



A Better Approach to PKI Based Digital Signatures

Authors:

Ramel Levin

Uri Resnitzky



Table of Contents

Introduction	1
CoSign in a Nutshell	1
Introduction to PKI Technology.....	1
Why Use PKI Based Digital Signatures	2
PKI Deployment Problems.....	2
Managing the Keys	2
Integration	2
Solving PKI Deployment Problems by Using CoSign	3
CoSign Architecture and Data Flow	3
Automated Enrollment Using a Company's Standard User Directory.....	3
Working with Other User Management Directories	4
Central Storage of Signing Keys.....	4
Graphical (wet) Signatures.....	4
Ease of use – Sign with a Click.....	4
CoSign Certified Solution.....	5
Turn-Key Solution	5
Improved ROI.....	6
CoSign Technical Overview.....	7
Components	7
Installation	7
End-User Operation	7
Directory Tracking and Publication (Active Directory or Novell/NDS)	8
Certificate Refreshing	8
Management	8
Security	9
High Availability	9
Subordinate CA Support.....	9
External CA Support	9



Introduction

In the last couple of years, new legislation has been passed supporting electronic and Digital Signatures as a way to authenticate electronic data and transactions around the world. The US e-Sign Bill, signed by former President Bill Clinton and the EU Directive for Electronic Signatures are just two examples of this global trend.

Organizations have still been reluctant to jump on the digital-signatures wagon due to the cost and complexity associated with typical PKI solutions. Although Digital Signatures offer an immediate reduction in paper-work, in handling and archiving costs, the technology has become associated with lengthy deployments, high expense and very difficult ongoing management for deployments beyond 100 users.

CoSign, an innovative digital-signature tool, offers a new approach to implementing Digital Signatures. This approach solves most of the deployment problems and dramatically reduces the TCO (Total Cost of Ownership) of deploying digital-signatures.

This white paper deals with the deployment problems that characterizes traditional digital-signature technology and explains how CoSign can solve these problems, resulting in an attractive ROI and a very low TCO for the benefits delivered.



CoSign in a Nutshell

CoSign is an appliance that offers a turn-key digital-signature solution for signing documents, forms and messages within major applications such as Microsoft-Word, Adobe-Acrobat, ERP and Content Management systems. It is based on Public Key Infrastructure (PKI) technology invented in the late 70's and proven as the only technology available today that ensures non-forgable signatures (for more on the PKI technology see "Introduction to PKI Technology" below).

CoSign offers a total digital-signature solution that can perform all the digital-signature related activities including management of the signature credentials and signing of any data and type or transaction with or without a graphical representation of the signature.

Introduction to PKI Technology

In order to gain a deeper understanding of PKI technology, the reader is encouraged to refer to the widespread literature published on the subject. A good starting point would be the PKI forum at www.pkiforum.org.

In a PKI system, each user has two keys: a public key and a private key. These keys can be used for encrypting and decrypting information, for digitally signing electronic information and for verifying the authenticity of their owner. This document focuses on the usage of PKI technology as related to Digital Signatures only.

In a PKI system, the public key is distributed widely, while the corresponding private key is held by its owner in a secure place. While both keys are mathematically related, the public key cannot reveal the private key. This makes PKI a great technology for Digital Signatures. As an example, when Alice wants to sign a document and send it to Bob, she is performing a mathematical function by using her private key. She then sends the original document, along with its signature and her Public Key to Bob. In order for Bob to ensure that the document actually came from Alice, Bob applies a certain computation method to the signature (known as a signature verification), using the Public Key. As a result, he gets a document fingerprint. If it is the same fingerprint as the document that Alice had sent him, then Alice's signature is verified. Otherwise, Bob knows that Alice was not the one signing this document, or that the document has been changed from the time that Alice had signed it.

Since only Alice knows her Private Key, and since this key cannot be computed from the Public Key, data-integrity and non-repudiation are ensured. This process results in signer accountability. In other words, in a courtroom the signer can never claim he/she hasn't signed the document.

There is still an ingredient missing. How can Bob know whether Alice who had sent him the signed document is indeed the same Alice that he wants to conduct business with? Bob needs certification from a trusted third party that knows Alice and can verify that she is indeed who she claims to be. Such entities are called Certificate Authorities (CA); they issue certificates to ensure the authenticity of the signer. Certificates can be compared to passports issued by countries to their citizens for world travel. When a traveler arrives at a foreign country, there is no way for authenticating the traveler's identity but to trust the passport issuer (in PKI terminology: the CA) and use the passport to authenticate its holder in the same way that Bob uses the CA's certificate for authenticating Alice's identity.

Why Use PKI Based Digital Signatures

In today's business and legal systems, paper-based signatures are the most common legal way to ensure the accountability of the signer. Despite the fact that signature forgery is prevalent, signatures are still the most popular (and legal) method used in business today. As more organizations and businesses migrate from paper to electronic transactions, better signer accountability is needed in the electronic world. Basic electronic signatures were devised and have become legal in most parts of the world during the past couple of years.

The US e-Sign Bill (which became active on Oct 1st, 2001) and the EU Directive 1999/93/EC for Electronic Signatures allow for a basic electronic signature: any form of electronic data that is attached to the original electronic information. Under such a definition, for example, a picture of the signer pasted into a Word document is sufficient. This is the equivalent, in paper documents, to placing an "X" or stamp in the signature area. Obviously, the biggest weakness with an "X", typed name, picture or similar such methods is in that there is no way of preventing others from using the same method to forge documents.

The EU Directive recognized this vulnerability and defined in the Directive a stronger type of electronic signature, the Advanced Electronic Signature. Although the Directive had done its best to remain technology-neutral, only PKI Based Digital Signatures meet the requirements for such signatures. Advanced Electronic Signatures provide not only stronger user authentication, but also protect the integrity of the data signed, thus ensuring non-repudiation of the transaction by the signer.

Strong signatures are critical to your organization. Basic electronic signatures that are non-PKI based signatures are vulnerable solutions that add data (text, sound, symbol, picture etc.) to a document and can only serve as a weak method of signer authentication. Only PKI based Digital Signatures offer the best technology to protect against forgery by providing data integrity and non-repudiation.

But as mentioned briefly earlier, PKI has had its own problems preventing it from becoming the leading technology for Digital Signatures. In the next section we shall discuss the deployment problems of PKI based systems.

PKI Deployment Problems

In this chapter we discuss the problems in deploying traditional PKI solutions.

Managing the Keys

As previously mentioned, each user in a PKI environment must have a pair of keys that are used for signing and validating information. The problem is that in order to keep private keys safe, a method for securely storing such keys is required. Usually, key storage solutions are divided into two categories: a hardware medium and a software medium. Hardware devices, often called Hardware tokens, store the keys either on smart cards or on USB tokens. When using a software medium, keys are stored in encrypted files on the users' desktop (or laptop). These encrypted files are often referred to as soft-tokens.

Though the concept is simple, many companies have found that both soft-tokens and hardware-tokens have proven to be very difficult to manage from both a technical and an operational point of view. People tend to lose and forget their hardware tokens, creating lots of administrative problems of re-issuing keys and certificates in case of a loss, or of issuing temporary keys and certificates in case of a user forgetting his/her HW token at home. Organization help desks are overloaded; IT personnel are needed to handle the management and distribution of keys and certificates continuously, resulting in an increase in the number of employees in the IT department or in a loss of time and efficiency.

For most organizations, soft-tokens are also not a suitable solution. In an organization where workers tend to be mobile and switch locations and computers, soft-tokens are problematic since there is no easy way for moving soft tokens from one computer to another. Moreover, computers do tend to crash from time to time, resulting in data loss, including the software token. There is no simple way for preventing the loss of soft tokens in such situations.

Integration

Standard PKI systems include multiple components: the CA (certificate Authority), the key-storage device (hardware or software), software for management of the key storage device, software for managing and enrolling users, and of-course, the components necessary for signing real-life applications (workflow applications, ERP, mail, or any other application). Integration of all these components is complex and hard to maintain on an ongoing basis.

Until recently, there have been very few standard interfacing options between the different components, and even when implementing these interfaces, each vendor defines their own variation of the interface. This has created long and expensive integration processes where integration costs have eventually been rolled over to the end-user, creating high TCO for the entire project.

Integration of the Digital Signature infrastructure with applications is complex and usually involves development with low-level cryptographic API's. Although the technology is maturing and vendors are

complying with standards more than ever before, the only way to interact with tokens (hardware or software) and with the CA is through these low-level cryptographic interfaces (such as PKCS#11, and MS-CAPI) that require in-depth knowledge of PKI technology.

Solving PKI Deployment Problems by Using CoSign

CoSign is a new and innovative Digital Signature application based on PKI technology. Unlike traditional PKI solutions, CoSign solves the deployment, integration and ongoing management problems discussed in the previous section, thus dramatically reducing the deployment and maintenance costs of a PKI based digital-signature system.

CoSign is most suitable for environments in which organizations already know the signing parties. This could be the case with an organization using PKI for Digital Signatures for its internal users (i.e. its employees), with business customers or with vendors.

CoSign Architecture and Data Flow

CoSign is a hardware appliance installed on the network. The appliance includes all the PKI ingredients including the Certificate Authority and the repository of the user's private signing keys. CoSign is integrated with the organization's existing user-management system to reduce the complexity and cost of enrollment and management of new users.

User authentication is performed either by the signing application or by the organizational User Directory. CoSign applies Single-sign-on authentication or authentication per signature. In order to sign, and once the user is authenticated, the document's hash (i.e. the document's digital finger-print) is sent to CoSign and is then signed within the appliance with the user's private key.

At enrollment, Users can optionally register their graphical (wet) signature using an electronic signature pad. The graphical signature image is stored within CoSign. The combination of Wet Signature and Digital Signature provides a visual indication that the user is accustomed to, as well as an assured method of sealing documents.

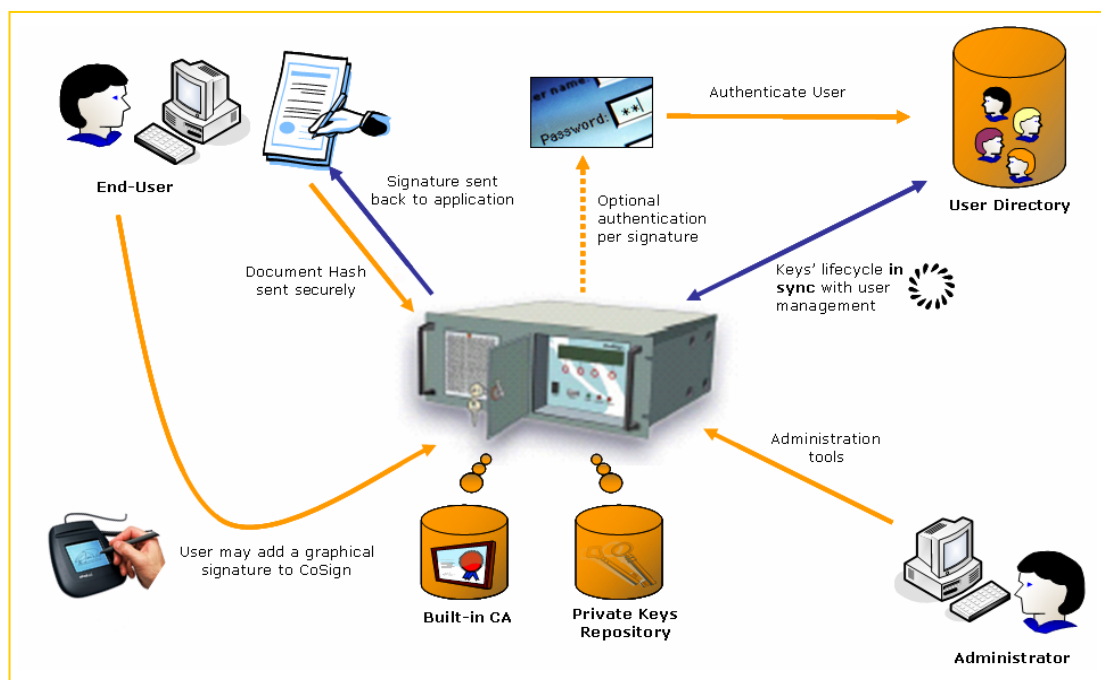


Figure 1: CoSign Architecture

Automated Enrollment Using a Company's Standard User Directory

CoSign provides an automatic synchronization with standard user management directories such as Microsoft's Active Directory, Novell/NDS and other LDAPs. With CoSign, enrollment and ongoing management of users (i.e. creating the keys, issuing a certificate and renewing certificates) is performed automatically once a new user joins the system.

The logic behind this idea is simple. If the organization adds a new user to its user management system, and at the same time decides to allow him access to various network resources such as email, databases and applications, it can also decide whether to allow him access to CoSign and automatically create for him his unique signing keys.

User enrollment in CoSign is tied to the user-management system.

- ▶ **Adding a new user** can automatically create the key-pair and the certificate needed for signing.
- ▶ **Certificate renewal** - Users certificates are renewed automatically just before the certificate expires, for users who are still part of the directory.
- ▶ **User updates** – With any changes to the user's profile (e.g. an employee changing his/her surname), an updated certificate is automatically issued.
- ▶ **Removal of user** - Once the user is removed from the users list (in most cases upon leaving the organization), the certificate is revoked and added to the CRL (Certificates Revocation List). Signatures of this user are no longer accepted even though past signed documents from that user can continue to be validated.

By working in sync with the user management system, CoSign customers eliminate the associated costs of managing users in two separate systems, one for the standard user-management and the other for the PKI system. The on-going management of CoSign is reduced to virtually zero for IT, and enables a very low TCO.

Working with Other User Management Directories

CoSign can also be integrated with other user management systems or environments with no user management to begin with. For example, CoSign can be integrated into a product (e.g. ERP) that has a proprietary user management system or when User management of the product/environment is not based on Microsoft Active Directory or Novell NDS, which are supported by CoSign out-of-the-box.

For such cases, CoSign provides an external API called SAPI (Signature API) that enables the integrator to manage users (add, update, delete) within CoSign or use the CoSign-provided GUI utility to manage users within CoSign.

Central Storage of Signing Keys

We have already discussed that in the traditional PKI architecture, users signing keys are stored in software or hardware tokens, creating technical and logistical problems and significantly increasing the TCO of the system. In CoSign, signing keys (private keys) are stored with the user certificates in a central secured repository.

Users can securely access their signing keys from whatever computer they are working on. There is no need for distributing keys or for issuing temporary keys or handling forgotten tokens, since all keys are centrally managed.

Consider CoSign's secure repository to be a huge network attached smart-card, which is combined with the organization's user-authentication system.

Out-of-the-box, user authentication to CoSign is performed by the same authentication method already in use by the organization before CoSign deployment. The same security measure taken by the organization to access file servers, mail servers etc. is also used by CoSign. If the organization prefers to use a certain authentication method, this method should be used for all purposes and usages. However, other authentication methods, if required, are supported, such as Smart Cards, USB Tokens, Biometric & OTP (One Time Passwords).

Graphical (wet) Signatures

Users may add their graphical (wet) signature using an electronic signature pad. The graphical signature image is stored within CoSign. The combination of Wet Signature and Digital Signature provides a visual indication that the user is accustomed to, as well as an assured method of sealing documents.

Ease of use – Sign with a Click

The CoSign signing process by end-users is simple and intuitive. Looking at Microsoft Word as an example, adding a signature in Word is a two step process: Add a new Signature Field by clicking the Add signature button from the CoSign toolbar and then select 'Sign' from the right-click menu of the Signature Field. If a reason for signing is required (e.g. compliance), the user will be optionally prompted to enter/select a reason.

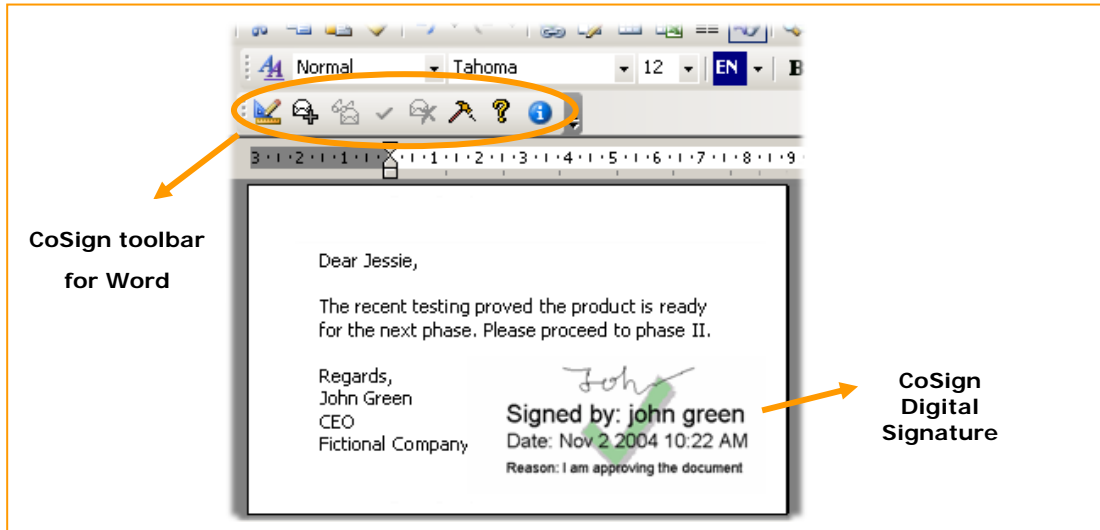


Figure 2: CoSign Digital Signature in Word

Once the user is authenticated, every time he/she signs a document, the document's hash (i.e. the document's digital finger-print) is sent together with the user's credentials (credentials retrieved from the organizational Users Directory) to CoSign. CoSign signs the hash with the user's signing key.

CoSign Certified Solution

CoSign is designed for FIPS 140-2 Level 3 CoSign and has been self certified as an SSCD (Secure Signature Creation Device) meeting the legal requirement for advanced Digital Signatures according to EU Directive for Electronic Signatures. In addition, CoSign is currently undergoing a Common Criteria EAL 4+ evaluation (CWA 14169).

Turn-Key Solution

CoSign provides a complete and integrated Digital Signature solution using industry standard PKI. CoSign includes the certificate authority, the user-management system and the repository of keys and certificates, providing a comprehensive PKI based solution. The appliance integrates with the signing applications using one of the following two methods:

- ▶ Cryptographic / Security interfaces. CoSign supports the major cryptography interfaces: Microsoft Cryptographic API (MS-CAPI), PKCS#11 and Java JCA. PKI-aware applications, which support these API's, will work with CoSign out of the box.
- ▶ SAPI (Signature API) - This easy to use, high-level API is used as a wrapper over the cryptographic APIs described in the previous bullet and intended to be used by applications that are not PKI aware and do not or cannot implement a full-blown cryptographic API. Integration with SAPI is simple and intuitive and supports signing, validating, user management functions and handwritten signatures.

Improved ROI

CoSign brings the TCO of the PKI implementation to an affordable price eliminating all hidden costs. The following table describes costs associated with the implementation of CoSign versus a traditional PKI solution. TCO includes the cost of managing keys, integration, and of adding security measures to secure the entire PKI solution. Obviously, in a traditional PKI based system, there are many hidden costs.

	Traditional PKI	CoSign	Notes
Cost	High	Low	
Integration	\$50,000-100,000	\$0	CoSign is a Turn-Key solution with no hidden integration costs. Traditional PKI takes at least several months to integrate.
Certificate cost	\$30-100 per user on an annual basis	\$0	A built-in CA is embedded in CoSign, eliminating the need to buy certificates and/or a CA.
Hardware token cost	~\$30 per user	\$0	CoSign: No HW tokens are needed. All keys are centrally stored inside CoSign. Traditional PKI: Cost depends on type of device.
CA Security Cost	High	\$0	CoSign is tamper-proof, undergoing C.C EAL4+ and is designed for FIPS 140-2 Level 3; sig. is non-reputable and doc. is sealed/unchangeable.

Figure 3: CoSign's Total Cost of Ownership

CoSign Technical Overview

This section presents the technical details behind CoSign's patent-pending technology.

Components

The CoSign system contains three components:

- ▶ **The CoSign appliance** - Connected to the enterprise's network at the corporate data-center. More than one appliance can be installed in high availability mode.
- ▶ **Client** - The CoSign client software installed on the corporate desktops (Windows 2000 and above) with plug-ins to support applications such as Microsoft Word, Adobe Acrobat.
- ▶ **Administrator** - The CoSign's Microsoft Management Console (MMC) snap-in software, installed on administrator machines. Also includes an electronic pad used to capture and register users' graphical signature images.

CoSign can be seamlessly integrated into the customer's existing IT infrastructure by interfacing with an existing user Directory. The currently supported Directories are Microsoft Active Directory and Novell/NDS with additional LDAPs on the roadmap.

Installation

The installation procedure performs the following:

Directory	Creates an object in the Directory for the CoSign appliance.
	Creates objects in the Directory to which the CA certificate and CRL will be published.
	Creates a Service Connection Point (SCP) object in the Directory for the CoSign service so that clients can automatically connect to the appliance
CoSign Appliance	Activates an internal CA. This includes the generation of the CA signing private key and the CA self-certificate ¹
	For each existing user in the Directory, generates a key and issues a user certificate in the internal CA. The private keys and certificates are all stored in the appliance's internal database.

End-User Operation

If the user is running a PKI-aware application (such as Microsoft Word, Adobe Acrobat, etc.), the application accesses the CoSign client's CSP (Cryptographic Service Provider) which then presents a key container for the user's key stored in the CoSign appliance. The application is then able to use the key container for performing Digital Signature operations.

Steps taken to accomplish this are:

- ▶ The user logs in to the corporate network.
- ▶ The user runs a PKI-enabled CAPI application (e.g. Microsoft Word).
- ▶ The CAPI subsystem activates the registered CSP modules looking for key containers.
- ▶ The CoSign CSP locates the CoSign appliance using the SCP entry in the Active Directory.
- ▶ The CoSign CSP establishes an SSL connection with the appliance, thus authenticating the appliance².
- ▶ Active Directory Single Sign On (SSO): The CSP performs a Security Support Provider Interface (SSPI) exchange over the SSL connection with the appliance using the user's Windows Active Directory logon credentials, in order to authenticate the user to the appliance³.

¹ The internal CA private key is stored in the appliance's internal database.

² The SSL private key used for identifying the appliance is unique for each manufactured appliance and is certified by AR during the manufacturing process.

- ▶ In Novell/NDS and DII (Directory Independent Installations), the user is prompted for his login credentials, which are then transferred over the SSL secured channel to the appliance. In Novell/NDS the credentials are verified against the Directory. In DII, the appliance verifies the credentials locally.
- ▶ In response to a request from the CSP, the appliance retrieves the user's certificate, private key properties (without the key itself⁴) and graphical signature image (if available) from the internal database⁵ and returns them over the SSL connection.
- ▶ The CSP presents the user's certificate as part of the local certificate store and presents the key container to the calling CAPI application.
- ▶ When a Digital Signature request is made by the application, the CSP forwards the request to the CoSign appliance over the SSL connection which performs the operation using the user's private key, logs the signature event into the audit log, and returns the resulting signature.
- ▶ The appliance can be configured to require re-authentication of the user for each signature event. In this case, the user will be prompted for his credentials which will be verified by the appliance against the Directory in AD/NDS or locally in DII.

The installation of the CoSign Client software is quick and simple. Since the installation is based on the MSI technology, the client software can be easily deployed and configured using Active Directory Group Policy or other software management applications.

Aside from CAPI, The CoSign client software also provides the PKCS#11 and JCA cryptographic token APIs enabling integration with other leading PKI enabled client applications.

Directory Tracking and Publication (Active Directory or Novell/NDS)

The appliance tracks changes in the Directory and takes the appropriate measures to reflect the change in the internal database:

- ▶ When a new user is added to the Directory, the appliance retrieves the new user's information, generates a new private key and enrolls it in the internal CA. The newly issued certificate is stored, along with the private key, in the internal database. The new user can immediately start using Digital Signatures after logging into the corporate network, without first having to go through a tedious enrollment process.
- ▶ When an existing user is deleted from the Directory, the appliance revokes the user's certificate from the internal CA and deletes the user's records from the internal database. This provides immediate revocation of the key material preventing any risk of forged signatures.
- ▶ When user details (such as name or email address) are updated in the Directory, the appliance retrieves the updated information, revokes the existing certificate and issues a new certificate for the user, based on the updated information and the existing private key.
- ▶ The CA certificate, CRL and the users' certificates are all published and kept current in the Directory by the appliance. This enables smooth integration of Directory enabled applications.

Certificate Refreshing

The appliance automatically refreshes soon-to-be-expired user certificates by re-enrolling the user's key in the internal CA. Thus the user certificate is updated transparently without user involvement.

Management

Management of the system requires minimal attention from administrators and is limited to system-wide tasks:

- ▶ Backup and restoring of the appliance's encrypted database.
- ▶ Secure loading of digitally signed firmware updates.
- ▶ System parameter settings.

These tasks are performed using the familiar MMC interface. The CoSign MMC snap-in communicates with the appliance in the same manner as the client CSP (SSL session with user authentication). Management functions are only allowed for authenticated users that belong to an administrators group.

³ This allows the use of 3rd party advanced authentication mechanisms such as one-time password and biometric authentication devices, which support the windows logon architecture.

⁴ User private keys are never exposed outside the CoSign appliance. This feature provides a level of security comparable to that of a smart-card.

⁵ All records in the internal database are referenced using the Directory GUID of the authenticated user which is retrieved following a successful authentication.

A per-user management tool is provided for Directory Independent Installations. This tool can then be used to create, modify and delete users, as well as to set and change user passwords.

The system's audit log maintained in the appliance can be downloaded and viewed using the standard Windows Event Viewer. Unlike other solutions, the CoSign audit log enables the administrator to closely track private key's usage (when/who signed).

Security

The CoSign appliance is designed for FIPS 140-2 Level 3 and Common Criteria EAL4+ validation. This ensures that the system meets the stringent security standards required for HSMs, as well as guarantees overall system security (hardware, operating system and application):

- ▶ Only approved standard algorithms are used for symmetric encryption, digital hash calculations and random number generation.
- ▶ Self tests are performed to ensure proper operation of the cryptographic algorithms and the random number generator.
- ▶ Tests are performed to ensure the integrity of the CoSign firmware and database.
- ▶ The appliance's internal database is encrypted to prevent any possible compromising of users' private keys.
- ▶ The appliance is encased in a special hardened enclosure with tamper detection sensors.
- ▶ In case the device is tampered with, all sensitive keys used for protecting the system (database encryption, etc.) are erased, rendering the information inside the appliance worthless (tamper resistant).
- ▶ The appliance's operating system is hardened by removing unneeded components, installing a network packet filter, etc.
- ▶ Validations include a review of the product's formal Security Policy, Finite State Machine and software development process documentation (source-code control procedures, product design, test plan, etc.). Functionality, interface specifications and implementation are verified by an independent, accredited 3rd party-testing laboratory.

High Availability

Several CoSign appliances can be installed concurrently to allow **Redundancy** and **Load Balancing**.

- ▶ Redundancy - In case of failure of one of the CoSign appliances, one of the other CoSigns will take over and perform Digital Signature operations.
- ▶ Load Balancing - Balancing workloads between multiple CoSigns, allowing organizations to confidently conduct large transaction volumes simultaneously.

Only the Master appliance will perform user synchronization operations, while other installed CoSign appliances will provide hot backup for signatures and will not handle new users.

Subordinate CA Support

If a company has already invested in a PKI infrastructure, CoSign can be configured to be used in an environment that already includes a CA, and can act as a subordinate CA. In this mode, CoSign still generates private keys and issues certificates. However, CoSign's CA is signed with the parent CA's key. This eliminates the need to distribute CoSign's root CA, as the parent's CA (assuming it has already been distributed) can be used to validate the certificates. The certificate chain of each user certificate will include the CoSign CA, the parent CA, and any other parent CAs that might be defined.

External CA Support

CoSign supports organizations requiring certificates from an external CA (e.g. national CA issuing qualified certificates). When using an external CA, the CoSign appliance does not generate end-user private keys and certificates during installation. In this case, you have to use other mechanisms which are part of the external CA's enrollment procedure for generating end-user private keys and certificates.



For more information please contact
sales@arx.com or visit www.arx.com

Your comments and feedback are welcome media@arx.com