can the user perform operations such as digitally sign data. Similarly, the Crypto Officer can connect securely to the Appliance and perform administrative operations.
- It is possible to configure the Appliance to use extended authentication, where any digital signature operation requires the end user to authenticate. There are two modes of extended authentication:
    - Radius based – the end user provides an additional password that is validated by an external Radius Server. Usually the extended password is a one time password.
    - PKI based – the end user signs the current time with a local SmartCard or a software token, the signature is validated by the Appliance.

3.7 Additional Security Issues

The four critical keys are used for:

1) Encrypt sensitive data in the database in non-volatile memory and MAC plaintext data in the database.

2) MAC individual user's records in the database.

3) Encrypt database for backup

4) MAC database for backup

The four critical keys of the Appliance are stored on a special backup token and in an internal tamper device. These keys are loaded into the Appliance's volatile memory during startup from the tamper device and erased from memory when the Appliance is shut down.

Any attempt to access the device that triggers the tamper response will cause power to be instantly cut off, preventing access to any useful information by zeroizing all plain text critical security parameters, including the Appliance's critical keys. Without these keys, it is not possible to start the Appliance or access the Appliance's stored data.

The critical keys will also be deleted from the internal tamper device. Upon next startup of the device a tamper detected message will be displayed in the touch screen.

Also, if there is an attempt to access the device when the power is off, the tamper response circuit is still active. If the tamper circuit is activated, the critical keys will be deleted from the internal tamper device and the tamper detected message will appear in the console upon next startup.

Module zeroization can be done by performing the *Factory Restore* operation from the console. This operation will zeroize all plain text critical security parameters, including the Appliance's critical keys. Also all users' information as well as the users' keys will be deleted from the Appliance's database.

The units are encased in a solid metal case rigged with micro-switches and only the specified physical interfaces permit access to the Appliance. The boundary of the module is the metal case. The Appliance meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (ClassB), and is labeled according to FCC requirements.
The cryptographic boundary is the metal case of the Appliance.
The power supply bays, internal power wires, power connectors, internal power circuit and fan are excluded components.

3.8 High Availability and Load Balancing

It is possible to deploy two or more appliances in the same organization. The purpose of having more than one active appliance is to enable the organization's users to continue and digitally sign in the event of a hardware or firmware malfunction to the Appliance.
The main appliance is named the Primary appliance, while the other appliances are named the Alternate appliances.
The whole content of the Appliance's database is replicated to the alternate appliances, thus enabling end user to sign data either using the primary appliance or an alternate appliance.

3.9 Interface to External CA in Automated mode

The Appliance can be configured to access an external CA in automated mode for the purpose of certificate enrollment.
Upon a creation of a user, the Appliance will connect to the external CA and the external CA will issue a certificate for the user. Upon updating user information such as email, a new certificate will be generated for the user.
If the user is deleted from the Appliance, the certificate of the user will be revoked.

3.10 Well-Defined Interfaces

The Appliance is a steel, rack mountable box, in which only the interfaces provide access to the Appliance.

The physical interfaces of the Appliance include the power connector, regular network connection (Ethernet Interface using TCP/IP), administrative network connection (Ethernet Interface using TCP/IP), power switches, LEDs, a touch screen and one USB slot for a smartcard-based USB token. All ports use standard PC pin outs.
Table 2 shows the mapping of the FIPS 140-2 logical interfaces to the Appliance's physical interfaces.

FIPS 140-2 Logical Interfaces	Appliance's Physical Interfaces
Data Input Interface	Network port (LAN1), USB slot for smartcard-based token[1]
Data Output Interface	Network port (LAN1), USB slot for smartcard-based token[2]
Control Input Interface	Network port (LAN0/LAN1), Touch Screen
Status Output Interface	Network ports (LAN0/LAN1), LEDs, Touch Screen
Power Interface	DC power connector

Table 2 - Interfaces

[1.] Used only in the case of restoration or a reset tamper event.

[2.] Used only during installation.

When the DocuSign SA Client is used, all requests for cryptographic services are performed through the DocuSign Signature Appliance API. This API, written in C/C++ and based on RPC (Remote Procedure Calls), provides a high-level interface to the cryptographic services provided by the Appliance that include RSA key generation and digital signature operations.

The Touch Screen displays the following status information: IP address, version information, and serial number.

The Front of the module has the following LED's:

- Power LED
- Hard Disk LED
- Tamper LED

Status information can also be sent via syslog protocol to a syslog server or can be retrieved by network monitoring systems via SNMPv2 protocol. This status information is sent using the network ports of the module.

3.11 Roles and Services

The Appliance employs password-based, identity-based authentication of users and operators secured by the TLS protocol. Multiple users and operators can connect and use the Appliance simultaneously. Each user has a user record that contains the user name, common name, email address, and administrative authorization mask. The administrative authorization mask controls whether the user can perform appliance management tasks or user management tasks. There are two roles that can be assigned to an operator, User and Supervisor (Crypto Officer).

In Active Directory, it is possible to authenticate users and Crypto Officers based on SSPI (Security Support Provider Interface), which is a Kerberos based ticketing mechanism. The user is authenticated to the domain and provided with a ticket from the domain. The ticket is sent from the DocuSign SA client to the Appliance during user authentication. The Appliance authenticates the user based on the given ticket.

3.11.1 Supervisor (Crypto Officer) Role

The Supervisor role is assigned to the Crypto Officer and is used for user and appliance management, appliance installation/restoration, and the Appliance's configuration. The Crypto Officer possesses the backup tokens necessary for reset tampering and restoring from backup. The Crypto Officer can log into the Appliance remotely using the standard appliance's authentication protocol.

The Crypto Officer can perform the following tasks. These tasks represent special services of the Appliance:

- Create users – DI Environment
- Update user information – DI Environment
- Retrieve user information
- Revoke Users – DI Environment
- Set user password – DI Environment
- Disable/Enable user logon – DI Environment
- Create groups – DI Environment
- Update groups – DI Environment
- Delete groups – DI Environment
- Attach/detach a user from a group – DI Environment
- Disable/enable a group – DI Environment
- Perform shutdown
- Load Firmware
- Perform backup of all data in the Appliance
- Retrieve log file
- Update system parameters
- Zeroize Module
- Asymmetric cryptography
- Authentication

- Graphical image Import/export
- Delete Keys
- Change user password – DI Environment
- Show FIPS mode Status
- Self-Tests

Locally, the Crypto Officer has the ability to access certain management operations of the Appliance, including resetting a tamper condition, which is performed using the backup USB token.

It is possible to set a specific Client IP address as a system parameter.

Only from this IP address, it is possible to perform a backup of the Appliance to a file without requesting for administrator User ID and a password, thus automate a periodical backup for the system.

3.11.2 User/Application Role

The User/Application role is used for accessing the cryptographic services provided by the Appliance. A user logs into the Appliance remotely using a user ID and a password or based on Active Directory ticket (SSPI). The session is protected using the TLS protocol. A user is not permitted to perform any user or appliance management operations.

A user can access the following services:

- Asymmetric cryptography
- Authentication
- Graphical image Import/export
- Delete Keys
- Change user password – DI Environment
- Show FIPS mode Status

The Crypto Officer and User role can use the Asymmetric cryptography service to generate an RSA key pair, Generate a digital signature, retrieve a public key and certificate, and upload a user certificate.

An operator assigned a User/Application role must first authenticate to the Appliance using the user ID and password or based on Active Directory ticket (SSPI). After successful authentication, an authenticated and encrypted session is created. During this session, the operator may only perform cryptographic services on RSA keys that belong to the operator.

Also, the user can change his/her password. The password length must be greater than or equal six Unicode characters.

In addition, the user can be authenticated based on a SAML or JWT token provided by a trusted Identity provider.

In Directory Independent environment the module enforces a minimum password length of six characters. Each character may be numeric (0-9) or alphanumeric (a-z, A-Z) or even Unicode. Just considering the alphanumeric set of characters there are 62 possible characters and the password is at minimum 6 characters long.

Therefore, the probability of a random attempt to succeed is:

One in (62 ^ 6) or 1 in 56,800,235,584. This is 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. This allows a maximum of:

Therefore, the probability of a random attempt to succeed during a minute is:

One in ((62 ^ 6) / 60,000) or 1 in (56,800,235,584 / 60,000) or 1 in 946,670.This is less than 1 in 100,000.

If SAML/JWT authentication is used, since the SAML/JWT token is based on a 2048bit digital signature, the probability that random access will succeed is far less than one in 1,000,000 attempts using this authentication mechanism. The authentication provides 1 in 2^161/(3000*60) probability of a successful random attempt during a one-minute period since the Appliance cannot process more than 3000 SAML/JWT validations per second.

An operator who has access to the role of Crypto Officer must first authenticate to the Appliance using the user ID and password of the Crypto Officer or based on an Active Directory ticket (SSPI). When using Active Directory authentication, the Crypto Officer must be part of an Active Directory administrative group. During this session, the operator may perform user management and appliance management services.

In the case of Active Directory environment, the user and Crypto-Officer authenticate by presenting a ticket over a TLS channel. The Kerberos ticket is encrypted and contains a domain session key with length of at least 56 bits.

Therefore, the probability of random attempt to succeed is:

One in (2^56) or 1/72,000,000,000,000,000. This is less than 1 in 1,000,000.

It takes the module 1msec to process a login attempt. A maximum of 1,000 login attempts may be processed in 1 second and 60,000 login attempts in 1 minute. This allows a maximum of: (2^56) / 60,000 ~ 1,200,000,000,000 attempts per minute.

Therefore, the probability of a random attempt to succeed during a minute is:

One in (1,200,000,000,000), this is less than 1 in 100,000.

The Appliance can be configured to use additional authentication for every digital signature operation.

The additional authentication is defined as the following:

- Either Username and Password authentication using a Radius Server.
  The user will provide his/her password. Both user ID and password will be authenticated by a Radius server using the Radius protocol.
- Or PKI based digital signature based on a SmartCard or Software token. The signature is done based on the current time. The digital signature is validated by the Appliance.

The Radius authentication is based on 32 bytes of authentication data sent from the Appliance to the Radius Server. 16 bytes are randomly generated by the Appliance.
Therefore the probability of random attempt to succeed is:
One in (2^128), this is less than 1 in 1,000,000.
It takes the module 1msec to process a signature request and 60,000 signature requests in 1 minute.
Therefore, the probability of a random attempt to succeed during a minute is:
One in (2^128/60000), this is less than 1 in 100,000.
Since the Radius authentication is done in addition to the authentication methods above both method (Active Directory and Directory Independent) probabilities are increased.
In the case of a PKI signature validation as part of the authentication process, is based on a 2048bit digital signature, The probability that random access will succeed is far less than one in 1,000,000 attempts using this authentication mechanism. The authentication provides 1 in 2^161/(3000*60) probability of a successful random attempt during a one-minute period since the Appliance cannot process more than 3000 signature validations per second.

Table 3 lists which roles have access to each service.

Services	**Role**
Create users – DI Environment	CO
Update user information	CO
Retrieve user information	CO
Revoke users – DI Environment	CO
Set user password – DI Environment	CO
Enable/Disable user login – DI Environment	CO
Create group – DI Environment	CO
Update group – DI Environment	CO
Delete group – DI Environment	CO
Attach/Detach user from a group – DI Environment	CO
Enable/Disable group – DI Environment	CO
Perform shutdown	CO
Load Firmware	CO
Perform backup	CO
Retrieve log file	CO

Self-Tests	CO
Update system parameters	CO
Asymmetric cryptography	CO/User
Authentication	CO/User
Graphical image Import/export	CO/User
Delete Keys	CO/User
Change user password – DI Environment	CO/User
Zeroize Module	CO
Show FIPS mode Status	CO/User/No Role
Setting network parameters	No Role
Time adjustments	No Role
Shutdown	No Role
Backup to a specified IP address	No Role
DRBG	No Role

Table 3 - Role Access to Services

3.12 Strong Cryptographic Algorithms and Secure Key Management

The DocuSign Signature Appliance supports and uses a variety of strong cryptographic algorithms. The Appliance implements these algorithms based on the following FIPS 140-2-approved algorithms:

CAVP Cert v8.5	CAVP Cert v8.51.9.0	Algorithm	Standard	Mode/ Method	Key Lengths or Moduli	Use
2616	2739	Triple-DES	SP 800-67	CBC	192bit	Session data encryption
5058	5448	AES	FIPS 197	CBC	128 and 256 bits	Session data encryption
3378	3607	HMAC	FIPS 198-1	HMAC-SHA-1 and HMAC-SHA-256	160bit and 256bit	TLS-based session scheme
4123	4368	SHS	FIPS 180-4	SHA-1 and SHA-256		TLS-based session scheme
1615	1894	CVL TLS 1.0/1.1/1.2	SP 800-135rev1			TLS Key Derivation Note: The TLS protocol has not been reviewed or tested by the CAVP and CMVP.
5058 (AES) 3378 (HMAC)	5448 (AES) 3607 (HMAC)	KTS	FIPS 197 SP 800-38F	AES\HMAC	128,256 bits	Key Transport
2616 (Triple-DES) 3378 (HMAC)	2739 (Triple-DES) 3607 (HMAC)	KTS	SP 800-67 SP 800-38F	Triple-DES\HMAC	192 bits	Key Transport
2743	2925	RSA	FIPS 186-4	SHA-1, SHA-256	2048 bits	RSA Signature Generation for TLS Note: This RSA PKCS1 v1.5 SigVer implementation was tested but not used by the module

CAVP Cert v8.5	CAVP Cert v8.51.9.0	Algorithm	Standard	Mode/ Method	Key Lengths or Moduli	Use
2603	2738	Triple-DES	SP 800-67	CBC	192bits	Backup Encryption
						Database Encryption
Vendor Affirmed		Triple-DES MAC	SP 800-67	CBC		Backup integrity
						Database Integrity
2603 (Triple-DES) (Triple-DES MAC)	2738 (Triple-DES) (Triple-DES MAC)	KTS	SP 800-67 SP 800-38F	Triple-DES, Triple-DES-MAC	192 bits	Key Wrapping
4108	4367	SHS	FIPS 180-4	SHA-1		Authentication
				SHA-256, SHA-384 and SHA-512		Hash for Digital signature generation
2729	2924	RSA	FIPS 186-4	SHA-256, SHA-384, SHA-512, PKCS1 v1.5, PSS	2048,3072 bit	RSA Key generation, Digital signature generation
2729	2924	RSA	FIPS 186-4	SHA-256, PKCS1 v1.5	2048 bit	Digital signature verification
1864	2133	DRBG	SP 800-90A	HMAC-SHA-256		Random Number generation
3363	3606	HMAC	FIPS 198-1	HMAC-SHA-256	256bit	Within HMAC DRBG

CAVP Cert v8.5	CAVP Cert v8.51.9.0	Algorithm	Standard	Mode/ Method	Key Lengths or Moduli	Use
						note: This HMAC-SHA-1 implementation was tested but not used by the module
98		DRBG	SP 800-90A	SHA-256		Random Number generation[1]
1465		SHS	FIPS 180-4	SHA-256		Within Hash_Based DRBG
Vendor Affirmed		CKG	SP 800-133			Key Generation
Vendor Affirmed		PBKDF	SP 800-132	Option 2a	192 bits	Password-based Key Derivation

Table 4 - Implemented Algorithms and FIPS Approved algorithms

[1] Provided by the internal Safenet eToken 5105 (FIPS 140-2 validation #1883)

The module implements the following Non-FIPS approved, but allowed, algorithms:

- RSA-TLS (key wrapping; key establishment methodology provides 112 bits of encryption strength). TLS protocol has not been reviewed or tested by the CAVP and CMVP.
- MD5 (used in TLS v1.1, used in Extended Authentication mode – Radius and by the TLS1.0 implementation)
- HW RNG (used in Safenet eToken 5105)

The module implements the following Non-FIPS approved algorithms:

- SHS (non-compliant) – used in RSA-RESTful-TLS in non-FIPS mode
- HMAC (non-compliant) – used in RSA-RESTful-TLS in non-FIPS mode
- Triple-DES (non-compliant) – used in RSA-RESTful-TLS in non-FIPS mode
- AES (non-compliant) – used in RSA-RESTful-TLS in non-FIPS mode
- RSA-RESTful-TLS (key wrapping; non-compliant)
- AES (no security claimed) – implementation used for IPSEC

The Appliance stores private keys in a key database. This database is stored encrypted (with Triple-DES CBC) on the Appliance's internal hard drive. Within the key database, each key is attached to a specific user.

Generated keys in the Appliance cannot be read outside the Appliance. User's public keys, certificates, and graphical images of the user's signature are stored in the Appliance's database and can be retrieved during a user's session. The user can retrieve only his/her objects.
Table 5 provides a list of keys, their key types, and access control.

Cryptographic Keys and CSPs	**Key Type**	**Crypto Officer Access (R/W/X)**	**User Access (R/W/X[1])**	**Generation/ Input/Output**	**Storage**	**Zeroization**
Appliance Critical Key 1 – Key and values encryption in database	Triple-DES 192 bit key, FIPS 46-2	X		Internal/ NA/NA	Tamper device (plaintext)	Tamper
Appliance Critical Key 2 – MAC of users database records	Triple-DES 192 bit key, FIPS 46-2	X		Internal/ NA/NA	Tamper device (plaintext)	Tamper
Appliance Critical Key 3 – Appliance Backup encryption	Triple-DES 192 bit key, FIPS 46-2	X		Internal/ NA/NA	Tamper device (plaintext)	Tamper
Appliance Critical Key 4 – MAC of the Appliance's Backup	Triple-DES 192 bit key, FIPS 46-2	X		Internal/ NA/NA	Tamper device (plaintext)	Tamper
Appliance's TLS RSA public/private key pair	RSA 2048 bit key	X		External/ NA/NA	Disk (encrypted)	NA
Triple-DES KEK for the Appliance's TLS RSA public/private key pair	Password-based key derivation is implemented in compliance with SP 800-132.	X		Derived/ NA/NA	Memory (plaintext)	End of usage
Password for accessing Triple-DES KEK for the Appliance's TLS RSA public/private key pair	N/A	X		External/ NA/NA	Disk (encrypted)	NA
PBKDF master key	N/A	X		Internal/ NA/Encrypted	Disk (encrypted)	NA
HMAC-SHA256 of PBKDF master key (for integrity of the DPK)[3]	32bytes	X	X	Internal/ NA/NA	Memory (plaintext)	Power cycle

Cryptographic Keys and CSPs	Key Type	Crypto Officer Access (R/W/X)	User Access (R/W/X[1])	Generation/ Input/Output	Storage	Zeroization
PBKDF HMAC key (for integrity for DPK) [3]	24 bytes	X	X	External / NA/NA	Disk (plaintext)	Hardcoded key zeroized by special firmware
The Appliance's Internal CA RSA key	RSA 2048 bit key – defined in installation	X		Internal/ NA/Encrypted	Disk (encrypted)	NA
DocuSign RSA public key – firmware validation – hard coded	RSA 2048 bit key	X		External/ NA/NA	Disk (plaintext)	NA
DocuSign RSA public key – DLM (downloadable module) validation – hard coded	RSA 2048 bit key	X		External/ NA/NA	Disk (plaintext)	NA
Session encryption/decryption keys	Triple-DES 192 bit keys, FIPS 46-2 AES 128/256 bit keys.	X	X	TLS key establishment	Memory (plaintext)	End of session
HMAC key	20 bytes	X	X	TLS key establishment	Memory (plaintext)	End of session
User public key certificates	RSA 2048/3072 bit public keys stored in certificates	X, R	R, W, X	Internal/ Encrypted/Yes	Disk (encrypted)	NA
User signature keys	RSA 2048,3072 bit	W	W, X	Internal/ Encrypted/Encrypted	Disk (encrypted)	NA

Cryptographic Keys and CSPs	Key Type	Crypto Officer Access (R/W/X)	User Access (R/W/X[1])	Generation/ Input/Output	Storage	Zeroization
DRBG Key	HMAC-DRBG RNG Input	X	X	Internal/ NA/NA	RAM (plaintext)	Power cycle
DRBG seed	DRBG seed in Safenet eToken 5105	X	X	Internal/ NA/NA	eToken	Power cycle
DRBG state[2]	DRBG state in Safenet eToken 5105	X	X	Internal/ NA/NA	eToken	Power cycle

Table 5 - Keys, Key Types and Access

[1] Execute a command on the key without the ability to Read or Write.

[2] The DRBG State is associated with the internal DRBG (eToken). The internal DRBG state is not accessible to the Appliance and is zeroized when the Appliance powers off.

All symmetric keys and generated seeds for asymmetric key generation are unmodified output from the Approved HMAC_Based DRBG

[3] The DPK is DATA Protection Key according to SP 800-132

Remark: The DRBG Key, which is of size 256bit is based on a 256bit random seed that is retrieved from an internal Safenet eToken 5105 (FIPS 140-2 validation #1883).
The estimated entropy is at least 5.74/8, which means that a random seed of 256bit, will produce minimum entropy of 184bit.
This assumes a residual security risk results from the incomplete testing of a third-party entropy source.

Policy for usage of Triple-DES 192 bit keys for encryption

Triple-DES is used for encryption in the following three cases. For each case a specific usage policy is defined.

A. Encryption of keys and values by Appliance Critical Key 1

This critical key is generated upon Appliance Installation and used for encrypting user signature keys and values (public keys, certificates and graphical signatures). Only the Primary Appliance use the key for encryption and no other module uses this key.

In order to avoid using this key for more than 2^{32} 64bit blocks a typical policy restrictions should be applied:

a. Overall time of using this Appliance Critical key 1, starting from May 2017 will be 3 years.
b. Maximum of 30,000 users in the system
c. Each user should have maximum number of 3 signature keys in a year. (Each key has a triplets of RSA Private Key, RSA Public Key and a Certificate).

   The normal size of used RSA key 2048 bit (ie 256 byte).

   The maximum size of a user certificate is 6K bytes.
d. Maximum number of graphical signatures for a user is 3. Each Graphical Signature has a maximum size of 20k.

In total, the encryption usage for the Appliance Critical key 1 is

$(30,000*(3*20,000+3*(4*(256+256+6000))))/8 = 5.1804*10^8 < 2^{32}$

$5.1804*10^8$ is approximately equal to 2^{29}.

Another example as the following can be used:

$(2,000,000*(0*20,000+3*(1*(256+256+4000))))/8 = 3.384*10^9 < 2^{32}$

$3.384*10^9$ is lower in ~22% than 2^{32}

Remark: Any other combination that will have the above formula reach a number that is lesser than 2^{32} is fine

B. Encryption of backup information using Appliance Critical Key 3

The critical key is generated upon Appliance Installation and used for encrypting the backup of the Primary Appliance. Another alternative for a backup operation is to use the High Availability mechanism. The High availability mechanism does not use Appliance Critical Key 3.

The size of the database of the appliance has high correlation to the above formula.

For example, in the first above example, no more than 8 backup operations will be possible to performed in 3 years.

As a reference, a size of 2^{32} 64bit Triple-DES Blocks means a backup of the size of 32 GigaBytes, which means that if all the sizes of backups do not exceed 32 Giga Bytes, the Appliance Critical Key 3 can be used.

Remark: Any other combination that will have the above formula reach a number that is lesser than 2^{32} is fine.

C. Session encryption/decryption keys

In a regular session, the server will not encrypt more than 2^{32} 64bits of Triple-DES blocks in a single TCP/IP connection.

In the cases that a TCP/IP connection that intends to encrypt more 64bit blocks, the DocuSign SA Client should list only the AES mechanism as a session encryption mechanism.

Self Testing

The DocuSign Signature Appliance monitors firmware operations using a set of self-tests to ensure proper operation according to the FIPS 140-2 standard. The Appliance includes both the power-up self tests and conditional tests. These tests are described in the following sections.

3.12.1 Power-Up Self Tests

- Critical Function Test - Low Level Hardware Check
- Firmware Integrity Test (RSA signature verification)
- Triple-DES encrypt KAT (for Appliance-internal Triple-DES implementation)
- Triple-DES decrypt KAT (for Appliance-internal Triple-DES implementation)
- Triple-DES encrypt KAT (for Appliance-TLS Triple-DES implementation)
- Triple-DES decrypt KAT (for Appliance-TLS Triple-DES implementation)
- AES encrypt KAT (for Appliance-TLS AES implementation)
- AES decrypt KAT (for Appliance-TLS AES implementation)
- Triple-DES MAC KAT (for Triple-DES MAC using underlying Appliance-internal Triple-DES implementation)
- SHA-384 KAT (for Appliance-internal SHA-384 implementation)
- SHA-512 KAT (for Appliance-internal SHA-512 implementation)
- HMAC SHA-1 KAT (for Appliance HMAC implementation)
- HMAC SHA-256 KAT (for Appliance HMAC implementation)

- HMAC SHA-1 KAT (for Appliance-TLS HMAC implementation)
- HMAC SHA-256 KAT (for Appliance-TLS HMAC implementation)
- RSA sign KAT (for Appliance-internal implementation)
- RSA verify KAT (for Appliance-internal implementation)
- RSA decrypt KAT (for Appliance-TLS RSA implementation)
- RSA encrypt KAT (for Appliance-TLS RSA implementation)
- RSA sign KAT (for Appliance-TLS RSA implementation)
- RSA verify KAT (for Appliance-TLS RSA implementation)
- DRBG KAT (Including instantiate/generate/reseed) as specified in SP 800-90A Section 11.3)
- Critical Function Test - Database Access

Following to failure of any of the above tests, the following error will be displayed in the *Critical Alerts* attribute in the Touch Screen :
On – Critical Error, On – DB Error
Or there will be a General Failure message in the Touch Screen.
The Appliance will not provide any service at this state.

3.12.2 Conditional Tests

- Continuous RNG test (for HMAC-DRBG).
  The Appliance's random is based on a non-deterministic seed key that is generated by the approved DRBG (Cert. #98) of internal Safenet eToken 5105 (FIPS 140-2 validation #1883).
  The seed key is updated every minute and checked for continuous test based on comparison errors.
  The output of the DRBG algorithm is checked for continuous test and statistical errors.
  If any of the tests fails, the module enters the error state.
- Continuous RNG test for DRBG output (for DRBG Cert. #98)
- Firmware Load Test [1]
- RSA Key Generation pairwise consistency test

[1] Make sure that the new firmware version is a FIPS 140-2 validated firmware version.
If a non-validated version is uploaded to the Appliance, the Appliance is no longer FIPS 140-2 validated.
RSA 2048bit with SHA-256 digital signature verification is used in this test.

3.13 Mitigation of Other Attacks

The DocuSign Signature Appliance does not include any mechanisms for the prevention of special attacks.

3.14 Maintenance

The Crypto Officer must check the Appliance’s case for any evidence of physical tampering. Special protective screw cover Tamper Evident cans are attached over two screws on the back of the Appliance.   These Tamper Evident cans would be damaged if the Appliance’s case has been opened. Verify that the Tamper Evident cans are attached to the Appliance and that they are not damaged. If you think the Appliance has been tampered with, contact DocuSign.

4 FIPS 140-2 Level 3 Compliant Mode

Cryptographic services should only use FIPS 140-2 approved algorithms. A list of these algorithms can be found in Section 3.12, *Strong Cryptographic Algorithms and Secure Key* Management.

Only one user can be assigned the role of Crypto Officer. Only the Crypto Officer may possess the backup USB tokens necessary to restore the Appliance or reset the tamper operation.

Directory Independent and Active Directory environments are FIPS 140-2 level 3 validated. The Appliance also supports LDAP environment, however, this is not included in the scope of this FIPS 140-2 level 3 validation process.

The Appliance can be interfaced through a SOAP based Web Services protocol or RESTful based Web Services protocol. Both SOAP based Web Services interface and RESTful based Web Services are not included in the scope of this FIPS 140-2 level 3 validation process.

To make sure the Appliance is running in FIPS Mode, inspect the value of **FIPS Mode** in the *settings* section in the console. When in FIPS 140-2 level 3 approved mode, the console displayed **FIPS Mode on**.

4.1 Configuring the Appliance to work in FIPS mode

There are several System Parameters that must be set to appropriate values for having the Appliance work in FIPS mode.
For changing system parameters, open the *Appliance Management* utility and login as the Appliance administrator. Go to the *System Parameters* section and set the values of the following System Parameters:

- *Advanced- Enforce FIPS Approved Algorithm*.

  This value must be set to *true*. When this value is set, it is not allowed to sign using a 1024bit RSA key. When this value is set, it is not allowed to use SHA-1 as part of the digital signature operation.

  Also, when this value is set The FIPS 186-4 based RSA key generation algorithm is used for generating RSA keys. This means that only RSA 2048bit and 3072bit keys can be generated.
- *Advanced – Web Services Support*

  This value must be set to false, since the SOAP based Web Services interfaces is not included as part of the FIPS 140-2 level 3 scope.
- *Advanced – RESTful Web Services Support*

  This value must be set to false, since the RESTFul based Web Services interfaces is not included as part of the FIPS 140-2 level 3 scope.

In Addition, the Primary and Alternate Appliances needs to be configured to use IPSEC configuration. This is done by activating the administrative option called *Set Appliance Communication Mode* using the *Appliance Management Utility*.
The value of *Replication Communication Mode* should be set to *IPSec* (the default configuration is *IPSEC/IKE*).
IPSEC is redundant to the cryptographic protection of this module and no security is claimed for it.
Note: The IPSEC protocol has not been reviewed or tested by the CAVP or CMVP.

5 Upgrade appliance firmware from version 8.0 to version 8.1

Perform the following instructions for upgrading appliance firmware version from version 8.0 to version 8.1.

- Contact DocuSign support to get appliance firmware upgrade package from version 8.0 to 8.1.
- Perform the upgrade in a secure environment.
- The upgrade procedure can be performed only when the appliance is in factory settings.
- Invoke the *Appliance Management* application from the DocuSign SA Client's control Panel.
- Locate the relevant appliance according to its IP address and Login as an appliance administrator.
- Invoke the *Upload Software* option for each upgrade file. Provide the set of upgrade files provided you by DocuSign.
- If the upgrade file is tampered with, the new firmware loading test fails and the module will reject the upgrade.

In each upgrade, a progress bar will indicate the progress of the upgrade operation. When the whole operation ends the Appliance is installed with firmware version 8.1.

6 Upgrade appliance firmware from version 8.0/8.1 to versions 8.5 and 8.51.9.0

Perform the following instructions for upgrading appliance firmware version from version 8.0 or version 8.1 to version 8.4.

- Contact DocuSign support to get appliance firmware upgrade package to 8.4 and upgrade package to 8.5.
- Perform the upgrade in a secure environment.
- Invoke the *Appliance Management* application from the DocuSign SA Client's control Panel.
- Locate the relevant appliance according to its IP address and Login as an appliance administrator.
- Invoke the *Upload Software* option for each upgrade file. Provide the set of upgrade files provided you by DocuSign. There should be an upgrade file to version 8.4 and an upgrade file to version 8.5.

- If the upgrade file is tampered with, the new firmware loading test fails and the module will reject the upgrade.

In each upgrade, a progress bar will indicate the progress of the upgrade operation. When the whole operation ends the Appliance is installed with firmware version 8.5.

Perform the following instructions for upgrading appliance firmware version from version 8.5 to 8.51.9.0

- Contact DocuSign support to get appliance firmware upgrade package to 8.51.9.0.
- Perform the upgrade in a secure environment.
- Invoke the *Appliance Management* application from the DocuSign SA Client's control Panel.
- Locate the relevant appliance according to its IP address and Login as an appliance administrator.
- Invoke the *Upload Software* option for each upgrade file. Provide the set of upgrade files provided you by DocuSign. There should be an upgrade file to version 8.51.9.0.
- If the upgrade file is tampered with, the new firmware loading test fails and the module will reject the upgrade.

A progress bar will indicate the progress of the upgrade operation. When the whole operation ends the Appliance is installed with firmware version 8.51.9.0.