Digital Signatures:
Best Practices for State and Local Government
Introduction

State and local governmental organizations have come under increasing pressure over the past few years to streamline processes and reduce costs despite the more limited human and budgetary resources available to help them achieve these goals. In order to effectively transform their workflows, they will need to identify operational zones that can be easily automated through the use of cost-effective solutions.

One initiative that many government entities have been investigating lately is the use of digital signatures, which rapidly transform signature-dependent processes, offering a compelling solution to making these processes highly efficient and cost-effective. In fact, the Association for Information and Image Management (AIIM) report ¹ showed that 81% of organizations that have deployed digital signatures reached ROI (return on investment) in less than a year.

Although governmental bodies generate masses of documents that require signatures, most of the paperwork is still being printed and routed manually for signature approval. Automating these processes enables them to replace their cumbersome and expensive paper-based approval processes with fast, low-cost and fully digital ones. Digital signatures produce legally enforceable secure electronic records that eliminate paper-related workflow bottlenecks and create truly paperless, highly efficient digital environments for government employees and for the communities they serve.

This white paper will help you better evaluate your options when it comes to selecting a digital signature solution for your government organization, and offers best practice guidelines for deploying it. Topics discussed in this document include:

- What are digital signatures and how do they work?
- What benefits do digital signatures offer governmental organizations?
- How can digital signatures be used across different government departments?
- What considerations need to be addressed when selecting a signature solution?
- What are the best practices for selecting and deploying digital signatures in government entities?

¹ Digital Signatures – Making the Business case – AIIM – January 2013
(http://www.arx.com/resources/white-papers/aiim-research-on-digital-signatures)
What are Digital Signatures?

The short answer is that digital signatures are the most advanced form of electronic signatures – the most secure, most flexible and most compliant with laws and regulations. For the longer answer you will first need to understand the differences between “digital signatures” and “electronic signatures”, which are sometimes (and incorrectly) used interchangeably.

**Electronic signature** Electronic signature is an umbrella term for any technology used to associate a person with the electronic content they are trying to sign. It is defined by ESIGN (the Electronic Signatures in Global and National Commerce Act of 2000) and UETA (the Uniform Electronic Transactions Act) as “an electronic sound, symbol, or process”. Examples include a scanned image of a signature, the “I Accept” checkmark on a website, and a signature captured using an electronic pad at a grocery store. By themselves, most electronic signatures cannot ensure signer identity or content integrity, nor do they eliminate the risk of signers denying that they signed the document.

**Digital signatures**, on the other hand, are the most secure form of electronic signatures. They are based on Public Key Infrastructure (PKI) technology, the only signature standard published, maintained and accepted by governments around the world, including the US, Canada, the European Union and Latin America, as well as by independent bodies such as ISO, OASIS, IETF and W3C. When governmental organizations explore their options regarding electronic signatures, they typically decide that digital signatures are the best option because of their non-proprietary nature, global acceptance, compliance with local regulations, security assurance, and ability to work with the most commonly used authoring applications.

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 (non-repudiation). Because they are based on international PKI standards, digital signatures can be easily validated by anyone anywhere using widely available applications such as Microsoft Word and Adobe Reader, without the need for proprietary software.

When it comes to laws and regulations, only digital signatures are compliant with the most stringent requirements set by government agencies, including major regulations such as ESIGN, UETA, EU directives and VAT law, FDA 21 CFR Part 11, HIPAA and SOX. For government agencies requiring a higher level of security, some digital signature solutions also offer FIPS 140-2 Level 3 systems that have been certified by the National Institute of Standards and Technology (NIST).
Why are Digital Signatures Needed in Government?

Digital signatures are in daily use by millions of people across the world at commercial enterprises as well as at governmental organizations. The public sector in particular has been paying more and more attention to digital signatures over the past few years due to several important economic, regulatory and technical reasons:

➤ **Doing More with Less:** Governments are always looking for ways to provide a high level 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.

➤ **Going Green:** Over the past few years, a noticeable “going paperless” trend has developed among government agencies at all levels due to their need to increase efficiency, reduce costs, and show that they are taking environmental considerations into account. In fact, many government agencies have made eliminating paper a mandatory goal for their various departments. 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.

➤ **Transparency:** Government agencies 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 you digitally sign a document, it cannot be modified without alerting the reviewer, providing irrevocable proof of authenticity when required.

➤ **Avoiding Vendor Lock:** An additional consideration for government entities is to ensure that they 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:** Government agencies require an enduring technology that will still be in use decades down the road. When it comes to PKI-based digital signatures, it’s important to remember that PKI technology has been available since 1976 and remains 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: Finally, most government entities 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 more, signature-dependent processes, a single, easy-to-use solution that can meet the requirements of all departments appeals to government executives, as they quickly realize that digital signature solutions can improve their operations while benefiting both their employees and the citizens they serve.
Making the Business Case for Digital Signatures in Government

Over the past few years, digital signature solutions have been adopted by forward thinking government organizations looking for effective, cost-efficient and secure signing processes. They have automated a wide range of signature-dependent processes in areas such as administration, engineering, procurement, human resources, public healthcare, legal departments, judicial systems, and many more.

Below are just a few examples of how digital signatures provide convenient, user-friendly and streamlined review and approval processes in various departments:

➢ **Transportation and Public Works**

For transportation and public works departments, a common pain point is found within the engineering department, which creates and modifies thousands of CAD drawings and change orders. Without digital signatures, drawings must be printed, signed and stamped with an engineering seal, and then physically transported for review and approval. With digital signatures, the documents can be printed to PDF, signed and stamped, and routed via email or workflow for review and approval. Digital signature solutions help these departments establish more efficient processes, expedite project schedules and significantly reduce paper-related costs.

➢ **Legal Departments**

Legal departments in governmental organizations draft and review vast volumes of documents, such as contracts and agreements, legal memos and resolutions. Attorneys, investigators, legal secretaries and other employees in the legal departments of local and state authorities use secure digital signatures to streamline a variety of processes. Contracts and agreements in particular lend themselves to the use of digital signatures, and organizations are now making use of self-hosted portals that allow external parties to review and sign documents that remain under internal control.

➢ **Court Systems**

Court systems worldwide have discovered how digital signatures ensure faster document processing, more efficient case management and reduced administrative workloads. By integrating digital signatures into existing work processes, courts can also enable electronic filing, allowing the process to start and stay electronic, thus reducing the need for scanning in paper documents. Judges, attorneys, and court clerks are also able to work remotely, preventing bottlenecks previously caused by the need for paper-based signatures.
Administration Departments

Internal administrative departments, such as procurement, human resources and finance, are often bogged down by paper-intensive approval and workflow processes that lead to costly delays which can easily be eliminated by automating signature-dependent processes. Digital signatures can be used to streamline a wide range of administrative processes - financial, payroll, records and taxation, human resources, and the entire requisition-to-payment process, among many others. For example, many organizations find that with digital signatures, the time it takes to process purchase orders can be reduced from weeks to a couple of days.

Archived Records

Due to the ever increasing threat of cyber-attacks, state and local government departments must ensure that their databases of archived records are impervious to malicious tampering. Batch-signing with a digital signature is being used by government entities to ensure that long-term records are preserved in their original form, and that any attempt to alter a signed document can be easily detected.

Point of Service

On the public-facing side, large numbers of signatures need to be captured at the point-of-service. The process is quick and simple: The government representative brings up a document on the screen and has the constituent sign it electronically on a signature pad. The representative then applies his or her own digital signature or seal, creating a binding document. The point-of-service process can be used in a wide variety of public-facing scenarios including public health organizations that require patient signatures, court houses that need to collect signatures from defendants and law-enforcement officers, constituents that must sign for permits and licenses, and many more.
Choosing the Right Digital Signature Solution

Prior to selecting the digital signature solution, there are several very important considerations that need to be kept in mind, both operational and technical:

» **Does it leave control in your hands?** The solution should be able to adapt to the specific processes, technologies, user management and authentication needs of your government organization — not the other way around. This provides you with the freedom to choose how to manage the digital signature solution in a way that best suits your internal regulations and standard operating procedures.

» **Does it enable you to sign the file types/content applications you 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 your existing content management applications?** The solution should be able to integrate directly into the electronic content/document management and/or workflow automation system of your choice, such as SharePoint, Laserfiche, OpenText, Oracle, Alfresco, Nintex, K2, etc.

» **Does it require you to route or save documents outside your IT domain?** For security purposes, the solution should ensure that your documents remain inside your domain and are never routed through, or saved on, external third-party servers.

» **Does it comply with the regulations that are relevant to you?** The digital signature technology should be based on internationally accepted standards that comply with the legal and industry-specific regulations that are relevant to your organization. If your organization needs higher level security, the solution should be validated for government agencies by NIST’s FIPS regulations.

» **Does it enable anyone 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, in order to verify who signed the document and whether it has changed since it was signed.

» **Does it provide web and mobile access?** The solution should allow users to sign using any device, whether they are 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 you to choose between an on-premises server and a managed cloud-based system so that you can set up the system according to your internal requirements.
Does it provide 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 work.
Best Practices for Selecting and Deploying Digital Signature Solutions

The best practice guidelines listed below need to be considered while evaluating digital signature solutions. Thinking through these issues ahead of time will ensure a much more efficient and effective implementation processes and maintenance procedures.

To help you through this process, we first need to define the elements that are a part of any standards-based digital signature solution:

- **Public-key (Asymmetric) Cryptography** – The technology behind standard digital signatures, it relies on two separate but linked keys, namely a private one and a public one.

- **Private Key** – The data used to create a digital signature. It binds the electronic identity of its owner with the document or data at hand, thus eliminating the possibility of having someone deny that it is their signature. This key must be kept private and maintained under the sole control of the legitimate owner, be it a natural person or a legal entity.

- **Public Key** – The data used to verify a digital signature. It is bound to the identity of the key owner in the form of a digital certificate (see below) and is made available to anyone who wants to validate the signed information.

- **Digital Certificate** – An electronic document that is used to confirm that a specific public key belongs to a specific individual or organization. It is issued to the key owner by a trusted Certificate Authority (CA) and includes the identity information of the key owner and the issuer, as well as certificate expiration date, key usage specification, public key value, and more.

### Selecting Digital Certificates

Choosing between the three basic types of digital certificates depends on the level of trust required by your organization. This in turn is based on the Certificate Authority responsible for issuing the certificate and for confirming the identity of the individual receiving it:

- **Individual Self-Signed Certificate** – The simplest form of certificate is one created by the user themselves using Microsoft Office or Adobe Tools. This form of certificate has limited value for regulated organizations since the user can say anything they want about their identity and can use any name or email address without this being verified.

- **Third Party Certificate** – There are a number of third party Certificate Authorities (CAs) that can confirm the identity of the certificate owner and issue his or her individual certificate. This may require face-to-face identification of the certificate owner, cross-validating his or her identity with an accepted and legal identity document (e.g., driver's license), or a review/audit of the organization's identity-proofing procedures by the CA.
• **Organizational Self-Issued Certificate** – A more advanced form of trust is achieved when the employer organization becomes the Certificate Authority. After the certificate owner has gone through an established and documented identity-proofing process, which is typically part of the hiring process, the organization creates and signs his or her certificate with an organizational (root) CA key.

### Managing Signature Credentials

The users’ signature credentials (private keys and digital certificates) need to be securely stored and managed to avoid misuse. There are two main approaches to this issue and the decision between the two should be made based on your organization’s needs, its existing infrastructure, and your choice of certificate type, as discussed in the prior section:

- **Decentralized approach** - Until a decade ago the only way to deploy a digital signature solution was to install the certificate and key either on each signer’s computer or on a physical token, such as a smartcard or USB device, that each signer had to carry around. This approach usually proved to be cumbersome, time-consuming and expensive, as the tokens had to be physically distributed, the certificates had to be renewed every year, and the certificates and keys had to be retrieved whenever an employee left the organization. An additional problem with this approach is that the organization has less control over the way the signature tokens are used.

- **Centralized approach** – This approach uses a central server to securely store and manage all signature credentials. The server enforces authentication in order to ensure that the end-user has sole control over his or her signature credentials. In fact, the server enables organizations to leverage their existing internal user management mechanism, such as Active Directory or LDAP, and to support two-factor authentication, as discussed below. In addition, this centralized approach greatly simplifies the management of the system, making it much more affordable and easier to deploy from both a technical and an operational point of view.

### Managing Users

The digital signature solution needs to be able to manage the users, either directly or (ideally) in automatic synchronization with an existing user management directory, such as Microsoft Active Directory, Novell/NDS and other LDAPs. This eliminates the associated costs of managing users in two separate systems, one for standard user management and one for the digital signature system.

User management needs to include the automated ability to enroll new users, create their keys, issue their certificates, and update/renew/revoke them when necessary. For example, an active user’s certificate needs to be renewed each time it is about to expire, using the same private-
public key pair or a newly created key pair (re-key). Conversely, if a user has left the company or if the private key is suspected to be lost or stolen, the associated certificate must be revoked. The user will no longer be able to sign but, as with pen and paper, any documents they have signed in the past will remain valid.

**Handling User Authentication**

You should select the user authentication method that best fits the security level your organization requires. The digital signature solution should be able to use the same authentication method already in use by the organization to access file servers, mail servers, applications, etc.

In the simplest terms, there are three types of factors that can be used for user authentication:

- “Something you know” such as a password
- “Something you have” such as a hardware token or smartcard
- “Something you are” such as fingerprint biometric

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/OTP). While much less common, three-factor authentication is also possible (for example, combining a password, a smartcard and biometric authentication).

**Identity Proofing the Signers**

While it is assumed that every government organization confirms the identity of employees at the time of hire, it is imperative to review these procedures in the context of issuing digital certificates that will be used to sign on behalf of the organization. Where appropriate, additional identity proofing may be necessary in organizations where higher levels of security and control are required to meet legal and risk requirements. By verifying the identity of a signer before providing a certificate or adding a digital signature, organizations can rest assured that their important documents are being signed by the real person represented in the signature. Identity proofing options include email verification, credit card verification, or 3rd party knowledge-based proofing services such as those offered by IDology, Lexis-Nexis and Experian, among others.

**Documenting Standard Operating Procedures (SOPs)**

Finally, you must not neglect documenting the standard operating procedures surrounding digital signature use in your organization and consolidating them in a single repository. Examples of procedures that should be established and documented include identity-proofing, signer enrollment/de-enrollment, training, authentication, identification of documents and
forms requiring signatures, information to be included in the signature block, use of graphical signature images, use of reason codes, and solution administration. Whether for the purpose of contingency, data breach and disaster recovery plans, quality control, or simply for the ease of training new users, thorough documentation of processes, procedures or methods is recognized as a sign of a quality organization. When each step is accurately detailed, continuity can be reliably maintained even if the individuals most familiar with the process become unavailable or leave the company.
Conclusion

All government organizations will sooner or later need to transition from paper-driven processes to electronic documents, processes and workflows. As part of this transition they will need to replace ‘wet ink’ signatures with their secure electronic equivalent. This is especially relevant in the short-term for the many government entities that are highly departmentalized, work out of multiple locations, administer large infrastructure and utilities projects, and manage engineering, legal, healthcare and judicial operations.

Digital signature technology provides the most secure form of electronic signature and presents a strong business case. Digital signatures help improve productivity, ensure security and increase responsiveness, while accelerating approval processes and eliminating the paper-related costs. An additional advantage is that digital signature solutions eliminate the traditional deployment challenges with the availability of easy-to-implement, centrally managed, and off-the-shelf solutions.

Thousands of government agencies and departments are already benefiting from implementing digital signature solutions. We encourage the reader to focus their research on standards-based solutions, to explore alternative vendor approaches to deployment, and to request demonstrations and hands-on user trials.