Arkansas Department of Information Systems
Arkansas Department of Finance and Administration

Title: Electronic Signature Standard
Document Number: SS-70-011
Effective Date:

Act 722 of 2007 requires state agencies to use or permit the use of electronic records and electronic signatures no later than June 2009. The Department of Finance and Administration and the Department of Information Systems were tasked with creating standards and policies governing the use of electronic signatures and this document serves as the technical standard. State agencies may comply with this standard or create their own standards pursuant to the legislation. Agencies determine the appropriate type of electronic signature for their transactions.

A determination of the level of risk involved in the agency's transactions will allow the agency to decide whether electronic signatures are feasible, and, if so, what type of electronic signatures are needed: digital signatures using a more secure PKI structure, or a less secure, but possibly less expensive type of electronic signature, such as an imaged signature along with a PIN number.

Technologies can mitigate risk by ensuring integrity of electronic information and ensuring the identity of a person signing electronic information while providing non-repudiation of that person.

Three determinations need to be made for each process during risk analysis:

- The importance of knowing the identity of the person who holds the ability to sign
- The importance of assuring that the person who signed, was in fact that holder that was originally trusted
- The importance that the document was unchanged since it was signed

Example 1:

A particular business transaction with a medium level of overall risk traditionally involves an acceptance and signing by a third party. The process owner provides a system to allow the end-user to accept and sign the agreement online.

It is very important that the signee is validated and their true identity is known. Therefore, the business process owner chooses a technology that provides a medium level of initial signee identification.

It is also important that the process owner can prove that the signee did sign the document with their chosen method. In other words, non-repudiation is necessary to protect from future adverse actions against the contract. Due to this need, the process owner chooses a technology that provides at least a medium level of assurance that the credential used was indeed the one which was assigned to the identified third party.

This particular process provides a document online for the third party to sign. It does not give them the opportunity to modify the document. Therefore, this process does not require that the integrity of the document is assured by the signing technology. The process owner determines a low level of record integrity is necessary.

An example of a technology which meets each of these requirements is a Medium Level X.509 Certificate.

Example 2:

A lawyer for an organization prepares a legal document to be sent to a third party for acceptance and signing. It is very important that the identity of the person who has the ability to sign is known. It is also important that the signature can be indisputably linked to the originally identified person. The organization's lawyer also wants to ensure that the document was not changed since its creation.

This process will utilize two sets of credentials. The organization's lawyer to assure the document has not changed will use one set. The other set will be used by the third party to agree to the terms of the document.

Set 1: Initially the organization's lawyer chooses a technology that will provide proof that the document has not changed since he created it. In this case, the initial signee validation is not important as the signee is the lawyer himself. However it is important that the lawyer can prove that his signature was the one used to secure and sign the original. It is also important that this technology provides a high level of integrity for the document. The organization's lawyer secures and signs the original document using a low level X.509 certificate.

Set 2: Since the identity of the accepting party is of critical importance to this process, the organization requires the third party to sign the document by using a high-level X.509 certificate.

The combination of these signature technologies provides integrity of the original document, validation of the third party, and non-repudiation of the third party signature.

Example 3:

An organization has a process which requires third-parties to accept a standardized agreement prior to receiving services from the organization. It is not of critical importance that the identity of the recipient be verified. It is also not of critical importance that the act of signing be indisputably linked to the initial verification of the third party. Due to the design of the system, changes the document by a third party are not possible, and therefore the integrity offered by the signature is of low importance.

For this process, the organization has chosen to utilize an electronic signature pad, which captures the written signature of the third party and electronically stores in a trusted database where it is associated with the document.

<table>
<tr><th colspan="3">Initial Signee Validation</th></tr>
<tr><td colspan="3">Description: This is the process used to initially authorize an individual to use a given method. This provides a level of assurance to the recipient that the signee's identity is known.</td></tr>
<tr><th>Validation Methods</th><th>Risk Mitigation</th><th>Examples</th></tr>
<tr><td>No validation beyond self-applied identification</td><td>Low</td><td>"Wet" signature, facsimile signature, self-applied digital signature, electronic signature pads Low Level X.509</td></tr>
<tr><td>Validation of Signee-supplied information with trusted data source</td><td>Medium</td><td>Entry of PIN pre-distributed to known address, assignment of a Medium Level X.509 certificate by validation of personal data known by signee, entry of verifiable personal data by signee</td></tr>
<tr><td>Validation of Signee through an established process involving physical presence or biometric validation of the Signee and proof of identity by trusted governmental documents or data sources</td><td>High</td><td>Assignment of a High Level X.509 through in-person proof of identity, enrollment or comparison of biometric data against trusted source</td></tr>
</table>

<table>
<tr><th colspan="3">Authentication (use) of Credential</th></tr>
<tr><td colspan="3">Description: This is the method used to ensure the credential was applied solely by the signee. This provides non-repudiation of the act of signing.</td></tr>
<tr><th>Authentication Methods</th><th>Risk Mitigation</th><th>Examples</th></tr>
<tr><td>None</td><td>Very Low</td><td>"Wet" Signature, Facsimile Signature, self-applied signature, electronic signature pads</td></tr>
<tr><td>Application of information known only to the signee</td><td>Low</td><td>Entry of PIN pre-distributed to known address, entry of pre-established password or other personal and verifiable information</td></tr>
<tr><td>Use of a cryptographic key or verifiable biometric</td><td>Medium</td><td>X.509 Digital Signature with or without a trusted hardware device such as a smart card or security token; a Biometric</td></tr>
<tr><td>Two-factor authentication</td><td>High</td><td>Combination of X.509 Digital Signature with a biometric (two-factor authentication)</td></tr>
</table>

<table>
<tr><th colspan="3">Integrity of Signed Record</th></tr>
<tr><td colspan="3">Description: This is the method used to ensure the signed record is in the original form, without modification, as signed by the signee.</td></tr>
<tr><th>Methods of Assurance</th><th>Risk Mitigation</th><th>Examples</th></tr>
<tr><td>Modification of data may not leave discernible evidence of tampering</td><td>Very Low</td><td>"Wet" Signature, Facsimile Signature, self-applied signature</td></tr>
<tr><td>System or application is reasonably trusted to invalidate signature upon modification of the record</td><td>Low</td><td>Electronic signature pads including a cryptographic or trusted invalidation feature, trusted applications or systems which provide auditable tracking of modifications and invalidation</td></tr>
<tr><td>System or application is reasonably trusted to invalidate signature upon modification of the record and which provide a secure method to transfer and store the signed record</td><td>Medium</td><td>SSL or VPN transport of signed record and encrypted storage of signed record in addition to a low risk method of integrity assurance</td></tr>
<tr><td>Verifiable cryptographic hash or encryption of signed record</td><td>High</td><td>X.509 Digital Signature or trusted biometric process which includes verifiable cryptographic hash of signed record</td></tr>
</table>

Digital Certificate Levels of Assurance	
Description: This defines the requirements for each level of X.509 certificate.	
Level	**Description**
Low Level X.509 Certificate	Identity of issuee of digital certificate is not verified.
Medium Level X.509 Certificate	Identity of issuee of digital certificate is verified through comparision of issuee provided data with known and trusted data.
High Level X.509 Certificate	Identity of issuee is verified by physical presence of the issuee to the CA organization or a state-recognized notary, along with government-issued documents sufficient to verify identity.

Related document: Policy Statement on the Use of Electronic Signatures by State Agencies