



About digital signatures

This document provides facts and basic concepts about the topology and architecture of (CoSign) digital signatures. The information is comprehensive and should supply you with a good grasp of digital signatures and the benefits of their deployment.

[What are digital signatures?](#)

[What is the difference between digital and electronic signatures?](#)

[What is CoSign?](#)

[Digital and Graphical signatures](#)

[What is the technology behind CoSign Digital Signatures?](#)

[How it works?](#)

[PKI digital signatures vs. CoSign](#)

[All the components of PKI in one box](#)

[What are the benefits of implementing digital signatures?](#)

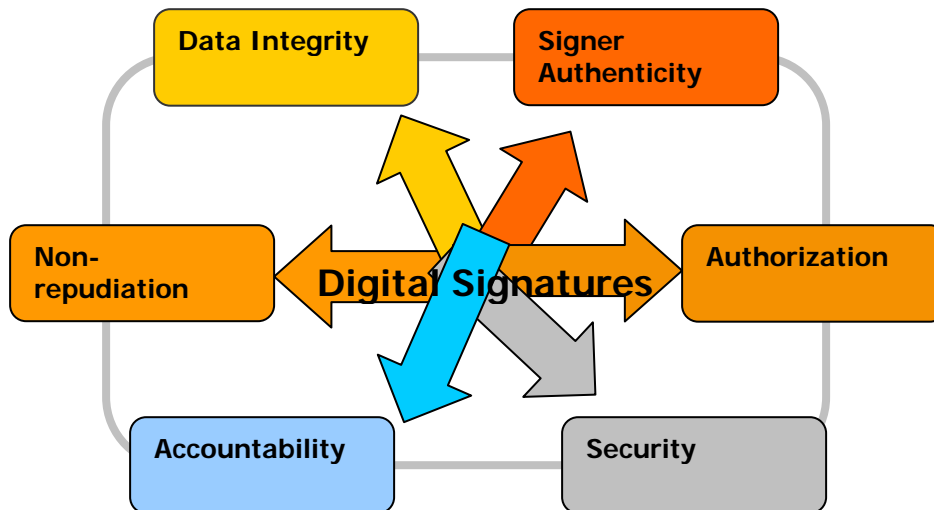
[Glossary](#)



What are digital signatures?

Digital signatures take the concept of traditional paper-based signing and turn it into a digital "**fingerprint**". Digital signatures enable you to easily migrate from cumbersome paper-based processes to a secure and efficient paper-free environment.

This "fingerprint", or coded message, is unique to both the signer and the document. This ensures that the person who signed is indeed the originator of the message. This fingerprint cannot be reused or reassigned to anyone else at any time. The digital signature authenticates the originator of the message and ascertains that the message has not been modified after sending. If any changes were made to the document after it was signed, they would automatically invalidate the signature, thereby protecting against forgery.



Digital signatures help organizations sustain signer authenticity, accountability, data integrity and non-repudiation of documents and transactions.



What is the difference between digital and electronic signatures?

There is a clear difference between electronic and digital signatures, though these terms are often used interchangeably:

Digital signatures (sometimes referred to as Advanced or Secure Electronic Signatures) are a result of a cryptographic operation. The technology behind digital signatures is an industry standard known as Public Key Infrastructure (PKI), which guarantees data integrity and non-repudiation of transactions. The digital signature cannot be copied, tampered or altered. On the other hand, **Electronic signatures** are electronic images that are physically or logically attached to the signed data. Adding a sentence “I, John Doe, sign this document” is good enough to be considered as an electronic signature; however, it is clear that electronic signatures are easy to forge, unlike Digital Signatures.

What is CoSign?

CoSign is AR's simple-to-use and quick to deploy, digital-signature solution that delivers an innovative way to digitally sign documents, files, forms and transactions, while enforcing iron-clad protection against signature forgery. With CoSign, organizations can easily sign in numerous applications such as Microsoft Word, Adobe Acrobat, TIFF images and leading Content Management Systems. CoSign digital signatures “seal” an electronic document, ensuring the authenticity, integrity and confidentiality of the electronic transaction, guaranteeing non-repudiation.

Digital and Graphical signatures

CoSign introduces a solution that merges both digital technologies and electronic graphical signatures (see illustration). This combination offers both unforgeable digital signatures and visual identification of the signer, using his/her visual graphical signature. CoSign provides users with an electronic representation (graphical image) of their handwritten signature which integrates with a digital signature on the electronic document. Both the graphical signature image and the digital signature are secure and easily deployed. The signature can also be validated ensuring the authenticity of the user.



Signed by: john green
Date: Nov 2 2004 10:22 AM
Reason: I am approving the document

What is the technology behind CoSign Digital Signatures?

CoSign generates digital signatures based on the "Public Key Infrastructure" (PKI) industry standard, also known as asymmetric cryptography. In a PKI system, each user has a key pair - a private key and a public key. These keys can be used for encrypting and decrypting information, for digitally signing electronic information and for verifying the authenticity of their owner.

The Private Key, as the name implies, is solely kept and used by the signer and stored securely, in CoSign's secure hardware device. The private key is used for signing, thereby adding a unique "fingerprint" to the document, while the public key is made available to other people who use it to validate the digital signature generated from the private key. These keys can be used for encrypting and decrypting important data, e.g., to scramble and unscramble the details of a bank transaction sent over public networks. The owner of the private key can digitally sign electronic information, while the holder of the corresponding public key can use it to verify the authenticity of the signature. CoSign provides robust security for issuing and managing the private-public key pairs, ensuring very strong authentication, integrity and non-repudiation.

Digital signature technology employs a cryptographic function known as "hashing" for both creating and validating a digital signature. The hash function is an algorithm, which creates a digital representation or "fingerprint" (referred to as a message digest) which is unique to the



signer. The digital signature is then appended to the message which is sent to the recipient. Any further changes made to the contents of the message will result in digital signature corruption. Users are certified by a Certification Authority (CA) or a trusted third party which assures the identity of the signer. CoSign has the ability to act as a CA.

In a PKI system, the public key is distributed widely, while the corresponding private key is held by its owner on a secure media (protected computer, token, smartcard). While both keys are mathematically related, the public key cannot reveal the private key. The strength of PKI is greatly enhanced by the CoSign solution which consists of a tamper-proof hardware appliance for centralized key generation, storage and signing operations together with software components for integration with various 3rd party applications (such as Microsoft Office) and User Management Systems (such as Active Directory).

AR's patented technologies are changing the industry's perception of PKI from something complicated and expensive, to digital signing technology that is simple-to-use and easy to manage thanks to CoSign,

How it works?

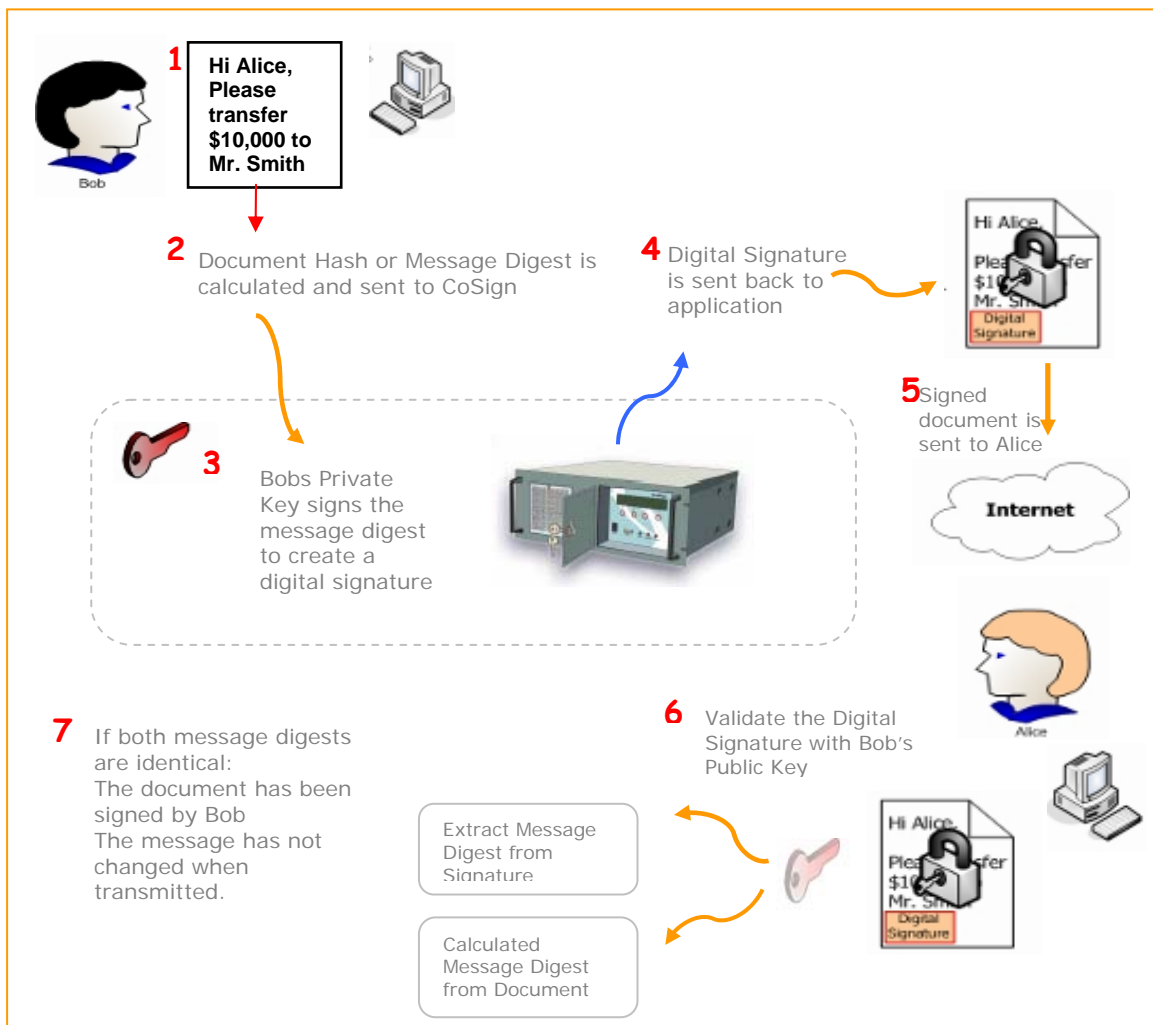
The following example refers to the illustration below: When Bob wants to send a document to Alice, he signs it with his private key. A mathematical function is then performed resulting in a Document Hash or message digest (Step 1-2). The document hash is digitally signed inside the CoSign appliance using Bob's private key and appended to the message (Step 4). The Digital Signature is a result of a RSA signature operation on the hash value.

Bob then sends the original document, along with the digital signature (fingerprint) and his Public Key to Alice (Step 4 – 5). Alice ensures that the document actually came from Bob using the public key, which applies a certain computation method to the signature (known as a signature verification). The hash value of the received message is calculated and compared to the hash value created above (step 1-2).

Results are compared, if Bob's document hash matches Alice's calculated hash, then Bob's signature is authentic and validate. If the hashes do not match, this can indicate impersonation or that the document was been changed from the time that Bob signed it.

Since only Bob has access to his Private Key, and since this key cannot be computed from the Public Key, data-integrity and non-repudiation are ensured. This process also enforces signer accountability. In other words, in a courtroom the signer can never claim he/she had not signed the document.

There is another factor still missing from this description. How can Alice know whether Bob is indeed the same person she intends to conduct business with, or even that it is really Bob? Bob needs to be certified by a trusted third party that knows him and can verify that he is indeed who he claims to be. These trusted third parties are called Certificate Authorities (CA); they issue certificates to ensure the authenticity of the signer. Certificates can be compared to passports issued by countries to their citizens for world travel. When a traveler arrives at a foreign country, there is no practical way to authenticate the traveler's identity. Instead, the immigration policy is to trust the passport issuer (in PKI terminology: the CA) and use the passport to authenticate its holder in the same way that Alice uses the CA's certificate for authenticating Bob's identity.



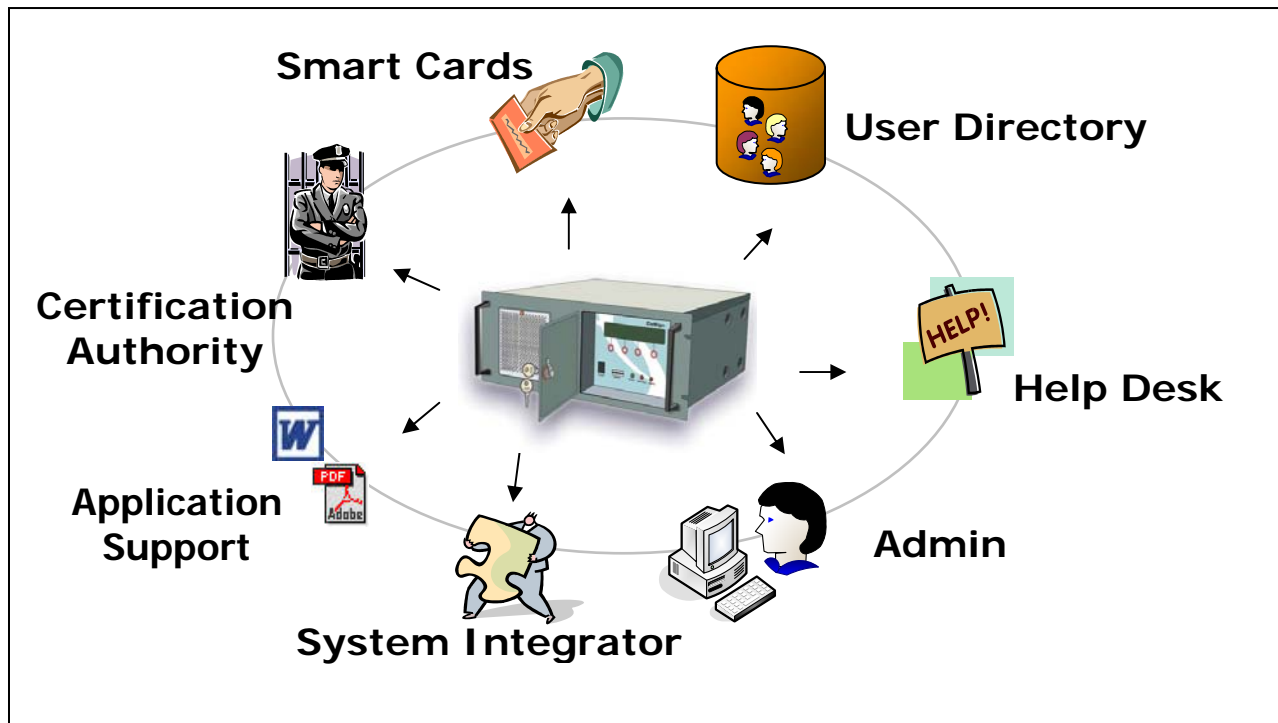
PKI digital signatures vs. CoSign

Traditional PKI-based solutions are expensive and difficult to deploy. The PKI environment consists of many components : Certificate Authority (CA), key-storage device (hardware or software), management application and, signing applications (workflow application, ERP, mail, others). Integrating all these players and components has proven to be a lengthy, complex and prohibitive process.

AR's vision is to make PKI affordable and easy-to-use for all companies, large and small. AR, with its patented technologies, has changed the PKI environment, by designing CoSign, a simple-to-use and cost-effective digital signature solution.

All the components of PKI in one box

CoSign is quick to deploy and offers ALL the components of a digital-signature solution in one box.



CoSign solves complex deployment problems and dramatically reduces the TCO (Total Cost of Ownership) of deploying digital-signatures. CoSign enables new users to automatically enroll in the PKI system (i.e., it creates the keys, issues certificates and renews them) ensuring that the system is always simple and easy-to-use. Organizations have the option to manage their users either inside CoSign or through MS Active Directory and Novel NDS.

What are the benefits of implementing digital signatures?

CoSign Security and Compliance Benefits

- Guarantee document security Ensure signer identity
- Ensure data integrity of documents and transactions
- Provide Non-repudiation of documents and transactions
- Ensure greater legal compliance and employment of worldwide regulations
- Provide audit trail
- Enable verification of document source

CoSign business Benefits:

- Streamline business processes (e.g., approval procedures, audit trails)
- Increase employee productivity and efficiency
- Facilitate a paperless environment
- Eliminate the risk of misappropriation of intellectual property
- Easy deployment of digital signatures
- Quick ROI
- Significant cost savings
- e-archiving
- Easy access to information

With CoSign digital signatures you can be reassured that your electronic documents are even more secure than your paper documents. No more printing an electronic form into paper, waiting for a signed paper to arrive or chase after a signature. Simply click the Sign icon and send your electronic document anywhere, any time.

Seamless, secure, and easy to use, CoSign lets you digitally sign, documents with the click of a mouse. It's the perfect digital signature appliance that enhances, seals and streamlines traditional paper processes!

Facts and Figures:

Did you know with Cosign you can sign more than 60 pdf files in one second?

Did you know digital signatures can save the printing of thousands of papers per day?

Did you know digital signatures can save \$thousands of dollars a month?

Did you know your digital signature locks the contents of the document?

Appendix

Glossary

Term	Definition
Advanced Electronic Signature	See Digital Signature.
Asymmetric Cryptography	There are two types of encryption schemes: <ul style="list-style-type: none">▶ Symmetric - Identical secret key for encryption & decryption▶ Asymmetric - Two Keys: Private Key for decryption and signing and Public keys for encryption and validating signatures. Knowledge of public key will not reveal the private key.
CA	An authority that creates and signs Digital Certificates for one or more users. Usually CAs form a hierarchy. The top of this hierarchy is called the root CA. See also RA.
CAPI	Cryptographic API (Application Programming Interface). An API provided by Microsoft to let applications encrypt or digitally sign data.
CDP	CRL Distribution Point – Definition used by application to find the CDP location.
CRL	Certificate Revocation List - the place where a CA stores the IDs of all the Digital Certificates that have been revoked.
Data-Integrity	Assures document authenticity; any changes made to the contents of the document will invalidate the signature.
Detached Signature	One possible method to add a Digital Signature to signed data, where the Digital Signature and the signed data are kept separately.
Digest	Used in the process of creating a Digital Signature, a Digest is a unique digital representation or "fingerprint" of the signed data. See also "Hashing".
Digital Certificate	Similar to a passport identifying a trusted a person (or entity such as application, etc.). Digital Certificate is issued by a CA and is used to ensure the authenticity of Public keys belonging to users. A Digital Certificate prevents a hacker from claiming they are someone else thanks to the CA which issued the certificates after ensuring the authenticity of Public keys belonging to users.
Digital Signature	Digital Signature (sometimes referred to as Advanced Electronic Signatures) takes the concept of the traditional paper-based signature into the digital realm, by adding a digital "fingerprint" as a signature to a document. This "fingerprint" is unique to both the document and the signer.
Electronic Signature	While Digital Signatures and Electronic Signatures are sometimes

	used interchangeably, there is a significant difference between the two. Electronic Signatures merely add data (text, sound, symbol, picture, etc.) to a document as a means of identifying the signer. These signatures should be considered forgeable.
Enrollment	The process of signing up a user for a Digital Signature "account", which includes generating a Key Pair and creating a Digital Certificate.
Enveloped Signature	One possible method to add a Digital Signature to signed data, where the Digital Signature is embedded within the signed document.
Enveloping Signature	One possible method to add a Digital Signature to signed data, where the signed data is actually embedded within the Digital Signature.
Graphical Signature	See Wet Signature.
Hashing	A mathematical process that converts a message (e.g., a document) into a unique "message digest" that represents the original message. A hash function will not produce the same message digest from two different inputs. A hash is a one-way function, making it infeasible to reverse the process to determine the original message from the "message digest".
Key Pair	The Public and Private keys generated for a user.
Non-Repudiation	Avoid denial of transactions.
OTP	One Time Password – An authentication method using a password that is only valid for a single use.
PKCS#1	A Public-key cryptography Standard published by RSA Laboratories defining the basic format syntax/format for a Digital Signature. This format does not include anything else other than the signature data.
PKCS#7	A Public-key cryptography Standard published by RSA Laboratories defining the syntax/format for a Digital Signature. This format includes on-top of PKCS#1 information such as timestamp, Digital Certificate and more.
PKCS#11	A Public-key cryptography Standard published by RSA Laboratories defining an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions.
PKCS#12	A Public-key cryptography Standard published by RSA Laboratories defining a format for storing or transporting a user's private keys, certificates, etc.
PKI	Public Key Infrastructure. The combination of standards, protocols and software that support Digital Signatures and Encryption.
Private Key	The secret key in a PKI system, used to validate incoming messages and sign outgoing ones. A Private Key is always paired with its Public Key during those key generations.
Public Key	The publicly available key in a PKI system, used to encrypt messages bound for its owner and to validate signatures made by its owner. A Public Key is always paired with its Private Key during those key generations.
Qualified Certificate	A Digital Certificate provided by a CA that has a national accreditation for providing those.



Qualified Digital Signature	A Digital Signature based on a Qualified Certificate.
Qualified Electronic Signature	See Qualified Digital Signature.
RA	Registration Authority – An RA does the required identification for certain certificate data and passes the info to the CA for issuing the Digital Certificate.
Signature Pad	An electronic device with a touch sensitive LCD screen which allows users to acquire and register a Wet Signature.
Smart Card	A card, typically the same size as a credit card that contains a built-in microprocessor and memory. In traditional PKI systems, Smart Cards are used to store user's Private Keys and in some cases, also perform the Hashing.
Wet Signature	A graphical representation of a wet-ink signature. A Digital Signature per say does not include a Wet Signature. The combination of a Wet Signature and a Digital Signature provides a visual indication that the user is accustomed to, as well as an assured method of sealing documents.
X.509	A standard for Digital Certificates from the ITU (International Telecommunication Union) used in many PKI implementations.