The Digital Signature Company

Algorithmic Research

# CoSign

# Hardware version 7.0

# Firmware version 7.7

# FIPS 140-2 Non-Proprietary

# Security Policy

**Level 3 Validation**

**February 2016**

# Table of Contents

# 1 INTRODUCTION

## 1.1 Purpose

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

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 CoSign in the technical terms of a FIPS 140-2 cryptographic module security policy. Additional information about CoSign and other ARX products is available at www.arx.com.

## 1.3 Terminology

In this document, ARX CoSign is referred to as the *appliance* or *CoSign*.

## 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 CoSign 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: CoSign Security Rules** – Details the general features and functionality of CoSign.
- **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 ARX-proprietary and may only be released under appropriate non-disclosure agreements.
For access to the FIPS 140-2 Validation Submission documents, contact ARX.

# 2 FIPS 140-2 security level

CoSign 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

CoSign 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, CoSign 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.

CoSign 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 CoSign; the asymmetric keys that are kept in the internal database; and the backup of CoSign's database.  They are also used to provide data integrity.

CoSign performs all cryptographic operations internally and, through self-tests, it ensures that these operations function correctly.

## 3.1 Secure by Design

CoSign 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.

Tamper Evident cans provide evidence of any attempt to tamper with module cover. The Tamper Evident cans are placed over a screw that joins the top cover and bottom enclosure.

The Tamper Evident cans are applied at manufacturing stage.

The Tamper Evident cans are shown in Figure 1.

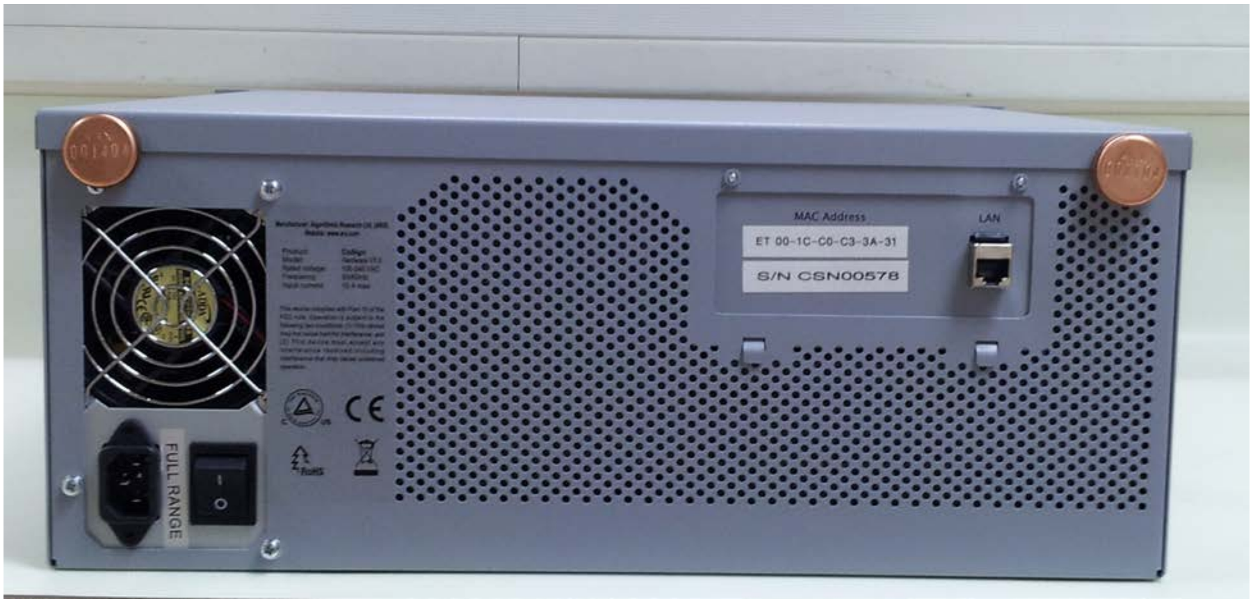

**Figure 1 - Tamper Evident cans**

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

## 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 CoSign, define that the IP address is retrieved using a DHCP protocol and set other networking related parameters. This operation is performed through CoSign'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 CoSign's console.
- **Installation –** This critical procedure must be performed in a secure environment. Only after CoSign is installed it can begin to provide its digital signature services.
  For additional details related to appliance initialization, see Installing CoSign 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 initialization, see *Installing CoSign* on following section.

### 3.3.1 Installing CoSign

The CoSign installation is performed using the administrative CoSign Client. The Cryptographic Officer uses the administrative CoSign client to send installation commands to CoSign. The installation commands are sent using the regular client/appliance secure protocol (see *Secure Operation* on page 11).

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 CoSign appliance.
  Assigning users to groups is relevant only for when CoSign is installed in Directory Independent mode.
- A set of four Server critical Triple-DES keys are randomly generated inside CoSign and are placed inside the internal tamper device. These keys 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 CoSign.
- 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 CoSign.

During normal CoSign operation, a USB-based license plug is plugged into the CoSign USB port. The USB token controls the number of possible existing users in the CoSign database.

ARX manufactures CoSign based on firmware versions 5.2, 6.0 or 7.7.
Also, it is possible to upgrade CoSign firmware version 5.2 to CoSign firmware version 6.0 or upgrade CoSign firmware version 6.0 to CoSign firmware version 7.7. For more information of how to perform a firmware upgrade, refer to Chapters 5 and 6.

### 3.3.2 Restoring CoSign from backup

If the appliance was physically damaged, reset to factory settings, or damaged in some other way, a backup of the CoSign database must be restored to a new or existing CoSign appliance. The restore operation is very similar to the installation of a new CoSign appliance and must be performed in a secure environment. In addition, the CoSign 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 CoSign appliance must be available.
- The Crypto Officer must have a valid backup token that includes the critical keys of that operational CoSign appliance.

During restoration:

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

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

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

## 3.4 Users Directories

CoSign 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.

CoSign provides two additional functionalities when using these environments:

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

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

## 3.5 Managing CoSign

### 3.5.1 Cryptographic Officer

The Crypto Officer performs both appliance and user/groups management of CoSign.

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 CoSign appliance.

The Crypto Officer connects securely to CoSign (see *Secure Operation* on page 11). 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 CoSign is installed in Directory Independent environment. In Active Directory environment, a user is created in CoSign when the Crypto Officer creates the user in Active Directory and defines the user as a member of the CoSign signers 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 CoSign is installed in

Directory Independent Environment. In Active Directory Environment users are deleted from CoSign when the Crypto Officer deletes the user in Active Directory or removes the user from the CoSign signers 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 CoSign to generate additional RSA keys. It is possible to store several graphical signature images in the user account in CoSign. These images are stored in the CoSign database, retrieved by the CoSign 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.

## 3.6 Secure Operation – CoSign Client

Any operator who wishes to use CoSign services can connect via a secure protocol using the CoSign 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 CoSign includes a different TLS Server RSA key.
- The TLS session is based on Triple-DES-CBC encryption and HMAC-SHA1 packet 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 CoSign or using a Kerberos ticket when CoSign is installed in Active Directory environment.
- Only after the user is authenticated, can the user perform operations such as digitally sign data. Similarly, the Crypto Officer can connect securely to CoSign and perform administrative operations.

## 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 CoSign are stored on a special backup token and in an internal tamper device. These keys are loaded into CoSign'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 CoSign critical keys. Without these keys, it is not possible to start CoSign 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 console.

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 CoSign critical keys. Also all users' information as well as the users' keys will be deleted from the CoSign 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 CoSign, it does not include the lockable door on the front panel or the air filter holder that attaches to the front panel.  The door on the front panel can be closed to cover: the LCD display, 4 button keypad, USB port, and the status LEDs.

## 3.8 High Availability and Load Balancing

It is possible to deploy two or more CoSign 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 CoSign appliance.

The main CoSign appliance is named the Primary CoSign appliance, while the other CoSign appliances are named the Alternate CoSign 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 CoSign appliance can be configured to access an external CA in automated mode for the purpose of certificate enrollment.

Upon a creation of a user, CoSign 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 CoSign, 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 include the power connector, network connection (Ethernet Interface using TCP/IP), one key slot, power switches, LEDs, an LCD display, key pad with four buttons, 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 | CoSign Physical Interfaces |
|---|---|
| Data Input Interface | Network port,<br>USB slot for smartcard-based token[1] |
| Data Output Interface | Network port,<br>USB slot for smartcard-based token[2] |
| Control Input Interface | Network port, keypads port |
| Status Output Interface | Network port, LEDs, display |
| Power Interface | AC 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 CoSign Client is used, all requests for cryptographic services are performed through the CoSign 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 LCD 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 SNMP protocol. This status information is sent using the network ports of the module.

## 3.11 Roles and Services

CoSign employs password-based, identity-based authentication of users and operators secured by the TLS protocol. Multiple users and operators can connect and use CoSign 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 CoSign client to the CoSign appliance during user authentication. The CoSign 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 CoSign remotely using the standard CoSign authentication protocol.

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

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 CoSign appliance to a file without requesting for administrator User ID and a password, thus automate a periodical backup for the CoSign 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 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.

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.

CoSign can be configured to use additional authentication for every digital signature operation. The additional authentication is defined as the following:

- 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.

The Radius authentication is based on 32 bytes of authentication data sent from the CoSign appliance to the Radius Server. 16 bytes are randomly generated by the CoSign 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.

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 Environnent | 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

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

| Type of Algorithm | Algorithm Name |
|---|---|
| **Session data encryption** | Triple-DES (ANSI X9.52) in CBC mode – 192 bits – Cert. #2074 |
| **Session packet integrity** | HMAC-SHA1 – Cert. #2441 (SHS Cert #3109) |
| **Database integrity** | Triple-DES-MAC – 192 bits |
| **Database encryption** | Triple-DES (ANSI X9.52) in CBC mode – 192 bits – Cert. #2087 |
| **Backup encryption** | Triple-DES (ANSI X9.52) in CBC mode – 192 bits – Cert. #2087 |
| **Authentication and secure session scheme** | TLS-based session scheme: RSA, Triple-DES CBC, HMAC-SHA1<br>CVL – Cert. #697<br>User ID/Password authentication scheme, based on SHA1 – Cert. #3122 |
| **Digital signature generation** | RSA – Cert. #1929 |
| **Random Number generation** | HMAC-DRBG General Purpose – Cert. #1028 (HMAC Cert #2453),<br>DRBG – Cert #98 |

**Table 4 - Implemented Algorithms**

The module implements the following FIPS approved algorithms:

Triple-DES (Certs. #2074 and #2087)

Triple-DES MAC (Triple-DES Cert. #2087 vendor affirmed)

SHS (Certs. #3109 and #3122)

HMAC (Certs. #2441 and Cert #2453)

DRBG (Cert. #1028)

RSA (Cert. #1929)

CVL (Cert. #697)

DRBG (Cert. #98)

PBKDF (vendor affirmed)

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.
- Triple-DES ( Cert #2074, Key wrapping; key establishment methodology provides 112 bits of encryption strength)
- MD5 (used in Extended Authentication mode – Radius)
- HW RNG (used in Safenet eToken 5105)

The module implements the following Non-FIPS approved algorithms:

- SHS (non-compliant)
- HMAC (non-compliant)
- Triple-DES (non-compliant)
- RSA-RESTful-TLS (key wrapping; non-compliant)

CoSign stores private keys in a key database. This database is stored encrypted (with Triple-DES CBC) on CoSign'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 CoSign appliance. User's public keys, certificates, and graphical images of the user's signature are stored in the CoSign 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])** |
|---|---|---|---|
| CoSign Critical Key 1 – Key and values encryption in database | Triple-DES 192 bit key, FIPS 46-2 | X | |
| CoSign Critical Key 2 – MAC of users database records | Triple-DES 192 bit key, FIPS 46-2 | X | |

| Cryptographic Keys and CSPs | Key Type | Crypto Officer Access (R/W/X*) | User Access (R/W/X[1]) |
|---|---|---|---|
| CoSign Critical Key 3 – CoSign Backup encryption | Triple-DES 192 bit key, FIPS 46-2 | X | |
| CoSign Critical Key 4 – MAC of CoSign Backup | Triple-DES 192 bit key, FIPS 46-2 | X | |
| CoSign TLS RSA public/private key pair | RSA 2048 bit key | X | |
| Triple-DES KEK for CoSign TLS RSA public/private key pair | Password-based key derivation is implemented in compliance with SP 800-132. | X | |
| Password for accessing Triple-DES KEK for CoSign TLS RSA public/private key pair | N/A | X | |
| CoSign Internal CA RSA key | RSA 2048 bit key – defined in installation | X | |
| ARX RSA public key – firmware validation – hard coded | RSA 2048 bit key | X | |
| ARX RSA public key – DLM (downloadable module) validation – hard coded | RSA 2048 bit key | X | |
| Session encryption/decryption keys | Triple-DES 192 bit keys, FIPS 46-2 | X | X |
| HMAC key | 20 bytes | X | X |
| User public key certificates | RSA 2048 bit public keys stored in certificates | X, R | R, W, X |
| User signature keys | RSA 2048 bit | W | W, X |
| DRBG Key | HMAC-DRBG RNG Input | X | X |
| DRBG seed | DRBG seed in Safenet eToken 5105 | X | X |
| DRBG state | DRBG state in Safenet eToken 5105 | X | X |

**Table 5 - Keys, Key Types and Access**

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

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.

Self Testing
CoSign 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 CoSign-Internal Triple-DES implementation)
- Triple-DES decrypt KAT (for CoSign-Internal Triple-DES implementation)
- Triple-DES encrypt (for CoSign-CKIT Triple-DES implementation)
- Triple-DES decrypt KAT (for CoSign-CKIT Triple-DES implementation)
- Triple-DES MAC KAT (for Triple-DES MAC using underlying CoSign-Internal Triple-DES implementation)
- SHA-1 KAT (for CoSign-Internal SHA-1 implementation)
- SHA-256 KAT (for CoSign-Internal SHA-256 implementation)
- SHA-384 KAT (for CoSign-Internal SHA-384 implementation)
- SHA-512 KAT (for CoSign-Internal SHA-512 implementation)
- SHA-1 KAT (for CoSign-CKIT SHA-1 implementation)
- MD5 KAT
- HMAC SHA-256 KAT (for CoSign HMAC implementation)
- HMAC SHA-1 KAT (for CoSign-CKIT HMAC implementation)
- RSA decrypt KAT
- RSA encrypt KAT
- RSA sign KAT
- RSA verify KAT
- HMAC-DRBG KAT
- Critical Function Test - Database Access

### 3.12.2 Conditional Tests

- ♦ Continuous RNG test (for HMAC-DRBG).
  CoSign 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 comparision 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

## 3.13 Mitigation of Other Attacks

CoSign 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 ARX.

[1] Make sure that the new firmware version is a FIPS 140-2 validated firmware version.

# 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 3.13, *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. CoSign also supports LDAP environment, however, this is not included in the scope of this FIPS 140-2 level 3 validation process.
CoSign 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 interface are not included in the scope of this FIPS 140-2 level 3 validation process.
CoSign can authenticate users based on a provided trusted SAML token. This is not included in the scope of this FIPS 140-2 level 3 validation process.

To make sure the CoSign 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 CoSign appliance to work in FIPS mode

There are several System Parameters that must be set to appropriate values for having the CoSign 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 SHA1 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 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.

- *SAML – SAML Working Method*

  This value must be set to 0, so that the appliance cannot accept SAML tokens as authentication credentials.

# 5 Upgrade CoSign firmware from version 5.2 to version 6.0

Perform the following instructions for upgrading CoSign firmware version from version 5.2 to version 6.0.

- Contact ARX support to get CoSign firmware upgrade package from version 5.2 to 6.0.
- Perform the upgrade in a secure environment.
- The upgrade procedure can be performed either on an installed appliance or a non-installed appliance.
- Invoke the *Appliance Management* application from the CoSign control Panel.
- Locate the relevant appliance according to its IP address and Login as an appliance administrator.
- Invoke the *Upload Software* option. Provide the upgrade file provided you by ARX.
- A progress bar will indicate the progress of the upgrade operation. When the operation ends the CoSign appliance is installed with firmware version 6.0.

# 6 Upgrade CoSign firmware from version 6.0 to version 7.7

Perform the following instructions for upgrading CoSign firmware version from version 6.0 to version 7.7.

In order to upgrade to CoSign version 7.7, the CoSign TLS Server key needs to be replaced. Such replacement can be done only when CoSign is in Factory State.

- Contact ARX support to get CoSign firmware upgrade package from version 6.0 to 7.1, from version 7.1 to version 7.4, from version 7.4 to version 7.5 and from version 7.5 to version 7.7.
- Perform the upgrade in a secure environment.
- The upgrade procedure can be performed either on an installed appliance or a non-installed appliance.
- Invoke the *Appliance Management* application from the CoSign 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 ARX.
- In each upgrade, a progress bar will indicate the progress of the upgrade operation. When the whole operation ends the CoSign appliance is installed with firmware version 7.7.

- If the CoSign is in Factory State, then continue to the next step. Otherwise backup the appliance and turn the appliance to Factory state.
- Contact ARX for getting a new TLS Server Key that is unique for your appliance. Use the *Appliance Management application/Upload Software* option, to upload the TLS Server Key that is packaged for you by ARX. Make sure that the operation ended successfully.
- You can now either perform an installation of the appliance or restoration using the previously kept backup file.