Algorithmic Research

ARX

CoSign

Hardware version 4.0
Firmware version 4.3

FIPS 140-2 Non-Proprietary

Security Policy

Level 3 Validation

February 2008

Table of Contents

1 INTRODUCTION 3

1.1 PURPOSE 3

1.2 REFERENCES 3

1.3 TERMINOLOGY 3

1.4 DOCUMENT ORGANIZATION 3

2 SECURITY RULES 4

2.1 SECURE BY DESIGN 4

2.2 PRODUCT DELIVERY 4

2.3 INITIALIZATION 4

2.3.1 Installing CoSign 5

2.3.2 Restoring CoSign from backup 5

2.4 MANAGING COSIGN 6

2.4.1 Cryptographic Officer 6

2.4.2 User 6

2.5 USERS DIRECTORIES 7

2.6 SECURE OPERATION 7

2.7 ADDITIONAL SECURITY ISSUES 8

2.8 WELL-DEFINED INTERFACES 8

2.9 ROLES AND SERVICES 9

2.9.1 Supervisor (Crypto Officer) Role 9

2.9.2 User/Application Role 10

2.10 STRONG CRYPTOGRAPHIC ALGORITHMS AND SECURE KEY MANAGEMENT 12

2.11 SELF TESTING 14

2.11.1 Power-Up Self Tests 14

2.11.2 Conditional Tests 14

2.12 MITIGATION OF OTHER ATTACKS 15

3 FIPS 140-2 LEVEL 3 COMPLIANT MODE 16

1 INTRODUCTION

1.1 Purpose

This document describes the non-proprietary Cryptographic Module Security Policy for the ARX 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/cryptval/.

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 Software 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: CoSign Security Rules** – Details the general features and functionality of CoSign.
- **Section 3: 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 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.

2.1 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* on page 8.

2.2 Product Delivery

When the Crypto Officer receives the appliance, the Crypto Officer must check the appliance's case for any evidence of physical tampering.. Special protective screw cover "cans" are attached over two screws on the back of the appliance. These "cans" would be damaged if the appliance's case has been opened. Verify that the "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.

2.3 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* on page 5.
- **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 page 5.

2.3.1 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 7).

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 and the CoSign appliance.
- 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.
- An RSA key is generated for the internal CA (Certificate Authority) of the appliance. This key is used for generating X.509-based Certificates for users. This key is encrypted and is located 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.

2.3.2 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.

2.4 Managing CoSign

2.4.1 Cryptographic Officer

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

The Crypto Officer connects securely to CoSign (see *Secure Operation* on page 7). The following sections describe in detail all operations that can be performed by the Crypto Officer.

The Crypto Officer creates users according to the organization's policy. For each user, a User-ID and a Password is provided.

By default, after a user is created, the appliance automatically generates a new RSA Private Key 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.

2.4.2 User

For new user accounts the user can change the password. The password length must be greater than six Unicode characters.

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.

2.5 Users Directories

CoSign supports installation in environments where a user directory already exists. Currently the following Users Directory environments are supported:

- Microsoft Active Directory
- Novell NDS

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.
- **Forward user login operation to the directory** – When a user attempts to securely connect to CoSign for any operation, such as signing a document, the login operation is performed in the directory. In this case, CoSign relies on the authentication procedure that is performed by the directory.

Besides Microsoft Active Directory and Novell NDS, 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 is FIPS approved.

2.6 Secure Operation

Any operator who wishes to use CoSign services can connect via a secure protocol. 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 pre-generated by ARX. 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.
- 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.

2.7 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.

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.

2.8 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, indicators, 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 1 shows the mapping of the FIPS 140-2 logical interfaces to the appliance's physical interfaces.

Table 1 – Interfaces

FIPS 140-2 Logical Interfaces	**CoSign Physical Interfaces**
Data Input Interface	Network port, USB slot for smartcard-based token[1]

Data Output Interface	Network port, USB slot for smartcard-based token[2]
Control Input Interface	Network port, keypads port
Status Output Interface	Network port, indicators, display
Power Interface	AC power connector

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

[2] Used only during installation.

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.

2.9 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).

2.9.1 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
- Retrieve user information
- Update user passwords
- Delete users
- Perform shutdown
- Perform software update
- Perform backup of all data in the appliance

- Retrieve information from the log file
- Update system parameters
- Install and restore the appliance

The Crypto Officer also have the following abilities:

- Insert, update or get graphical images of another user.
- Get other users certificates.
- Delete user information such as keys, certificates and graphical images.

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.

2.9.2 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. 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:

- Generate an RSA key
- Generate a digital signature
- Import an RSA key
- Export an RSA key (if the key was defined as exportable)
- Retrieve a public key and certificate
- Upload a user certificate
- Set and retrieve the user's graphical signature images
- Change password

An operator assigned a User/Application role must first authenticate to the appliance using the user ID and password. 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.

Each character may be numeric (0-9) or alphanumeric (a-z, A-Z) or even Unicode. For simplicity lets assume that the set of characters are only alphanumeric. The probability of a random attempt to succeed is: (1 / 62 ^ 6) = 1 / ~56,000,000,000.

The module can handle 60,000 authentication attempts a minute. The probability success in a minute of random attempt is: 1/((62 ^ 6) / 60,000) = 1/ ~946,000.

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. During this session, the operator may perform user management and appliance management services.

Table 2 lists which roles have access to each service.

Table 2 – Role Access to Services

Services	**Role**
Create users	CO
Retrieve user information	CO
Revoke users	CO
Set user password	CO
Perform shutdown	CO
Perform software update	CO
Perform backups	CO
Retrieve log file	CO
Asymmetric cryptography	CO/User
Authentication	CO/User
Graphical signature Import/export	CO/User
Change user password	CO/User
Insert, update or get graphical images of another user	CO
Get other users certificates	CO
Delete user information such as keys, certificates and graphical images.	CO
Zeroize Module	CO
Show Status	CO/User/Unauthenticated
Setting network parameters	Unauthenticated
Time adjustments	Unauthenticated
Shutdown	Unauthenticated

2.10 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:

Table 3 – Implemented Algorithms

Type of Algorithm	Algorithm Name
Session data encryption	Triple-DES (ANSI X9.52) in CBC mode – 192 bits – Cert. #523
Session packet integrity	HMAC-SHA1 – Cert #241 (SHS Cert. #586)
Database integrity	Triple-DES-MAC – 192 bits
Database encryption	Triple-DES (ANSI X9.52) in CBC mode – 192 bits – Cert. #498
Authentication and secure session scheme	TLS-based session scheme: RSA, Triple-DES CBC, HMAC-SHA1, MD5 User ID/Password authentication scheme, based on SHA1 – Cert. #554
Digital signature generation	RSA – Cert. #227
Random Number generation	FIPS 186-2 General Purpose – Cert. #265

The module implements the following FIPS approved algorithms:

Triple-DES (Certs. #498 and #523)

Triple-DES MAC (Triple-DES Cert. #498, vendor affirmed)

SHS (Certs. #554 and #586)

HMAC (Cert. #241)

RNG (Cert. #265)

RSA (Cert. #227)

The module implements the following Non-FIPS approved algorithms:

RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

MD5 (used in TLS)

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.

Keys can be defined in advance as non-extractable or extractable. Keys that are defined as non-extractable cannot be read outside of the CoSign appliance. Keys that are defined as extractable will be encrypted using the TLS protocol when extracted from 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 4 provides a list of keys, their key types, and access control.

Table 4 – Keys, Key Types, and Access

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	TDES 192 bit key, FIPS 46-2	X	
CoSign Critical Key 2 – MAC of users database records	TDES 192 bit key, FIPS 46-2	X	
CoSign Critical Key 3 – CoSign Backup encryption	TDES 192 bit key, FIPS 46-2	X	
CoSign Critical Key 4 – MAC of CoSign Backup	TDES 192 bit key, FIPS 46-2	X	
CoSign TLS RSA public/private key pair	RSA 1024 bit key	X	
CoSign Internal CA RSA key	1024,2048,4096 – defined in installation	X	
ARX RSA public key – firmware validation – hard coded	RSA 1024 bit key	X	
ARX RSA public key – DLM (downloadable module) validation – hard coded	RSA 1024 bit key	X	
Session encryption/decryption keys	TDES 192 bit keys, FIPS 46-2	X	X
Session MAC keys	TDES 192 bit key, FIPS 46-2	X	X
User Public key certificates	RSA 1024, 2048 and 4096 bit public keys stored in certificates	X, R	R, W, X

Cryptographic Keys and CSPs	Key Type	Crypto Officer Access (R/W/X[*])	User Access (R/W/X[1])
User signature keys	RSA 1024 - 4096 bit	W	R[2], W, X

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

2.11 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.

2.11.1 Power-Up Self Tests

- **Low-Level Hardware Tests:** When power is first applied to the appliance, the hardware performs a series of checks to ensure that it is functioning properly.
- **Firmware Integrity Test:** After completing the hardware tests, the appliance performs RSA digital signature verification to ensure that the firmware has not been modified.
- **Cryptographic Algorithm KATs:** Known Answer Tests (KATs) are run at power-up for the following operations:
  - Triple-DES-CBC KAT
  - Triple-DES-MAC KAT
  - SHA-1 KAT
  - HMAC-SHA1 KAT
  - PRNG KAT
  - MD5 KAT
- **RSA Pairwise Consistency Test:** All RSA operations are tested to ensure the correct operation of RSA key generation, encryption/decryption, and signatures.

2.11.2 Conditional Tests

- **RSA Pairwise Consistency Test:** All RSA operations are tested to ensure the correct operation of RSA key generation, encryption/decryption, and signatures.
- **Continuous RNG Test:** This test is run on a continuous basis to detect failure of the RNG.
- **Firmware Upgrade Test:** Appliance firmware can only be upgraded remotely from the management system with proper authentication to the appliance. However, in order to

strictly control the loading of new firmware to CoSign, the new firmware must be digitally signed by ARX. [1]

2.12 Mitigation of Other Attacks

CoSign does not include any mechanisms for the prevention of special attacks.

[1] After loading firmware into this module will no longer be a FIPS 140-2 validated module.

Only if the new firmware is an upgrade to a FIPS approved firmware version.

3 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 2.10, *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.

The appliance can be installed in a MS Active Directory or Novell NDS environments. This type of installation is not FIPS 140-2 level 3 approved. Only the Directory Independent environment is FIPS 140-2 level 3 approved.

The appliance can be installed as an alternate appliance to a primary appliance and thus provide high availability for several CoSign appliances. This mode is not FIPS 140-2 level 3 approved.

The appliance can interface with an external CA and automatically receive certificates from the external CA upon generation of a new user key. This mode is not FIPS 140-2 level 3 approved. Only using an internal CA or uploading a user certificate through the regular client interface is FIPS 140-2 level 3 approved.

There is a special CoSign hardware model called CoSign SSCD (Secure Signature Creation Device). The CoSign SSCD model is based on an internal hardware device that contains a series of smartcards. The users' keys are kept inside the smartcards.
The CoSign SSCD model is not in the scope of FIPS 140-2 level 3 validation.

In order to make sure you are running in FIPS Mode, activate the CoSign Configuration Utility from the CoSign Control Panel in the CoSign client.
Activate the Help\Create Report option and look for the Server\FIPS MODE parameter. Only in FIPS 140-2 level 3 approved, this parameter is set to TRUE.