DocuSign Signature Appliance Release Notes **September 2016**

DocuSign
The Global Standard for eSignature

This file is part of DocuSign Signature Appliance distribution
and is covered under the same License Agreement

This document contains technical release notes for all DocuSign Signature Appliance versions and complements information written in the DocuSign Signature Appliance User Manual.

Please read through the DocuSign Signature Appliance documentation and the release notes before installing the DocuSign Signature Appliance.

Updated: October 5, 2016

Table of Contents

Release Notes – DocuSign Signature Appliance Version 8.2

General Information

DocuSign Signature Appliance version 8.2 can be based on either hardware version 7.0 or hardware version 8.0. It can also be deployed on DocuSign SA Enterprise hardware.
The functionality of Appliance version 8.1 (interfacing with the Symantec CA service) is not supported.

The Appliance version is in the process of Common Criteria certification (EAL4+) as a Qualified Signature Creation Device (QSCD) or as a Qualified Seal Creation Device according to the eIDAS regulation (EU) No 910/2014.
The new DocuSign SA Client (Signature Appliance's Client) as well as the appliance are DocuSign branded.

DocuSign Signature Appliance version 8.2 release date – 22 Aug 2016

DocuSign SA client version 8.2 release date – 29 Sep 2016

New Features and Fixes

DocuSign Signature Appliance – General

- The main interface of the appliance can be accessed through the TLS 1.2 or TLS 1.1 protocols in addition to the TLS 1.0 protocol.
- The Console enables the Appliance Administrator to duplicate backup tokens from an existing backup token. This functionality is not available when the Appliance is deployed in Common Criteria mode.
- A new Out Of Band authentication mechanism is introduced. In this mode, the user can request a One-Time-Password from the Primary or Alternate Appliance. This OTP can be used as the second factor for producing a digital signature.
- The problem of performing a *Reset Tamper* to a working appliance was fixed. (***8.0-srv-006)***
- The problem that arose in a Multiple-Domain environment, where a client that interfaces an alternate appliance fails to create a new user, has been fixed. The client is properly redirected to create the user account in the Primary Appliance. ***8.0-SRV-010*** is fixed. (this problem was also fixed in Appliance version 8.1)
- The DocuSign Signature Appliance Administrator Guide includes updated information for the Centralized DocuSign SA Client Installation. In particular, there is a fix for a problem with deploying the DocuSign SA Printer driver.

DocuSign Signature Appliance – Common Criteria

- The Appliance can be installed either as a Qualified Signature Creation Device or as a Qualified Seal Creation Device. When the Appliance is installed as a Qualified Seal Creation Device, a digital signature can be created based on presenting a static password.
- The Appliance can be configured to allow the creation of several digital signatures within a configurable time frame following user authentication.
- When the Appliance is installed in Common Criteria mode, it is now possible to perform a secure backup of the Appliance's information and perform a restore operation if necessary.
- When the Primary Appliance is in a temporary fatal error, it is possible to use a selected Alternate Appliance for the purpose of digital signature creation.

DocuSign Signature Appliance – REST API and SOAP API

- A Users Administration API was added to the Appliance's REST API. For example, operations such as *disable user* and *delete user* were added. More detailed information is found in the Signature APIs Developers' Guide.
- It is now possible to sign Office documents using SHA-2 using the DocuSign Signature Line Provider using the Appliance SOAP and REST interfaces.
  Problem ***7.1-CLI-010*** is fixed.
- Appliance Hardware version 7.0 can be accessed through TLS 1.2 or TLS 1.1 protocols to access REST interface.
  Problem ***8.0-SRV-005*** is fixed.

DocuSign SA Client

- There is a new naming convention for former CoSign related components:
  - The CoSign Appliance is now the DocuSign Signature Appliance
  - The CoSign client is now the DocuSign Signature Appliance Client or DocuSign SA Client
  - OmniSign is now Prepare & Sign
  - OmniSign Printer is now the DocuSign SA Printer
- In cases where certificates from external CAs are used to sign and it is required to embed an OCSP response information as part of the signature for Long Term Archiving, a problem arises when only the end user's certificate has an OCSP responder URL, while other certificates in the chain do not refer to a relevant OCSP responder (see ***8.0-SRV-013).***
  Through the Configuration Utility and SAPI, it is possible to define one of the following configuration:
  - All certificates in the chain have their OCSP response embedded into the digital signature
  - All certificates in the chain have their CRLs embedded into the digital signature
  - Only the end user's OCSP is embedded into the digital signature
  - End user's OCSP and the CRL's of the intermediate CAs and ROOT CA are embedded into the digital signature
- Problem signing .docx files in Win2012 and some other environments was fixed. (***8.1-CLI-001****)*

Known Problems/Limitations/Warnings

DocuSign Signature Appliance

- The REST interface does not support embedding OCSP in a signature when the hardware version is based on XP Embedded (i.e., Hardware version 7.0 and below). (***8.2-SRV-001***).
- The REST interface cannot retrieve or delete graphical signatures with a space character in the graphical signature filename. This problem exists in version 8.0 as well. (***8.0-SRV-007***).
- There are problems with Umlaut support when using the REST interface, particularly when used as characters in the user password field. (***8.0-SRV-008***).
- There is a problem with special characters in the user name when using the REST interface. (***8.0-SRV-009)***

DocuSign SA Client

- There are some locations in the Client user interface where the name CoSign or ARX still appears. (***8.2-CLI-001***).
- There are some translations of rebranded text that require improvements. This will be done in future versions. (***8.2-CLI-002***)
- PDF Documents that are signed with *Prepare&Sign* version 8.0 or above, cannot be validated with DocuSign SA Client versions prior to version 8.0.
  The reason for this behavior is that the default signature format is aligned with PAdES, which involves a format that was unknown before version 8.0.
  The newly signed documents can be validated using either a new DocuSign SA client version or using a PDF reader. (***8.2-CLI-003***)
- When using SAPI in direct mode, the application name is not written as part of the signature details in the Appliance's log file. (***8.2-CLI-004***)
- The DocuSign SA Signature Line Provider does not support viewing the signature in recovery mode. Recovery mode may happen when an information that is required for proper validation is missing. In this case, Microsoft Office shows a signature validation image that refers to the current time and not to the signature time. (***8.2-CLI-005***)

Release Notes – DocuSign Signature Appliance Version 8.3

General Information

DocuSign Signature Appliance version 8.3 is based on Appliance version 8.0 and has functionality similar to Appliance version 8.2.
The version has the following functionality:

- Ability to limit the TLS protocol version used when accessing port 443 (the regular client-server interface).
  To limit the TLS protocol version, set the *Minimum server TLS version* in the *System Parameters*→ Advanced section as defined below, and then perform a server software restart.
  - 0 – in this case TLS1.0, TLS1.1 and TLS1.2 protocols are allowed.
  - 1 – in this case TLS1.1 and TLS1.2 protocols are allowed.
  - 2 – in this case only TLS1.2 protocol is allowed.

  Note that the DocuSign SA client must also be configured to use the same TLS protocol version (the client's default TLS version is 1.0).
  Set the following entry *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ARL\CoSign\CkitCli]*"SSLLibraryVersion" to any of the following possible values to define TLS protocol version:

  - dword:00000000 – Using TLS version 1.0
  - dword:00000001 – Using TLS version 1.1
  - dword:00000002 – Using TLS version 1.2
- When the REST based Web Services is enabled, it is always based on TLS version 1.2.
- When the SOAP based Web Services is enabled, it supports TLS version 1.0, 1.1 and 1.2. However, when the SOAP based Web Services interface is disabled, there is no network access to port 8080 of the appliance. In the previous functionality, even when SOAP based Web service was not accessible, clients could connect to port 8080 of the appliance.
  Version 8.3 can be upgraded **ONLY** from Appliance version 8.0 and **CANNOT** be upgraded from appliance version 8.2 or appliance version 8.1.

DocuSign Appliance version 8.3 release date – 22 Aug 2016

Release Notes – DocuSign Signature Appliance Version 8.1

General Information

DocuSign Signature Appliance version 8.1 is based on hardware version 8.0 and is enhanced with the functionality of interfacing Symantec Certificate management services in an automated manner. This functionality cannot be used together with hardware version 7.0.

A new DocuSign SA Client (Signature Appliance's Client) was produced with many enhancements and fixes. This client can be used to interact with Appliance version 8.0, Appliance version 8.1 and also with Appliance version 8.2 described above.

DocuSign Signature Appliance version 8.1 release date – 22 Aug 2016

DocuSign SA client version 8.1 release date – 22 Aug 2016

New Features and Fixes

DocuSign Signature Appliance

- The Appliance can be configured upon installation to interface with the Symantec CA services automatically such that every new user can be automatically enrolled for a certificate provided by the Symantec CA. A special managed account must be defined in Symantec for automated provisioning of user certificates.
- The problem that arose in a Multiple-Domain environment, where a client that interfaces an alternate appliance fails to create a new user, has been fixed. The client is properly redirected to create the user account in the Primary Appliance. ***8.0-SRV-010*** is fixed.

DocuSign SA Client

- The client is based on .NET Framework 4.0 and does not require installing older .NET Framework versions.
  Problem ***8.0-CLI-001*** is fixed.
  Problem ***6.2-CLI-001*** is fixed.
  Problem ***6.2-CLI-003*** is fixed.
- It is now possible to sign Office documents using SHA-2 using SAPI.
  7.1-CLI-010 is fixed.
- There is no need to configure .NET to allow performing SHA-2 signatures on XML documents and InfoPath documents.
  7.1-CC4SP-002 is fixed.

Known Problems/Limitations/Warnings

DocuSign Signature Appliance

- Appliance version 8.0 can be upgraded to Appliance version 8.1 only in Factory State. Also, you must perform a reset to Factory Settings right after the upgrade.
- Appliance version 8.1 is supported only for FIPS Appliance Hardware version 8.0.
- When the Appliance interfaces the Symantec CA, you must set up a special account with special configuration in the Symantec CA service. Please follow the instructions in the Appliance Admin guide.

If configuration is not performed properly, interface problems may occur after installation is complete. For example, if the uploaded *CA Information* does not refer to the correct account ID in Symantec, the Administrator receives no error message but users will not get a Symantec certificates and the *CA Information* will need to be uploaded again. (***8.1-SRV-002***)

- When the Appliance is installed in external CA mode – Symantec, all system users except for *csnadm* must adhere to the following policy:
  - *User ID* or *User Display Name* in Active Directory may not contain special characters or Umlauts
  - The common name must be in the format "<First Name> <Last Name>"
  - Email is a mandatory field

  Both Users Administrators and Appliance Administrators must follow the above policy. (***8.1-SRV-003***)
- The value of the *Renewal Window* parameter in the *Additional Certificate Options* in Symantec must be large enough that any automatic refresh certificate request performed by the appliance or any attempt at updating parameters such as the user's email will not be rejected by the Symantec CA service.
- When the Appliance local time is different from the correct time by more than a few hours and the administrator tries to configure an NTP, NTP configuration might be unsuccessful yet the administrator may not receive an error message. As a workaround, update the local time to the correct time and then update the NTP service parameters. (***8.1-SRV-001***).

SAPI

- Calling the function PKCS7BlobGetValue (in C#) with the SAPI_ENUM_PKCS7_FIELD_TIME returns a null value instead of the time. (***8.0-CLI-012)***
- A problem arises when directing SAPI to embed OCSP as part of the signatures in cases where not all certificates in the chain support OCSP. This problem happens when CAs such as Symantec provide OCSP information in the end user's certificate, but not as part of the intermediate CAs or ROOT CA. In this case, the whole signature operation fails.(***8.0-SRV-013)***
- Problem signing .docx files in Win2012 and some other environments (***8.1-CLI-001)***

Admin Client

- There is a problem installing an alternate appliance in a complex domain environment. Specifically, the Alternate Appliance joins a domain different from the domain of the Primary Appliance.
  As a workaround, the following registry entry needs to be set:
  (*HKEY_LOCAL_MACHINE\SOFTWARE\ARL\CoSign\SnapIn*
  "*ComputerAccountPath*"="<*path to the relevant path*>" - for example: set the following string "OU=Servers,DC=root,DC=com" before installing the alternate appliance. This directs the client to deploy the alternate appliance in the intended location.

Release Notes – CoSign Version 8.0

Release Date: March 15, 2016

General Information

CoSign version 8.0 appliance is based on a new hardware and a new operating system.
The new hardware provides better performance rates, especially in digital signature operations, which can reach 750 2048bit RSA digital signatures/sec.

Older Appliance Hardware versions (such as software version 7.5, hardware version 7.0) can be upgraded to CoSign Software version 8.0.

As in previous version, there are two available form factors:

- CoSign FIPS Appliance - 3U appliance that is in the process of FIPS 140-2 level 3 and Common Criteria EAL4+ certifications.
- CoSign Enterprise Appliance – 1U appliance in a standard commercial casing

There is a new licensing scheme that in addition to maximum amount of users also include a maximum number of digital signatures limitation and a license expiration.

This version includes an updated admin guide, user guide and SAPI guide.

The release of version 8.0 includes the following components:

- CoSign Appliance version 8.0
- CoSign client version 8.0

Starting from CoSign version 8, the CoSign Appliance is now named the DocuSign Signature Appliance.

New Features and Fixes

CoSign Appliance – Hardware version 8.0

All following functionality is not applicable for the case that CoSign Hardware version 7.0 is upgraded with Appliance Software version 8.0

- CoSign Hardware version 8.0 supports also IPv6 in addition to IPv4
- The new hardware appliance supports two LAN interfaces.
  The first LAN interface is used for the regular client/administrator operation based on a secure TLS communication. The second LAN interface is dedicated to Web based Console Administration.
- The Administrative console is based on a Web Console and offer similar console operations as in previous versions. For more information refer to the CoSign Administrator's Guide.
  For connecting to the Web Console, connect a PC or laptop and access the following URL : http://10.0.0.2:8088
- To view updated alert information through the CoSign Web Console it is advised to manually refresh the Web browser as needed.
- The new FIPS Appliance includes a touch screen that displays some information such as the status of the CoSign Service and deployed software/hardware versions. The touch screen will get to sleep mode if not operated in a few minutes.
- In the case of using the FIPS appliance, when the appliance is shutdown, touching the Touch Screen can perform an Appliance startup. This is in addition to the special hidden startup button in the front panel of the appliance.
- The new FIPS appliance has a dual power supply that can be replaced without opening the secured appliance and does not interrupt the appliance from providing its service.
- A new cloud based event monitoring system can be used for addressing appliance performance problems and other technical issues.
- CoSign SOAP Based Web Services supports using TLS version 1.0, 1.1 and 1.2. Previous version supported only TLS 1.0.

CoSign Appliance – Software version 8.0

- The audit log is implemented using a different mechanism. Former versions were based on Windows Event Log format.
  Starting from CoSign version 8.0, the event log is implemented inside the database of the CoSign appliance.

When the administrator is retrieving the audit log, the replied file is based on CSV format.
In a high availability environment, each appliance maintains its own audit log.

- The Administrator can control the amount of kept audit events based on defining a time window, where older events will be deleted.
- A new mechanism is introduced for systems that are running in a high performance rates. An RSA Key Pool mechanism can be defined such that when a new user account is created, an RSA Signature key will be automatically assigned to the account without the delay of the RSA key generation algorithm.
  The relevant system parameter can define the maximum amount of RSA keys that can be stored in the pool.
  This mechanism is not supported when CoSign is deployed in Common Criteria mode.
- CoSign SOAP based Web Services modified the behavior of the Add User function such that if the user already exists, the user will be updated and no error will return.
  This behavior is relevant for regular users and not for administrators.
- CoSign SOAP based Web Services modified the behavior of the Get Users. When there are more than 1000 users a maximum number of 1000 users will be returned. There will be no indication that there are more than 1000 users in the system.
  This behavior is relevant for regular users and not for administrators.
- For installation with very large user volumes (more than 200,000 users) when there is a substantial user community that rarely sign, it is possible to direct CoSign not to automatically perform a refresh certificate when close to certificate expiration. For example, it can be defined to perform that actual certificate refresh only upon next user logon. More information is available in the CoSign Administrator guide.
- Problem related to signing with a given requested time-zone and the given time-zone is 0 (i.e., GMT), the time-zone used is PST (Pacific Standard Time) was fixed (***7.4-REST-001***).
- CoSign is fully compliant with the FIPS 186-4 standard.
- CoSign REST Based Web Services supports using TLS version 1.0, 1.1 and 1.2. Previous version supported only TLS 1.0. This is relevant only when Hardware version 8.0 is used.

CoSign Client

- Microsoft Office 2016 is supported.
- Problem of long delays when using OmniSign to sign PDF files that are located in a network file system were resolved.
- There were problem showing specific PDF documents in OmniSign. The problem is resolved.
- CoSign Client now supports also Macedonian.

SAPI/Restful API

- SAPI and REST include API for enrolling a new key and certificate from external CA for a user.
  The enrollment can be achieved using the following two new SAPI functions:
  - SAPIGenerateKeyPair
  - SAPIImportCertificate

  Certificate request generation can be achieved by calling the SAPIBufferSignEX API.
  This functionality is supported also when using CoSign REST API.
- PDF signatures are full PAdES compliant. A small issue related to PKCS#7 claimed time was fixed.
- CoSign REST API supports authentication based on SAML token.
- CoSign REST API supports authentication based on binary representation. This can be used for enabling SmartCard based authentication.
- OCSP information that relates to CoSign Internal CA can also be appended to the digital signature, thus enabling a more standard LTV (Log Term Validation) signatures.
  This is based on an internal service provided by the Appliance.

Known Problems/Limitations/Warnings

CoSign Client

- When CoSign Client is installed on Windows10, .NET Framework 3.0 (or .NET Framework 3.5) is not automatically installed as part of the preliminary installation phase. This effect the CoSign Signature Line Provider for Office. (***8.0-cli-001***)
  Other means should be used for enabling .NET Framework 3.0.
- CoSign legacy add-in for Word and Excel does not support Office 2007. Only Office 2010/2013 versions are supported. (***8.0-cli-002***)
- CoSign Client is not supported when installed on Vista. (***8.0-cli-003***)
- *Microsoft Office Compatible Signature* option is not supported when signing an *Entire File* signature on .doc files. This mode creates an addition Office Signature that is compatible with Office XP/2003. (***8.0-cli-004***)
  6.2-CLI-005 problem is irrelevant.
- When Using SAPI to sign Word documents, where the Word document contains an invalid URL (in terms of the URL format) fail the signature operation. The error occur since there is a Microsoft Code that fails parsing the URL. (***8.0-cli-005***)
- When CoSign Client is installed on Windows7, the following Microsoft update must be installed - https://technet.microsoft.com/en-us/library/security/3033929. This is due to that DLLs of the CoSign Client and CryptoKit are signed using SHA256 hashing algorithm. (***8.0-cli-006***)
- When performing an enrollment through browser (such as Internet Explorer) and the CoSign Appliance is configured to use *Prompt For Sign*, it may that the window that asks the user for

providing an extended password will not appear and thus eventually the enrollment will fail. (***8.0-cli-007***)

- The CoSign Client installation will try to install .NET Framework 3.5 if does not exist in the user's PC/laptop. There are programs such as WSUS that will prevent such an installation. In these cases, the end user should manually install .NET Framework 3.5. (***8.0-cli-008***)
- In some rare cases, when Office 2016 is used, the CoSign add for office is not automatically added as a COM Add-in. In such cases, the add-in should be manually added. (***8.0-cli-009***)
- In Windows 10, after uninstalling the CoSign Client, there are some undeleted registry entries that forbid performing a reinstallation of the CoSign Client.
  (*[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F75D2B1D-5309-41DF-BC96-DFC3C3568C1D}] "sEstimatedSize2"=dword:00002ecb)*.
  Removing this entry, will allow the reinstallation of the CoSign Client. (***8.0-cli-010)***
- When MS updated identified as MS16-035 is installed, it affects the .NET library that validates XML signatures. Using special registry entries will allow continue and validating signed files:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Security\SafeTransformMethods@XmlDsigXPathTransform=http://www.w3.org/TR/1999/REC-xpath-19991116
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Security\SafeTransformMethods@XmlDsigXsltTransform=http://www.w3.org/TR/1999/REC-xslt-19991116

  (***8.0-cli-011)***

CoSign Appliance

- CoSign Appliance hardware version which is lower than Hardware Version 5.0 cannot be upgraded to CoSign Software version 8.0. (***8.0-srv-001***)
- NTP definitions cannot be set using IPv6 and only set using IPv4. (***8.0-srv-002***)
- If Internet Explorer 11 is used as console, the URL must be provided with explicit IP address (i.e. http://10.0.0.2:8088) and not by specifying a DNS name (e.g http://console.dom.com:8088) (***8.0-srv-003***)
- The CoSign Web Console enables you to access the www.arx.com web site for information. If the console is detached from the Internet, the attempt to connect to www.arx.com will not succeed. (***8.0-srv-004***)
- Problem using tls1.1 or tls1.2 with CoSign REST based Web Services for CoSign Appliances that were upgraded from a previous version (e.g version 7.5) to CoSign version 8.0. (***8.0-srv-005***)
- It is forbidden to perform a Reset Password operation to a working system (not in tamper state) using a wrong Backup Minikey. (***8.0-srv-006***)

SAPI

- The new SAPIGenerateKeyPair and SAPIImportCertificate API does not support authentication using SAML tickets. (***8.0-SAPI-001***)
- When there is no restriction of *Prompt for Sign* in the appliance, there is inconsistency between variant CoSign Applications that send a wrong extended password. Some of the applications will fail the operation and some of the applications will ignore the wrong password and thus succeed. (***8.0-SAPI-002***))
- When trying to import a certificate that does not match the user key, it will not succeed, but no error code is replied to the caller. (***8.0-SAPI-003***)

CoSign Web App

- If Firefox is used (for example, versions 40.0, 41.0, 44.0), when the user connects to a Cloud Storage, there is a problem choosing a different folder within the cloud storage. (***8.0-WEBAPP-001***)

Release Notes – CoSign Connector for SharePoint 7.3.2

General Information

Release Date: January 12, 2016 – CoSign Connector for SharePoint version 7.3.2

Features and Improvements

- Domain Filter – It is now possible to limit http redirections to specific domains and sub domains for all CoSign Connector for SharePoint web pages. This feature was designed to prevent URL hijacking.
- Signature Locators Configuration is now available in Central Administration.
- Script Filtering – Strings containing client side scripts that might be displayed on one of the CoSign Connector web pages are now filtered. This prevents execution of malicious scripts that could be injected during signing of documents.

Bug Fixes

- Microsoft Signature Line appearance mask for date/time was fixed. Now date\time will be shown only if specified in the appearance mask. ***(XX-CC4SP-001)***

Release Notes – CoSign Version 7.5

General Information

Release Dates:

- July 15, 2015 – CoSign Web App version 7.5
- August 6, 2015 – CoSign Client version 7.5
- October 13, 2015 – CoSign Appliance version 7.5

The release of version 7.5 includes the following components:

- CoSign Web App version 7.5
  The default deployment of CoSign Web App version 7.5 is CoSign Client version 7.23.
- CoSign Appliance version 7.5 – this version is Common Criteria EAL 4+ certified
- CoSign client version 7.5
- CoSign Mobile App for Android and iOS version 1.1

New Features and Fixes

CoSign WebApp

- In addition to support of Identity Providers based on ADFS using WS Federation protocol, it is now possible to use SAML2 protocol either using Microsoft ADFS or other Identity Provider solutions. As in previous versions, when CoSign Web App integrates with an Identity Provider, the local Identity Provider is responsible for authenticating the user and a proof of authentication will be sent to the CoSign Web App.
- The External Identity Provider interface can be used together with the CoSign Web Agent (referring to the CoSign Web App that is integrated with a document management solution).
- End users can logon to CoSign Web App based on an Active Directory Kerberos tickets. Using this procedure, the user is automatically logged on to the CoSign Web App without being required to enter a User ID and password.
  This option can also be used when the CoSign Web App is deployed as a CoSign Web Agent integrated with a document management system.
- The CoSign WebApp is now capable of using PDF forms using the RADPDF product (http://www.radpdf.com/), which should be installed in the CoSign Web App platform. In this

configuration, users can enter the form fields through the CoSign Web App interface and then sign the filled-in PDF form.
This option can also be used when the CoSign Web App is deployed as a CoSign Web Agent integrated with a document management system.

- The user can now press the *Log Off* link to exit from the current CoSign Web App session. Once the Logoff link is pressed, the Login window is displayed.
  If an External Identity Provider is used, it can be configured to notify the Identity Provider that the user has finalized the session with the CoSign Web App.
- CoSign Client version 7.5 supports the use of field locators in PDF documents. The field locators are viewed as regular signature fields to the signer. Upon performing a signature operation a new signature field is created and signed.
  When the CoSign Web App is installed with CoSign Client version 7.5, the CoSign Web App can be configured to use Field Locators.

CoSign Appliance

- CORS Support in REST. This allows invoking CoSign RESTful based web services based on running JavaScript code as part of a Web Application.
- Supports High Availability for Radius Servers when CoSign is deployed in Common Criteria mode
- License mechanism is now based on time expiration.
- Appliance can be optimized to reduce the amount of TLS session initiatives in a loaded environment.
- The appliance uses an improved protocol for CoSign REST interface (updated TLS/SSL version) and for the regular client interface.

CoSign Client

- Windows10 is supported.
- The Client Optimization mode also provides faster signature performance
- OmniSign has some new GUI experience and some additional fixes related to the display of PDF documents. Following are some of the improvements:
  - New design of the Welcome Screen
  - More functionality to control the design of texts and graphics inside the graphical signature
  - Ability to rotate a PDF document

  - Better page scrolling
  - Mouse-wheel can be used to perform zoom-in and zoom-out
  - Better multi-page signing experience
- OmniSign is now using an updated viewer. There were cases where some PDF files were not presented properly.
- The CoSign Configuration Utility now supports the distribution of configuration through AD Group Policy to 64bit systems.

SAPI

- The PKCS#7 signature (relevant to Buffer Signing, PDF Signing, Tiff Signing and Word Entire file signature) also includes the ROOT certificate when available.
- SAPI provides mechanisms for embedding signature field locators inside PDF documents. The PDF locators are viewed as empty signature fields when either OmniSign is used or when CoSign Web App is used. When the end user perform a digital signature operation, a PDF signature is created and signed.
- Adobe XI supports having a digital signature mark of all form fields to be protected as part of the digital signature operation. When SAPI is used to sign these signature fields, the form fields will be marked as protected.
  Only the *All Fields* attribute is supported.
- For the purpose of Long Term Validation signatures, it is possible to embed the CRL into the signature object when PDF signatures are used or when Buffer signature are used.
- SAPILogon accepts a variant of authentication modes that can be different than the default authentication mode that is used by the CoSign Client.

CoSign Mobile version 1.1

Some fixes to CoSign Mobile version 7.4.

This is a relatively minor version for both the CoSign Mobile App for Android and the CoSign Mobile App for iOS

- UI Changes and Improvements:
  - The login screen has been simplified
  - The Signing Ceremony experience has been improved
  - User will see clearer icons
  - Improved input fields offer ease of use across the app
- Users are now able to send app logs to support without prior log-in
- Bug fixes

Known Problems/Limitations/Warnings

CoSign Web App

- Pressing the back button in the browser may lead to a situation that requires the user to close and reopen the browser and then reopen a new session with CoSign Web App. (***7.5-WEBAPP-001***)
- If One Drive is used for Cloud-based file storage then there may be problem if the CoSign Web App is deployed on a port that is different than 443 (the SSL default port). (***7.5-WEBAPP-002***)
- Password protected PDF documents are not supported.
- If large files are used through the CoSign Web Agent (PDF files are sent ahead as part of the Web Agent API), it is recommended to increase the size of the UploadReadAheadSize parameter. For more information please refer to
  http://blogs.catapultsystems.com/rhutton/archive/2012/07/22/request-entity-is-too-large-over-ssl-in-iis-7.aspx
  and a more detailed explanation can be found in:
  http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/7e0d74d3-ca01-4d36-8ac7-6b2ca03fd383.mspx?mfr=true
  (***7.5-WEBAPP-003***)
- Some issues have been found with Internet Explorer 9, and it is recommended to use a higher version of Internet Explorer. (***7.5-WEBAPP-004***)
- It is impossible to sign in with Customer mode (POS) on an existing electronic signature field if the logged in user has more than one certificate. (***7.5-WEBAPP-005***)
- When using an authentication method based on an External Identity Provider, the new logoff option can be accessed by having the user logoff from the CoSign Web App session and notifying the External Identity provider. The problem can be solved by configuring the Web Server of the External Identity provider *not* to keep authentication information in the Browser Cache.
  Another option would be to direct users to reopen the browser and try again. (***7.5-WEBAPP-006***)
- When using Form Filling with CoSign Web App, the use of toggle buttons is problematic. (***7.5-WEBAPP-007***)
- When using the Active Directory Kerberos ticketing mechanism, it is advised to connect with the Fully Qualified Domain Names (FQDN) of the CoSign Web App and not with the Intranet name of the Server that is installed with the CoSign Web App. In such cases where only the Intranet is given, it may be that the user will see the full path of the locally loaded file instead of seeing only the file name. (***7.5-WEBAPP-008***)

CoSign Appliance

- When radius interface is used for validating OTP, the Shared Secret maximal length is 16 characters. This limitation is not enforced by the CoSign Administrative interface. (***7.5-SRV-001***)

CoSign Client

- When the radius interface is used for validating OTP, the Shared Secret maximal length is 16 characters. This limitation is not enforced by the CoSign Administrative interface. (***7.5-CLI-001***)
- When the Signature locators are used, pay attention to insert them as part of the text in a transparent color. Make sure the locators are not embedded into another object of the document (e.g. a text box). (***7.5-CLI-002***)
  Also, make sure you follow the rules that are described in the SAPI developer's guide. For example, the locator text should be placed in a single line.
- PDF files that are PDF/A-1 compliant (PDF/A—1a and PDF/A-1b) can be used to sign by SAPI. However the following PDF/A standards are not supported by CoSign: PDF/A-2(PDF/A-2a, PDF/A-2u, PDF/A-2b) and PDF/A-3(PDF/A-2a, PDF/A-2u, PDF/A-2b). (***7.5-CLI-003***)
- There is a problem using signature locators in PDF files that are rotated.
- OmniSign new help pages required that Internet Explorer is installed in the user's PC. Remember not to disable the *Show Pictures* attribute in the advanced settings. (***7.5-CLI-004***)
- OmniSign allows adding a new signature field and sign them even if there is a digital signature in the document that protects all form fields in the PDF document. (***7.5-CLI-005***)
- When using Entire file signatures in a Word document in combination with other types of content based signatures, remember to use the old Word document format (.doc) prior to adding any digital signature to the document. (***7.5-CLI-006***)
- PDF signatures that are created with CoSign Client V7.5 using the new PDF signing method will not show the "Signed By" caption on a machine installed with CoSign Client 7.2. (***7.5-CLI-007***)
- When SAPI is configured to use CRL embedded into the PKCS#7 purpose, be minded that the client's PC clock needs to be accurate and in line with CoSign appliance time. If the client's PC time is earlier than the CoSign time, the CRL embedding process may fail. (***7.5-CLI-008***)

Release Notes – CoSign Version 7.4

General Information

Release Date: February 8, 2015 – CoSign Appliance version 7.4 and CoSign Client version 7.2

The release of version 7.4 includes the following components:

- CoSign Mobile App for Android and iOS
- CoSign Appliance version 7.4
- CoSign Client version 7.2.2

CoSign Mobile App enables end users to sign via a mobile application. Mobile App currently supports signing PDF files. CoSign Mobile App interfaces with the CoSign Appliance through the CoSign RESTful API.

The new CoSign Appliance and CoSign Client versions are based on technical improvements and bug fixes. There are updated versions of the CoSign Appliance Admin Guide, the CoSign Client Guide and the CoSign SAPI Guide.

The user guide for CoSign Mobile App is not yet available.

New Features and Fixes

CoSign Appliance

- In rare cases, the CoSign Appliance service had to be restarted after running for long periods of time. The problem was related to the internal database services of the appliance.
  Problem ***XX-SRV-001*** is fixed.

CoSign Mobile App

- The CoSign Mobile App for Android or CoSign Mobile App for iOS can be downloadable from:
  - Android Store - https://play.google.com/store/apps/details?id=com.arx.cosignapp
  - Apple Store - https://itunes.apple.com/us/app/cosign-secure-digital-signing/id932750932?ls=1&mt=8
- The CoSign Mobile App can be configured to use one of the following CoSign Appliances:
  - CoSign Trial
  - CoSign Cloud
  - Organizational CoSign appliance – by supplying its primary DNS name and an optional alternate DNS name.

    These appliances must be accessible, therefore, the organizational firewalls must be configured to pass communication from the Mobile App users to the CoSign Appliances using port 8081.
- When the CoSign Mobile App is installed, it is associated with the .pdf extension.
  Upon accessing any PDF file (for example, through an attachment to email or via a cloud-storage provider like DropBox), the user will be given the option to activate the CoSign Mobile App on the selected PDF file.
- Using the CoSign Mobile App under Android, local PDF files can also be signed.
- The CoSign Mobile App will lead the user via a GUI-based signing ceremony to perform a digital signature operation upon the selected PDF file.
- The CoSign Mobile App enables the end user to perform the following operations:
  - View a PDF document by browsing the PDF file's pages
  - Execute the Signing Ceremony including either by marking a new Signature Field to be signed or signing existing signature fields
  - Validate signatures for existing signed fields
  - Manage Graphical Signatures
- When the document is signed, it is possible to share it with any installed Mobile App that can handle PDF files. For example, if the document is shared with an email application, the PDF file can now be sent as an email attachment.
- If the CoSign Mobile App is used to access the organizational CoSign appliances, make sure that the appliances are loaded with a worldwide verifiable certificate. See the CoSign Administrator Guide for information on how to upload an SSL Private Key and Certification for the CoSign RESTful Web Services interface.
- The following list of mobile devices were tested by the ARX qualification process:

Device	OS Version
Nexus 5	4.4.2/5.0.1
iPhone 5	7.1.1/7.1.2/8.1
iPhone 5S	7.1.1/7.1.2/8.1
Nexus 7	4.4.4
iPad Air	7.1.2/8.1.2
Nexus 10	4.4.4
Samsung Tab 2	4.1.2
Samsung Note 3	4.4.2
Samsung Galaxy S3	4.3
Samsung Galaxy S4	4.4.2
Samsung Galaxy S5	4.4.2
Samsung SM-T325	4.4.2
iPad Mini	7.1
Samsung Galaxy S4 mini	4.2.2
LG G3	4.4.2
IPAD Air Cell	8.1
SONY XPERIA Z2 Tablet (Cell)	4.4.2
iPhone 6	8.1.2
iPhone 6 Plus	8.1.2

Client

- The internal PDF processing in SAPI is now based on a new mechanism. This mechanism is also utilized when the OmniSign application is used for signing a local PDF file.
  You can revert back to using the old mechanism by setting the SAPI/Misc./PDF Method attribute. See the CoSign User Guide for relevant information.
- The file-hashing calculation in SAPI was improved to provide better performance, especially in multi-tasking/multi-processing environments.
- In the CoSign Administrator's Guide, new instructions are provided for deploying the CoSign Client using Microsoft System Center Configuration Management (SCCM). Using this Microsoft tool, organizations can easily deploy the CoSign Client in large-scale client platforms.
- A problem related to the quality of a graphical signature in .docx/.xlsx files was fixed.

Known Problems/Limitations/Warnings

CoSign Rest Web Services

- When signing with a given requested time-zone and the given time-zone is 0 (i.e., GMT), the time-zone used is PST (Pacific Standard Time). (***7.4-REST-001***)

CoSign Mobile App

- When using the CoSign Mobile App under Android to access the organizational CoSign Appliance, an entire certificate chain must be uploaded to the CoSign Appliance.
  Please contact ARX support to obtain the tool for uploading the certificate chain. (***7.4-MBL-001***)
- When using iOS-based mobile devices (IPhone6), if the screen is rotated during an operation such as during user authentication, the process will show a distorted screen. Screen rotation should be performed at the start of the session. (***7.4-MBL-002)***
- Signing Word/Excel files is not supported. (***7.4-MBL-003)***
- Password-protected PDF files are not supported. (***7.4-MBL-004)***
- Electronic Signatures are not supported. (***7.4-MBL-005)***
- Signing invisible signatures are not supported. (***7.4-MBL-006)***
- When Android Mobile App is used, you cannot update the requested signing time-zone. (***7.4-MBL-007)***
- If you are using both the Mobile App and the CoSign Client to manage graphical signatures, in order for the CoSign Mobile App to be synchronized with the newly created/updated graphical signature, you will need to exit and reactivate the CoSign Mobile App. (***7.4-MBL-008)***
- CoSign Mobile App might work improperly if a damaged PDF file is used. (***7.4-MBL-009)***

- There is a problem when sharing a PDF document from the CoSign Mobile App with Box. Two instances of Box are opened. (***7.4-MBL-010)***
- There are problems navigating to a certain page when the PDF document is defined in landscape mode. (***7.4-MBL-011)***
- There is a problem signing local PDF files when the CoSign Mobile App is based on Samsung devices. (***7.4-MBL-012)***
- On a Nexus 5, when opening a PDF file from OneDrive, the user will receive an error message. (***7.4-MBL-013)***
- In iOS, when sharing a signing PDF document with the email application, the trailing section of the email's text does not contain the name of the sending user. (***7.4-MBL-014)***

Release Notes – CoSign Connector for SharePoint 7.3

General Information

Release Date: April 13, 2014 – CoSign Connector for SharePoint version 7.3

Features and Improvements

- Claim Based authentication support
- Support for SharePoint 2013 upgraded from SharePoint 2010
- Auto filling of Title(Position) field when signing (not supported in SharePoint Foundation 2010 and 2013)
- Default settings for Microsoft Signature Lines (Word / Excel)
- "Prepare with CoSign" feature now supports Word and Excel template files (Dotx and Xltx)

Bug Fixes

- Multilanguage support – Translation of signing ceremony page with alternative foreign language
- Correct signature field location in nonstandard and rotated PDF documents
- SharePoint Designer workflow error when executed on a "non-English" site
- "Prepare with CoSign" correct error message in case an empty field wasn't created
- Signatures on List Items are no longer affected by regional and language settings
- Issue with PDF extension in uppercase letters
- Redundant configuration added to SharePoint web.config
- Navigation between document pages in IE9+ and Chrome browsers
- Multilanguage support – Signing list items in lists with alternative language different than English

Multilanguage support – SharePoint Designer workflows – Signature action comments are not properly translated

Release Notes – CoSign Connector for SharePoint 7.2

General Information

Release Date: December 2, 2014 – CoSign Connector for SharePoint version 7.2

Features and Improvements

- New default settings were added to CoSign Settings in SharePoint Administration:
  - Logged-in username display
  - Enable/Disable create and sign new fields
  - Enable/Disable edit new fields settings
  - New signature field default settings

Bug Fixes

- SyncObject error after signature operation
- CoSign buttons in document library ribbons are not affected by default settings, set in Central Administration
- List signature workflows not working properly (SharePoint Designer and Nintex Workflows)
- SharePoint 2013 - Overlapping error messages in Signing Ceremony dialog
- Better support for “invisible” signatures
- UI issue with “one page” documents

Release Notes – CoSign Version 7.1

General Information

Release Date 1: June 19, 2014 – CoSign Appliance version 7.1 and CoSign Connector for SharePoint version 7.1

Release Date 2: May 1, 2014 – CoSign Client version 7.1, CoSign Web App version 7.1

The release of version 7.1 includes the following components:

- CoSign Connector for SharePoint version 7.1
- CoSign Client version 7.1
- CoSign Appliance version 7.1
- CoSign Web App version 7.1 that includes CoSign Signature Web Agent version 7.1

The main new functionalities of the version are as follows:

- The CoSign Appliance is Common Criteria EAL4+ certified as a qualified remote signing solution.
- CoSign supports ADFS based authentication. The functionality can be used either through deployment of CoSign Client (Active Mode) or the CoSign Web App (Passive Mode).
- The CoSign Appliance supports a new Web Services interface based on RESTful API.
- CoSign Web App supports the signing of Office 2007/2010/2013 documents.
- A new and advanced OmniSign printer is used. The printer keeps textual information during the conversion to PDF thus minimizing the size of the converted PDF file.
- The new functionality of the CoSign Connector for SharePoint version 7.1 is described in the section below.
- CoSign Web App supports a POS (Point of Sale) mode of operation where the organizational agent accompanies an end customer's electronic signature.

A new set of manuals was updated to include the new functionality mentioned above.

New Features and Fixes

Client

- CoSign Client supports Windows 8.1.
- ARX CoSign Printer now functions when CoSign Client is installed on Windows 8/Windows 8.1 or Windows Server 2012.
  Problem ***6.2-CLI-002*** is fixed.
- CoSign Signature Line Provider for Office supports all the languages that are supported by the CoSign Client: French, Spanish, German, Dutch, Italian, Portuguese, Japanese and Greek.
- CoSign Client supports Greek.
- When using Word/Excel ARX legacy Add-in, it is now possible to incorporate into the signature information that relates to whether content was marked with a strikethrough font.
- When ADFS Active Mode is used (based on the CoSign Client), the user can authenticate to the local Active Directory system either based on UserID-password authentication or Kerberos authentication.

Appliance

- A new type of "Common Criteria" installation is introduced in CoSign version 7.1, This installation type should be used when CoSign needs to operate in Common Criteria EAL4+ mode.
  This mode of operation is restricted and supports the following configurations:
  - CoSign is installed in Directory Independent mode
  - CoSign internal CA is not supported and all user certificates are based on an external CA
  - Any signature operation requires the user to enter his password together with a One Time Password (OTP). Only OATH-HOTP and Vasco OTP are supported.
- The new RESTful based Web Services API supports end user operations such as signing a document. It is possible to activate the SOAP based Web Services API in addition to the RESTful based API.
- The new SAML based authentication enables automatic generation of accounts for new users from a trusted organization based on presenting a SAML ticket. As part of the account creation, a signature key and a certificate are generated for the new user.
  In the user's following attempts to sign by presenting new SAML tickets, the existing signature key and certificate will be used for the new digital signature operation.
- CoSign internal CA certificates now are based on SHA256.

Web App 7.1

- It is now possible to sign Office 2007/2010/2013 documents. The digital signature operation is based on signing existing empty signature fields.
  The empty signature field can be prepared using Microsoft Word/Excel either by employing the Microsoft Signature Line Provider or the ARX Signature Line Provider.
  In the event that the Office document does not contain any signature fields, it will be converted to a PDF, and the CoSign Web App will sign the PDF document.
- As part of the new POS functionality, the end-customer's electronic signature is entered graphically by him/her. In the event that a tablet is used (such as iPad), the signature can be entered directly upon the tablet's display.
- Microsoft mobile devices such as Microsoft Surface or Nokia Lumia are now supported.
- It is now possible to define whether a cloud storage provider is sensitive or not.
- When sending the signed document via email, the system will suggest email addresses based on emails that were previously used by the user.
- Problems with the interface to Box file storage provider due to API changes in Box were resolved.

Web App 7.2

- It is now possible to define for every cloud storage provider whether it appears as an option to the user or not.
- A problem where initiating a signature operation from Box was fixed.

Known Problems/Limitations/Warnings

General

- Starting from CoSign version 7.1, CoSign Desktop is no longer supported. (***7.1-CLI-001)***
- CoSign Client is not supported when installed on Windows XP. (***7.1-CLI-002)***
- CoSign Legacy add-in for Word and Excel does not support Office XP or Office 2003. Only Office 2007/2010/2013 versions are supported. (***7.1-CLI-003)***
- CoSign Client supports Adobe Acrobat or Adobe Reader of version X and above. (***7.1-CLI-004)***
- CoSign Appliances that were manufactured originally as version 4.5 are supported. Any manufacturing version prior to version 4.5 is not supported. Contact ARX Support for additional information. (***7.1-SRV-001)***

- CoSign SMB Is no longer supported.

CoSign Client

- The new OmniSign printer generates several operational problems. Some of them can be addressed as follows:
  - Use a newer version of the CoSign Client namely CoSign Client version 7.1.2
  - The OmniSign printer should not be used from within Adobe Reader or Adobe Acrobat since there is no point in converting a PDF file. (***7.1-CLI-005)***
  - Avoid trying to reprint the same document. (***7.1-CLI-006)***
  - If OmniSign is open and you activate OmniSign Printer, you will not see the newly printed document until OmniSign is closed. (***7.1-CLI-007)***
  - If you experience any queue problem with the new ARX OmniSign Printer, use the following command to release the queue: (***7.1-CLI-008)***
    - Go to the C:\Program Files (x86)\ARX\PDFCreator directory
    - Type Pdfcreator.exe /clearcache
- Due to the fact that the new ARX OmniSign printer is based on PDFCreator, please uninstall existing or older versions of PDFCreator before installing CoSign Client with the ARX OmniSign Printer support. (***7.1-CLI-009)***
- Due to Microsoft limitations, SAPI does not support signing Office 2007/2010/2013 documents using a SHA2 signature. This means that in configurations that mandate using SHA2, such as when CoSign is installed in Common Criteria mode or FIPS mode, signing through the Web Services interfaces or using SAPI is not possible. (***7.1-CLI-010)***
- In environments that mandate using SHA2 signatures, only Microsoft Signature Line Provider can be used for generating these signatures. For information regarding how to configure Office to support SHA2 signatures, please contact Microsoft. (***7.1-CLI-010)***
- Encountering difficulty when adding a graphical signature that is based on Tablet/Mouse in Windows 2012. (***7.1-CLI-011)***
- Encountering difficulties when printing documents that contain digital signatures. These problems are caused because the signature validation operation is part of the printing operation. For more information contact ARX Support. (***7.1-CLI-012)***
- When using a signature line field with different layout settings than the default (in-line with text), the signature field cannot be viewed properly, making signing impossible.
  If the field is already signed, it will not be visible, i.e., there will be no indication that the field is signed. This is a Microsoft implementation issue. (***7.1-CLI-013)***

SAPI

- Encountering difficulty when adding a new signature field in documents created by Office 2013. This problem also appears when trying to create a signature field through CoSign Web Services. (***7.1-CLI-014)***

CoSign Appliance

- Only appliances that are based on manufacturing version 6.0 and above are able to use SHA256 based certificates. (***7.1-SRV-002)***
- Only appliances that employ manufacturing version 6.0 and above are able to use SAML tickets that are based on SHA256 as part of ADFS Authentication mode. This issue is relevant for many SHA2 based certificates or signatures that are used throughout the appliance (for example, when uploading a ROOT certificate that is based on SHA256). (***7.1-SRV-003)***
- When CoSign is used in ADFS, users that were deleted from the original Active Directory of the trusted organization must be manually deleted from the CoSign appliance. (***7.1-SRV-004)***
- Using PKCS#1 signatures through the SOAP based web services API provider lowers performance rates. Use the RESTFul based web services interface to acquire better performance rates. (***7.1-SRV-005)***
- A signature validation failure on given XML data using the SOAP based web services will fail additional validation attempts even if the signature is acceptable.
  This problem does not occur when using the RESTFul Web Services interface. (***7.1-SRV-006)***
- The permissions mask for a user cannot be empty. At least one of the permission bits must be on. In former version, an empty permissions mask was equivalent to user permission. (***7.1-SRV-007)***
- CoSign Enterprise does not support the use of 4096bit RSA keys. (***7.1-SRV-008)***

CoSign WebApp

- When signing existing signature fields that were created using ARX Signature Line Provider, the signature fields will appear in the browser with the "Software Required" text at the location of the signature field. This is only a display issue. The signer should keep in mind that signature operation in Office 2007/2010/2013 documents is based on signing a selected field according to the suggested signer of the empty signature field. (***7.1-WEBAPP-001)***

Release Notes – CoSign Connector for SharePoint 7.1

General Information

Release Date 1: June16, 2014 – CoSign Connector for SharePoint version 7.1

The CoSign Connector for SharePoint has been enhanced with features enabling ad-hoc signing as well as a better overall user experience.

New Features, Improvements and Fixes

Features and Improvements

- Prepare with CoSign – This is a new feature. Preparing a document for signing refers to the creation of empty signature fields (placeholders for signatures) and specifying various parameters for these fields
- Conversion of Microsoft Office documents to PDF format (using *Prepare with CoSign* feature)
- Multiple Signatures – Users can apply more than one signature on a document without being redirected to the document library
- UI/UX improvements

Bug Fixes

- Auto Verify issue in columns with empty values
- InfoPath template name issue
- InfoPath "preview is not available" page was replaced
- Signing Ceremony action buttons are disabled when signing is in progress
- Sign and verify list operation utilizes an 'On item updating' event that enables running workflows that start when there is an item change event.
- Sign and verify document operation 'On item updating' and 'On file check-in' event that enables running workflows that start when there is an item change event.

Known Problems/Limitations/Warnings

- The minimal required version of Microsoft Internet Explorer is **9 -** (***7.1-CC4SP-001)***

- Special configuration is required for supporting SHA-2 signatures in InfoPath Web Forms (in SharePoint). Contact ARX for information regarding the necessary configuration steps (***7.1-CC4SP-002)***
- In some cases (such as a very large page size or partially rotated pages), a signature will be created with a small offset (location) (***7.1-CC4SP-003)***

Release Notes – CoSign Connectors for SharePoint 6.5.4

General Information

Release Date 1: February 17, 2014 – CoSign Connector for SharePoint version 6.5.4.

Bug fixes for deployment and upgrade.

Bug Fixes

- Signing on documents from within document sets
- Upgrade Issue – "force" flag was added to features that are being installed programmatically to overcome upgrade issues
- Upgrade Issue – ARX workflow signature task upgrade
- Sign InfoPath forms in WebParts issue
- Batch script provided with "wsp" file was modified to prevent the SharePoint Administration service to interfere with installation / upgrade

Release Notes – Client Version 6.2.7

General Information

Release Date 1: December 10, 2013 – CoSign Client 6.2.7

Create signatures

New Features, Improvements and Fixes

Improvements

- Support "Aspose.Words" library. http://www.aspose.com/.net/word-component.aspx
  The Aspose Words library is used by developers to preview Word documents. Digital signatures for Word created by SAPI 6.2.7 can now be validated correctly by Aspose. Digital signatures for Word are a *de facto* standard set by Word itself. SAPI signatures for Word have always conformed to the standard.

Release Notes – CoSign Connectors for SharePoint 6.5.3

General Information

Release Date 1: December 10, 2013 – CoSign Connector for SharePoint version 6.5.3

Bug fixes for "Word document preview" feature

New Features, Improvements and Fixes

Bug Fixes

- Word Documents with SHA2 signatures cannot be signed.

  Fixed: Word and Excel documents with SHA2 signatures will not be previewed before signing. The document can still be signed, only the preview will not be shown.
  Notes: SHA2 signatures are only used by Office 2010 and more recent versions.

Known Problems/Limitations/Warnings

- If a Word document has two or more signature fields, and one or more are not yet signed and the signed field(s) were signed with CoSign Client version before 6.2.7 then, when the document is signed, the pre-existing signatures may appear as "invalid" in the preview window
- Some complex Word documents with the following attributes:
  - Have two or more signature fields
  - One or more are fields are not yet signed
  - Were signed using Microsoft Word itself, (they were not signed using CoSign SAPI) .

In this case, the existing signatures may appear as invalid in the document preview.

Release Notes – CoSign Connectors for SharePoint and Nintex 6.5

General Information

Release Date 1: November 11, 2013 – CoSign Connector for SharePoint version 6.5 and CoSign Connector for Nintex version 6.5

The two connectors were enhanced with new workflow features and a refresh of the "Signing Ceremony" user experience.

New Features, Improvements and Fixes

Features and Improvements

- Support for Microsoft SharePoint Designer workflows

  Workflows created with SharePoint Designer or Visual Studio can now include digital signature tasks and actions: "Sign with CoSign", "AutoSign with CoSign" and "Verify with CoSign"
- Improved and unified "Signing Ceremony" screen

  A visual preview of a document is now a main part of the signing ceremony screen

  Support for visual preview of Microsoft Word and Excel documents
- The CoSign Connector for Nintex Workflow was enhanced:

  Delegation and "Group Signing" are now supported when using Nintex "Assign to-do" task to create a signature task

  Two new custom actions were added: "AutoSign with CoSign" and "Verify with CoSign"

- Browser navigation buttons ("Back" and "Forward") now provide in-page navigation between document pages in a Signing Ceremony preview screen
- Fix redirection issue after signing/verifying/reviewing signatures. A user will be redirected to the original location where he initiated the action.

Known Problems/Limitations/Warnings

- Nintex Workflow – Delegation for groups supports only Active Directory groups. SharePoint groups are not supported. (***6.5-CC4SP-001)***
- Nintex "Assign to-do task" when used with "CoSign Workflow Signature Task" to create a signature task, will ignore the "All must respond" setting and will always behave as "first reply applies". This means that the first person to complete a signature task by signing will be the one completing the signature task for all other users that were assigned to the same task. (***6.5-CC4SP-002)***
- SharePoint can only sign Microsoft Word/Excel documents if they include one or more "Microsoft Office Signature Lines." For each "Microsoft Office Signature Line", a "Suggested signer" must be specified. The suggested signer does not need to sign the signature field, but a suggested signer must be entered when the Microsoft Office Signature Line is added to the document. (***6.5-CC4SP-003)***
- Word and Excel documents cannot be signed from within SharePoint if the document only includes a "CoSign Signature Field." Such documents can be signed outside of SharePoint. Sectional signatures and individual Excel cell signatures cannot be signed from within SharePoint. (***6.5-CC4SP-004)***
- SharePoint 2013 redirect problem after signing: In some rare cases, when the "Minimal download strategy" feature is enabled for a SharePoint site, a user might be returned to the site's main page instead of the document library / form library / list where the signing operation was originally initiated. Disabling "Minimal download strategy" feature solves this issue. (***6.5-CC4SP-005)***

Release Notes – CoSign Version 6.2

General Information

Release Date 1: March 1, 2013 – CoSign Connector for SharePoint version 6.2 and CoSign Client version 6.2

Release Date 2: June 13, 2013 – CoSign Server version 6.2, CoSign Web App version 6.2 and CoSign Signature Web Agent version 6.2

The release of version 6.2 includes the following components:

- CoSign Connector for SharePoint version 6.2
- CoSign Client version 6.2
- CoSign Appliance version 6.2
- Introducing CoSign Web App version 6.2
- Introducing the interface to CoSign Web App version 6.2 named *CoSign Signature Web Agent version 6.2*

The main enhancement of this version is the introduction of CoSign Web App that is also installed as part of CoSign Cloud.

A new set of manuals was updated to include the new functionality mentioned above.

New Features, Improvements and Fixes

General Issues

- A new CoSign Connector for SharePoint that supports Microsoft SharePoint 2013.
- CoSign Client supports Windows 8 and Windows Server 2012. CoSign Client uses .NET Framework version 2 on some of its components. During the CoSign Client installation, .NET Framework version 2 will be activated if necessary.
- CoSign Client supports Office 2013. Both ARX Signature Line Provider and the ARX Legacy Add-in.
- CoSign Web App is a web application that can be installed on an organizational web server. It provides a web-based solution to sign documents without the necessity to install CoSign Client on every end user platform. The new CoSign Web App manual provides information on how to install CoSign Web App and describes the given functionality.

- The following browser types and versions are supported when accessing CoSign Web App: IE9 and above, Chrome, Firefox, Safari and Opera. A large variety of tablets and smart-phones are supported as well.
- CoSign Web App also provides a very powerful interface of web applications such as the document management application, enabling a simple interface for signing a document. The end user will be redirected to CoSign Web App for the digital signature ceremony, then back to the web application for integrating the signed document into the web application. This interface is called CoSign Signature Web Agent.
  The reference manual for the CoSign Signature Web Agent is described in a new book as part of the SAPI manual.

Known Problems/Limitations/Warnings

Client

- If CoSign Client enables .NET Framework version 2 during installation, the operating system must be restarted after enabling .NET framework version 2. The user will have to continue with the CoSign Client installation after the operating system restart. (***6.2-CLI-001)***
- ARX CoSign Printer does not function when CoSign Client is installed on Windows 8 or Windows Server 2012. (***6.2-CLI-002)***
- When CoSign Client is uploaded on to Windows Server 2012 featuring Office 2007/2010/2013, .NET Framework version 2 must be enabled manually prior to CoSign Client installation. (***6.2-CLI-003)***
- Capturing graphical images in the Windows 2008R2 operating system may be problematic. (***6.2-CLI-004)***
- When signing with ARX Legacy Provider in Office 2010/2013 with Entire File mode and XP compatible mode, the digital signature is invalid. (***6.2-CLI-005)***
- When using the CoSign Legacy Add-in, transparent signature fields are no longer supported. (***6.2-CLI-006)***
- Interlink ePad Ink Signature Pads are no longer supported. (***6.2-CLI-007)***
- Problems may arise when handling large PDF pages in OmniSign (A0 and A1 pages). (***6.2-CLI-008)***
- Zooming in and zooming out of a .docx/.xlsx file may invalidate the digital signature when using the Microsoft Signature Line Provider or the ARX Signature Line Provider. (***6.2-CLI-009)***
- When printing a .docx or .xlsx document, the existing visible digital signature will not be output to the printer. (***6.2-CLI-010)***
- Problems may arise when embedding Excel files into Word documents by dragging the Excel document into Word. When reopening the Word document, it may be difficult to access the

embedded Excel content. (***6.2-CLI-011)***

CoSign Connector for SharePoint

- Problems may arise when marking signature fields using Microsoft mobile devices such as the Microsoft Surface mobile device. (***6.2-CC4SP-001)***
- In the event that you receive the "Failed to retrieve CoSign Connector for SharePoint configuration from database" error, upon reaching the "CoSign digital signature settings" on the library settings page, go to the "Cosign Server authentication mode" page at the administration site, open this form and press OK. This operation will initiate necessary required data. (***6.2-CC4SP-002)***
- In the event that digital signatures are enabled for a specific document library using "CoSign Connector for SharePoint Document Library default settings" but the CoSign ribbon is disabled, go to "Cosign digital signature settings" on the library settings page and visit the page. This operation will initiate necessary required data. (***6.2-CC4SP-003)***
- CoSign Connector for SharePoint does not support Microsoft Surface or other mobile solutions based on Microsoft when attempting to create and sign a digital signature within PDF documents. (***6.2-CC4SP-004)***
- When uploading .doc files with auto-validation set to "off", an invalid validation state may appear in the "Signature Status" column. Performing a manual signature validation operation will enable the correct signature status. This problem may arise due to an invalid state retained as part of the document's internal meta information. (***6.2-CC4SP-005)***
- A problem may arise when signing a PDF file that does not feature any empty signature field in the event that no information is required for entry by the user aside from the location of the newly created signature field. (For example, if the user has a single certificate and a single graphical image, no reason is required for entry and the user uses the Kerberos ticketing mechanism). In this case an error will be prompted. It is recommended to request a reason so that the signature ceremony will be presented to the user, thus impelling him/her to enter the location of the newly generated signature field. (***6.2-CC4SP-006)***
- When using SharePoint 2013 with a Safari browser on mobile devices, the PDF preview window does not function properly. Other browser types do function properly. (***6.2-CC4SP-007)***

CoSign Web App

- The server that hosts CoSign Web App must be installed with CoSign Client version 6.23 or above.
- The CoSign appliance version that supports CoSign Web App must be installed with CoSign version 6.2 software.
- Microsoft mobile devices such as Microsoft Surface mobile device or Nokia Lumia are not supported. (***6.2-WEBAPP-001)***
- The size of the uploaded file for signing is limited. In the event of PDF files, the limitation is 30Mb. In the event of a Word/Excel file, the maximum size is 30Mb or 200 pages. (***6.2-WEBAPP-002)***
- A user who has two or more certificates cannot select which certificate to use as part of the signature ceremony. (***6.2-WEBAPP-003)***
- Problems using the *Browse* option in Android-based tablets or Smart Phones: In this event (and similarly when IPads or IPhones are used), you can access documents via cloud-based file storage systems such as Dropbox or Box. (***6.2-WEBAPP-004)***
- In rare cases, some information is omitted when converting a Word/Excel file to a PDF file during document upload or when used for signing through CoSign Web App. (***6.2-WEBAPP-005)***
- You cannot sign Google Doc formatted .doc and .xls files. The files must either be original PDF files or Microsoft formatted .doc and .xls files. (***6.2-WEBAPP-006)***
- Problems may arise when handling large PDF pages (A0 and A1 pages). (***6.2-WEBAPP-007)***
- Some performance problems may be experienced in High Availability environment when either the primary appliance is down or the alternate appliance is down. (***6.2-WEBAPP-008)***

Release Notes – Appliance Version 6.0

General Information

Release Date: November 13, 2012

Version 6.0 includes a new CoSign Administrator Guide.

The following main functionalities are included in this version:

- The CoSign version 6.0 internal database offers improved capabilities when compared to the internal database of the previous versions.
- A group (or account) entity is supported. The group entity can be used for assigning several users to a group. The CoSign Users Management Utility, as well as CoSign SAPI/SAPIWS, supports the new entity.
  The new group entity can be used by services providers to deploy a single CoSign appliance for multi-tenant environments.
- SNMP support.
- The CoSign web services functionality is aligned with SAPI of CoSign Client version 6.0.
- The CoSign appliance was hardened to accept only SHA1/3DES for IPSEC replication communication between primary appliance and alternate appliances; The CoSign appliance was hardened to accept only TLS1.0 for the CoSign web services interface.

New Features, Improvements, and Fixes

General Issues

- The CoSign version 6.0 internal database features improved capabilities when compared to the internal database offered in the previous versions. The new internal database can manage larger user communities than its predecessor. A CoSign appliance version that is updated to version 6.0 retains the older type of database.
  To differentiate between the older database version and the newer one, refer to the CoSign support report:
  - Master Disk Version 7.1 and above – new database
  - Master Disk Version less than 7.1 – old database
- As specified earlier, a new group entity can be defined and managed by a CoSign appliance. The group entity includes certain parameters that can be shared by all users that belong to a designated group.

In the event that a group is disabled, all users that belonged to the group will no longer be able to logon to the CoSign appliance.

- The backup format was changed to support larger user backups.
- It is now possible to update the CoSign license via remote administrative operation without requiring physical replacement of the license token. For more information, contact ARX.
- The CoSign appliance now supports SNMP. Some information can be accessed by the SNMP based monitoring system.

CoSign Appliance

- When using a Radius based extended authentication, it is now possible to set an extended user ID (up to 64 characters) and an extended password (up to 128 characters).
- Login performances have been improved. When CoSign is deployed in an Active Directory environment, there are less Active Directory accesses upon a regular user logon.
- When CoSign is deployed in a directory independent environment, the user login name is now case insensitive.
  In the event that an existing installation is upgraded to CoSign version 6.0, case sensitivity is retained.
- The problem which arose when simultaneously signing from different client applications with the same user has been resolved.
- A user can be defined as disabled in a directory independent environment. Once the user is disabled, he/she cannot login.
  If a user belongs to a group, both the user and the group must be enabled for the user to be able to login.

Certificate Management

- It is now possible to specify key renewal upon certificate renewal when using CoSign internal CA.
- The user's default signature key sizes can be changed. This process takes effect upon the renewal of the user's certificate and can be enforced by applying the certificate refresh operation.
  If the user belongs to a group, the user's key size is defined according to the group definitions.

CoSign Web Services

- The option of returning the tail of a newly signed PDF file is applicable only in the event that an existing field requires signature. In the event that a file needs to be both created and signed, this option is not available.

Known Problems/Limitations

General Issues

- In the event that CoSign is installed in a directory independent environment and you are using a CoSign version 6.0 that was not upgraded, make sure that the CoSign clients are from version 6.0 and above (due to the introduction of case insensitivity for the user login name).
  For more information, contact ARX.
- CoSign SSCD is no longer supported.
- CoSign installed in Novell NDS environments is not supported.
- When using CoSign groups to define classes of signers using the "Prompt for Sign" option and signers not using the *Prompt for Signature* option, the following action should be taken:
  - Configure the overall system to use the *Prompt for Signature* configuration (e.g. *Radius Server IP address*).
  - Define the *Prompt for Sign*ature system parameter as false.
  - Define only groups that mandate the usage of *Prompt for Signature* as such.
  - The relevant users must ensure that their clients are configured to use the *Prompt for Sign*method using the CoSign Configuration utility.

CoSign Web Services

- A small memory leak occurs for each signature operation when using the signer's automatic graphical signature. We therefore advise to upload a monochrome-based graphical signature for every signer.
- A small memory leak occurs for every signature operation when signing .docx files if a non-monochrome image is used as the graphical signature of the signer. We therefore advise to use a monochrome-based graphical signature for every signer.
- Creating new signature fields through CoSign Web Services interface is possible only if the CoSign Appliance version 6.0 was manufactured at ARX (Master Disk version 7.1 and above).
- Problem when using a signature password when creating and signing a signature into a PDF document.

Release Notes – Client Version 6.1

General Information

Release Date: November 13, 2012

This client version offers some new functionalities.

New Features and Fixes

OmniSign

- When printing a PDF document through OmniSign, it is possible to print signature-related information.
  To set this option, activate the CoSign configuration utility and go to the OmniSign Advanced tab. Adjust the *Show Validation Watermark* to on.
- OmniSign can be configured to view the PDF document version at the time of the document's signature.
  To set this option, activate the CoSign configuration utility and go to the OmniSign Advanced tab. Adjust the *Indicate Document Changes Performed after Signing* to on.
  To enable this function, make sure to perform a signature validation before inspecting document changes.
- Improvements were introduced in the OmniSign viewer.

SAPI

- Improvements were introduced when using SAPI for signing InfoPath forms.
- In the event of an OCSP failure when SAPI is configured to include OCSP response in the digital signature, the digital signature operation will fail as well.
- The problem connected to signing XML files/data from a 64-bit application has been resolved.
- It is now possible to acquire SHA2 (Sha-256, SHA-384 and SHA-512) based time-stamp requests and replies.
- In the event of failure of the time-stamping operation, the entire digital signature operation will fail as well.

Release Notes – CoSign for SharePoint Version 6.1

General Information

Release Date: October 18, 2012

The version includes a new CoSign for SharePoint Guide.

The following main functionalities are included in this version:

- Support signing documents in SharePoint custom libraries or custom lists.
- Support SharePoint standard extended columns for displaying signature related information as part of the document or list element information.

This version is based on a CoSign client version 6.0 installed in the SharePoint host server.

New Features, Improvements, and Fixes

General Issues

- Some new definitions are required on the SharePoint site collection level. For more information, refer to the CoSign for SharePoint updated manual.
- As noted above, it is now possible to define extended columns for documents or list items in a standard SharePoint manner.
  However, to preserve backward computability, any upgrade of CoSign for SharePoint from a former version will still necessitate the use of the old mechanism for selecting additional columns in document library or a list. For information on how to utilize the new extended column mechanism, refer to the updated CoSign for SharePoint manual.
- It is now possible to include a reason in the PDF signature without displaying it in the visible signature field.
- The new CoSign for SharePoint enables the use of a title in the visible signature field.

Release Notes – Client Version 6.0

General information

Release Date: Aug 26, 2012

The version includes a new CoSign User Guide and a new CoSign SAPI® guide.
This client version is used by end users as part of the CoSign® Cloud solution.

Highlights include:

- The CoSign client can connect securely to a CoSign server through an organizational http proxy using a variety of authentication mechanisms. This is in addition to existing http proxy support with no authentication.
- Users can now sign PDF attachments through Outlook 2010 using the *Sign with CoSign* option that executes OmniSign.
- SAPI can be used to sign PDF and XML files in memory without requiring them to reside in the local hard disk. This option increases digital signature performance in case where the files are located in memory.
- SAPI can be used to locate signature field markers in PDF documents and help the application automatically generate signature fields in their appropriate locations. This can help streamline the digital signature operation when using PDF templates or files that are converted to PDF as part of a workflow.
- In windows 7 and Windows 2008 R2, it is possible to install or configure the CoSign client to show the following additional languages: French, Spanish, Italian, German, Dutch, Portuguese and Japanese.

In other Windows systems, you will need to use the localized Windows version.

- SAPI supports adding new signature fields to Office 2007/2010 documents (.docx and .xlsx files). Only ARX/MS signature line provider is supported.
- Starting from CoSign version 5.6.4, the visible signature in PDF files is made from a single image rather than from textual and graphical components. This means that languages such as Chinese and Japanese, among others, are better supported in PDF files. It is possible to use the previous visible signature format as well.
- A new low-level API can now be used to perform PKCS#1 signatures. This API can be used for maximizing digital signature performance. For more information, please contact ARX.

New features and fixes

Client

- The CoSign client can connect securely to a CoSign server through an organizational http proxy using a variety of authentication mechanisms. This is in addition to existing http proxy support with no authentication. The following http proxy products were tested: Qbik Wingate Proxy server and Microsoft Forefront TMG.
  The proxy with authentication support requires using CoSign appliance version 6.0 or above.
  It is recommended to fully restart the CoSign client after setting http proxy settings.
- In a high availability environment, it is possible to define a set of preferred servers that the client can connect to. Only in cases where every preferred server is down will the client connect to non-preferred servers.
- It is possible to configure that only the ARX signature line provider toolbar will appear in Office 2007/2010 while the legacy add-in toolbar will not appear.
- The CoSign client installation configures all installed Adobe Acrobat and Adobe Reader installations to validate signatures created with CoSign. Please read the CoSign client manual for instructions on ensuring that the CoSign root certificate is trusted.
- It is now possible to export configurations from the CoSign configuration Utility to Windows 64-bit operating systems.

SAPI

- SAPI can be used to sign PDF and XML files in memory without requiring them to reside in the local hard disk. This option increases digital signature performance in case where the files are located in memory.
- There is now support for enabling applications to create signature fields in PDF files based on signature field markers. This functionality can streamline the generation of PDF templates that include signature fields, for example in cases where templates that are based on files converted to PDF are being used.
- There is now support for creating signature fields in Office 2007/2010 documents (.docx or .xlsx files). New signature fields can be created in the first and last pages of the document.
- Starting from CoSign version 5.6.4, the visible signature is made from a single image rather than textual and graphical components. The visible signature can now support additional languages beyond English and western European languages, such as Chinese and Japanese. The new format

is compatible with the PDF/A standard.

When specifying the *Default PDF Font* parameter in the configuration utility in the Signature API\Graphical Signature section, the specified font is used to build the single visible image that is embedded as the visible signature inside the PDF document.

Using the configuration utility, it is possible to revert to the former configuration, which has better performance figures.

OmniSign

- It is possible to define who can clear a signed field in a PDF file using OmniSign. The permission may be one of the following: no one, only the signer, anyone.
- It is possible to configure OmniSign to show a validation watermark when printing a PDF document from OmniSign. Each page of the PDF will include information about the PDF signatures.
- It is possible to configure OmniSign to ask the user to perform a digital signature operation if there are only electronic signatures in the PDF document. This option is relevant to *Point-of-Sale / Point-of-Service* deployments where end users are signing electronically and eventually the sales representative needs to digitally sign the entire document.
- Performing silent signature with default reason and title was fixed.

ARX Signature Line Provider for Office 2007/2010

- The problem printing .docx files that included ARX signature line provider fields (both signed and non-signed) was fixed.
- The problem where opening a document from a template in Office 2010 prompted to save changes when no changes were made was fixed.
- A known Microsoft problem of validating Excel 2007 documents that include formulas and are signed by ARX signature line provider is solved using the ARX signature line provider add-in.

ARX Legacy Add-in

- Several problems were fixed when signing and verifying legacy signatures when the *scope of signature* is defined to include *location & size of Tables and Objects*.

- Office legacy add-in in 64-bit now supports the following additional languages: French, Spanish, Italian, German, Dutch, Portuguese and Japanese.
- Fixed Excel problem when performing print preview using some printers.

Known problems/limitations/warnings

Client

- It is not possible to invoke OmniSign upon a PDF attachment in the case that an Outlook email is in compose mode. This means that if you compose a new email, forward an email or reply to an email, the functionality cannot be used. Therefore, if you want to forward a signed document, first sign the attachment and then forward it.
- Previewing an email with attachment after signing will open a new attachment temporary file instance. As a result, all changes in the file (such as adding a new digital signature) can be viewed only after closing and reopening Outlook.
- When using the CoSign client to enroll for an external CA using Internet Explorer browser 9 in Windows 7 platform, an error message is displayed during the certificate enrollment.
  The overall enrollment process is successful and a user's key and certificates are generated within the CoSign appliance.

SAPI

- There is a problem signing XML files/data from a 64-bit application.
- Only SHA1 based time-stamp requests and replies are supported.

ARX Legacy Add-in

- If you include *Location and Sizes of Tables and Objects* in Word and the digital signature is based on CoSign client version 5.6, you must use either CoSign client version 6.0 or CoSign verifier version 6.0 to validate the digital signature.

OmniSign

- There is a problem opening PDF files that are encrypted with Acrobat X security.

Release Notes – Client Version 5.6

General information

Release Date: Jan 17th, 2012

This version includes a CoSign client version and version 6.0 of the CoSign add-on for Microsoft SharePoint.

The CoSign add-in for SharePoint v6.0 is based on CoSign client version 5.6.

The version includes a new CoSign User Guide, a new CoSign SAPI guide, and a new CoSign for SharePoint guide.

Highlights include:

- Support digitally signing InfoPath 2007/2010 forms using InfoPath 2007/2010 application.
- Signing InfoPath 2007/2010 forms using SAPI and SAPI-COM.
- Signing InfoPath 2007/2010 forms through CoSign add-on for Microsoft SharePoint.
- CoSign add-on for SharePoint v6.0 enables viewing PDF documents embedded inside the SharePoint web application during the signature operation. It is also possible to graphically create a new signature field during the digital signature operation.
- Improvements in the graphical signature management utility in terms of the quality of the images as well as additional functionality such as downloading all graphical signatures from the CoSign appliance to the end user's local disk.

New features and fixes

Client

- It is now possible to capture or upload a monochrome graphical signature and change its color after capturing.
- The quality of the graphical signature while capturing was improved.
- The http proxy configuration in the CoSign client supports servers that use HTTP version 1.1.

- The CoSign Configuration utility can export configurations for 64-bit operating systems in addition to the existing 32-bit operating systems.

SAPI

- Digital signatures created by Adobe Acrobat 10.1 and higher and based on SHA2 algorithms can now be validated with SAPI or OmniSign.

ARX Legacy Add-in

- While signing a table that has merged cells and *location and size of table and objects* are required in the scope of the signature, there is a signature verification problem. The problem is now fixed.
- When using protected forms in Word, there were cases where existing digital signature were invalidated. This problem was fixed.

ARX Signature Line Provider for Office 2007/2010

- Microsoft invalidates Excel 2007-based digital signatures that are based on formulas when opening the signed fields in Excel 2010. If the CoSign Client or CoSign Verifier is installed, the problem is bypassed. For information how to bypass the problem, contact ARX.

Tiff

- The problem where after signing a TIF file, you are not able to view the file using the *Windows Picture and Fax Viewer*, was fixed.

CoSign Add-on for Microsoft SharePoint

When signing .docx or .xlsx documents, the list of profiles are based on the *Suggested Signer* field and not the technical identity of the signature field.

Known problems/limitations/warnings

Client

- The former support for InfoPath 2000/2003 was removed from the CoSign client. This also includes the form designer functionality that was invoked from the CoSign control panel.
- The new feature for downloading images to the local hard disk using the graphical signature management utility does not support Unicode based graphical signature name.
- 16-bit bmp images cannot be used as graphical signatures.
- When selecting a font in the *SAPI/Graphical Signatures* section in the CoSign configuration utility, any *Font Style* selection is neglected, so the user will need to specify it one used.

SAPI

- In case an InfoPath template has been used to fill-in and sign a specific form, and later the template itself has been updated, the signature on the signed form will remain valid, i.e. the SAPI Signature Verification function will reply with a success. However, the extended signature information will alert via error code, that the general template for this form has been changed.

ARX Legacy Add-in

- If you include *Location and Sizes of Tables and Objects* in Word and the digital signature is based on Client version 5.6, you need to use either CoSign client version 5.6 or CoSign verifier version 5.6 to validate the digital signature.

- After signing/validating protected documents, it is not possible to edit a text or rich text field. This is due to a Microsoft problem when an ActiveX item is selected prior to signature or signature validation operation. Reopening the document solves the problem. Contact ARX for more information.
- Due to the new support of signing merged table cells in Word, there might be a performance problem if there are many cells in the table.

OmniSign

- When one-touch signature is used, there is a problem positioning the signature field in the cases that a user is required to log on during signature field creation. This also happens when using an electronic signature.

ARX Signature Line Provider for Office 2007/2010

- When using Office 2007 to verify signed files that were created either by using Microsoft signature line provider or ARX signature line provider, it may take several minutes to open the signed file on a terminal server. The problem does not occur when using Office 2010.

CoSign Add-on for Microsoft SharePoint

- A user that is required to sign or verify documents or forms needs to have permissions to the document/form library and the files or else either the user will not be able to use the CoSign ribbon or perform signature/verification operations.
- If you upload InfoPath forms that are based on local templates or templates that are located in other form libraries, the digital signature operation may be validated although the digital signature operation was completed based on a different document template or different document template version. Therefore it is recommended to upload InfoPath forms to their origin library.
- If you have a long list of signed items, when pressing the "*verify all*" operation, you will need to make sure that all items are validated by inspecting all of the items.
- If you *Save as* a doc/docx/xlsx document from SharePoint, when you reload the document again to MS SharePoint it will be marked for automatic validation although the automatic validation is turned off.

Release Notes – Appliance Version 5.3

General information

Release Date: Jan 17th, 2012

This version includes a set of enhancements for CoSign Appliance version 5.2.

Highlights include:

- Comodo CA requires using users' keys that are based on 2048-bit size. The version includes two enhancements:
  - It is possible to define the required key size of the end user through a new system parameter.
  - It is possible to define that when a Comodo certificate is renewed, the user key is generated. In the case that the required key size is different from the current one, the key will always be generated.
- The SAPI Web Services API is lined up with SAPI of CoSign version 5.41. CoSign client 5.41 is based on CoSign client version 5.4, with a compatibility to CAdES-BES in the case that the digital signature is based on SHA2.

Release Notes – CoSign add-on for SharePoint version 5.4

General information

Release Date: July 21th, 2011

This version includes CoSign add-on for SharePoint. The version is based on CoSign client version 5.4.

The version includes a new CoSign for SharePoint guide.
Highlights include:

- Support CoSign for Microsoft SharePoint functionality when operated from a mobile device such as an iPad or iPhone.
- There is a new CoSign add-on for SharePoint ribbon that enables end-users to sign or verify signatures in addition to the regular, pop-up menu based actions. This option also enhances ease of use when using mobile devices.

Release Notes - Version 5.4

General information

Release Date: May 3th, 2011

This version includes a CoSign client version. The version includes a new CoSign User Guide and a new CoSign SAPI guide.
Highlights include:

- The OmniSign application has a brand new GUI that is aimed to improve the user experience when signing PDF files. It also includes capabilities for multi-page signatures. Also, there is improved support for electronic signatures.
- There is an improved and unified GUI for the signing ceremony. All CoSign signature add-ins and applications use the same signing ceremony dialogs.
- The use of graphical signatures with sizes larger than 30K is now available. Also, the number of graphical signatures to select from is now unlimited.
- A new graphical signature designer utility enables users to design their own graphical signature. It allows, for example, an engineer to merge his professional seal and personal graphical signature into a single image and resize the new image to the desired dimensions.
- Support of SHA2 hash algorithms (SHA-256, SHA-384 and SHA-512) for all CoSign applications as well as SAPI is now available. Support for ARX office signature line provider is available through Microsoft Office definitions. This functionality does not support signing Office 2007/2010 files through SAPI.
- Certificate Path validation criteria according to DoD PKI is now checked prior to digital signature operation. This option is configurable.

New features and fixes

Client

- The communication between the CoSign client and the CoSign appliance was improved.
- ePad and Topaz signature capture devices are now supported for Windows 7 64-bit operating systems.
- CoSign client software that is installed on a single server (e.g. SharePoint Server, a web server, etc.) can work with multiple CoSign appliances when each appliance handles users from different domains. This configuration is useful in cases where one domain is used to mange internal users

while the other is used for external users, and they have no trust between each other.
Contact ARX for more information on how to configure the CoSign client for this purpose.

SAPI

- Support PKCS#1 v1.5 based signatures upon a given buffer is now available.
- Digital signatures can now be validated providing only a hash value rather than the whole signed data.
- When signing a PDF file, you can now specify the font size of the textual elements in the signature. This feature allows changing the size of the graphical signature without affecting the font size of elements such as Name, Date and Reason. This functionality is also applicable to OmniSign by setting the value of *Default PDF Font* through the configuration utility.

Unified Signing Ceremony

- The reasons list that can be used as part of the signing ceremony is now unified, so there are no separated reasons lists for ARX Office add-ins and OmniSign.
  Upon installation of the CoSign client, user-related reasons as well as machine-related reasons are gathered from previous reasons lists. This means that any configuration restoration from older versions will not impact the existing reasons lists.
- The image quality of the automatic graphical signature (created when user account has no graphical signature) was improved.
- Graphical signatures of a large size can now be uploaded to CoSign. The image size is automatically reduced without affecting the image quality.
- Graphical signatures can now be added during signature operation when signing Office 2007/2010 files. This was not possible in former versions.
- Users who wish to capture their graphical signature every time they sign a document instead of storing the image in CoSign may now do so.

OmniSign

- The CoSign client can be configured to prevent users from modifying any signature-related configuration. This was previously possible only for users using the ARX legacy add-in for Microsoft Word and Excel.

- Better support for *Point-of-Sale / Point-of-Service* deployments. External users can incorporate their electronic signature to PDF documents in a very user-friendly manner.

Known problems/limitations/warnings

Client

- Only a single Logo per user account is permitted.
- If the CoSign verifier is installed in the end user's PC, it needs to be uninstalled prior to installing a CoSign client.
- It is not possible to capture a graphical signature and change its color after capturing.

SAPI

- Digital signatures created by Adobe Acrobat and based on SHA2 algorithms fail to validate due to an Adobe Acrobat problem.
- Adobe Signatures that are based on *adbe.pkcs7.sha1* are not supported. The *adbe.pkcs7.detached*, which are more common, are supported.
- SHA-2 hash algorithm is supported only for XP SP3 and above.
- Supporting XML Signatures to use SHA-2 hash requires a .NET framework configuration change. Contact ARX for more information.
- Embedding fonts in PDF files as part of the digital signature operation is not supported.

OmniSign

- OmniSign does not support signing PDF with owner protection.

ARX Office legacy add-ins

- Automatic verification of Excel signatures may show invalid signatures although the signatures are valid. This problem is caused by delays in loading Excel documents to memory. Manual signature validation after the document is opened will show the correct signature status.
- The following problem description describes a case that prevents a user from signing Excel data when using Excel 2003:
  When the data in one of the cells is too long (more than 1020 characters with spaces), the cell size exceeds the buffer size Excel permits in the 2003 version, which causes memory violation.
  The problem is resolved in Microsoft Office 2007/2010.
  The problem occurs only if the *Scope Of Signature* in the field's settings includes *Cell Formula*.

ARX Signature Line Provider for Office 2007/2010

- There are cases where Microsoft invalidates files that are signed either by the ARX signature line provider or the Microsoft signature line provider (for example, formula-based Excel files).
  Although there are fixes for Office 2007, the problem still exists in Office 2010.

Release Notes - Version 5.23

General information

Release Date: November 14th, 2010

This version introduces the CoSign Add-on for SharePoint as an official feature of the CoSign solution. There is a dedicated manual that explains how to install, configure and use the Add-on. Environment restrictions and limitations are also described in the manual.
The CoSign Add-on for SharePoint can be used for signing documents and SharePoint List Items in SharePoint 2007/2010. Also, it can be integrated to workflow applications that are based on SharePoint, such as Nintex workflow.

The CoSign Add-on for SharePoint requires CoSign client version 5.23 or higher.

CoSign client version 5.23 can only be used in conjunction with CoSign Add-on for SharePoint and cannot be used for regular CoSign client installations.

Known problems/limitations

- You can disable the function of CoSign Digital Signature on every SharePoint Document Library or List. The disable operation automatically removes the signature configuration parameters in the Document Library and the List. Also, be minded that digital signature parameters in List Items will be removed as well.
- When assigning a new document template to a content type in a Document Library, all existing signature profiles in the relevant content type are deleted.
- Assigning a .doc template to certain content type will generate new signature profiles based on digital signatures in the document. Location information (e.g. x, y, width and height) in the signature profiles may need to be changed to lower values in order to enable updating other fields in the signature profile.
- When integrating the CoSign Add-on for SharePoint in a workflow environment, you might not be able to reject the signature operation. This happens when the user is not required to provide any information during the signature operation.
  A workaround to this limitation can be achieved by mandating the user to enter a reason or requiring login credentials.
- Verifying signatures in documents or in List Items requires read and write permissions to the document or List Item.

Release Notes - Version 5.21

General information

Release Date: October 6th, 2010

This version is a CoSign client version as well as CoSign Desktop version. The version includes a new CoSign User Guide and a new CoSign Desktop Guide.

New features and fixes

- Office 2010 (32-bit version as well as 64-bit version) is now supported in both the CoSign Client and the CoSign Desktop versions.
- A new and improved enrollment mechanism is supported as part of the new CoSign Desktop version. The new mechanism does not use a browser for the enrollment purpose.
- It is possible to backup and restore key material and licenses when using CoSign Desktop.
- It is possible to define a transparent visible signature when using the ARX legacy add-in for Word and Excel. Using the transparent visible signature it is possible to view some of the content underneath the visible signature.
- The problem when signing PDF documents that include floating point value representations, was resolved.

Known problems/limitations

- There is a problem adding a new graphical signature while signing Office 2007/2010 using ARX signature line provider. The problem is relevant when using a pad, tablet or mouse for entering the graphical signature. The problem started to occur in CoSign client version 5.0.
- There is a problem adding one-time signatures while signing in Office 2007/2010 using the ARX signature line provider. The problem is relevant when using a pad, tablet or mouse for entering the graphical signature. The problem started to occur in CoSign client version 5.0.
- In both Office 2007 and Office 2010, when a certificate of a signed document expires, the signature is presented as invalid. By setting the following registry the signatures will not be presented as invalid when the certificate expires:

  HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Signatures\IgnoreExpiredCert= (DWORD)1.

  Or

  HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Signatures\IgnoreExpiredCert= (DWORD)1.
- When using a zoom option in Word/Excel documents that have a transparent visible signature, text may appear blurred.

- If Office 2007/2010 was installed after the CoSign client/desktop was installed, you need to uninstall and re-install the CoSign Client/desktop.

New known problems/limitations for CoSign Appliance versions 5.0/5.2

- There is a problem signing using the roaming ID interface when the signature key is larger than 1024-bit.
- There is a problem signing the roaming ID interface when CoSign is installed in an LDAP-based environment.
- There is a problem using the CoSign Web Services interface for signing XML data or Office 2007/2010 documents (.docx, .xlsx) on old CoSign platforms (based on Windows 2000 server).
- When CoSign Web Services is used for signing XML data, the XML data should be encoded twice in BASE64 format. This issue will be reverted in the next CoSign Web Services version.

Release Notes - Version 5.2

General information

Release Date: September 7th, 2010

This version includes several bug fixes for server version 5.0.

New features and fixes

- A new CoSign Enterprise model has been introduced: *CoSign Server IBM (4251)*.
- Memory leaks - there are some scenarios that, when run in for long periods of time, cause memory leaks and eventually may cause the CoSign appliance to stop its service. The problem is fixed.
- Performance reductions - there was some reduction in performance of digital signature operations when signing either through the CoSign client interface or through the Web Services interface. The problem is fixed.
- The problem of publishing AIA and CRL to Active Directory or Novell NDS when CoSign is installed as a subordinate CA has been fixed.
- The problem of publishing AIA and CRL to Active Directory or Novell NDS when upgrading CoSign from version 4.5 has been fixed.

Known problems/limitations

- There are some problems when attempting to modify the network speed of the new CoSign Enterprise appliance through the CoSign console.

Release Notes - Version 5.0

General information

Release Date: April 1, 2010

This version applies to new versions of both an appliance and a CoSign client.

The version includes a new CoSign Administrator Guide, a new User Guide and a new Programmers Guide.

The following are the major functionalities included in the version:

- CoSign client supports Windows 7 as well as 64-bit operating systems such as Windows 2008 R2, Vista – 64-bit.
  A SAPI 64-bit version is available as well. 64-bit applications can now be integrated with CoSign using SAPI.
- A new automatic external CA can be used. The CA vendor is ChosenSecurity.
  If you intend to have CoSign interface automatically the ChosenSecurity CA, you must contact ARX prior to installing CoSign.
- There is additional functionality added for CoSign installed in High Availability mode, such as changing the role of an alternate appliance to become a primary one.
- SAPI/SAPI-COM/SAPI-WS can also be used for signing XML files based on either using the XML Advanced signatures (XAdES) or the native XML signatures standard.

New features, improvements, and fixes

General issues

- For upgrading the CoSign appliance from a previous version to version 5, refer to the CoSign Administrator guide in Chapter 5.
  If a High Availability configuration is used, read carefully the required steps for upgrading CoSign High Availability cluster to version 5.

CoSign Appliance

- A new administrator operation called *Set as Primary* enables changing the role of an alternate appliance to become the primary appliance. This operation is relevant in cases where there is an unrecoverable failure to the Primary appliance. For more information refer to the CoSign Administrator Guide in Chapter 7.
- Some additional operations which relate to a High Availability installation are introduced. These operations ease subscribing/unsubscribing an Alternate appliance to a Primary appliance. For more information refer to the CoSign Administrator Guide in Chapter 7.

Also, it is no longer required to manually restart the Primary appliance after installing the Alternate appliance.

- There were improvements related to the backup/restore mechanism. During restore operation, the administrator can now inspect parameters that were used during installation.
- It is possible to set up the CoSign appliance to log the signing application name in addition to the signer ID, signature and hash of the signature. Set the system parameter *Auditing And Accounting/Report Apps Names to Event Log* value to true and restart the CoSign appliance.
- Decrypt operations are no longer supported by the CoSign appliance, even if a CoSign Client prior to version 4.6 is used.
- The CoSign appliance can be configured to use an SSL proxy that can be setup to use a User-ID/password authentication. This configuration is required when CoSign interfaces an external CA and the organization can access the Internet only through an SSL proxy.
- When uploading an update to the CoSign appliance (DLM), the progress-bar now indicates the real progress of the update process. This feature is not relevant to the DLM for upgrading CoSign to version 5.
- When using Smartcard based extended authentication, a new system parameter called *CRL Retrieval* can be used to define exactly how CRLs are downloaded and used when authenticating the user prior to digital signature operation.

Certificate Management

- CoSign can interface to a new CA vendor named ChosenSecurity in addition to the existing CA vendor - Comodo.
  Contact ARX before installing CoSign if you intend CoSign to interface with the ChosenSecurity CA service.
- It is now possible to update the current AIA or CDP when CoSign is installed in Internal CA configuration. Use the Administrator Guide to locate the appropriate system parameters and modify the system parameters according to the new possible values.
  After updating the CDP or the AIA it is advised to use the new *Refresh Certificates* operation in order to update all the users' certificates accordingly
- It is now possible to set the Certificate Policy extension in the users' certificates. Use the Administrator Guide to locate the appropriate system parameters and modify the system parameters according to the new possible values.
  After setting the Certificate Policy certificate extension it is advised to use the new *Refresh Certificates* operation in order to update all the users' certificates accordingly.
- An administrator can choose to refresh all user certificates. This operation is needed whenever a global parameter such as the CDP (Certificate Distribution Point) is modified.
  Special care must be taken using this operation when CoSign is automatically interfacing an external CA.

Performance related new features

- There is a new option that enables administrators to monitor the performance of the CoSign appliance. For more information refer to the CoSign Administrator Guide in Chapter 5.
  Whenever a performance problem is inspected, please contact ARX support for assistance.
- It is possible to define that only the built-in administrator can administrate the CoSign appliance. If this parameter is set the overall performance of the system will be improved when regular users connect to the appliance.
- In previous versions, when CoSign was installed in Active Directory or Novell NDS installations, CoSign automatically published the users' certificates into the user record in the directory. For the sake of improved performance, as of CoSign version 5 the default is not to publish the certificates. In order to publish the certificates, please refer to the CoSign Administrator Guide Chapter 5 and look for the *User Certificate Publishing* system parameter.

CoSign Client

- Windows 7 support – Starting from CoSign Client version 4.64, Windows 7 is supported.
- Windows 64-bit support – CoSign version 5 now supports all Windows 64 bit variants such as: Vista - 64 bit, Windows 7 – 64 bit, Windows 2008 R2, Windows 2003 – 64 bit.
- Fixed a problem related to setting a *preferred server* using the CoSign Configuration utility in a high availability cluster.
- CryptoKit is one of the software components of the CoSign client. The updated installation of CryptoKit is now based on MSI. This can simplify group policy based installations. For more information, refer to the CoSign Administrator Guide in Appendix-B.
  If a former CoSign client version was installed using a centralized mechanism such as group policy or an installation script, you should first uninstall the former version and install the new CoSign version.

SAPI

- SAPI now includes a new file provider that handles XML digital signatures. This new XML file provider enables signing XML data based on the XML digital signature standard. Both Enveloping and Enveloped signatures are supported.
  In addition, the advanced XML signatures (XAdES) are supported. The advanced signatures are conformed with XAdES-BES and XAdES-EPES.
  SAPI Web Services interface support signing XML data as well.
- The CoSign client can be configured to require a new user login for every digital signature operation. This option is relevant in kiosk configurations where several users work on the same PC, and often within the same application.
  This configuration can be defined either by setting the *Automatic Log Off* parameter in the SAPI section of the configuration utility, or by setting the configuration value of AR_SAPI_AUTO_LOGOFF_HANDLE with value 1 when initiating a SAPI session.
- The SAPI File provider for TIF files was modified. When using embedded visible signature, the size of the file usually does not increase.

- SAPI, SAPI-COM and SAPI-WS provide a similar functionality. For more information refer to the CoSign Programmers Guide.

OmniSign

- PDF Certify operation is now supported within OmniSign. For more information refer to the CoSign User Manual.
- A remote PDF file can now be accessed and signed using the WebDAV protocol in addition to signing PDF files on the local hard-disk. All recently accessed remote files are listed in the OmniSign File menu.
- Internet Explorer can now be configured to activate OmniSign when the user right-clicks a link to a PDF file.
- It is now possible to Drag & Drop a PDF file into the OmniSign applications window.
- A problem that ignored setting the *Display Caption* attribute in the Signature Settings dialog is now fixed.
- OCSP-related parameters can now be set through the CoSign configuration utility in the *Signature API* section.

Word/Excel legacy add-in

- There is a new option to prevent installing the CoSign menu bar in the ARX Office add-in. There were cases where the CoSign menu interfered with other Word/Excel add-ins. In this mode, only the toolbar can be used for operating the digital signature functionality.
  Please contact ARX for instructions on how to activate this option.
- There are some known problems when activating automatic signature validation in Excel. In CoSign client version 5 it is now possible to define a different flag for automatically validating signatures in Word and Excel.
- Default parameters for the ARX Signature Line Provider can now be set from the CoSign configuration utility.

Known problems/limitations

General issues

- RSA keys with sizes larger than 2048-bits are not supported when using the CoSign Enterprise model.
- CRL and Root certificates are not published to the Parent Domain when CoSign is installed on a Child Domain in an Active Directory environment.
- When CoSign is configured to use the extended authentication with a Radius interface, the maximum size of Radius password that can be used is 16 bytes.
- If CoSign is installed in a high availability cluster and interfaces with Comodo in an automated external CA mode, when intending to upgrade the alternate appliances to version 5, you must

reset the alternate appliance to factory settings, upgrade the software version and then install the alternates again.

CoSign Appliance

- The backup MiniKey token in this version is not compatible with previous CoSign appliance versions. Therefore these tokens should not be used to install CoSign appliance of versions prior to version 5.
- Changing the SSL proxy system parameters requires a full hardware restart rather than a soft restart.
- After restoration from backup, the system parameters that relates to AIA and CDP must be re-entered. Failing to setup these values right after the restoration may lead to users having wrong AIA and CDP fields in their certificates.
- After restoration from backup in a LDAP environment, the base-DN must be re-entered.
- When restoring CoSign installed as a subordinate CA/Comodo CA/ChosenSecurity CA, related parameters such as the indication of the subordinate CA is not shown in the *CA Setup* window. However, the restored appliance will be operated according to the backed-up system.

CoSign Client

- ePad and Topaz signature capture devices are not supported for Windows 7 64-bit operating systems.
- CoSign client does not support Microsoft Windows 2000 starting from CoSign Client version 5.

SAPI

- Documents that are signed with Adobe 9.3 and are cleared or re-signed using SAPI or OmniSign cannot be signed again using Adobe Acrobat.
- Requested Date and Time formats are ignored when using SAPI to sign .docx or .xlsx files.

ARX Signature Line Provider

- A new feature introduced in version 5 enables setting SAPI to require login of a new user for every signature operation. This mode is relevant for operating CoSign in a kiosk mode, where different users can access the PC for signature operations.
  There are some cases that the first user that runs Office 2007 will need to log in twice.
- When signing an XML file using the XML digsig standard, the digital signature does not include a signature time. Therefore, it is advised to use the Advanced signature format (XAdES).
- No CRLs are checked when signing using the ARX Signature Line Provider.
- It is not possible to add *One Time Signatures* that are based on Topaz/Interlink pads.

ARX Legacy Add-in

- Office 2000 is not supported starting from CoSign Client version 5.

- There are some problems detected when selecting the *Location and Size of Tables & Objects* parameters. For example, re-signing a signature field that includes a table with merged cells may present an error to the end user.

Tiff

- If the TIF file is compressed or created in Macintosh, the file's size may increase after the signature operation.
- Problems when signing TIF files with sampling of 40-bit per pixel. The visible signature may appear reversed.
- There are cases where after signing a TIF file, you will not be able to view the file using the *Windows Picture and Fax Viewer*.
- The signature time is increased if signing TIF files that have large width and height (over 1000X800 pixels of the whole TIF image).
- If the graphical signature is based on JPEG, the graphical signature will be viewed as a black box if the original TIF file is not monochrome.
  In addition, if you perform a clear signature operation, the original file will not be fully restored.

OmniSign

- When using electronic signatures, the signatures are not presented properly when using the *View Signed Version* option in Adobe Reader or Adobe Acrobat. This is an Adobe implementation limitation.
- The end user will be presented with an error message when viewing the signature details with Adobe Reader. The error is presented in the "legal" tab in the Signature properties dialog. The user will see a red cross with an error message "Unrecognized PDF content: The document contains PDF content or custom content not supported by the current version of Adobe Reader." The above occur if using SAPI or OmniSign for the digital signature operation.
- The following operations need administrative permissions in OmniSign: enable the Add "*Sign With CoSign" to PDF files* and *Show in Internet Explorer popup menu*.

Release Notes - Version 4.6

General information

Release Date: April 1th, 2009

This version explores a new product called "CoSign Desktop", which is very similar to the CoSign client but enables users to sign documents based on a software key installed in the user's PC.

CoSign version 4.6 is a client version as well as a CoSign Desktop version.

The version includes a CoSign Client user manual as well as CoSign Desktop User manual.

The following are the major functionalities included in the version:

- CoSign Desktop enables the user to digitally sign documents via a software key that is located in the user's PC. The certificate that is provided is based on a World Wide verifiable CA.
  All enabled applications such as *OmniSign* or ARX's *Signature Add-In for Office* can be used by CoSign desktop as well.
- OmniSign was enhanced to include all signature field management in addition to digitally signing PDF documents. Users can now create empty signature fields, clear the signature of a digitally signed field, as well as explore the state of all existing signature fields in the document.
- Visible digital signatures can be embedded into TIFF documents instead of adding an additional page at the start of a TIFF document.
- When a PDF document is digitally signed using either SAPI or OmniSign, it is possible to include OCSP (Online Certificate Status Protocol) with the digital signature. The OCSP information, as well as secure time-stamping information, is necessary for long-term archiving of documentation. This functionality is compliant with the PDF standard.
- You can embed a Logo or user's initial images into the visible signature. This functionality is provided for SAPI-based applications, OmniSign, and ARX Office add-ins.

Note: If not specified, any issue related to the CoSign client also applies to CoSign desktop.

New features, improvements, and fixes

General issues

- Adobe 9 is supported.

SAPI

- When performing a signature operation upon .docx or .xlsx files in a multi-user environment, a login window will no longer appear for the default user.
- In previous versions some latin1 characters (such as ú) where not inserted and displayed correctly when using them as part of a reason or a common name.
  The issue is fixed.
- *PDF certification* operation through SAPI now supports all 3 levels of permissions for modifying the document after the digital signature operation. In the previous version, only one level could be used. For more information refer to CoSign 4.6 SAPI manual.

Word/Excel legacy add-in

- There are some issues related to signing or validating Word documents containing ActiveX objects such as embedded Excel documents inside a Word document. Some of the information incorporated in the signed content cannot be accessed during verification. Therefore, the scope of signature also includes a flag called ActiveX information that enables the user to avoid including information from ActiveX objects.
  If the user chooses to include ActiveX information, an alert will be displayed to the user indicating that there may be verification problems once the document is verified.

Known problems/limitations

General issues

- Windows 64bit Operating Systems are not supported.
  There is limited support for 32bit applications executed on these platforms. For more information contact ARX.
- Open Office includes a built-in digital signature mechanism that does not work when using the CoSign client due to a failure in Open Office. For more information refer to http://www.openoffice.org/issues/show_bug.cgi?id=78341.
- There is memory leakage when performing signature operations through SAPI in XP SP3. This is due to Microsoft memory leakage.
- SharePoint web browser does not support digitally-signed documents that are based on Microsoft or ARX Signature Line provider. This is a Microsoft limitation.
- It is not possible to capture new graphical objects when signing in Office 2007 on the Vista platform. In this scenario, the user should add their graphical signature separately.
- There is a problem accessing the CoSign control panel in the Vista Home edition directly after the installation. Users can access the CoSign control panel from the tray or restart their machine after the installation is complete.
- There are problems in some of the CoSign forms when the user is not using the default DPI settings of the PC.

- There is a problem in the change password option when CoSign client is used in the Directory Independent environment. Only the first half the new password and confirmation password are verified for compliance.
- A graphical signature image can be created by capturing mouse movements. This option is not available via default in WinXP or Win2000, but will become available if Office 2003 is installed.
- If the user specifies in the CoSign configuration utility that they would like to use a specific pad model for capturing a graphical image, the user will not be prompted with an alert if the pad is disconnected.

CoSign Desktop

- Users must install a valid license before using the CoSign desktop. Some operations, including a digital signature operation, will fail without an installed license.
- If the desktop is based on VISTA, It is recommended to use Service Pack 1.
- In Vista with no service pack, the certificate enrollment website must be added manually to the trusted sites or certificate enrollment cannot be performed.
  You should add https://*secure.comodo.net* to your trusted sites.
  In some cases the following web site should be added as well: http://www.arx.com
- Certificate enrollment can only be done through Internet Explorer. User's need to verify that if they have a different default browser, Internet Explorer is used for certificate enrollment purposes.
- If the user re-installs the CoSign desktop over an existing installation, a restart window request will be presented during the installation and not at the end of the installation.
  The user's PC should be restarted at the end of the installation.
- During a signature operation or certificate enrollment operation, a window requesting a password may appear at the back of the relevant application (for example, Internet Explorer or Microsoft Office) or in the taskbar. Make sure the password window is presented, enter a password, and continue with the operation.
- There are some cases where software token initialization is not successful. To solve the problem, the user needs to restart their PC, then close the CoSign control panel and restart the CoSign control panel with administrative permissions.
  Then the user needs to perform the token initialization using the *Change Password* option.
- There are some cases where the password request dialog will re-appear even if the user pressed the *Cancel* button. The user will need to press *Cancel* again.
- In Vista, if the user did not download their certificate at the final stage of the certificate enrollment, there may be invalid objects in their software token. These invalid objects may cause problems if the user tries to enroll for a signature key and a certificate.
  In this scenario, it is recommended that the user initializes their token and tries to enroll for a certificate again.
- The InfoPath icon is not shown directly after installation. After restart the icon will be displayed in the CoSign control panel.

OmniSign

- There are some rare cases where using the OmniSign printer from Excel will generate a PDF file that is different than the correct one. In many of these cases some of the information will be distilled.
  Selecting OmniSign to be the default solves the issue.
- When uninstalling Adobe Reader, the *Sign with CoSign* menu option is removed when clicking a PDF file. Use the *Add Sign with CoSign to PDF Files* option in OmniSign to add the option back to the menu. This option requires administrative permissions.
- When using OmniSign in silent mode, and a *default folder* is specified in order to have the signed files copied to the specified folder, original files will be signed as well. To avoid this problem, make sure you have a copy of the original files.
- There is a problem setting the *Display Caption* attributes in the Default Signature Settings dialog. It is possible to set this value through the CoSign configuration utility.
- OmniSign can only be activated on valid PDF files. If the loaded PDF files are damaged, then OmniSign does not operate as expected.
- There are no OCSP-related parameters that can be configured through the CoSign configuration utility. For information on how to configure OmniSign for OCSP use, contact ARX.
- If the user intends to add an invisible signature, they are still requested to draw a rectangle for the signature.

SAPI

- An automatic graphical image is used when the user does not have any graphical image defined. There are some cases when the image appearance has poor quality. In these scenarios it is recommended that the user capture a new graphical image.
- Digitally signing PDF files from SAPI or OmniSign that involve Unicode characters as part of the signer's common name or the signature's reasons are not supported and will not be displayed correctly.
- Signing using a certificate without a common name is not supported. This scenario only happens when an external CA issues certificates for CoSign users.
- There are cases when *Create and Sign* will fail if the user does not have a graphical image.

TIFF Signatures

- There is no support for Logo or Initials for TIFF files.
- When using a visible signature embedded in the TIFF file, the user must provide a valid and existing page or the digital signature may be corrupted.
- There is a problem adding visible signatures on TIFF files that are based on 32bit colors.
- There is a problem adding a visible signature on TIFF files with a Photometric value of *MinIsBlack*. Colors may be inverted in such scenarios.
- Signing on very large TIFF files (50 pages or more) may damage the TIFF file during a digital signature operation that includes a visible signature.

- Note that if a standard TIFF viewer is used to view a signed document and the user performs a *Save As* operation, it may damage the digital signature in the TIFF file.

Word/Excel legacy add-in/ARX Signature Line Provider

- There are some cases where a signature field is created using CoSign client version 4.6 with a CoSign 4.6 functionality. However, when trying to sign using CoSign 4.42, no message will be displayed to the user requiring them to upgrade their CoSign client to the latest version. This issue is specific to CoSign version 4.42.
- If the ARX Verifier is installed in a non-administrative environment, there is no presentation of signature details after pressing the *Details* option. The user can still see details of existing signatures via the *Digital Signatures* panel.
- When using section-based signatures, adding a new section before a signed section may invalidate the digital signature due to section renumbering when the new section was created.
- Any default parameters that are set from the CoSign configuration utilities for the ARX Signature Line Provider are ignored. Contact ARX if it is necessary to use different parameters than the defaults.

Release Notes - Version 4.52

General information

Release Date: September 18th, 2008

This version is based on CoSign appliance version 4.5, which provides an enhanced upgrade procedure that enables customers to perform an upgrade from version 4.1 to version 4.5.

New features, improvements, and fixes

- A problem was fixed when upgrading a primary CoSign appliance from version 4.1 to 4.4. After the upgrade was done, it was impossible to install an alternate appliance.
- If CoSign was installed in *NO CA*, the upgrade to version 4.4 would fail. This problem was fixed.
- In Some cases, CoSign would not respond after installing isp4_4.dlm. This dlm was fixed.
- The following section describes how to upgrade CoSign from version 4.1 directly to version 4.52.

Remark: If CoSign is installed in NO-CA mode, there is a problem when trying to backup the appliance. Please contact ARX support for getting a special dlm that fixes the problem. The dlm is named *fnocb.dlm* and can be installed only after CoSign is upgraded to version 4.5. After the dlm is installed a hard restart is required.

Upgrading the CoSign appliance from version 4.1 to version 4.52

Refer to chapter 5 in the CoSign Administrator Guide for general information on how to upload a DLM (downloadable module) to the CoSign appliance.

Version 4.5 upgrade includes the following two files:

- *isp4_5.dlm* - An upgrade of appliance system functionality.
- *Verupd45f.dlm* - The actual software upgrade of CoSign version 4.5.

Important – Read prior to any installation:

If you have special DLMs installed in the CoSign appliance (Radius, authentication, Biometric authentication, Web Services, etc.) contact ARX support prior to the upgrade procedure.

Please complete the following instructions:

- Backup the appliance you intend to upgrade.
- Upgrade your CoSign administrative client version to CoSign administrative client version 4.42.

- In the case of a High Availability/ Load Balancing environment, you will first need to select the **Return to Factory settings** on all of the appliances that are *Alternates*. **This is a mandatory requirement** since there is a database configuration change in version 4.4. Having a mixture of Appliances of version 4.1 and version 4.4 databases on the same network will cause errors.
- Upgrade the Primary CoSign internal system using the file *isp4_5.dlm*. The procedure will take 10-20 minutes. Check the CoSign Master Disk Version in the CoSign Support report. (Server parameters section). The Master Disk Version should be 4.3.
  Upgrade the Primary CoSign appliance to version 4.5 using the *verupd45f.dlm*.
  The upgrade procedure will take between 10-20 minutes. As an indication of a successful upgrade, you should see *Version SW4.5* in the console of CoSign in the *Status* menu.
- In the case of a High Availability/Load Balancing environment, perform the above step on all of the *Alternate* appliances. Make sure they are all set to the *Factory Settings* state prior to installing the dlms.
  After the upgrade is done, install the appliances again from their Primary CoSign appliance (refer to chapter 7 in the CoSign Administrator Guide for instructions).

Using the CoSign console, validate that the software version is indeed *4.5*.

Please contact ARX Technical Support should you experience any problems.

Release Notes - Version 4.5

General information

Release Date: June 10th, 2008

This version is a fix for CoSign server version 4.4.
Version 4.5 includes the enhancements/bug fixes detailed below.

New features, improvements, and fixes

- In very rare cases a newly generated certificate could not be used to properly sign/verify using Office add-ins, OmniSign, and other SAPI based applications. This problem was corrected.
- Signing PDF files that are protected by passwords through CoSign Web Services was not possible. This problem was corrected.
- The problem encountered when attempting to list users via SAPI web services was rectified.
- It is possible to order a CoSign appliance that is not capable of executing the following operations:

  Performing backup operation

  Allowing an administrator to set a new password for a given user

  Performing CoSign database replication in high availability mode.

  These limitations are due to strong regulations (generally in EU countries) that forbid any attempt of exporting keys out of the application (even in encrypted mode) or allowing an administrator to set the password of a given user.

Upgrading the CoSign appliance from version 4.4 to version 4.5

Refer to chapter 5 in the CoSign Administrator Guide for general information on how to upload a DLM (downloadable module) to the CoSign appliance.

Version 4.5 upgrade includes the following file:

- *verupd452.dlm* - The actual software upgrade of CoSign version 4.5.

Important – Read prior to any installation:

Please complete the following steps:

- Backup of the appliance you intend to upgrade.
- Upgrade the Primary CoSign appliance to version 4.5 using the *verupd452.dlm*.
  The upgrade procedure is immediate.
- Wait a minute and then perform a hardware reboot.
- As an indication of a successful upgrade, you should see *Version SW4.5* in the console of CoSign in the *Status* menu.
- In the case of a High Availability/Load Balancing environment, perform the above 3 steps on all the *Alternate* appliances.

Release Notes - Version 4.4

General Information

Release Date: April 14th, 2008

The version includes major new functionalities that are fully described in an updated version of the CoSign Administrator Guide and the CoSign User Guide.

The version is based on CoSign Appliance firmware version 4.4 and CoSign client version 4.42.
The following is a list of the major enhancements:

- Users from multiple Active Directory domains that have common trust can access a Single CoSign appliance.
- The CoSign appliance can be accessed via the Web Services interface. There are two Web Services methods that can be used:

  SAPI Web Services that are based on OASIS DSS standard.

  Roaming ID protocol that can enable accessing the CoSign appliance from Adobe Reader 8+ or Adobe Acrobat 8+ for a digital signature operation.
- A variant of user directories that are accessed via LDAP can be used: IBM Tivoli, Sun Directory Server, and Oracle OID.
- Extended User authentication methods can be used to enhance the authentication of the user prior to performing a digital signature operation. The possible extended authentication methods that can be used are: One Time Password devices, Authentication Smart Cards, and Biometric devices.
- As part of the above extended authentication methods, an RSA One Time Password device can be used.
- There are additional mechanisms to import end user's graphical images: Tablet PC, Mouse and a text based on script fonts.
- A digital signature can be time stamped using commercial time stamping service. The interface to a time stamping service is based on standard protocols.

Upgrading the CoSign appliance from version 4.1 to version 4.4

Refer to chapter 5 in the CoSign Administrator Guide for some general information on how to upload a DLM (downloadable module) to the CoSign appliance.

Version 4.4 upgrade includes the following two files:

- *isp4_4.dlm* - An upgrade of appliance system functionality.
- *verupd4_4.dlm* - The actual software upgrade of CoSign version 4.4.

Important – Read prior to any installation:

If you have special DLMs installed in the CoSign appliance (Radius, authentication, Biometric authentication, Web Services, etc.) contact ARX support prior to the upgrade procedure.

Please complete the following instructions:

- Backup of the appliance you intend to upgrade.
- Upgrade the CoSign administrative client version to CoSign administrative client version 4.42.
- In the case of a High Availability/ Load Balancing environment, you will first need to select the **Return to Factory settings** on all the appliances that are *Alternates*. **This is a mandatory requirement** since there is a database configuration change in version 4.4. Having a mixture of Appliances of version 4.1 and version 4.4 databases on the same network will cause errors.
- Upgrade the Primary CoSign internal system using the file *isp4_4.dlm*. The procedure will take 10-20 minutes. Check the CoSign Master Disk Version in the CoSign Support report. (Server parameters section). The Master Disk Version should be 4.3.
  Upgrade the Primary CoSign appliance to version 4.4 using the *verupd4_4.dlm*.
  The upgrade procedure will take between 10-20 minutes. As an indication for a successful upgrade, you should see *Version SW4.4* in the console of CoSign in the *Status* menu.
- In the case of a High Availability/Load Balancing environment, perform steps 4 and 5 on all the *Alternate* appliances. Make sure they are all set to *Factory Settings* state prior to installing the dlms.
  After the upgrade is done, install the appliances again from their Primary CoSign appliance (refer to chapter 7 in the CoSign Administrator Guide for instructions).

Using the CoSign console, validate that the software version is indeed *4.4*.

Please contact ARX Technical Support should you experience any problems.

New features, improvements and fixes

Read the CoSign manuals for information on all of the new features of CoSign version 4.4.

The following are additional features, improvements, and fixes:

CoSign Appliance

The implementation of the internal CA of CoSign was changed to a more robust implementation that greatly influences the performance of CoSign during installation, backup, and restore.

- It is possible to use the display name field of the user in the directory as the common name of the user certificate. Until now, the only option was to use the common name field of the user in the directory.

- Set the Certificate Common Name value in the CoSign System parameters or use the Certificate Common Name origin in the CoSign configuration utility/Admin section to be used as part of the CoSign installation.
- When installing a CoSign appliance in an Active Directory environment, a window will pop-up whenever an operation that requires a special administrative permission will pop-up for the user. You can enter another administrator account to perform the failed operation.
- In the case of a Join to the domain operation, the administrative account must be provided in a dedicated form in the installation wizard.
- When using CoSign in Directory Independent mode, additional password policy limitations can be used such as defining expiration to the user's password. For additional information use the CoSign administrator guide.
- CoSign Web Services is deployed with a fixed self-signed SSL certificate. It is possible to upload an organizational specific SSL private key and SSL certificate to CoSign. Follow instructions in the CoSign administrator guide on how to upload an already generated SSL private key and certificate.

For more information on how to enroll for an SSL Server certificate please contact ARX.

CoSign Client

- The graphical signatures utility was enhanced to support additional mechanisms in their ability to upload a graphical image into the CoSign appliance. It is now possible to capture a graphical signature from a tablet PC/mouse or use a script font.
- If you use a script font, make sure you are using as large a font as possible to get a better graphical image.
- In environments that request for a user to logon, such as Directory Independent, the user will only be requested to logon once. All future operations will prompt for logon only in the case of a digital signature-related operation or the upload of a new graphical image.

SAPI

- An ability to include a time stamp as part of the digital signature was added. SAPI can be configured to communicate with a time stamping service in order to include a reliable time as part of the digital signature.

  The interface to the time stamping service is based on RFC 3161 and ETSI TS 101 733 standard.

  Additional custom fields can be kept inside signature fields in the document. The custom fields can be helpful to SAPI developers to enhance their application logic, depending on applicative data that can be kept inside the signature fields.

- It is also possible to use a new title/additional text field. This field can be added through the OmniSign application.

- It is possible to certify PDF documents through SAPI. Supply the AR_PDF_FLAG_CERTIFY as a flag to the SAPISignatureFieldSign, SAPISignatureFieldCreateSign or the appropriate SAPI Web services function to certify a PDF document.
- It is possible to sign a given hash value in addition to signing a given data. This mode is useful when you do not want to locally calculate the hash and have SAPI sign the given hash. Supply the AR_SAPI_SIG_HASH_ONLY to SAPIBufferSignEx function, and as data provide the hash value.

Currently only a given SHA-1 hash value is supported.

Word/Excel add-in

- It is recommended to upgrade to CoSign client version 4.42 to be able to verify both signatures that were generated with CoSign Client version 4.42 and former versions. It is possible to use CoSign verifier version 4.42 as well.
- The ARX Legacy add-in can also be used on .docx and .xlsx files using Office 2007. The ARX legacy add-in can be used in the cases where standard digital signature support for 2007 is limited, such as supporting section-based signatures.
- In this case, only content-based signatures are supported.
- A new ARX ribbon was added to Office 2007 to enable operations such as one touch signature operation or getting info related to ARX Signature line provider. It is also possible to add a new digital signature field through the ARX ribbon.
- There is a new option in the ARX legacy add-in that enables you to exclude values from Form Fields and values from Content Controls as part of the digital signature. This ability can be useful in cases where elements in the document are modified and thus invalidate the digital signature performed within the document.
- A new policy option can be used by the designer of the document. The policy can be set up to define whether it is possible to clear an existing signature in the document. Also the policy of the signature field can be configured to allow only the signer to clear his/her digital signatures.

OmniSign

- A tablet PC or a mouse can be used to enter electronic signatures in addition to the Topaz and Interlink pads.
- To avoid damaging signatures in an existing PDF document, a special notice appears to the signer when activating the print option in Adobe Acrobat or Acrobat Reader. Users that wish to sign a PDF document should use the Sign with OmniSign option, using the right click on the mouse.

Known problems/limitations

CoSign Server

- After an Alternate CoSign appliance is installed using the option Install Alternate from the CoSign MMC Snap-in, both the CoSign primary appliance and the CoSign alternate appliance should be manually restarted.
- For the following Alternate CoSign installation it is not required to restart the CoSign appliance.
- If CoSign is installed in a Directory Independent environment, during restoration the CoSign administrator name and password are checked against the defined password policy.
- When CoSign is installed in a LDAP environment, CoSign users must use passwords, which are not empty ones.
- When CoSign is installed in Directory Independent mode, an administrator can unlock a user only by setting a new password for the user.
- Make sure CRL validity period system parameters are smaller than CRL publishing frequency in the CoSign system parameters – certificate management section.
- When using smartcard-based extended authentication, there is a chain validation problem. To solve the problem, all the chain up to the root should be uploaded to the CoSign appliance using the subordinate CA menu option in the administration snap-in.
- The user's key must be deleted and a new key must be re-enrolled when an SSCD password is locked.
- Problem changing system parameters that are specific to an alternate CoSign appliance.
- It is impossible to use Adobe Roaming ID with CoSign in SSCD mode or when Prompt for Sign mode is active.

CoSign Client

- When the CoSign Primary server is not available and the CoSign client is accessing the alternate CoSign appliance, the logoff button in the CoSign control panel is not functioning.
- When using an RSA One Time Password (OTP) token, there are times when the user needs to wait for a few seconds before providing a new OTP. Make sure to increase the timeout of the password prompt window to avoid an automatic closure of the password window. Increase the value in the Close Dialog when inactive in the Client/Login dialog form.
- There are some rare cases where the same user is displayed several times in the CoSign Users management utility. This usually happen when users are sorted according to their user name or common name.
- Adobe 9 is not fully supported.
- When a primary CoSign appliance is not available, two irrelevant icons may appear in the CoSign Control Panel.

SAPI

- There is a small memory leak whenever a thread finishes in an application that is using SAPI.

- When performing a signature operation upon .docx or .xlsx files in a multi user environment, a login window may pop for the default user. Contact ARX for assistance.

Word/Excel add-in

- When using ARX's Signature Line provider and there is an error during the signature operation, the next digital signature attempt will display an error. A new attempt to sign the document will be successful.
- When using office 2007 with Microsoft SharePoint, use the checkout option in SharePoint and not the one in Microsoft Office. Using the checkout option in Office 2007 will invalidate an Entire File digital signature.

Release Notes - Version 4.31

General Information

Release Date: July 1th, 2007

This version is **based on CoSign server version 4.1**.

The version includes several new enhancements. All enhancements are fully described in a new revision of the CoSign User Guide.

The following list highlights the major new functionality of the CoSign client.

- Support for Office 2007: The CoSign client offers a new add-in called ARX Signature Line Provider. The Add-In provides a standard based digital signature solution for Office 2007 for the new type of files (.docx, .xlsx).

  The Legacy ARX signature add-in is also supported for old style Word and Excel files (.doc and .xls files)

- Support for Vista: The CoSign client can be installed on Window Vista in addition to the supported Windows based platforms.
- Support for Electronic Signatures in OmniSign: OmniSign enables the addition of electronic signatures using a signature pad. This feature is required in PoS (Point of Sale) deployments, whereby customers sign with a graphical (electronic) representation of their signature and eventually the local sales representative signs the whole document with their digital signature.
- Support of a new signature pad: The CoSign client supports additional signature pads, manufactured by Topaz Systems (http://www.topazsystems.com).

  The supported models are: SigLite LCD 1x5 USB and SigLite 1x5 USB.

The following sections also include descriptions of problem fixes and also known problems and limitations of this version.

New features, improvements and fixes

CoSign Client

- The maximal amount of data that can be used for all graphical images for a user was increased to 140K. A single graphical image is still limited to 29K.

SAPI

- Supports the new office 2007 file type called OXMLP (Office Xml Package). Read about the limitations of signing this type of file in the following sections.

Word/Excel add-in

- Office 2007 - The new ARX Signature Line provider can be used to add new digital signatures through the Insert tab's special Signature Line option. Click ARX CoSign Signatures Add-in for Office to add the signature field and the popup menu on that field to generate a digital signature.
- Office 2007 - The legacy ARX add-in for old style office documents can be activated through the Add-Ins tab in Office 2007 (MS Word and MS Excel). Both the ARX Legacy Word Add-in pull-down menu and its toolbar will appear.
- The problem with the implementation of dependent digital signatures in an active sheet was resolved.

OmniSign

- OmniSign supports inserting several electronic signatures into the PDF document before digitally signing the document. Upon electronic signature request, the currently installed signature pad will be activated and the user will be requested to enter their graphical signature.
- You must select the ARX CoSign Admin component to be able to add electronic signatures.
- The problem of losing document location when zooming in/out of a document was resolved.

PDF signatures

- Adobe Acrobat 8 and Adobe reader 8 are supported.

Known problems/limitations

CoSign Client

- There is a problem when performing an upgrade that includes the OmniSign component on a machine that is installed with an HP-desktop printer. In this case it is advisable to uninstall and then reinstall the new CoSign client version.

SAPI

- If you intend to use SAPI to sign the Office 2007 new file format, you need to install .NET Framework version 3 prior to using SAPI.
- You cannot create or delete signature fields inside .docx or .xlsx files using SAPI. You can only sign or clear the signatures. In order to create or delete the files you need to use Microsoft Office 2007 with the ARX Signature line provider.

- SAPI can be used to sign .docx and .xlsx documents only for the currently logged-on user. Any attempt for using the SAPILogon API with a different user will cause a failure to the digital signature attempt. This is also true when using the arsignfile utility.
- You cannot re-sign an already signed field when using .docx or .xlsx files. You must clear the digital signature before attempting to re-sign the field.

Word/Excel Legacy add-in

- It is recommended to upgrade to CoSign client version 4.31 to be able to verify both signatures that were generated with CoSign Client version 4.31 and former version. It is possible to use CoSign verifier version 4.31 as well.
- If you generate a new document using Office 2007 and create an old style digital signature you need to save the document as an old style document before continuing to sign the document. Upon signing an unsaved file you will be prompted to save the file or get another type of error.
- Also, do not save the file as a .docx or .xlsx files if it contains a legacy digital signature field.
- In office 2007 there is an enhanced digital signature mechanism for old style documents (.doc and .xls files). Upon using the Microsoft Office Compatible Signature feature and signing the document, the document will be locked for any modification. Therefore, in these cases, any operation of the ARX legacy add-in such as clear digital signature or re-signing a document is not permitted.
- When using word 2007 to generate Microsoft Office Compatible and the option Sign on Location & Size of tables and objects option is checked, the ARX content-based signature gets invalidated since some of the properties of the document cannot be accessed.
- There are some rare cases where when printing the document it will not be fully verified prior to printing. Therefore the user is advised to manually validate all signatures before printing.
- Problems using MS SharePoint on Vista, when signing Entire File based signatures.
- Deleting a sheet on an Excel document might affect signatures in other sheets, even though they are not defined as workbook-based digital signatures.
- The legacy ARX add-in Menubar entry still remains in Excel 2007 plug-ins tab after uninstalling the CoSign client.
- When using shared documents on Vista platform, there are problems when performing operation such as adding signature field or signing existing signature field.

PDF signatures

- The ARX plug-in for Adobe 5 is no longer supported.

- The maximal size of electronic signature for use by OmniSign is 100K.

Release Notes - Version 4.32

General Information

Release Date: September 3th, 2007

The version includes enhancements in the CoSign client and is **based on CoSign server version 4.1**.

The following list highlights the major new functionality of the CoSign client.

- Multi language support for end user operations

  Languages currently supported are: German, Spanish, Portuguese, Italian and Dutch.

- CoSign verifier is released and supports also Windows VISTA

  The CoSign verifier can be downloaded from the ARX web site or be deployed in the customer web site.

  For more information refer to the CoSign user manual, chapter 4.

- Proper support for signing .docx files through the SAPI SDK

  In the previous version it was impossible to sign .docx and .xlsx files in multi-user environment.

- Additional enhancements and bug fixes

Additional language support in the CoSign Client

The CoSign client was enhanced to provide local language user experience in the major forms that are used by end users.

The following client modules were enhanced:

- CoSign Control Panel
- OmniSign
- Office Legacy add-in for Word 2000/XP/2003/2007 and Excel 2000/XP/2003/2007
- User Login and Signature forms.
- Graphical signature selection

The support for additional languages is based on Microsoft MUI (Multilingual User Interface). Depending on the currently used language, the CoSign client is adaptive and interacts with the end user using the selected language.

CoSign Verifier

The CoSign Verifier can also be installed on Microsoft Vista platforms. The verifier is aimed on making the verifying party of signatures created by CoSign as smooth as possible and includes the following capabilities:

- Installation of the CoSign ROOT certificate in the verifier PC.
- Automatic configuration of Adobe Acrobat and Acrobat reader in the verifying PC.
- Enable validation of signatures in Word/Excel 2000/XP/2003 documents. The verifier also support validating these documents in Office 2007.

There are cases that the verifier is not required (for example, when the CoSign user certificate is based on WWV certificate) since CoSign is based on PKI standards that do not require any special functionality or shared secret in the verifier side.

For more information about the CoSign verifier please refer to the CoSign user manual.

The CoSign Verifier can be downloaded from the following link:
http://www.arx.com/support/downloads.php.

Limitations:

- In Windows VISTA only administrators can download and install the ROOT certificate. On other platforms such as Windows XP, a regular user can also download and install the ROOT certificate.
- In Windows VISTA only administrators can update the Adobe-related parameters for proper verification. On other platforms such as Windows XP, a regular user updates these parameters.
- The CoSign Verifier can only be installed on a Windows platforms using Internet Explorer 6/7. Browsers such as FireFox are not supported.

New features, improvements and fixes

CoSign Admin Client

- Problem with disable options when trying to install CoSign as a subordinate CA of an external CA was fixed.

SAPI

- It is now possible to use SAPI for to sign and clear fields inside .docx and .xlsx files. In previous version it was possible only on rare scenarios.

Word/Excel add-in

- Performance was improved where using the entire file mode to validate signed documents maintained using Microsoft SharePoint.

Release Notes - Version 4.34

General Information

This version is the base for supporting CoSign for Laserfiche. All information about this version is located in the CoSign for Laserfiche documentation.

This version is **based on CoSign server version 4.32**.

Release Notes - Version 4.35

General Information

Release Date: January 29th, 2008

The version includes some client enhancements.

The version is **based on ARX Cryptokit version 4.2**.

OmniSign

The following enhancements were made to OmniSign. The following three options were added to the OmniSign enhancement:

- Show Settings– If this option is selected, the end user cannot change any of the settings of OmniSign.
- Continuous Scrolling – If this option is selected, the end user will continuously scroll the PDF file, while the default option is to scroll within the current page.
- On-Touch signature positioning – If this option is selected, the end user can only click on the location of the signature and does not need to drag with the mouse to get the signature's rectangle.

CoSign Client

- It is now possible to request a certificate from an external CA using a built in option in Vista Operating system.

Release Notes - Client Version 4.2

General Information

Release Date: February 1th, 2007

The version is a client-only version and is intended to address several problems.

The version also has some enhancements that support using CoSign in the OID (Oracle Internet Directory) environment.

The client functionality enables the following:

- An administrator will be able to install/restore CoSign in the OID environment.
- Upon the first login to the CoSign appliance, the end-user will enroll for a key and a certificate.

  If WWV (Worldwide Verifiable) certificates are used, the user will be prompt with a special wait-for-certificate window (until the WWV certificate is ready for use).

New features, improvements and fixes

Word/Excel add-in

- The Word add-in enables users to sign a document using the entire file mode and incorporate the document into Microsoft SharePoint 2007.

  In order to be compatible with SharePoint, you need to set the toggle *SharePoint 2007 Compatible* in the Scope of Signature tablet in the Signature settings window.

  Users may also define a global definition to this parameter in the CoSign Configuration Utility under the Word Specific section.

SAPI

- The problem when indicating to sign at the last page of a PDF file by providing page = -1 as an indication, was resolved.
- Memory corruption issues that arose when using SAPICOM were resolved.
- The following problem in CoSign Client version 4.13 was resolved: There are some TIFF formatted files configured to use the parameter FillOrder = Lsb2Msb could not be signed using a visible signature.

PDF signatures

- The problem when indicating to sign at the last page of a PDF file by providing page = -1 as an indication, was resolved.
- The following problem in CoSign client version 4.13 was resolved: There was a problem using graphical signatures that were based on a JPEG gray scale image format.
- The following problem in CoSign Client version 4.13 was resolved: The Update Acrobat option in the Graphical Signature application degraded the quality of a new monochrome graphical image that is loaded to Acrobat application. The problem was resolved.

Client Configuration Utility

- Problem downloading very large CRLs from CoSign. Size bigger than ~50k was resolv

Release Notes - Client Version 4.21

General Information

Release Date: March 19th, 2007

The version includes several enhancements and fixes:

- Tiff opening signature page can be compressed using the following methods in addition to LZW algorithm:

  Packbits compression

  Group4Fax compression

- SAPICOM was extended to support Visual Basic application when using the SAPI_FILETIME type.
- ARX add-in for office was extended to provide additional functionality for OEMs. For more information please contact ARX.

New features, improvements and fixes

Tiff signatures

- When directing SAPI (through arfilesign application) to digitally sign a tiff file, a graphical image can be appended as the opening page to the tiff file.

  This page can be compressed in two additional methods:

  Packbits compression

  Group4Fax compression

- In default the compression type would be LZW, but the user can change the flags parameter in the signing API as follows:

  2 – Packbits compression - both monochrome and colored graphical images are supported when this method is used.

  4 – Group4Fax compression - if the graphical image is grayscale or there is no graphical image stored in CoSign. There will be no compression if the graphical image is colored

SAPICOM

- There was a problem when SAPI-COM was invoked from a Visual-Basic application when using SAPI_FILETIME for getting signature time. The SAPI_FILETIME was extended to be able to retrieve the time by these types of applications.

Release Notes - Version 4.22

General Information

Release Date: May 13th, 2007

The version includes the following improvement

- Support Microsoft SharePoint 2003/2007 in SSL mode.

New features, improvements and fixes

ARX Word Add-in

- The problem of using Microsoft SharePoint in SSL mode was fixed.

  The problem occurred when the user performed operations such as signature, verify signature or clear signature and the signature was based on *Entire File*.

Release Notes - Version 4.1

General Information

Release Date: January 1th, 2007

The version includes major new functionalities that are fully described in an updated version of the CoSign User Guide.

An updated Reference Guide for SAPI is also located in the CoSign SDK CD.

The new functionality includes:

- A new GUI for the CoSign client: The CoSign client includes a new control panel from which all client functions may be activated.
- Enhanced support for graphical images: There are three major enhancements in the support of graphical images:

  A user can have more than one graphical image. In the case that a user has more than one graphical image, the user will be prompted to select the desired graphical image when commencing a digital signature procedure.

  CoSign can handle the following images formats: JPEG and multicolor BMP, in addition to the monochrome BMP format.

  Users can manage their own graphical images and import images to the CoSign appliance either via a signature pad (ePad or ePad Ink) or from a file.
- CoSign's signers list – Active Directory group: The CoSign signers list (CoSign users) can be defined according to a special Active Directory group that may contain other users or groups.
- Automatic certificate management using an external CA: CoSign can be configured to interface an external World Wide Verifiable (WWV) CA. The version support WWV CA for generating users' certificates that can be verified on any PC with a recent operating system (i.e. Windows XP).
- CoSign SSCD hardware model: Outwardly similar to CoSign Enterprise, CoSign SSCD is built to meet stringent EU regulations (Common Criteria SSCD certified (CWA-14169)), securely storing a users' private key inside the appliance on an array of smart card chips. This model enables key generation and signature operations to take place inside the smartcards.

The following section will illustrate to current CoSign users how they can upgrade their existing CoSign from version 3.1 to version 4.1.

The following sections also include descriptions of problem fixes and also known problems and limitations of this version.

Upgrading the CoSign appliance from version 3.1 to version 4.1

Refer to chapter 5 in the CoSign User Guide for some general information of how to upload a DLM (downloadable module) to the CoSign appliance.

Version 4.1 upgrade includes the following two files:

- *verupd41.dlm* - The actual software upgrade of CoSign version 4.1.
- *csnsp1.dlm* - An upgrade of appliance system functionality.

Please complete the following instructions:

- Backup of the appliance you intend to upgrade.
- Upgrade the CoSign administrative client version to CoSign administrative client version 4.13.
- In the case of a High Availability/ Load Balancing environment, you will first need to select the **Return to Factory settings** on all the appliances that are *Alternates*. **This is a mandatory requirement** since there is a database configuration change in version 4.1. Having a mixture of Appliances of version 3 and version 4 databases on the same network will cause errors.
- Upgrade the Primary CoSign appliance to version 4.1 using the *verupd41.dlm*.
- The upgrade procedure will take some time. As an indication for a successful upgrade, you should see *Version SW4.1* in the console of CoSign in the *Status* menu.
- If the previous step is successful, upgrade the Primary CoSign appliance system using *csnsp1.dlm*.
- This procedure will take a long time. For an indication of a successful upgrade, use the CoSign report utility, which is activated via the CoSign configuration utility operated from the CoSign Control Panel.
- Activate the option *create report* from the *Help* menu bar entry.
- In the *server* tab check the parameter Console - *Master Disk Version*. The version should be 2.7.
- In the case of a High Availability/Load Balancing environment, perform steps 3 and 4 on all the *Alternate* appliances. Make sure they are all set to *Factory Settings* state prior to installing the dlms.

  After the upgrade is done, install the appliances again from their Primary CoSign appliance (refer to chapter 7 in the CoSign User Guide for instructions).

Validate using the CoSign console that the software version is indeed 4.1.

Please contact ARX Technical Support should you experience any problems.

Important – Read prior to any installation:

- After the upgrade procedure, some system parameters will be available in the CoSign appliance management application which is not supposed to be displayed (for example, system parameters that are relevant to CoSign SSCD). *Please refrain from updating these system parameters.*

- If you have special DLMs installed in the CoSign appliance (Radius, authentication, Biometric authentication, etc.) contact ARX support prior to the upgrade procedure.

New features, improvements and fixes

CoSign Appliance

- Contact ARX if you intend to install CoSign to use the Worldwide Verifiable (WWV) certificates. Should you choose this option, you will need to sign an agreement and set up an account with ARX. The account will be limited by the maximum number of certificates that can be generated for your organization. The maximum number of available WWV certificates is presented in the CoSign console's settings under the *WWV certs* section.
- The problem that a CRL was not published properly is fixed.
- Problems with replications in High Availability/Load Balancing configuration were resolved.

CoSign Client

- There is a new method for deploying the CoSign client installation and ARX plug-ins to all relevant PCs inside the organization. For more information, refer to Appendix B of the CoSign manual.
- In environments that prompt for User Logon (such as Directory Independent environment), there is an option to perform a logoff operation using the option *Logoff* in the CoSign Control Panel.
- It is possible to define the list of reasons that can be used in OmniSign through the CoSign configuration utility. (It was not possible in version 3.47).

SAPI

- Digital signatures generated with CoSign client version 4.1 and above will include the signature date and time inside the PKCS#7 signature structure. In addition, the digital signature verification operation will relate to this date and time as a baseline for checking certificate expiration or revocation. This enhancement is also available when signing using ARX word add-in and OmniSign.
- Support for multiple graphical images for each user.

Word/Excel add-in

- It is possible to define the appearance of the graphical data of the newly created digital signature using the appearance style value (*Variable font size or Fixed font size*) in the CoSign configuration utility in the *Office* section.

  Prior to version 4.1, the appearance style was *Variable font size*, while in version 4.1 the default value is *Fixed font size*.

- It is possible to allow an automatic verification of digital signatures upon opening Word or Excel documents.
- This option can be set using the CoSign configuration utility. The default value is not automatically verified.

CoSign User Management Utility

- There is a new and improved user management utility for Directory Independent environments. This utility also enables administrators to view the current list of users in MS Active Directory and Novell NDS environment.
- The utility enables you to view global signature counters and user based signature counters. There is also an option to reset these counters.

Known problems/limitations

CoSign Server

- Restore operation will always generate the group *CoSign Signers* although the administrator might be using a different group name for CoSign users.
- It is not possible to enroll a WWV certificate for a user whose email address only contains blank spaces.

CoSign Client

- In some configurations, such as Directory Independent configuration, a *logoff* button appears in the CoSign Control panel. There are some rare scenarios where the user needs to manually refresh the CoSign Control panel to get the actual state (enabled/disabled) of the *logoff* button.

  The refresh operation can be done using the *Refresh* panel option in the menu bar of the CoSign control panel.
- The Graphical Signature management application might crash in some very rare cases while entering the graphical signature through ePad or ePadInk.

  If this occurs, restart the graphical signature management application and reenter your graphical image.
- The maximal amount of data that can be used for all graphical images for a user is 30K.
- The hyperlink cannot be activated when using Web Mail to view the SSCD enrollment email. Therefore, it is recommended to use a different email client for viewing the enrollment request email.

SAPI

- There might be a validation error when trying to validate digital signatures that were created using a client version older than 4.1. These signatures were either created using ARX Word add-in, *arfilesign* utility, or SAPI and do not include the signature time within the PKCS#7 signature structure.

  The validation error will occur if the signature operation was performed either within a period of one day in the start date or end date of the certificate validation period or within a day of the certificate revocation time.

  Upgrading to the new client is recommended for digital signature and verification purposes.
- JPEG based graphical signature images cannot be incorporated into TIF files.
- There are some TIFF formatted files that are configured to use the parameter *FillOrder = Lsb2Msb* that cannot be signed using a visible signature. In these types of files only a non-visible signature is supported.

Word/Excel add-in

- In Excel, a save request will be popped even though no changes were made to the Excel document. This is true for any add-in that is used by the Excel application.
- The CoSign menu entry appears also in MS Outlook when setting the value of *use Microsoft Word to edit e-mail messages*. In this case, do not activate the CoSign menu.
- In cases where Word/Excel were first used AFTER the CoSign client is installed, the CoSign menu entry in the menu bar of Excel or Word will remain after uninstalling the CoSign client.
- When choosing the setting for automatic verification on Excel documents, there might be an Excel crash when opening simultaneously several files (depending on the PC performance).
- Automatic verification is not supported when using Microsoft SharePoint document management product in conjunction with Word/Excel documents.
- There is a problem using content-based signatures in protected Word documents in Office 2000 and Office XP. This problem does not occur in Office 2003.

  The problem is related to information that cannot be accessed by ARX add-in when using protected documents in Office 2000 and Office-XP.
- In some cases the end user can be prompted with a message that the disk is full when trying to save a Word/Excel document. This error is caused by broken links that should be removed from the references list of the Word document's VB settings.
- Certificates that do not contain a CDP will have a failure in the certificate validation section in Word/Excel plug-in.
- If a graphical image of type JPEG or multicolor BMP is selected during digital signature operation using CoSign version 4.13, you cannot use an older version of CoSign client to view this document. The graphical image will not be displayed and may cause Word or Excel to crash.

  In such cases it is recommended to upgrade the CoSign client version to version 4.13.

PDF signatures

- There is a problem using graphical signatures that are based on a JPEG gray scale image format.
- The *Update Acrobat* option in the *Graphical Signature* application degrades the quality of a new monochrome graphical image that is loaded to Acrobat application.
- When setting to use vector mode in OmniSign or PDF documents, only monochrome graphical images should be used.

CoSign users management utility

- It is not possible to change the password of the built-in administrator when CoSign is installed in MS Active Directory or Novell NDS environments.
- It is not possible to add a user with a user ID containing non-ASCII characters.

Release Notes - Version 3.41

General Information

Release Date: February 21th, 2006

This version is **based on CoSign server version 3.1**.

In the following sections the intermediate CoSign versions 3.452, 3.47 and 3.48 are described.

The version includes a new signature method for Microsoft Word documents that is based on the document's entire content, or a specific section's content, in addition to the existing Entire File-based digital signature.

Section-based signatures enable several users to fill and sign different parts of the document without invalidating the digital signatures of other users.

For example, an employee may complete the employee section of a form and sign it. The manager, who receives the signed document, may fill in the manager's section and sign it without invalidating the employee's signatures. In the past, with File-based signing, changes made to the document after it was signed would invalidate any existing signatures on this document, making the above scenario impossible to accomplish.

In addition, this new functionality improves the support for signing Word documents within Document/Content Management systems.

This new functionality is described in detailed in the CoSign version 3.41 User Guide.

The new version also enables installing CoSign in Active Directory environments, where the administrator has limited permissions. The CoSign User Guide provides information on how to install CoSign in these types of environments.

This version also includes problem fixes, which will be described in the following text.

New features, improvements and fixes

General problems

- The problem with installing CoSign in Active Directory environment where the *Cert Publishers* group does not exist in the Users container was fixed. The new installation will alert users as to the problem and the administrator will be able to continue with the installation.

  Please refer to CoSign User Manual, Appendix A for more information.
- The Problem with manually installing CoSign ROOT Certificate in client machine was solved.

- The Problem with the unnecessary prompt for user to Logon was solved. One of the cases where the problem occurred was in Windows XP, when using the *ArFileSign* utility.

Configuration Utility

- When activating the configuration utility in end-user mode, the option of importing values from existing configuration files (*import configuration file*) did not function. This has been solved.
- The Problem when setting the value *of Prompt for sign method* in the *Appliances* section was solved.

ARX Word Plug-in

- The Problem whereby documents that include several dependent and empty digital signatures fields - generated using older CoSign clients (prior to version 3.31) - and are signed using CoSign client version 3.31, was solved.

OmniSign/SAPI

- PDF file names based on Unicode names are now supported.

Known problems/limitations

General problems

- When upgrading the CoSign client on Windows XP, the desktop icons change their locations.

ARX Word Plug-in

Currently, the following information will be signed when choosing the content-based digital signatures option: document text, header & footer text, remarks, text in tables, text in forms and the existence of Active-X Objects in the document and their geometry.

Other types of content, such as images, are not included in the digital signature scope

- In some cases, changing the zoom in the Word document affects the size of the objects in the document and thus invalidates the digital signature. If the Location & Size of Tables and objects in the *Scope Of Signature* tablet is deselected, changing the zoom will not affect the digital signature.
- If you are signing an entire Word document using either a file-based or a content-based signature, keep in mind that after the first signature is generated, it is not possible to add new digital signature fields to the document. Therefore, make sure to first create all the desired digital signature fields before you sign them. This may also be said regarding the placement of several digital signatures in a certain section.
- If the document includes a table with different-sized rows and columns, content based signature will fail to sign. To remedy this, please uncheck the *Location and Size of Objects and Tables* value in the Signature Settings → *Scope of Signature form*.

- When choosing the Adobe Distilling option by selecting the *Convert* command, digital signatures in the Word Document may become invalid.

  This occurs because Adobe uses a temporary Word file that is different from the original Word file, which invalidates the original digital signature.

  Also, there are problems activating the conversion operation using Adobe Acrobat 7. The problem is solved using Adobe Acrobat version 7.07.

- The locality type of the Microsoft Word installation may affect the generation of the digital signature. For example, the parameter alternative text that is one of the parameters of a Text Box inserts localized information into the digital signature. This will cause signature validation failure in machines with different locality settings.

SAPI

- The signing of content-based signatures and Excel files through SAPI is not supported.

CoSign Configuration Utility

- The Administrator's Group Name in the Admin / Appliance Installation section should not include a CN=Value. For example, write Administrators not CN=Administrators.

CoSign Version 3.452

General Information

This version includes a signature verification package called CoSign Verifier that is installed through a web interface. The package includes the following functionalities:

- Installation of an Office verifier capable of verifying Word and Excel digital signatures.
- Installation of an organizational ROOT certificate.
- Automatically setting Adobe 6 and 7 configuration parameters to enable signature verification without having the end user manually set any parameters.

The *CoSign Verifier* is deployed in ARX web site http://www.arx.com/support/downloads.php and may also be deployed in the customer's web site (all packages may be deployed except for the *AR word verifier.msi* and *AR SAPI verifier.msi* files).

It is possible for users without administrative rights to install the *ARX Verifier* on their own.

This version is currently in Beta stage and has not been released for general use.

In the following text we cover topics such as the *CoSign Verifier* installation and a list of limitations and known problems.

Setting installation parameters

The installation setup may include the following parameters:

- ROOT Certifier of organizations; and
- Setting up which components are installed

The ROOT certificate is set up as follows. Edit the textual file *variables.js* and set the URL of the location of the ROOT certificate as the value of the parameter: ROOT_CERT_LOCATION. Currently this parameter points to the ARX ROOT certificate.

In order to define which components to install, edit the *variables.js* and set the value of the parameter MASK_VALUE as the mask of the following parameters:

- Do not verify CRL - Value=1: If this flag is set, then the installation will automatically unset the value *of Require Certificate Revocation checking for validation* in Adobe Acrobat or Acrobat Reader verify signature preferences.
- Trust windows store –Value=2: If this flag is set, then the installation will automatically set the value of *Enable importing entities from the windows certificate store* in Adobe's Verify Signature preferences.
- Load Root Certificate - Value=4: If this flag is set, then the installation will automatically install the ROOT certificate that its URL is specified in the above ROOT_CERT_LOCATION url.

- Install Office package - Value=8: If this flag is set, then the installation will install the Office verification package that enables the client to verify Word or Excel documents signed using the CoSign client.
- Install Tiff package - Value=16: If this flag is set, then the installation will install the Tiff verification package that enables the client to verify Tiff files that were signed using the CoSign client.

For example: to install the Office package and Tiff package, a sum 8 + 16 = 24 should be calculated and set to MASK_VALUE = 24;

Known problems/limitations

- The *CoSign Verifier* cannot be installed in a machine that already has the CoSign Client installed.
- Due to problems when performing re-installation or upgrade, it is recommended to first uninstall existing *CoSign Verifier* versions, *close all Internet Explorer processes* and then reinstall the new version.
- When security settings are set to High in Internet Explorer, it is not possible to install the *CoSign Verifier*.

  Also, it is mandatory to enable installing Signed ActiveX by Internet Explorer Security Settings.
- It is recommended to maximize your Internet Explorer browser windows to assure a complete display of information.
- If Word or Excel is running in the background during the installation process the user needs to restart these applications for the CoSign Verifier plug-in to be available.

CoSign Version 3.47

General Information

This intermediate version offers the following enhancements to the CoSign client:

- Organizations that use OmniSign may now define in advance a set of reasons that can be selected by the end user.
- When opening a Word or Excel document when the AR office plug-in is installed in a Citrix environment a delay was apparent. This is no longer the case as overall performance has been improved.
- The toolbar of AR Office plug-in will not appear by default when editing an email using Outlook with the option: use *Microsoft Word to edit e-mail messages*.

  Prior to this version, end-users activated options in the toolbar and received error messages.

  Remark: The toolbar still appear when setting the value of send *this message format: Microsoft Outlook Rich Text* when using Microsoft Outlook 2000.

Setting the list of possible reasons for using OmniSign

In this version it is possible to define a list of possible reasons through the registry.

There are two possible registry locations:

- HKEY_CURRENT_USER\SOFTWARE\ARL\SAPI\OmniSign\BasicProfile\SigSettings\

  Reasons - In this case every user in the PC can define their own list.
- HKEY_LOCAL_MACHINE\SOFTWARE\ARL\SAPI\OmniSign\BasicProfile\SigSettings\Reasons - In this case all users will view the same reasons list.

  This information is relevant only if the entry of HKEY_*CURRENT_USER*\…*Reasons* does not exist.

In either of the above entries the following values can be defined: *reason_1, reason_2,…, reason_40*. Each value can contain a reason's text.

Please make sure the names of the values contain consecutive numbering or only part of the list will be displayed.

Remarks:

- If none of the above entries are defined, OmniSign will present an internal reasons list as done on former versions of CoSign.
- The reason that was used in the previous signature operation (either selected automatically or entered manually) is appended to the current list of reasons and marked as the default. When activating the Restore Defaults option, the last reason is reset.

Known problems/limitations

- The version number is not displayed in any of the *about* dialogs. The version number is displayed in the setup installation screen, and also can be viewed in the following DLLs' version attribute*: SAPIcrypt.dll, OmniSign.exe, arwaddin.dll.*
- The User/Admin *CoSign Configuration Utility* does not support the ability to define the list of reasons for OmniSign (as supported in other applications such as MS Word).
- The automatic hiding of the ARX Office toolbar when editing emails using outlook is not working properly if the user never activated Microsoft Word.

CoSign Version 3.48

General Information

This intermediate version offers the following enhancements/problem fixes for the CoSign client:

- Enhancements and problem fixes in ARX Microsoft Office add-in (Word and Excel).
- Problem fixes in SAPI relating to implementing digital signatures in PDF documents. These fixes also solve problems found in OmniSign.

SAPI/OmniSign

- An occasional problem found when using OmniSign to sign PDF documents generated by the CutePDF product. This problem was solved.
- A problem found when using OmniSign to sign PDF documents protected against printing. The problem was solved.

AR Office Add-in

- There were several problems related to signature operation with a Microsoft Word document based on templates. The template contains empty digital signatures (file-based or document content-based digital signatures).

  A list of problem found and resolved:

  Several pop-up messages were raised during signature operation or when saving the document, asking the user if they wanted to save content to the document template. This problem was solved.

  There were cases whereby an error was raised during signature operation. This problem was solved.

  Occasional Word crash when using CoSign client version 3.47. This problem was solved.

- It is possible to modify the text of an empty signature block. The default text is *CoSign Digital Signature*.

  For modifying the text, set the following string based registry entry to define a different empty signature block string:

  HKEY_LOCAL_MACHINE\SOFTWARE\ARL\Word\Params\sig_empty_label with the new String Value (i.e. *Please sign here*:).

Release Notes - Version 3.31

General Information

This version is **based on CoSign server version 3.1**.

The version includes several new enhancements. All enhancements are fully described in a new revision of the CoSign User Guide.

There is no new SAPI guide. All SAPI new functionality is described in the following release notes.

The four new major enhancements are:

- Graphical digital signature support for Excel documents: A new CoSign add-in for Excel enables end users to generate graphical digital signatures in Excel documents. The functionality of this add-in is similar to the functionality of CoSign add-in for Microsoft Word.
- OmniSign, a digital signature enabler for any application: OmniSign enables any application, including those without built-in digital signature support, to create digitally signed files such as a graphical signature.

  The solution is based on generating (distilling) a PDF file using an application's Print command. This will open OmniSign, allowing the user to locate the signature field anywhere on the document.

  OmniSign signs PDF documents without having to install Adobe Acrobat Professional or Acrobat Reader on the user's PC.
- Graphical digital signature support for InfoPath documents: Version 3.31 enables Microsoft InfoPath users to add graphical digital signatures to InfoPath documents.
- A new administrator and user configuration utility: Version 3.31 includes a new client configuration utility that replaces the functionality of activating *.adm* files in older versions. This utility can be activated in two modes: Administration Mode and User Mode.

  In the Administration Mode, the configuration utility enables administrators to configure client-based parameters for a group of users using a group policy mechanism.

  In the user mode, the utility enables a single user to configure his/her own client parameters.

  The *.adm* mechanism is no longer supported.

This version also includes problem fixes, which will be described in the following paragraph. The next paragraph will include known problems and limitations of this version.

New features, improvements and fixes

CoSign Client

- In the case that a *prompt for logon* or *prompt for sign* mode is used, the end-user is limited to 20 seconds for providing a password. Failing to provide a password in this period will automatically close the login window and cancel the CoSign login operation.
- A bug that caused hidden login windows to pop up unexpectedly has been fixed. The problem caused services to hang.
- The fix relates to the above problem, which limits the time a login window can remain open.
- A new uninstall CoSign utility is included as part of the CoSign client installation.

SAPI

- A limitation for not using the characters "(" and ")" as part of the field name that contains the digital signature was fixed.
- Three new functions were added: SAPISignatureFieldSignEX, SAPIBufferSignEx, and SAPIBufferSignEndEx. These functions are similar to the functions: SAPISignatureFieldSign, SAPIBufferSign and SAPIBufferSignEnd, respectively, but requires an additional input parameter. The new parameter is the end-user password to be sent to the CoSign Server when *Prompt For Sign* is required.
- Some specially formatted PDF files could not be signed correctly. The PDF signature mechanisms associated with those files are more robust.
- It is possible to sign encrypted PDF files as long as the permission bits allow the user to add a digital signature to the document.
- The SAPI also includes a new API for filling PDF forms. For more information regarding this functionality please contact ARX.

ARFileSign utility

- The utility enables passing a parameter called *–pfs* <password>. This parameter is required when the *prompt for sign* mode is required by the CoSign server.

Known problems/limitations

General problems

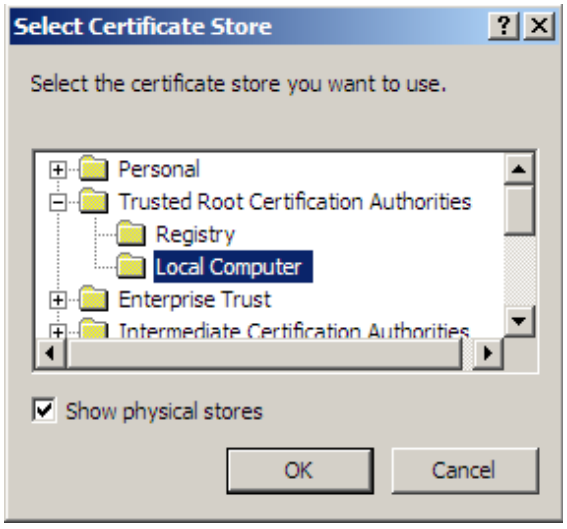
- The following limitation is relevant to CoSign Server installation when using this version or previous versions.

  When installing CoSign to an Active Directory environment please note that if the *Cert Publishers* group doesn't exist in the Users container, the installation will fail.

- In Directory Independent environment, the CRL is refreshed only once a year. By restarting the CoSign service, the new and updated CRL will be generated.
- In any environment where the user needs to manually add the CoSign ROOT certificate to the trusted ROOT CA list (such as with Directory Independent environment), the certificate should be imported to the *Trusted Root Certification Authorities* store.

  When the user activates the *Certificate Import Wizard*, the user should select the option *Place all certificates in the following store* and then click *Browse*. Then, the *Select Certificate Store* window is displayed. The *show physical store* option should be checked

  Finally the user should select the *Trusted Root Certification Authorities* → *Local Computer* item in the list (as shows in the following illustration):



- Any environment that prompts for CoSign user logon, for example, Directory Independent, there are some cases in Windows XP and Windows 2003 where the user will be prompted for logon even though there is no relevant signature operation.

  Typically this includes signature verification operations; or activating the *ArFileSign option* while already providing a user name and password as part of the command line parameters.

SAPI

- Signing Excel files through SAPI is not supported.

Configuration Utility

- The CoSign configuration utility cannot update empty group policies
- When activating the configuration utility in end-user mode, the option of importing values from existing configuration files (*import configuration file*) does not function.
- If a problem occurs while setting the value *Prompt for sign* method in the *Appliances* section please contact ARX to set this value correctly.

ARX Word Plug-in

- Documents that include several dependent and empty digital signatures fields, were generated using older CoSign clients (prior to version 3.31), and are signed using CoSign client version 3.31, will fail to properly validate. By activating the *Clear All Signatures* option in the toolbar using CoSign client version 3.31, the problem is rectified.

ARX Excel Plug-in

- When including cell properties as part of the digital signature scope, not all the properties are included. Please refer to the CoSign user guide for the exact list of properties included in the digital signature operation.
- The Excel plug-in supports only one selection area when the end-user specifies to use Selection as the scope of the digital signature.

  In the case that the user selected more than one selection area prior to the graphical signature operation, only the last selection will be used as the digital signature scope.
- Only cells that have values will be signed. For example, if the scope includes empty cells that have colors, changing the color of the empty cell will not invalidate the digital signature.
- Activating the signature operation or activating the *View Signatures* option in the tool-bar will disable all recent operations in the Undo list.
- If the *Cell Properties* are included in the signature content, the signature will be affected by the workstation settings. For example, the parameter *font style* string will be included inside the signature but since it is dependent on the locality of the MS Office installation, this will cause signature validation failure.

OmniSign

- PDF files names that are based on Unicode name are not supported.

ARX Acrobat/PDF Add-in

- If the CoSign client was installed prior to the installation of Acrobat reader or Adobe Acrobat, the CoSign client should be re-installed in order to support the newly installed Acrobat Reader or Adobe Acrobat. This limitation is relevant also to former versions of the CoSign client.

Troubleshooting

ARX Acrobat/PDF Add-in

- Activating right-click option for PDF files will present an option called *Sign with OmniSign*. This option activates the OmniSign application that enables the user to add a digital signature to the selected PDF document.

  The installation of Adobe Acrobat 7 removes this option from the right-click menu.

After re-installing the CoSign client, the option will be presented again in the right-click menu.

Word/Excel Add-inn

If the ARX CoSign Signature toolbar does not appear in the screen, activate the option *Disabled Items* ...in the *help\about Microsoft Word* or *help\about Microsoft Excel* window. If the *digital signatures toolbar* is listed in this window, you need to enable it. This option is relevant for Office-XP and Office-2003.

Release Notes - Version 3.23

General Information

This version is **based on CoSign server version 3.1**.

The version includes a new component called SAPI (Signature Application Programming Interface). This component enables integrators to interface CoSign through an API and perform digital signature operations upon buffers or files such as PDF, TIFF or Word.

The SAPI can also be accessed from an application written in C# or Visual Basic using a COM interface.

SAPI is described in detailed in the CoSign SAPI Programmer's Guide.

This version also includes enhancements and problem fixes, which will be described in the following paragraphs.

These release notes also include the modifications/enhancements for **version 3.23.1 and version 3.23.2.**

New features, improvements and fixes

The version includes the following new functionality:

General

- When using ARX Word add-in or ARX SAPI for signature operation, the signature time is taken from the CoSign appliance, while the time zone is taken from the end user's machine.

  Take note that when using Adobe Acrobat the signature time is calculated using Adobe Acrobat.

  Other applications that use ARX CAPI provider or ARX PKCS#11 provider

  (i.e. Outlook) are responsible for the calculation of the signature time.

Adobe Acrobat

- CoSign support for *Adobe Acrobat 7* and *Adobe Reader 7* similar to the support for *Adobe Acrobat 6* and *Adobe reader 6*, respectively.

  When using Adobe Acrobat 7 products, the Adobe configuration and preferences menu options may differ from those available on Adobe Acrobat 6 products (as described in the CoSign User Manual). However, the functionality of the digital signature operation and the digital signature verification are quite similar

- A problem was fixed relating to graphical images with complex graphics not displaying as part of the digital signature. In Version 3.31 the graphical image is displayed properly.
- A new ADM parameter was defined called *Graphic Image*, which has two values: *BMP* or *Line Vectors*. This parameter affects only the *AR PDF Signature setup for Acrobat 6 and 7* utility.

The *ARX PDF Signature setup for Acrobat 6 and 7* utility generates/updates a digital signature appearance. By setting the Graphic Image parameter it will direct the utility to select the format that the graphical image will be saved as, either as BMP or as line vectors.

ARX Word add-in

The CoSign client CD includes a verification-only installation that enables an end-user to verify documents signed by the ARX Word add-in.

The installation is located in the directory *WordVerifier* of the CoSign CD and is self-extracting.

- An improved graphical image when downscaling the graphical signature field.
- A new option in the *Configure Signature Defaults* dialog box. Called *Restore Defaults*. If the user presses the button, all the signature parameters are taken from the defaults as defined using the *ARX Word Add-In* ADM screens.
- A new option in the *ARX Word Add-In* ADM called *Disallow Local User Settings*. When this option is set, users will not be able to define their own setting. Settings will always be taken from ADM settings.
- A problem was fixed regarding using ARX Word Add-In within a Citrix session. The displayed signature time was the server time and not the client time.

  This problem requires additional settings in the Citrix Server. For more information, please contact ARX support.
- A problem was fixed regarding time presentation in relation to GMT. In some cases, the time was presented as: "14:00 - -2" instead of "14:00 –2".
- A problem was fixed regarding proper display of signature time in cases where the end user machine was using the daylight savings setting.

Directory Independent User Management Utility

- The following features were changed in the menu-bar:
- Admin Menu: *StartSyncCoSign* and *EndSyncCoSign* options were removed (They were not documented).

  User Menu (Was changed to Current User): Info option was removed.
- The *Update User* option was temporarily disabled. The option will be enabled in CoSign version 3.5.
- The Rights field in the Insert User form was modified and now includes the following options: *Appliance Admin and User Admin*.

  When defining a new user, the user is automatically defined as a regular user.
- It is not possible to use this utility in Active Directory environment or Novell NDS environment. Only Directory Independent environment is supported.

Batch Utilities

- The batch utilities *ARTiffBatchSign* and *ARPDFCmd* no longer exist. The utility *arfilesign* utility can be used to sign PDF files, TIFF files and Word documents.

  Please see following section describing the *arfilesign* utility.

Client Installation

- The Tiff module was removed from the installation. The ability to sign Tiff files is now part of the CoSign basic client installation.
- When the client is installed in a Win2003 environment, a Windows popup appears. This window appears whenever an installation program is named *setup.exe*.

CoSign Admin Client

- A problem was fixed when trying to override the default values of CDP or AIA. These values appear in the CA setup window during the CoSign installation. The end user received a message indicating that some characters are invalid.

  In CoSign Admin client version 3.23 the problem is fixed.

  In the case of Active Directory, the end user will get a warning that these new values cannot be updated to the directory. Ignore this warning and continue the installation.

Signing an Adobe/Word/Tiff Document Using a Command-Line Utility - arfilesign

As part of CoSign Client version 3.23, the installation includes the arfilesign.exe *command-line utility*. The utility can sign the following file types: Adobe PDF, MS Word and Tiff files.

This utility signs a document in automatic batch processing, without requiring you to open MS-Word or Adobe Acrobat and sign the documents manually. The utility accepts a file name and a set of options, and performs a signature operation on the file.

Signing multiple files is possible by providing a wildcard pattern rather than a single file name.

> **Note**: *The signatures performed by the arfilesign utility upon a PDF file are compatible with Adobe 6 and Adobe 7 (Acrobat and Reader). You can therefore validate the signatures using Adobe 6/7 (Acrobat and Reader).*
>
> **Note**: *If you need to sign a PDF file, it is not necessary to have any Adobe product installed on the machine running the arfilesign.exe utility.*
>
> *If you want to sign a Word file, you need to have MS-Word installed in the machine running the arfilesign.exe utility*

> **Note**: *This utility can be used for other operations such as creating a signature field or performing verification.*
>
> **Note**: *Multiple graphical signatures are not support in Tiff files. Only the first signature in Tiff file is Visible and the rest should be defined as Non Visible.*
>
> **Note**: *For signing Word files you need to contact ARX for additional directions.*

Executing arfilesign.exe

The utility is executed as follows:

arfilesign.exe –fn <file-name> [options]

Where file-name is the file used for performing the operation such as signing, it is possible to provide a file mask and have the *afilersign* program sign several files.

The arfilesign options include:

- **[-op <operation number>]** – One of the following numbers needs to be supplied for directing the required operation.

  Create field

  Sign field (creates a field if needed)

  Verify field.

  Clear field.

  Remove field.

  List fields.

  The default operation is: 2
- **[-ft <file type>]** - Indicate one of the following file types: MS Word (.doc), Adobe Acrobat (.pdf), Tiff file (.tif). The default value is set according to the file name extension
- **[-v <Visible/Invisible>]** - Visible or Invisible signature (default: Visible). In the case of a Tiff file please specify whether the signature is Visible or Non Visible. In a Tiff file only the first digital signature may be Visible.
- **[-p <page number>]** – The page number where the signature field will be created (default: 1). If –1 is provided, the signature will be put on the last page. This option is not available for Tiff files.
- **[-x <x coordinate>]** - Signature field's left x coordinate (default: 100). This option is not available for Tiff files.
- **[-y <y coordinate>]** - Signature field's bottom y coordinate (default: 100). This option is not available for Tiff files.
- **[-w <width>]** - Width of the signature field (default: 200). This option is not available for Tiff files.

- **[-h <height>]** - Height of the signature field (default: 100). This option is not available for Tiff files.
- **[-sff <flags value>]** – Reserved - do not use this flag.
- **[-r <reason text>]** - Reason for signing, or Reason label when creating fields.
- **[-sfi <field index>]** - Signature field index. If -sfi is not provided, the first field that matches the operation is used. This parameter is not available for Tiff files.
- **[-sfn < field name>]** - Signature field name (alternative to -sfi). If -sfn is not provided, the first field that matches the operation is used. This parameter is not available for Tiff files.
- **[-ser <certificate serial number>]** - Certificate serial number. The program will use this certificate and its relevant Private Key for the digital signature operation.
- **[-d <dependency mode>]** - Dependent or Independent Signature (default: Independent). This parameter must be defined as Dependent in the case of a Tiff file.
- **[-am <appearance mask>]** - (default: Image,Name,Time). Combine any of the following: Image,Name,Time,Reason separated with commas or use the value: None. This parameter is not available for Tiff files.
- **[-lm <labels mask>]** - (defualt: None). Combine any of the following: Name,Time,Reason separated with commas or use the value: None. This value will define whether a label will be presented in the digital signature
- **[-tf <time format>]** - (default: "h:mm:ss"). Time format of the displayed signature.

  Possible values are:

  hh:mm:ss

  hh:mm am/pm

  hh:mm

- **[-df <date format>]** - (default: "MMM d yyyy"). Date format of displayed signature.

  Possible values are:

  YYYY.MM.DD

  DD MMM YYYY

  MMM DD YYYY

  DD MMM YYYY

- **[-to < time offset>]** - Show signature time offset: GMT or None (default: None)
- **[-c]** - Certificate chain flags. If this parameter is set, the digital signature will contain all certificates until the ROOT certificate inclusive.
- **[-cfg]** - For further information of using this parameter, please refer to the ARX SAPI manual or contact ARX.
- **[-flg]** - For further information of using this parameter, please refer to the ARX SAPI manual or contact ARX.

Known problems/limitations

Client problems/limitations

- When the CoSign client is loaded by a Windows Service, there are rare cases where a user logon window is opened by the service. Since the window is not visible by the end user, the service may freeze.
- Please contact ARX support for obtaining information how to prevent the service from activating the user prompt.
- For signing Word files through SAPI or the *arfilesign* utility please contact ARX. This functionality is not supported by default.

ARX Word add-in

- When trying to perform a digital signature or verify a digital signature upon a protected document in Word XP or Word 2003 you need to set the option *Tools → Macro → Security to High (default), Medium or Low*.

  If you set the value to *Very High* you will not be able to sign.

  If you set the value to *High*, you have to sign the Macros of the Word document. It is possible to use a CoSign certificate for the signature operation of the Macros.
- Cannot insert a signed Word document into PowerPoint or Excel documents. The digital signature cannot be verified since the document is modified upon the insertion operation.
- Cannot sign Word documents or verify Word documents in a Microsoft RMS (Right Management System) environment.
- When the Word document has a single signature and is verified by Word XP/2003 without a plug-in, the graphical image of the digital signature may look disrupted.

ARX Adobe add-in

- If the document is certified and the user tries to verify the signature using ARX Adobe add-in, Adobe Acrobat will crash.
- If the end user will use the built-in Adobe Acrobat mechanism for verification, the document will be properly verified.
- A digital signature generated using Adobe Acrobat 6 with the Windows signature mechanism, cannot be verified using the ARX plug-in when operated as the verifying plug-in in Adobe Acrobat 6. Use Windows verification mechanism to verify such signatures.
- When using the ARX plug-in in adobe 5 and using verification mode that compares words or pages, a problem may arise when opening the properties window. The window opens, but contains no information.
- Cannot sign an encrypted PDF file through *arfilesign* utility or the Signature API (SAPI).

Tiff signatures using SAPI

- Cannot sign the same field twice. If a signed field needs to be re-signed, please clear it first, and then sign it.
- When "prompt for sign" is set and the digital signature operation is performed upon a Tiff file, and the end-user fails to enter the proper password - the digital signature will not be created but the graphical image will be displayed in the first page.SAPI general errors/limitations
- Do not use the characters "(" and ")" as part of a digital signature field.

Troubleshooting

ARX Word add-in

- If the CoSign client 2.6 was installed on the client machine and needs to be removed, uninstalling the client will not remove the digital signature toolbar.

  The toolbar may be removed as follows:

  Go to the Tools → Templates and add ins …option. The Templates and Add- ins window is presented.

  Select the Organizer… option.

  Select the Toolbar tablet.

  Delete the Digital Signatures entry in the right-hand list.

Application Notes

The following list includes problems that occurred with applications such as Adobe Acrobat 7 that interface the CoSign appliance using ARX plug-ins.

- Adobe Acrobat 7 CRL problem: Adobe Acrobat 7 cannot verify a signature when the end user requires to validate CRL, which is located using the LDAP protocol (using the CDP field in the end user's certificate).

  In such cases, the user will warned the certificate is invalid - even though the certificate is not included in the CRL and the CRL is accessible.

Release Notes - Version 3.23.1

Modifications/Enhancements

The version includes the following enhancements:

- ARX Word Add-In - Compatibility problem with signatures created in CoSign version 3.1.

  Signatures created using Word Add-In version 3.1 were shown with different geometry in version 3.23. Also, signatures created with version 3.23 where shown with different geometry in version 3.1.

  In Version 3.23.1 this compatibility problem is fixed.

- ARX Word Add-In - Added support for Word signatures upon documents that are managed through ODMA (Open Document Management API). The new functionality support activities such as: Digital Signature operation, Signature Verification, Signature properties, while opening a Word Document within a document management third party product.

Release Notes - Version 3.23.2

Modifications/Enhancements

The version includes the following enhancement:

- ARX Word Add-In - A module exception/crash was fixed when performing a signature operation on a document that was generated using a .dot file by performing a save as operation.

Release Notes - Version 3.11

General Information

This version is **based on CoSign server version 3.1**.

The version has the following fixes:

- ARX Word Add-in supports protected documents.

  On former versions the user received a message that protected Word documents cannot be signed.

- An improvement on the presentation of user's graphical signature in the case that the signature fields are scaled down.

  In former versions, the downscaling of the signature field damaged the display of the graphical image.

- A correct error message when using the artifbatchsign application for verifying Tiff signatur

Release notes - Version 3.1

General Information

CoSign version 3.1 is a major version.

The version includes the following new functionalities:

- High Availability: Enables organizations to set up several CoSign appliances to enable the following:

  Redundancy - In case of a failure of one of the CoSign appliances, one of the other CoSign appliances will take over and perform digital signature operations.

  Load Balancing - balancing workloads between multiple CoSign's, allowing organizations to confidently conduct large transaction volumes simultaneously.

- Directory Independent Environment: CoSign can be installed in a directory independent environment in which users are not managed in Active Directory or NDS.

  In such cases, users will be managed inside CoSign using one of the following methods:

  Users managed with an API provided with CoSign allowing user creation, deletion and password change.

  Users managed with CoSign *Directory Independent User Management Utility* allowing user creation, deletion and password change.

  The API can be used for developing a proprietary user synchronization program for automatic user synchronization of CoSign and the customer's users database.

- New client installation: Flexibility in the client and plug-ins installation have been incorporated in this version. This enables a much smoother and scalable installation of CoSign client components. For example: automatic client installation using AD standard tools.
- Improved support for Adobe Acrobat 6: CoSign client now supports graphical digital signatures in Adobe Acrobat without requiring a plug-in. This is achieved by relying on the built-in support for graphical digital signatures of Adobe Acrobat 6 using the "Windows Certificate Security" signing method.
- Improvements in the ARX Word Add-in module: Numerous improvements were introduced in the new ARX Word add-in.

  For example, CoSign signatures can be configured to be Word XP/2003 compliant and do not require the Word plug-in for validating the signature.

- TIFF signatures: For signed TIFF files, a new page is created at the beginning of the TIFF document. This page specifies the signer name and the signature date.

- Subordinate CA support: CoSign can be configured to be used in an environment that already includes a CA, and act as a Subordinate CA.
- Multilingual Support: Enable the use of Unicode-based characters in items such as the user name which appears in the user certificate. Multi lingual support enables CoSign to generate certificates that include localized characters.

In depth descriptions of these new functionalities as well as other CoSign features can be found in CoSign 3.1 User Manual.

To perform an upgrade of CoSign/SignLet please refer to the CoSign User Manual chapter 5 – *Managing the CoSign Appliance- Uploading Firmware update*.

To perform an upgrade of CoSign Client and its components, please refer to CoSign User Manual chapter 4 – *Deploying the CoSign Client*.

The following is a list of fixes from earlier versions and a list of known problems/limitations.

Fixes for problems

ARX Adobe Acrobat add-in

- The support for Adobe Acrobat 6 does not include add-in and is based on

  Adobe Acrobat 6 "Windows Certificate Security" built-in signing method. Some of the problems that were raised in previous versions are not relevant for

  Adobe Acrobat 6.
- In former versions, the fixed Reasons list could not be configured by the organization. In CoSign version 3.1, the Administrative Template for Adobe 5 can be used for setting up the Reasons list, thus enabling the organization to configure its own reasons for digital signature generation. This issue is not relevant when using Adobe Acrobat 6 without the ARX PDF add-in.

ARX Word add-in

- The activation of the digital signature operation is based on COM add-in technology. In former versions it was based on an MS Word macro, which had the following problems:

  Interference with other macros.

  The end user had to acknowledge the macro activation upon first usage.

  The macro had to be signed by an AR key. Due to Microsoft limitation, the macro had to be re-signed every year.
- It is possible to send signed Word documents using OutLook without damaging the digital signature.

- It is possible to enter long reasons (more than 64 characters). In previous versions it was limited.

CoSign Appliance Installation

- It is possible to install a CoSign Appliance in the non-English Active Directory environment, while in previous versions; there was an error during the installation procedure.

Client Installation

- The new client installation is based on MSI technology and many former installation problems were fixed. One of the problems was an improper uninstall procedure, which failed to remove all components in uninstall.

  Also, this version of CoSign provides enhanced support for Active Directory based automatic client installation. Please refer to CoSign User Manual for more information.
- The new client installation removes the old AR Word macro.

Known problems/limitations

General

- CoSign version 3.1 includes multilingual support, however, there are several points not supported in this release:

CoSign MMC Snap-In

- Cannot manually specify AIA or CDP based on Unicode characters. If the default is chosen then Unicode based AIA or CDP is supported.
- CA name cannot be specified in Unicode characters.

Server Operation

- If the common name of the user in the CoSign certificate includes Unicode characters, the name will not be displayed correctly in the Event Log in the case of digital signature or administrative operation.

Directory Independent User Management

- It is impossible to view the users' names in the users' list. Though it is possible to insert a new user with a name that contains Unicode characters.
- The CoSign Installation rejects using ascii but accepts non-English characters for the CoSign CA name.

ARX Word add-in

- Digital signatures created using CoSign version 2.5 or below are not supported.
- The default digital signature does not cover document summery information (which means that if the document summery information is modified, the digital signature can still correctly validated). This default is selected because some Microsoft applications such as MS Outlook modify the summery information, thus invalidating the digital signature.

  It is possible to include the summary information in the digital signature using the ARX Word Signatures administrative template (please refer to CoSign User Manual).
- If the "Create word compatible signatures" is set and the user tries to print the document, the visual digital signature will not be printed. Visual digital signatures can appear only in cases when the "Create word compatible signatures" is not selected.
- If both the "Create word compatible signatures" and the "Prompt for Sign" parameter are set, the user will be prompted twice for his/her password during digital signature operation.

ARX Adobe add-in

- If you open a certified (not signed) document with Adobe Acrobat 6, and the ARX PDF plug-in is configured as the plug-in that is used for verification, and the "verify signatures when the document is opened" option is set, the program crashes.
- If the system parameter "Prompt for Sign" is used when signing in Adobe Acrobat 6, the "User/Password" window will be presented three times.

Directory Independent Environment

- The following parameters need to be configured in the client station using the CoSign Client Administrative Templates (either locally or through Active Directory Group Policy): CoSign IP Address, "Prompt for Login" value and "Prompt for Sign" value.

  If these parameters are not properly set, the user will fail to connect to the CoSign appliance.
- It is possible to delete the admin user using the Directory Independent User Management utility. By doing so, it will not be possible to manage users anymore (adding users, deleting users, and so on)

Release Notes - Version 2.6

General Information

This version is **based on CoSign version 2.5** and a modified ARX Word add-in.

The following release notes will include information related to the new ARX Word add-in.

The new ARX Word add-in supports the following functionality:

- Support of multiple graphical digital signatures. The graphical digital signatures can be placed in any location in the Word document.
- There are two types of relationships between the graphical digital signatures of the document:

  Dependant digital signatures - Any modifications due to re-signing or clearing of previous digital signatures will invalidate newer digital signatures. This feature is very useful for typical workflow procedures that are based on MS-Word documents.

  The end user is able to see, at any time, all the previous dependent digital signatures and analyze them.

  Independent digital signatures - Modifications to a digital signature or re-signing a digital signature does not influence other digital signatures in the document.
- The visual representation of a graphical digital signature was greatly enhanced to include other information such as: the reason of the digital signature operation, name of signer, signing date and time. It is possible to define the requested display format of the date and time.
- The geometry (width, height) of the graphical digital signature can be controlled by the document designer. This functionality enables flexible and adapted usage of digital signatures in the organization documents.

Release Notes - Version 2.5

General Information

This major version includes the following improvements:

- General User Management Support (Push Mode): Up to CoSign version 2.1. CoSign used all User Management information either from Microsoft Active Directory or Novell NDS directory.

  Version 2.5 enables integrators and customers who have other types of user management systems to use CoSign.

  The integrator needs to notify CoSignusing an API to register every new user or removal of an existing user. CoSign will generate a certificate for the new user or revoke the certificate of an existing user and remove the user from the CoSign.

- Improvements to CoSign's Adobe Add-in: Adobe Acrobat is one of the leading document handling applications that uses digital signatures.

  Many improvements were added to the CoSign's Adobe add-in:

  Support for Adobe Acrobat version 6.

  Reason and date fields can be added to the signature appearance on both to the graphical representation and the digital signature details window.

  It is possible to define the format of the displayed date.

  The end user can configure the Adobe add-in not to check CRLs during signature operation. This can reduce the time of signature creation.

  It is possible to set up the last digital signature to be invalid in the case that the document is modified.

> **Note**: Normally, in a PDF document, the digital signature is bound to a dedicated version of the document. This means that if the document is modified a new version is created and the last digital signature is still valid.

Set the following values in the registry in the location:

HKEY_LOCAL_MACHINE\SOFTWARE\ARL\adobe

VerificationMode	= 0x02	- the above functionality is enabled
VerificationFlags	= 0x4 or 0x8	- 0x4 comparing pages

0x8 comparing words.

It is possible to extend the functionality of the digital signature menu and the digital signature's properties of every digital signature in the document.

The dialog/menu to show the version of the document that relates to the digital signature and to compare the differences between the current document and the version of the document that relates to the digital signature.

Set the following values in the registry in the location:

HKEY_LOCAL_MACHINE\SOFTWARE\ARL\adobe

SigVersions	= 0x01	- To open the comparison report or the signed version in a new Adobe instance.
SigVersions	= 0x100	- To open the comparison report or the signed version in the same Adobe instance.

- Command-Line/Batch Mode PDF signature: CoSign enables organizations to use a command-line based script to sign existing PDF documents. The command-line based program will get definitions from a configuration file regarding location of the graphical signature, certificate to user and other parameters to produce automatically a signed PDF files. It is also possible to sign automatically on several files during the execution of the batch signature program.
- Tiff file signatures: CoSign enables the users to sign TIFF files, which in many cases represent a scanned document.

  A command line utility enables to perform the signature, where the signature is put on a special signature TAG.

  Also, a special verification utility enables the end user to validate the digital signature.
- Improvements for CoSign support for Novell NDS environment.

Known problems/limitations

ARX Adobe Acrobat add-in

- In Adobe Acrobat 5, resizing a signature object might change the signature appearance in a way it won't fit best the new rectangle dimensions.
- When working in "prompt for logon" mode, making any changes in the document while the logon dialog box is open, can lead to unexpected results.

New Compare Adobe Acrobat Versions feature

- When working with Adobe Acrobat 5 it is recommended to set the "compare pages" on, since the "compare words" feature is not reliable in this Adobe Acrobat version.

- Working with Adobe Acrobat 5 with a file that was signed by Adobe Acrobat 6 and with "compare pages" set to On, can cause to some signatures to be referred as invalid because of different rendering methods in the two Adobe Acrobat versions.
- Working with Adobe Acrobat 6 and verifying a signature that was created by Acrobat 5 might fail, because of the differences between the 2 versions signature appearance.
- The special buttons in the properties dialog box (view signed version and compare versions) will not work for the following configuration:

  The special buttons open the new document or report in a new Adobe instance.

  You have more than one Adobe program is installed on your machine.

  The default Adobe program configured in the registry is different than the one you are running (e.g. you are running Adobe Acrobat 5 while in the registry it is configured to Adobe Acrobat 6)

Validating Last signature in the document

- Working with Adobe Acrobat 5 with more than one document opened in cascade mode, and verifying the last signature or pressing the special buttons in the properties dialog box (view signed version and compare versions) might change the way the open documents are ordered within the Adobe Acrobat window.

ARX Word add-in

- The ARX Word add-in uses signed macros. In office XP, if the user is working with security level set to high – which is the default setting – and is not connected to the internet, opening Word might take time due to Office's automatic macro signing certificate verification feature.
- Scrolling a signed Word document with a verified graphical signature, scrolls the whole document content but leaves the verified symbol (V or X) and the signature object until the mouse button is released. When the scrolling operation is done, the signature object and the verification symbol are located in the right place.
- Opening a signed word attachment in Outlook, when Outlook is configured to work with Word as the default editor, applies some changes to the original document and therefore the verification fails.

Install/restore using MMC Cosign Snap-IN

- When restoring a Cosign database, pressing the Cancel button on the progress bar window before the backup file was fully transferred to the server, will terminate the restore operation, but will also prompt CoSign to wait for the rest of the file; which will never be received. Before starting a new restore or install operation CoSign must be manually restored to factory settings via its console.

- If the first backup MiniKey is taken out and the second is entered too fast, the CoSign might not identify the insertion of the new MiniKey, and will keep asking for its insertion. In this case you should take out the second backup MiniKey and insert it again.

CoSign Console

- Some time after starting the restore to factory settings process a message saying "restoring factory settings done." is displayed on the console.
- Actually, this process is done only after the CoSign is restarted. You should expect the messages "Please wait." And "Cosign is now starting please wait", before getting the main menu. This will indicate that the process has ended.
- In some circumstances setting static IP address fails. When this problem occurs, choose the set DHCP option, restart CoSign and then set the static IP again.

Administrative utilities

- Registering a user's new graphical signature image to the CoSign, requires all the signing applications that use graphical signature representation to be restarted so they'll be able to work with the new or updated image.

Release Notes - Version 2.1

Known problems

Installation

- If a message saying CoSign is not in factory settings mode pops up while installing and CoSign is not installed already, it usually means CoSign did not complete the last installation attempt properly (for example, when asking for one of the MiniKeys, it was shut down or turned off), see the console section in the user guide for checking the CoSign's current install status. In order to start another installation process, please first return CoSign to factory settings.

Network

- When changing the default gateway to NULL (0.0.0.0), an error message is displayed on the console (error number 47). In fact the change was saved and the CoSign will work with no default gateway.
- Changing the IP of a CoSign in factory settings requires restarting of the CoSign before starting an installation process (applies to Active Directory environment only), or the installation will fail in joining the domain.

CoSign Admin Snap-in

- The task of downloading any of the logs from the CoSign requires choosing a file name for storing the downloaded data. If the file that was chosen by the administrator cannot be opened for writing (it is either a read only file, or is currently being used by another application), the operation will fail, **but** no error message will be displayed.

ARX MS Word Add-In (Graphical Signature)

- When signing an already signed Word document, the last signature is deleted, and then the new one is added. If a user signs a signed document and has more than one certificate, the old certificate will be removed and a dialog with all his certificates will be displayed, so he can choose the certificate he wants to sign with. If the user presses the cancel button, the signing operation will terminate and the new signature will not be added to the file, but still the old signature will be gone.
- There might be some cases (usually when verifying a signature) that a message saying "Automation error invalid callee" will occur. This message is a harmless warning and should be ignored.

Other

- If new users were added to the directory, but they cannot see their certificates in the CoSign, and in the CoSign debug log, you find error messages such as "CertRequest->submit failed, hr=8007005", it might be due to problems accessing the internal CA. Please restart CoSign and choose "sync with the directory" task from the CoSign admin snap-in.
- If you enrolled a new certificate from an external CA and the certificate is for a signing key, as oppose to exchange key, you might have problems when signing with this key. Please contact AR technical support for getting the latest patch of the CoSign client that solves this problem.

Limitations

Installation

- Installing the CoSign client on Win98 platform requires prerequisites, and some special installation techniques. Before installing the CoSign client on any Win98 variant, please contact AR technical support for assistance.
- Currently there is no automatic method for uninstalling a CoSign server from the directory (Active Directory or NDS), in order to manually remove the CoSign from the directory (and thus stop seeing it in the CoSign admin snap-in), please do the following:

  In Active Directory, remove the computer object from the container it is located in (e.g.

  Computers container)

  In NDS delete the CoSign object from the NetSVC class

Note that both in NDS and in Active Directory the name of the object is the CoSign computer name and it is written on the CoSign box (for example CSN00001 or SIG00010).

- We do not support more than one active CoSign appliancein a single Environment. If there is such a requirement please contact ARX technical support for assistance.
- Uninstalling the CoSign client does not remove the addin's files (for Office and Adobe applications). Leaving these files will not harm to the system, but if you would like to remove them, please contact ARX technical support for assistance.
- Installing the ePad (used for capturing graphical signatures) and working with it requires administrative rights on the machine it is installed on.
- Add-in's are installed under Adobe and Office applications, only if these products already exist. In case any of these applications is installed after the CoSign client installation, run the setup batch file under the addin's folder, in the CoSign installation CD, again.
- If the CoSign installation process is initiated by 2 different snap-ins simultaneously, the result is unpredictable.

Network

- Changing the IP address of an installed CoSign requires a restart to the CoSign, so its new IP will be published in the directory. In cases where the CoSign IP is defined in the client's registry, an update to the registry is required.

CoSign Admin Snap-in

- When the CoSign admin snap-in is started, or when it is displayed in the "add standalone snap-in" dialog, it is trying to connect the CoSign server. If a server was installed, but is not connected, it might take the operation some more time to complete (approx. 40 seconds for each CoSign that is not connected).

  Make sure you have only one entry in the CoSign appliances folder in the CoSign snap-in (see the note related to manually uninstalling a CoSign server in installation sub section), and that this server is operational and can be reached via the network.
- The admin snap-in does not refresh its display automatically. If there was any change in CoSign's status (it was stopped, reinstalled etc.) a manual refresh is required (by either pressing the refresh button or pressing the F5 key).

Users directory

- The CoSign do not support user names that are represented in Unicode form.
- The users synchronization between the CoSign and the NDS directory is time based, which means CoSign always asks for changes with a timestamp greater than the last update timestamp (LastUpdateTimestamp). If the clock of the NDS server is changed to a time prior to LastUpdateTimestamp, there might be problems in synchronizing all users that will be changed, added or deleted before the clock will reach back LastUpdateTimestamp.

AR MS Word Add-In (Graphical Signature)

- Managing the signatures using both AR's Digital Signature toolbar and office XP buttons (or menu options), might lead to unpredictable results. Therefore a user should handle his signatures using one method only.
- Copying and pasting a signature object is not supported.
- "save as" operation of a signed file is not supported.
- Signing a file run from a command line with the file name as a parameter is not supported (e.g., "winword.exe SignedFile.doc").
- Signing a mail message that is edited by Word is not supported.
- Signing within a text box is not supported.