cosign by arx The Digital Signature Company

The Ultimate Guide to Digital Signatures

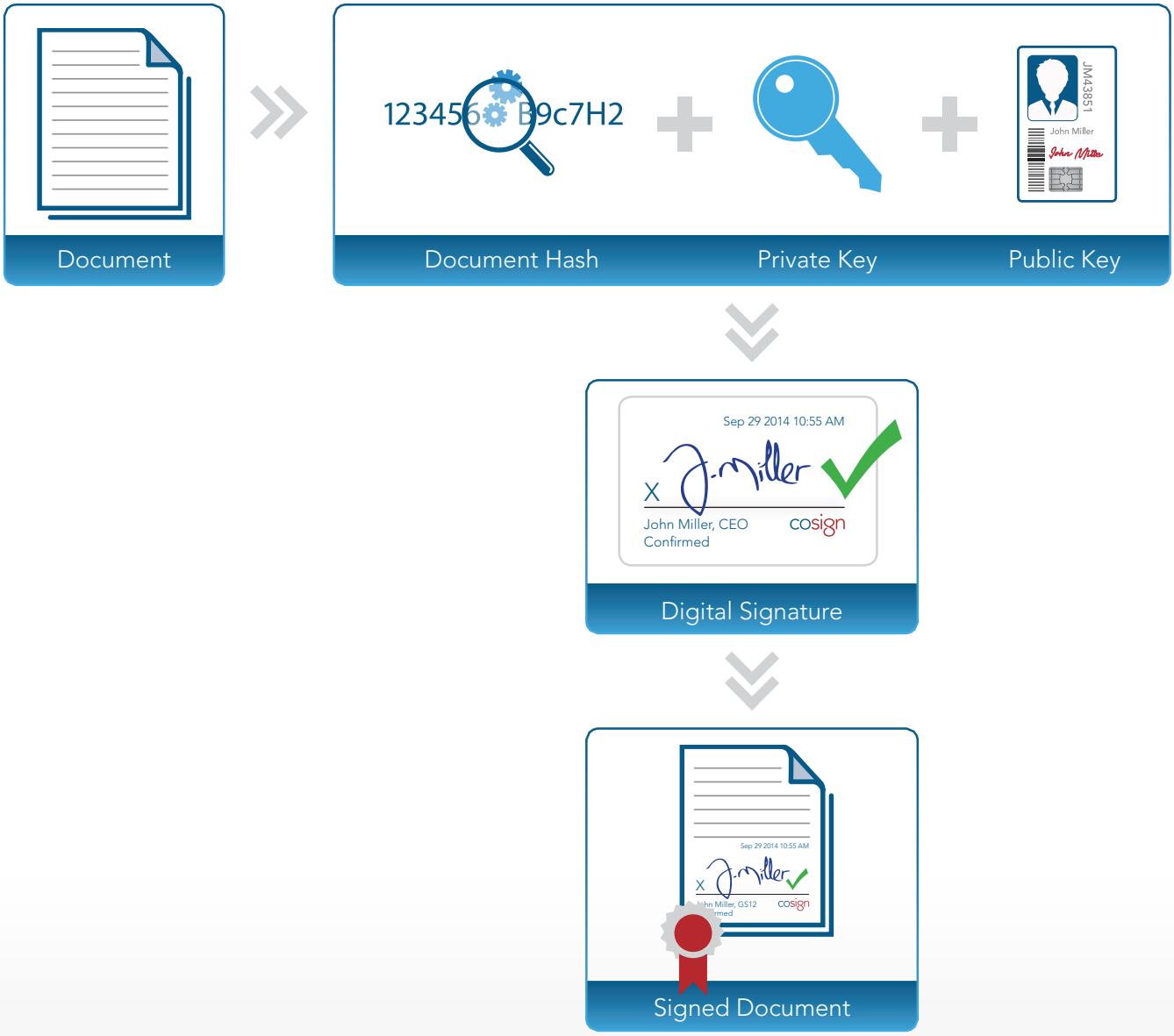
Comprehensive Answers to the 20 Most Important Questions

ARX | 855 Folsom St. Suite 939, San Francisco, CA 94107 | Tel. (415) 839-8161 | www.arx.com | sales@arx.com

Introduction

As organizations increasingly adopt paperless processes and automate their document workflows, the "wet ink" signature is rapidly becoming an anachronism in our digital world. Companies and government organizations around the world have invested huge sums in automating their business workflows, yet they still find themselves printing paper for the purpose of obtaining signature approvals. Projects can be held up for days and costs are accrued while documents are mailed between offices, partners, suppliers or customers in order to collect signatures.

Professionals often share the concerns voiced by compliance officers over how to ensure the integrity and accountability of electronic documents and records, and by CIOs over how to best secure them. Meanwhile, COOs are concerned with avoiding project delays and CFOs are seeking ways to cut costs associated with paper handling. Digital signatures address each and every one of these concerns.



1. What are Digital Signatures?

Digital signatures, which are often referred to as advanced or standard electronic signatures, take the concept of traditional paper-based signing and turn it into electronic "fingerprints", or coded messages, which are unique to both the document and the signer and binds the two together. They are based on international standards that guarantee their secure implementation.

Digital signatures seal documents signed by one or more people, providing evidence of user identity, guaranteeing data integrity, ensuring the non-repudiation of documents, and complying with laws and regulations. This helps organizations ensure signer authenticity, accountability, data integrity, and the verifiability of signed electronic documents and forms. Any changes made after the document has been signed invalidate the signature, thereby protecting against signature forgery and information tampering.

2. What Does a Digital Signature Include?

A digital signature is composed of three elements:

1. A unique digital certificate for each signer
2. A private key which only the signer can access
3. A public key which allows anyone to validate the signature

Digital signatures can also include graphical signatures (i.e., the scribble of a signature or initials) or any other image such as an official seal (for example, engineering seals for each US state). In addition, signers can include their typed out name, title, date/time stamp, and their reasons for signing (or reason codes).

3. What are Electronic Signatures?

Electronic signatures are an umbrella term for any technology used to associate a person with the electronic content they are trying to sign and can be as basic as a typed name or a digitized image of a handwritten signature. They are defined by the US ESIGN (the Electronic Signatures in Global and National Commerce Act of 2000) and UETA (the Uniform Electronic Transactions Act) acts as "an electronic sound, symbol, or process."

Examples of electronic signatures include a scanned image of a signature, the "I Accept" checkmark on a website, and a signature captured using an electronic pad. Consequently, e-signatures by themselves cannot guarantee integrity and security, as nothing prevents one individual from using another individual's name, or a signer denying that they signed the document. Due to this reality, an electronic signature that does not incorporate additional measures of security is considered an insecure way of signing documentation.

4. What is the Difference between Digital and Electronic Signatures?

Digital signatures are a sub-group of electronic signatures that provides the highest levels of security and universal acceptance so that they cannot be copied, altered or tampered with. Digital signatures are based on Public Key Infrastructure (PKI) technology, the only signature standard published, maintained and accepted by governments around the world, including the US and the European Union, as well as by independent bodies such as ISO, OASIS, IETF and W3C. For more information on PKI, please refer to question # 18.

Through the use of cryptographic operations, digital signatures create a "fingerprint" unique to both the signer and the content, thus ensuring both signer identity and content integrity, while preventing the risk of deniability. Since they are based on international PKI standards, digital signatures can be easily validated by anyone, anywhere without the need for proprietary verification software in widely available applications such as Microsoft Office and Adobe Reader that alert users if a change has been made to the document and/or if the signature is invalid.

Electronic signatures, on the other hand, are based on proprietary formats that may use a digitized image of a handwritten signature, a symbol, voiceprint, among other options, to identify the author of an electronic document. While they are legally enforceable in certain parts of the world, such as the US, electronic signatures are vulnerable to copying and tampering and require proprietary software for validation. Unlike digital signatures, they cannot by themselves guarantee signer identity and intent, data integrity, and the non-repudiation of signed documents.

When it comes to laws and regulations, only digital signatures are compliant with the most stringent requirements set by governments around the world. For organizations requiring an even higher level of security, some digital signature solutions also offer systems that have been certified at FIPS 140-2 Level 3 by the National Institute of Standards and Technology (NIST) and/or at the EAL4+ level based on the Common Criteria standard.

5. What are Cloud-Based (SaaS) Electronic Signature Solutions?

These are electronic signature cloud services that have routing and workflow capabilities. A document can be uploaded to the SaaS (Software as a Service) vendor's website, which sends an email to the intended signer containing a link to the document which remains on the vendor's site. The person can review the document and sign it, after which the sender is notified that it has been signed. This type of signature is very handy in B2C use cases, for example for the low-risk documents that realtors want their customers to sign.

Nevertheless, there are several important considerations:

- The identity of the signer cannot be irrefutably proven, only that someone clicked on an email link, and then clicked on a button in a website. In other words, the direct link between the signer and the signed document is absent unless strong authentication mechanisms are added.

- Documents, which may contain sensitive information, have to be loaded onto a third-party website and thus depend on their security protocols. When it comes to confidential or sensitive information, this type of signature is most likely not acceptable.

- The validation of the individual signature has to be done using proprietary mechanisms, such as through the vendor's website, so that the organization is dependent on the longevity of the vendor.

6. Why Are Organizations Using Digital Signatures?

Digital signatures are used by millions of people every day across the world at commercial enterprises as well as governmental organizations, due to several important economic, regulatory and technical reasons:

- **Doing More with Less:** Organizations are always looking for ways to provide high levels of service with fewer human and budgetary resources. Automating signature-dependent processes can quickly ease some of these burdens by reducing the number of people required to handle documents, while significantly cutting down paper processing costs and turnaround times.

- **Transparency:** Organizations are inevitably held accountable for every project, transaction, document and procurement order that they sign, even years down the road. Digital signatures ensure long-term accountability by maintaining documents that are completely transparent, easily auditable, and fully compliant with the relevant laws and regulations. In fact, once a document is digitally signed, it cannot be modified without alerting the reviewer, providing irrevocable proof of authenticity when required.

- **Avoiding Vendor Lock:** An additional consideration is to ensure that organizations are not locked into a specific vendor. Many electronic signature solutions on the market today are proprietary by nature with signature validation remaining dependent on the vendor's software. Proper digital signature technology is based on international standards and enables anyone inside or outside the organization to validate the signed documents independent of any particular software vendor.

- **Solution Longevity:** Organizations typically prefer enduring technologies that will still be in use decades down the road. When it comes to digital signatures, it's important to remember that the PKI technology that they're based on has been available since 1976 and remains both highly secure and impenetrable to hacking. In addition, because digital signatures are based on international standards, anyone can validate them using widely available applications such as Adobe Reader for PDF files and Microsoft Office for Word and Excel files.

- **Enterprise-wide Deployment:** Most organizations prefer to deploy a single technology solution across all their departments for easier IT management and user acceptance. Since all departments have at least one, and typically many more signature-dependent processes, a single, easy-to-use solution that can meet the requirements of all departments appeals to executives, as they

quickly realize that digital signature solutions can improve their operations while benefiting their employees, customers and partners.

- **Going Green:** Finally, over the past few years, a noticeable "going paperless" trend has developed at all levels due to the need to increase efficiency, reduce costs, and take environmental considerations into account. One of the fastest and most effective ways to achieve this goal is by deploying digital signatures to eliminate expensive and cumbersome paper-based processes.

7. What Are the Benefits of Digital Signatures?

Organizations throughout the world invest millions of dollars every year in automating their operations and business processes. As a result, electronic documentation permeates every aspect of the business workflow in industries ranging from life sciences and financial services to engineering and government.

Despite the great strides achieved in automation, the PSS (Print > Sign > Scan) problem persists everywhere. A hard copy is printed whenever signature authorization is required, adding time-consuming steps to what can and should be a completely paperless process. Not only does the reintroduction of paper into the workflow increase costs due to printing, scanning, sending, filing and other manual tasks, but it adds considerable delays and keeps companies from realizing the true benefits of a fully electronic workflow.

Signature automation solutions eliminate the need to print documents only in order to sign them, enabling organizations to replace their slow and expensive paper-based approval processes with fast, low-cost and fully digital ones. Businesses around the globe and across industries use them to securely and compliantly expedite approval processes, while also enhancing collaboration, reducing costs, improving efficiency, and supporting green paperless initiatives.

Digital signatures enable organizations that have invested in business automaton systems and electronic content management systems to cover "the last mile" by eliminating the need to reintroduce paper into the workflow for signature approvals. These organizations can gain the full benefit from their investment in automation by seamlessly integrating a digital signature solution with their existing processes and applications.

Digital signatures effectively streamline processes, helping entire organizations reach a quick ROI (Return on Investment) through:

- Expedited paper intensive business processes
- Improved efficiency and collaboration
- Enhanced legal compliance
- Reduced operational costs
- Established paperless office

8. What Types of Documents Can Be Digitally Signed?

The list of documents that can be signed using digital signatures is very long. A few examples include:

- Purchase orders, agreements with partners
- Contracts, agreements, board actions, SEC documents
- Sale proposals, point of sale/service forms, contracts with clients
- Lease agreements, loan agreements, expense reports, reimbursement approvals
- Human Resources: Employee on-boarding documents, time sheets
- Life Sciences: Applications and submissions; QC documents, SOPs, policies, work instructions
- Engineering: Designs, drawings, plans, manufacturing instructions, reports
- Healthcare: Patient and consent forms, health records, prescriptions for drugs, lab reports

9. Are Digital Signatures Legally Enforceable?

Most countries around the world have adopted legislation and regulations that recognize the legality of a digital signature and deem it a binding signature equal to "wet signatures." Many industries have also established specific regulations that define digital signatures as a replacement for handwritten signatures.

For example, in 1999, the EU passed the "EU Directive for Electronic Signatures" (replaced by the eIDAS regulation in 2014), and in 2000, the Electronic Signatures in Global and National Commerce Act ("ESIGN") was signed into law in the US.

Examples of legislation from around the world:

- U.S. - Electronic Signature in Global and National Commerce Act (ESIGN)
- U.S. - Uniform Electronic Transactions Act (UETA) - adopted by 48 states
- U.S. - Digital Signature And Electronic Authentication Law (SEAL)
- U.S. - Government Paperwork Elimination Act (GPEA)
- U.S. - The Uniform Commercial Code (UCC)
- Canada - Uniform Electronic Commerce Act (UECA)
- UK - Electronic Communications Act 2000 (chapter 7)

- Europe - EU Directive for Electronic Signatures (1999/93/EC)
- Europe - Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) regulation
- Europe - EU VAT Directive
- China - Electronic Signature Law of the People's Republic of China

Examples of industry-specific regulations:

- Life Sciences - FDA's 21 CFR Part 11
- Healthcare - Health Insurance Portability and Accountability Act (HIPAA)
- Healthcare - Joint Commission on Accreditation of Healthcare Organizations (JCAHO)
- Homeland Security - Public Law 108-390
- Engineering - PE Board Regulations
- Finance - Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley)
- Environmental - Cross-Media Electronic Reporting Regulation (CROMERR)
- Public Companies - Sarbanes-Oxley Act of 2002
- Veterinary/Equine - USDA EIA (Coggins) Testing
- Aviation - FAA's CFR Title 14
- Telecom - European Telecommunications Standards Institute (ETSI)

10. Can a Digital Signature Be Forged?

Assuming an organization implements a digital signature solution that requires an authentication mechanism (which is recommended), the only way someone can sign with another person's unique certificate is if they reveal their authentication credentials. The digital signature systems that are available today will leverage and use the organization's user management and authentication systems. Some systems also support two-factor authentication to fully ensure the security of the signing process. For more information on certificates, please refer to questions #19 and #20.

In comparison, handwritten signatures can easily be forged. One need only consider the example of Nicholas Leeson, who forged the handwritten signatures of his boss and caused the collapse of Barings Bank, the UK's oldest investment bank. While both handwritten and digital signatures (standard electronic signatures) are legally-binding, only digital signatures ensure the non-repudiation of documents.

11. How Are Digital Signatures Validated?

Digital signature solutions allow anyone to use widely available software, such as Adobe Reader or Microsoft Office, to verify the identity of the signatory and ensure that the document has not been modified since it was signed. Depending on the software applications used to review the signed document, the receiver initiates the validation process by either selecting the Validate option or by clicking on the signature itself.

The validation process consists of two simple steps:

1. **Verifying document integrity** (ensuring that nothing has changed in the document since it was signed): When someone tries to validate a digital signature the original algorithmic hash is compared to the one that is automatically recalculated. If the document hasn't been changed, they will be the same and the signature will appear as valid. If anything has been altered, the signature will be shown as invalid.

2. **Verifying signer identity** (confirming that the individual signer certificate was issued by an entity the reviewer trusts such as a third party or the organization itself): The Certificate Authority's root certificate that is included in the digital signature is examined, as it is used to sign the individual users' signer certificates. The signature is validated if the computer recognizes the root certificate. If the computer doesn't recognize it, the reviewer will receive a validation error message.

Within an organization, the organizational root certificate can be easily distributed so that all computers will recognize it. The first time a signed document is sent to someone outside the organization, all that needs to be done is to send them a link to the organization's website from which they can easily download the certificate for ongoing validation of all the organization's signed documents.

12. How Should User Credentials be Managed?

All digital signature systems must first and foremost securely store and manage their users' signing credentials (private keys and digital certificates) to avoid misuse. This can be done in one of two ways based on the organization's needs, existing infrastructure, and choice of certificate type.

The signing credentials can be managed using a decentralized approach where they are installed on each signer's PC or on a token, such as a smartcard or USB device. This method can become cumbersome, time-consuming and expensive for any organization with more than a few signers due to control and credential management issues.

The other approach is a centralized one where a central server is used to securely store and manage the signing credentials. This method greatly simplifies system management, making it much more affordable and easier to deploy from both a technical and operational point of view. In addition, it enforces authentication and ensures that the users have sole control over their signature credentials.

13. How Should Signers Be Managed?

The digital signature solution must be able to manage the users, either directly or, better yet, through automatic synchronization with an existing user management directory, such as Active Directory and other LDAPs. This eliminates the associated costs of managing users in two separate systems, the one that already exists and the one required for managing signers. The system should be able to automatically enroll new users, create their keys, issue their certificates, and update/renew/revoke them when necessary.

The digital signature solution should also be able to work with the authentication method that is already used by the organization to access file servers, mail servers, applications, etc. Most common authentication systems rely on a single factor such as a password. More complex systems typically involve two-factor authentication (for example, a fixed password and a changing One-Time Password). While less common, three factors (for example, a password, a smartcard and biometric authentication) are also possible.

In addition, it is imperative to review the organization's identity proofing procedures in the context of issuing digital certificates. Where appropriate, additional methods may be necessary if higher levels of security and control are required to meet legal and risk requirements. Proofing options include email verification, credit card verification, or third-party, knowledge-based proofing services such as those offered by IDology, Lexis-Nexis and Experian, among others.

14. What is the Best Way to Set Up a Digital Signature System?

Organizations can create a very basic system by purchasing individual certificates from a third party and having the signers use the native signing capability available in Microsoft or Adobe products. The main challenge with this approach is managing all the user credentials, which need to be installed on each signer's laptop or PC (or used via tokens), and then removed when necessary and renewed every year.

Technically advanced organizations can attempt to build their own digital signature solution which requires the same components that are available in vendor solutions, including:

- A way to manage user enrollment
- A way to manage key and certificate creation, issuance, renewals and revocation
- A mechanism to authenticate the users at the moment of signing
- A tamper-evident or tamper-proof physical appliance

While the above is possible, buying a centralized system from a digital signature vendor is ultimately far less expensive, as well as much more convenient and easier to deploy. End-to-end solutions that are available on the market today, either on premises or in the cloud, can be up and running very quickly.

Organizations can also provide digital signing capabilities to their vendors, partners and customers via the organization's web portal. This allows external signers to sign in a secure environment that is controlled by the organization where the document is ready for processing immediately after they sign.

15. How Long Does it Take to Deploy a Digital Signature Solution?

This depends on the deployment approach and the number of signers. For example, a department with ten signers can purchase third-party certificates and immediately start using the signing capabilities in Microsoft and/or Adobe after the administrator has set up the system and installed the certificates.

For an organization with more signers, the deployment process for an internal solution may take a while as the administrator's work is more complex and cumbersome. In contrast, a centralized digital signature solution can be up and running in a couple of hours, regardless of the number of signers.

16. Why is it Important to Document Signing Procedures?

It is very important for organizations to establish and document their signature-related SOPs and consolidate them in a single repository for the purpose of contingency, data breach and disaster recovery plans, quality control, or simply for the ease of training new users. Examples include identity-proofing, signer enrollment/de-enrollment, training, authentication, identification of documents and forms requiring signature, information to be included in the signature block, use of graphical signature images, use of reason codes, and solution administration.

17. How to Choose the Right Digital Signature Solution?

Several operational and technical considerations that should be kept in mind prior to selecting a digital signature solution:

- **Does it leave control with the organization?** The solution should be adaptable to the specific processes, technologies, user management and authentication needs of the organization — not the other way around. This flexibility provides the freedom to manage the digital signature solution in a way that best suits the organization's internal regulations and standard operating procedures.
- **Does it enable users to sign the file types/content applications they typically use?** The solution needs to work with all commonly used content authoring apps and file types such as Word, Excel, Outlook, PDF, InfoPath and even AutoCAD.
- **Does it work with the existing content management applications?** The solution should be able to integrate seamlessly with the electronic content/document management and/or workflow

automation systems the organization already has in place, such as SharePoint, OpenText, Oracle, Alfresco, Nintex, K2, etc.

- **Does it allow users to customize signatures and/or signature locations?** The solution should enable users to determine the visible contents of their signature (images, date/time stamp, reasons, etc.), as well as to pre-embed, customize and name their signature fields.
- **Does it require the organization to route or save documents outside the IT domain?** For security purposes, the solution should ensure that all documents remain inside the organization's IT domain and are never routed through, or saved on, external, third-party servers.
- **Does it comply with the regulations that are relevant to the organization?** The digital signature technology should be based on internationally accepted standards that comply with the legal and industry-specific regulations that are relevant to the organization. If a higher level security is required, the solution should be validated for NIST's FIPS regulations.
- **Does it enable individuals to validate the signature even without access to the system?** The solution should allow anyone inside or outside your organization to use widely available software, such as Adobe Reader or Microsoft Office, to verify who signed the document and whether it has been modified since it was signed.
- **Does it allow signing online and using mobile devices?** The solution should allow users to add digital signatures to documents using any device, whether at the office on their PC, at home on their tablet, or in the field using a mobile device.
- **Does it provide the option to self-host the system?** The solution should allow organizations to choose between an on-premises server and a managed cloud-based system so that the system can be set up according to the organization's internal requirements.
- **Does it ensure cost-effective IT management?** Besides the paper-related cost savings, such as printing, mailing, scanning, couriering and archiving, the solution should provide a low TCO (Total Cost of Ownership) through quick installation, minimal operational impact, and minimal IT maintenance.

18. What is PKI?

Public Key Infrastructure (PKI) is the basis for digital (standard electronic) signatures. PKI provides each user with a pair of keys - a private key and a public key - used in every signed transaction. These keys can be used for encrypting and decrypting information, for electronically signing electronic information, and for verifying the authenticity of their owner.

In a PKI system, the public key is distributed widely, while the corresponding private key is held by its owner in a secure place. While both keys are mathematically related, the public key cannot reveal the private key. This makes Public Key Infrastructure the ideal technology for digital signatures.

The private key, as the name implies, is not shared and is used only by the signer to electronically sign documents. The public key is openly available and used by parties who need to validate the signer's electronic signature. A PKI system includes additional components such as a Certificate Authority (CA), end-user enrollment software, and tools for managing, renewing, and revoking keys and certificates.

19. What are Certificate Authorities and Digital Certificates?

To make sure that a signer is indeed the same person they claim to be, he or she needs to be certified by a Certificate Authorities (CA) that knows them and can verify that they are indeed who they claim to be. A CA can be the company/organization itself, which issues digital certificates to its corporate employees, or it may be a commercial CA from which certificates can be purchased.

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 (or the CA in our case) and use the passport to authenticate its holder in the same way that the CA's certificate is used to authenticate the signer's identity.

In cryptography, a Digital Certificate is an electronic document that uses a digital signature to bind together a public key with an identity - this information can be a person's name or the name of an organization, or some other identity feature. Only this person can sign with that particular certificate and key, and once authenticated, the signature certificate details are embedded in the document along with the unique algorithmic hash based on the contents of that document.

20. What Options Are Available Regarding Digital Certificates?

The type of digital certificate used in an organization depends on the level of trust it aspires to achieve.

There are three basic types of certificates:

1. **Self-signed individual certificates:** The simplest type of certificate is one created by the users themselves using Microsoft or Adobe applications. It has limited value since the user can create that certificate for any identity, using any name or email address, without having to go through a verification process. It can be compared to a person issuing themselves a passport. For organizations in general, and certainly for regulated industries, this type of certificate should not be considered a viable option.

2. **Third-party certificates:** There are dozens of third-party CAs that will confirm the identity of the certificate owner and issue individual certificates to organizations, including well-known names such as VeriSign, Entrust, Comodo, and GlobalSign. This process requires either face-to-face identification of the certificate owner using an accepted and legal identifying document such as a driver's license, or a CA review and audit of the organization's identity-proofing procedures.

3. **Self-issued organizational certificates:** A more advanced form of trust is achieved when the organization itself becomes the CA. In this case, individual certificates can be created and signed with an organizational root certificate only after the identity of the owner of each individual

certificate has been made using an established and documented identity-authentication procedure. Organizations can get root certificates through Microsoft Certificate Services or by using the root certificate that is included in a centrally managed digital signature solution.

An important point that needs to be kept in mind in this regard is that there are no automatically and globally trusted certificates. For example, World Wide Verifiable (WWV) certificates automatically validate Microsoft Office documents, but not PDFs (unless Adobe Reader is manually configured to trust that certificate), while Certified Document Services (CDS) certificates automatically validate PDFs, but they never validate MS Office documents.

ARX | 855 Folsom St. Suite 939, San Francisco, CA 94107
Tel. (415) 839-8161 | www.arx.com | sales@arx.com