State of Arkansas
Policy Statement on the
Use of Electronic Signatures by State Agencies
June 2008

Background
In the last ten years Arkansas has enacted several laws to facilitate electronic transactions in State government and to make government more accessible to its citizens. In 1999 the Arkansas Electronic Records and Signatures Act was passed (A.C.A. §25-31-101 et seq.) to promote the development of electronic government and commerce. Following the passage of the federal Electronic Signatures in Global and National Commerce (E-Sign) Act (U.S. Public Law 106-229) in 2000, Arkansas passed its own Uniform Electronic Transactions Act or UETA (A.C.A. §25-32-101 et seq.) in 2001. Act 722 of 2007 requires state agencies to permit the use of electronic signatures by June 2009. The responsibility for the adoption of standards and policies lies with the Department of Finance and Administration and the Department of Information Systems. The following policy statement is the result of a collaborative effort between these two agencies.

Purpose and Scope
This document is intended to provide guidance to state agencies to evaluate new and existing electronic signature transaction processes pursuant to the UETA. The goal is to assist agencies in assessing the benefits and risks of using electronic signatures, determining whether their use is appropriate for the agency's business needs and ensuring that they can be used with an appropriate level of assurance of authenticity. The policy statement is designed to be a tool and framework for agencies to follow when determining the best course of action.

Definitions
Asymmetric crypto-system: an electronically processed algorithm, or series of algorithms, which uses two different keys where one key encrypts the message, one key decrypts the message and the keys do not allow one key to be discovered through the knowledge of the other key.

Certificate: an electronic document attached to a public key by a trusted certification authority, which provides proof that the public key belongs to a legitimate subscriber and has not been compromised.

Certification Authority: a person or entity that issues a certificate.

Digital Signature: a type of electronic signature that relies on a public key infrastructure (PKI) to provide a unique identifier and link the signature to the record, authenticating both the signer and the document.

Electronic Signature: an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. The term "electronic signature" is often confused with that of a "digital signature." However, a digital signature (defined above) is a specific type of electronic signature. The definition for "electronic signature" is not technology-specific; it does not require the use of any particular hardware or software application, but allows for any technology that can properly authenticate the signer and the signed document. It can include the use of such technologies as email (using a personal identification number), faxes and imaging, or more exotic technologies like biometrics (such a iris scans).

Key Pair: a private key used to create a digital signature, and its corresponding public key used to verify a digital signature in an asymmetric crypto-system.

What is a Public Key Infrastructure (PKI)?

Digital signatures generally use a public key infrastructure technology based on a "key pair" managed by a trusted third party called a "certification authority": a private number or "key" belonging to the sender and used to create the signature, and a mathematically related public "key" made publicly available and used by the recipient to validate the authenticity of the signature. In effect, the certification authority uses a mathematical operation involving the content of the message and the signer's private key and attaches the resulting digital signature to the original message. This process 1) authenticates the signer, since only the owner should have access to both the private key and the message, and 2) verifies the integrity of the original message, since any subsequent changes to the message would invalidate the signature.

Issues to Consider

1) Agency Business Needs

It is important first for the agency to clarify the reasons for using electronic signatures. Do the current electronic records need to be signed at all, and, if so, by what electronic method? What business needs will be met by this technology? The agency should consider:

- The public need for accessibility;
- Who will use and rely on the electronic signatures;
- The potential reduction of transaction costs and saved staff time;
- The initial cost for system design, development and implementation;
- The cost of management and preservation of electronically-signed records over time;
- Whether electronically-signed transactions will provide similar functions as were provided by paper transactions;
- How electronically-signed transactions fit into the agency's and the state's overall technology architecture;
- State and federal laws applicable to the agency's transactions. It is important to consult with legal counsel; and
- The financial and legal risks to the agency as outlined below.

2) **Risk Assessment**

Types of transactions: The agency should evaluate the risk involved in the types of transactions it performs. Consideration should be given to:

- The dollar value of the transactions;
- The value of the information to outside parties;
- The relationship between the parties to the transaction:
  - Intra or inter-state agency transactions (within the agency, or between state agencies): these involve relatively low risk of later repudiation.
  - State agency and local or federal government: these involve relatively low risk, especially if they are routine in nature.
  - State agency and private organizations or individuals: these transactions involve the highest level of risk, especially if a transaction is one-time only and there is no on-going relationship between the parties.
- The risk of intrusion on the transaction: higher risk is associated with regular transactions than with intermittent or unpredictable transactions; and
- The nature of the agency's mission: some agencies may deal with more sensitive subjects than others.

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.

General risks: Secondly, the agency should consider the general risks involved in the use of electronically-signed records:

- The likelihood of legal challenges to the records;
- The potential financial or political loss to the agency if the trustworthiness of its electronically-signed records could not be documented; and
- The need for information at a later date: Would the conversion from a paper system to an electronically-signed transactions system mean the loss of needed information, such as postmarked envelopes? Will the long-term maintenance of electronically-signed documents involve expensive conversions through multiple software and hardware systems? Can the system under consideration re-validate electronic signatures at a later date?

Checklist for Digital Signature Technology

If, after following the cost-benefit analysis and risk assessment procedures outlined above, an agency decides to implement a digital signature system, the agency should consider these suggestions:

1) Become familiar with the technology issues related to digital signatures and PKI service providers. The American Bar Association's publication "Digital Signature Guidelines" offers detailed technical and legal information about public key encryption systems. It is available on the ABA's website. Also, the National Institute of Standards and Technology (NIST) has published "Minimum Interoperability Specifications for PKI Components", which can be found on the NIST website. Agencies doing business

nationally or internationally should be aware that most states have enacted UETA statutes and widely use electronic signatures, and many foreign countries, especially in Europe, have signed mutual agreements recognizing common signature security requirements.

2) Choose an acceptable technology and Certification Authority (CA). Arkansas does not currently limit state agencies to a specific list of acceptable CAs. However, agencies may obtain a list of registered CAs (or "electronic signature verification companies") from the Secretary of State's Business and Commercial Services Office. As of June 2008 there was only one registered company, in part because of the $250,000 surety bond requirement in A.C.A. §25-31-103(2).

   State agencies should carefully evaluate each CA to determine whether it meets the standards set by the American Institute of Certified Public Accountants Statement on Auditing Standards No. 70, and whether the technology it offers is suitable for the agency's particular security needs. Consider hardware and software obsolescence, and interoperability with other state, local, federal and private entities. Agencies should remember that no technology will completely address all legal requirements. However, a reliable CA is crucial to the reliability and security of the digital signatures it manages. Consult the NIST website for technical guidance and publications on the security and interoperability of PKI components.

3) Consult with all levels of agency management in the decision. Records managers and auditors will play an important part in system design.

4) Consider whether the agency's overall records retention schedule needs to be revised, and develop plans for the retention and disposal of all digitally signed records.

5) After implementation, validate that the system has operationally achieved the required assurance level. Then periodically reassess to determine whether the business needs have changed or technology updates are needed.

Summary

An agency's selection of an appropriate electronic signature technology means assessing business needs, costs, benefits and risks, and then determining if the system and application meet those criteria. Where feasible, state agencies are encouraged to use electronic signatures to improve efficiency and access to government information and services.

Addendum: DIS Technical Standard for Electronic Signatures

This document serves as the technical standard for agencies to use as a tool for electronic signatures. State agencies may comply with this standard or create their own standards pursuant to the legislation by determining 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, or that the act of signing be indisputably linked to the initial verification of the third party. Due to the design of the system, changes to 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.

The following three tables describe the methods or procedures used for proper verification of electronic signatures in various situations and the associated risk:

Initial Signee Validation		
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.		
Validation Methods	**Risk Mitigation**	**Examples**
No validation beyond self-applied identification	Low	"Wet" signature, facsimile signature, self-applied digital signature, electronic signature pads Low Level X.509
Validation of Signee-supplied information with trusted data source	Medium	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
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	High	Assignment of a High Level X.509 through in-person proof of identity, enrollment or comparison of biometric data against trusted source

Authentication (use) of Credential

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.

Authentication Methods	Risk Mitigation	Examples
None	Very Low	"Wet" Signature, Facsimile Signature, self-applied signature, electronic signature pads
Application of information known only to the signee	Low	Entry of PIN pre-distributed to known address, entry of pre-established password or other personal and verifiable information
Use of a cryptographic key or verifiable biometric	Medium	X.509 Digital Signature with or without a trusted hardware device such as a smart card or security token; a Biometric
Two-factor authentication	High	Combination of X.509 Digital Signature with a biometric (two-factor authentication)

Integrity of Signed Record

Description: This is the method used to ensure the signed record is in the original form, without modification, as signed by the signee.

Methods of Assurance	Risk Mitigation	Examples
Modification of data may not leave discernible evidence of tampering	Very Low	"Wet" Signature, Facsimile Signature, self-applied signature
System or application is reasonably trusted to invalidate signature upon modification of the record	Low	Electronic signature pads including a cryptographic or trusted invalidation feature, trusted applications or systems which provide auditable tracking of modifications and invalidation
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	Medium	SSL or VPN transport of signed record and encrypted storage of signed record in addition to a low risk method of integrity assurance
Verifiable cryptographic hash or encryption of signed record	High	X.509 Digital Signature or trusted biometric process which includes verifiable cryptographic hash of signed record

The following table describes the levels of assurance of the authenticity of electronic signatures and the corresponding certificates:

<table>
<tr><th colspan="2">Digital Certificate Levels of Assurance</th></tr>
<tr><td colspan="2">Description: This defines the requirements for each level of X.509 certificate.</td></tr>
<tr><td><b>Level</b></td><td><b>Description</b></td></tr>
<tr><td>Low Level X.509 Certificate</td><td>Identity of issuee of digital certificate is not verified.</td></tr>
<tr><td>Medium Level X.509 Certificate</td><td>Identity of issuee of digital certificate is verified through comparison of issuee provided data with known and trusted data.</td></tr>
<tr><td>High Level X.509 Certificate</td><td>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.</td></tr>
</table>

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