South Carolina
Enterprise Architecture

Uniform Electronic Transactions Act

SC Standards for Electronic Signatures

February 28, 2007

Table of Contents

1.0 Standards

1.1 Applicability and Scope

Background

The standards promulgated in this document were created in an effort to comply with the purpose and intent of the Uniform Electronic Transactions Act (UETA - S.C. Code Ann. 26-6-10 et seq.). South Carolina Code Section 26-6-190 of UETA, entitled Development of standards and procedures; service of process, states, in part:

> The South Carolina State Budget and Control Board shall adopt standards to coordinate, create, implement, and facilitate the use of common approaches and technical infrastructure, as appropriate, to enhance the utilization of electronic records, electronic signatures, and security procedures by and for public entities of the State. Local political subdivisions may consent to be governed by these standards.

Applicability

As UETA states in S.C. Code Section 26-6-190, the standards set forth in this document are applicable to all State government entities including agencies, boards, commissions, colleges and universities. Local government entities may, at their option, consent to be governed by these standards. Model procedures for the use of electronic records, electronic signatures, and security procedures for private commercial transactions and contracts may be developed, implemented and facilitated by the Secretary of State. Such model procedures addressed in this document may prove applicable for this purpose.

Scope

The UETA does not require State government entities to utilize electronic records or electronic signatures. The extent that State government entities do use such records or signatures, they are subject to these standards (UETA, S.C. Code Section 26-6-180). The purpose of this document is to define the responsibilities and procedures to be used by State government entities when establishing and implementing electronic signatures with regard to the authentication, security, non-repudiation and integrity of such electronic signatures and the electronic records which are to be considered as signed.

Development, Periodic Review and Updating of these Standards

In November 2005, the State Budget and Control Board established a Task Force composed of subject matter experts from a number of state agencies to develop the standards set forth herein. This Task Force submitted its recommendations to the State's Architecture Oversight Committee (AOC) for review, evaluation and adoption. The AOC submitted final recommendations to the State Budget and Control Board, which shall be responsible for maintaining and updating these standards on an ongoing basis. The Task Force has been converted to an UETA Advisory Committee to provide ongoing comments, feedback and advice in this effort.

The Architecture Oversight Committee (AOC), by requiring these standards, does not state or provide the means of funding the assessment, establishment, implementation, or operation of electronic signatures or the electronic transactions which use electronic signatures.

1.2 Applicability to Transactions

The Uniform Electronic Transactions Act (UETA) defines an electronic signature as "*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*." This broad definition becomes problematic when considering the possible types of electronic records as defined by UETA. An electronic record is "*a record created, generated, sent, communicated, received, or stored by electronic means*." This definition includes not only database records and network-based or web-based data exchanges, but also emails, fax transmissions, voice mails, PDA communications, tape backups and so on. Fax transmissions, voice mails, PDA communications, and tape backups are out of the scope of these standards.

There are four important parts to an electronic signature: 1) an electronic sound, symbol, process, etc. which is unique to the signer; 2) the agreement, either implied or explicit, by both parties to accept an electronic sound, symbol, process, etc. as a valid signature; 3) the intent to sign the record and 4) the action of applying the electronic signature to a specific document or record. These are discussed in greater detail below.

The phrase in UETA "with the intent to sign the record" presupposes that a signature is desired. Fortunately, not all types of electronic records require an electronic signature, nor do they require one to be permanently stored. By their nature, many electronic records do not require a signature, as no contractual, financial or confidential information is being exchanged. Other electronic records, such as a PDF created from a signed paper document, fulfill the requirements of an electronic signature as an intrinsic part of their structure.

The presence of an electronic signature presumes the originality of the record that has been signed. Electronic records must have an authoritative version, which may be treated as an original record, whether or not there are multiple copies of that record. To clarify further, during progressive processing of an electronic record, any information that is added or changed must create a new version of the record, to which the original signature no longer applies. This new record may be stored as (a) separate, duplicate or ancillary record(s). The version to be treated as an original signed version may not change. The new record may in turn be signed, creating a new, separately verifiable electronic signature.

1.3 Standards for Electronic Signatures

All programs implemented by State government entities which utilize electronic signatures shall meet the following conditions. The degree to which these conditions are met will vary by program, as dictated by law or regulation, by risk to the program, or by desire of the participants. Later sections will discuss each of these conditions in greater detail.

> **Use of signature unique to the signer:** The electronic signature must uniquely identify the signer, and must be under reasonable control of the signer. That is, it must be unlikely that any other unauthorized entity provided the signature.
>
> **Agreement by the parties:** A party signs a document in order to convey a mutually understood message to another party, such as authorship, receipt, or approval of the document. In the case of an electronic signature, both the signer and the intended recipient of the signed document must agree, either explicitly or implicitly, that the

electronic sound, symbol, or process will serve as a signature for the electronic document or record.

Intent to sign: The application of the electronic signature to the electronic record must be an intentional act. Intent can be determined by the contents of the document or record and the facts and circumstances surrounding the transaction.

Association of the signature with the signed record: The electronic signature must be physically or logically associated with the electronic record that is signed, and that association must persist for as long as the signature is in effect, which may be the life of the record.

The degree to which each of the above conditions is met is dependent on several factors normally associated with security concerns:

- **Authentication:** the ability to prove that the actual signer is the intended signer,
- **Non-Repudiation:** the inability of the signer to deny the signature, and
- **Integrity:** the assurance that neither the record nor the signature has been altered since the moment of signing.

However, it is important not to confuse the strength of the electronic signature with the strength of the security surrounding a given transaction. For example, an electronic record signed with a digital signature utilizing public key infrastructure (PKI) may be transmitted without authorization over an unsecured network, while a record signed with a weak password may be transmitted in encrypted format over a highly secured line.

Note that this standard does not deny or supersede the implementation standards established by law, regulation, or qualified body for any specific program, such as an IRS / State program or a program governed by HIPAA regulations. Rather, this standard for South Carolina governmental entities is intended to provide a framework for such program specific standards, and to provide governance where no such external standards are in place.

1.4 Use of Signature Unique to the Signer

The electronic sign, symbol, or process serving as the electronic signature must uniquely identify the person, business, agency, or system which is the signer of the electronic record, and be under the reasonable control of that party. The most commonly used form of identification in electronic transactions is the Personal Identification Number (PIN) or password, either assigned arbitrarily to the party by a service provider or self-selected by the party, and used in conjunction with a unique user identification. This PIN or password serves as an electronic signature either by being entered in response to a request to sign a transaction, or by the party's executing an action with intent to sign, while authenticated by the PIN or password. The longer and more complex (use of alpha, numeric, and special characters) the PIN or password is, the less likely that it can be replicated by an unauthorized party. However, the uniqueness of the PIN or password to a given party is still dependent on the security measures taken by the party. The strongest password loses any characteristic of authentication or non-repudiation if it is posted on a sticky note in plain view.

For an individual signer, the strongest form of electronic signature is based on some inherent physical characteristic of the person. A digitized version of a hand-written signature is the simplest example of this class. More sophisticated biometric signatures, such as a digitized fingerprint, retinal scan, or voice print, require more costly technology not readily available at time of this writing to the general public.

For a business, agency, or computer system, the most secure form of electronic signature requires the application of a public/private key pair, often referred to as Public Key Infrastructure (PKI). The business acquires a digital certificate from a Certificate Authority, and installs it on a computer system under secured control. The business or agency utilizes its uniquely assigned private key to sign an electronic record, and the electronic signature generated by this process becomes an intrinsic part of the electronic record. While a digital certificate can be assigned to an individual, this is not general practice, in part because a household computer system is generally shared by multiple parties.

The nature of the sound, symbol, or action to be utilized by a South Carolina agency in a program requiring electronic signatures will depend on several factors. One is the risk to the program of unauthorized or repudiated transactions, and the likelihood of the need to verify the signature in a contested context, such as a court of law. This risk must be balanced against factors of cost and availability of the means of signing for the intended population of signers. A technology which is cost justifiable for a bounded, controlled population such as agency employees or a small, known constituent base, may not be feasible for an unknown and unbounded general public.

It must be noted that while the signing party bears primary responsibility for maintaining control of the means of creating the electronic signature, the recipient of the electronic signature also bears a responsibility to protect the signature on behalf of the signer. For example, an agency that issues PINs or supports PIN self selection must protect those PINs from access by parties who might make unauthorized use of them.

1.5 Agreement by the Parties

For an electronic signature to be valid, both the signing party and the recipient party must agree that the sound, symbol, or process will in fact serve as a signature for the electronic record in question. This agreement may be either formal or informal, and can be determined from the context and surrounding circumstances, including the conduct of the parties. In the business world, electronic commerce is generally established between two parties by means of a Trading Partner Agreement (TPA). The Trading Partner Agreement (TPA) establishes the normal terms and conditions under which the transactions may occur; it sets forth the terms required by the nature of the electronic transaction; and it defines what will constitute a signature if electronic record(s) are to be generated and signed in the course of the transaction. Partners must understand what aspects of an electronic signature are to be implemented, and must understand their responsibility in working with, recognizing and preserving the electronic signature and the associated electronic record(s). In the context of two governmental agencies, whether both agencies are at the state level or at differing federal, state, or local levels, such an agreement is often known as a Memorandum of Understanding or MOU.

For governmental programs involving the general business community or individual constituents, it is not reasonable for an agency to negotiate separate agreements with each party. In this case, the agreement is generally issued unilaterally by the agency through legislation, regulation, or program documentation. Participation in the program by the business or individual party then constitutes acceptance of the agreement and of the program parameters. In all cases, however, there should be advance notice that a sound, symbol, or process generated by the business or individual will be considered to be a valid electronic signature for an electronic record. The simplest form of such notice, in the context of an online transaction, may be wording or a pop-up box on the screen explaining that a subsequent action will be considered to be an act of signing.

1.6 Intent to Sign

There can be no electronic signature without the intention to execute or adopt the sound, symbol or process for purposes of signing the related document or record. There is a sequential relationship between the agreement by the parties and the act of signing: there is agreement that a certain action will create or serve as an electronic signature, and then that action is intentionally executed. An electronic signature may be created by the signing party or on behalf of a party by an authorized agent, including an electronic agent.

In order to reduce the uncertainty regarding the intent to sign, there should be a prior agreement (or notification) that the execution of the transaction will constitute a signature, followed by the action itself executed with intent to sign. For example, the intent to sign may be demonstrated by a simple mouse click in an online transaction, in response to an on-screen notification that the action will constitute an act of signing. In this case, the signer is generally logged onto an application using credentials such as a user identification and PIN or password, and those credentials may become logically associated with the transaction record to constitute the electronic signature. However, it must be noted that, without the requisite intent to sign, merely executing an online transaction while authenticated by means of certain credentials does not in itself constitute an act of signing, even if those credentials can be associated with the transaction record.

An expression of intent to sign may cover multiple applications of an electronic signature; for example, a system may be programmed to apply a digital signature to all electronic records of a certain type.

1.7 Association of the Signature with the Signed Record

An electronic signature has value only in the context of an electronic record. It may signify that an electronic record is acknowledged or approved, that its contents are agreed to, or that the record is authentic. In the case of the record of a transaction, it may signify that the transaction was properly authorized. The value lies in the ability to verify the signature, and therefore reaffirm its significance to the electronic record, at a later date. For this reason, the electronic signature must be physically or logically associated with the electronic record for the lifetime of the electronic record.

Corollary to this requirement is the assumption that neither the electronic record nor the electronic signature itself is altered during this timeframe. A program utilizing electronic signatures should therefore implement appropriate security measures at both the originator of the signature and the recipient of the signature to prevent unauthorized alteration to either the electronic record or the electronic signature. The nature of these measures may be dictated by external governance, as in the case of an IRS or HIPAA program. If the application of security is at the discretion of the participating South Carolina agency or agencies, then the nature of the security measures should be commensurate to the risk and consequences of unauthorized alteration. A risk assessment should be performed early in the development of the program, in order to determine appropriate security measures to protect the electronic record and electronic signature both during transactions and in subsequent storage.

The simplest of these measures is to ensure that access controls are in place to prevent unauthorized access to modify or delete the electronic record and electronic signature. Stronger measures include the use of unalterable media such as write-once, read many (WORM) disks to store the electronic record and electronic signature. One of the strongest detection measures is the use of digital signatures, where an algorithmic hash of the electronic record is encrypted using the private key of the signer. In this case any alteration to the electronic record by a party not in possession of this private key will invalidate the digital signature, because the digital signature, when decrypted with the signer's public key, will not yield the hash of the altered record.

2.0 Examples

The standard for electronic signatures for South Carolina governmental agencies does not dictate the use of any specific technologies or authorize any specific models for implementation. This is done for two reasons: first, because the array of technologies and implementation models for the use of electronic signatures is extremely large, and would not provide useful guidance for all situations, and secondly so that the technology-neutral standard will not require modification or become invalidated by the invention or adoption of future technology. However, in order to provide some measure of guidance, the following examples of the use of electronic signatures are offered as illustration of the standard.

2.1 Digitized Human Signature

A digitized signature is a graphical image of a handwritten signature. Some applications require an individual to create his or her handwritten signature using a special computer input device, such as a digital pen and pad. The digitized representation of the entered signature may then be compared to a previously-stored copy of a digitized image of the handwritten signature. If special software judges both images comparable, the signature is considered valid. This application of technology shares the same security issues as those using the PIN or password approach, because the digitized signature is another form of shared secret known both to the user and to the system. The digitized signature can be more reliable for authentication than a password or PIN because there is a biometric component to the creation of the image of the handwritten signature. Forging a digitized signature can be more difficult than forging a paper signature since the technology digitally compares the submitted signature image with the known signature image, and is better than the human eye at making such comparisons. The biometric elements of a digitized signature, which help make it unique, are in measuring how each stroke is made (duration, pen pressure, etc.). As with all shared secret techniques, compromise of a digitized signature image or characteristics file could pose a security (impersonation) risk to users.

2.2 Online Tax Filing

The South Carolina Department of Revenue (DOR) offers a web-based application to allow individuals to file their Individual Income Tax returns online. Users are authenticated by means of a pre-assigned PIN which is sent by the DOR to the taxpayer's address of record. At the conclusion of the filing transaction, the user is presented with a "jurat" (Latin for "been sworn") affirming that the information is true and accurate. The user is then prompted to re-enter the PIN as a signature to the jurat and thus the return. By re-entering the PIN, the taxpayer accepts the agreement for that PIN to serve as an electronic signature, and indicates an intent to sign. This use of the PIN therefore constitutes a valid electronic signature.

By contrast, DOR also offers a web-based application to allow businesses to file their Sales and Use Tax returns online. The user must be authenticated by means of a user identification and self-selected PIN prior to utilizing the application. However, the application does not present any jurat to the taxpayer or ask for re-entry of the PIN, nor does it state at any time that any subsequent action will be considered as an act of signing. For this reason, although the online filing is legal and binding, and although proper authentication is required, the transaction is not considered to have been signed.

2.3 Federal / State Tax Filing

When a taxpayer files an electronic income tax return using commercial software such as TurboTax ® or utilizes a paid preparer such as H&R Block, both the federal and state tax returns are transmitted to the IRS. The IRS, in turn, splits off the state returns and transmits them to the participating states.

The electronic returns are signed by various means, as part of the transaction between the taxpayer and the tax preparer or host of the commercial software, and subsequently the IRS. The DOR considers those returns to be signed, even though the signatures are not verified on receipt by the DOR. This example serves to illustrate the difference between electronic signatures and transactional security. There are a number of security measures in place governing the transactions between the DOR and IRS to retrieve the South Carolina tax returns. However, the authentication of these transactions has nothing to do with the original taxpayers' electronic signatures which are associated with the transmitted electronic records.

3.0 Additional Considerations for Electronic Signatures

3.1 Risk Assessment

Risk Assessment: A risk assessment should be performed to determine the best means of implementing electronic signatures and the level of security for the type of program. This assessment should take into consideration the following issues:

- The nature and value of the data and records in the transactions. Differing types of data and records will have different requirements. Data and records which fall under HIPAA requirements, for example, will have much stricter requirements than some other types of data and records.
- The susceptibility of the transaction's data to fraud. Some data will be of a higher profile, and possibly more susceptible to fraud than other types of data.
- The type of communication for the transactions.
- The security of the systems which host the transaction processes and data.
- The reliability of the systems which host the transaction processes and data.
- The consequences of successful fraud for participants, their organizations and the system(s).
- The role and authority of the user base, especially on those systems where there are multiple levels of authorization on the data.
- The existing technology base and the cost of technology.
- The required level of confidence in establishing the users' identity.
- The required level of communication integrity.
- The required level of record integrity.
- The required level of non-repudiation for records.

Risk Mitigation Plan: After the possible risks have been identified, a risk mitigation plan must be created. This plan will ensure that for all known risks, action will or can be taken to resolve the risk, mitigate the risk, or have a contingency for the risk. Critical risks should be resolved fully prior to proceeding with the implementation. The risk mitigation process should be fully documented.

3.2 Additional Features

There are several additional implementation features of electronic signatures that are not included in the South Carolina standard (as defined in section 1), as they may not apply to all implementations.

These features can fulfill specific business requirements in certain types of business transactions. In some cases, they mimic the process that exists when working with paper documents.

- **Continuity of signature capability:** The ability to ensure that public awareness of the means or technology used to create or apply an electronic signature, such as the identification of the algorithm utilized, does not compromise the ability of the signer to apply additional secure signatures at a later date.
- **Countersignatures:** The capability to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where a party signs a document that has already been signed by another party. In an electronic signature, the

issue of record originality must be considered, especially if a copy of the record(s) is made during the process of applying a countersignature.

- **Independent verifiability:** The capability to verify a party's signature (electronic record or digitized signature) without the cooperation of the signer.
- **Interoperability of Electronic Signature Technology:** The assurance that applications, systems or other electronic components used during phases of communication between trading partners and/or between internal components of an entity, are able to read and correctly interpret the transaction information communicated from one to the other.
- **Multiple signatures:** The capability of multiple parties to sign an electronic record, document or transaction. Conceptually, multiple signatures are simply appended to the document or record. Depending upon the implementation, the issue of originality may arise.
- **Data Transportability:** The ability of a signed document to be transported over an insecure network to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

4.0 Definitions

AOC: The Architecture Oversight Committee is the governing body of the South Carolina Enterprise Architecture.

Authentication: The use of passwords, tokens (such as smart cards), digital certificates or biometrics to verify that an entity is the one claimed.

Authorization: The process of granting an entity permission to do or have something, or of verifying that permission at time of action.

Ciphertext: The representation of encrypted information. This text may be viewable, but requires decoding. For example, a decryption algorithm is required to convert the ciphertext back into plaintext or its original form.

Credential: A credential is a set of data used for user/system authentication, which is established during a registration process, is stored in an identity management system, and is retrieved for comparison during an authentication process. In some cases, a credential is as simple as a login id and password. Examples of more complex credentials include digital certificates, electronic profiles of a user, a One-Time-Password device, a hardware token, or a biometric device (with the storage of biometric information for a user).

Digital Certificate: A digital certificate is an electronic record issued to a properly authenticated individual or organization by a Certificate Authority (CA). The digital certificate contains a mathematically related pair of encryption keys assigned uniquely to the individual or organization. The "public key" is published by the CA, so that any party may use it to encrypt data intended for the individual or organization. The "private key" must be kept secured by the individual or organization, and is used to encrypt data which can only come from the individual or organization. The digital certificate is installed on a computer system or server controlled by the individual or organization, and is utilized by various communication services, such as web browsers and communication protocols, to perform encryption and decryption services.

Digital Signature: A digital signature is an electronic record created by the mathematical operation of a private encryption key on an electronic record or document. A short record or "digest" is created from the original record or document. The digest is then encrypted with the private key to create the digital signature. The digital signature is generally appended to the document or record for transmission. A digital signature may be verified by the receiving party by decrypting it with the sender's public key, and then comparing the resulting short record with the digest of the transmitted record or document. Digital signatures are considered among the strongest forms of electronic signature for two reasons: 1) they can only be created by an entity's private key, so they are difficult to repudiate, and 2) they are based on a mathematical reduction of the original record or document, so that they cannot be validated if the transmitted record or document is altered in any way.

DOR: Department of Revenue

Electronic Agent: An electronic signature may be created by an electronic agent on behalf of a person. An electronic agent may take the form of software that performs automated processes. An application which accepts electronic signatures from an individual may also need to be configured to authenticate and authorize electronic agents, and to record an electronic signature with the electronic agent as the signer. Note that a computer application may also create an electronic signature on its own behalf, without reference to any specific person.

Electronic Record: A record created, generated, sent, communicated, received or stored by electronic means.

Electronic Signature: Means 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**.**

Embedding: The inclusion or linking of electronic signature elements into the electronic record to which the signature applies.

Encryption: The transformation of confidential plaintext or other information into ciphertext to protect it. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted. Decrypting data reverses the encryption algorithm process and makes the plaintext available for further processing.

HIPAA: Health Insurance Portability and Accountability Act (Pub.L. 104-191, Aug. 21, 1996)

Integrity: The means to ensure that data is complete and unaltered despite aging, transmission, duplication, migration, encryption, decryption or restoration.

IRS: Internal Revenue Service

Jurat: Latin for “been sworn”. It pertains to not just affirming the signature is yours but also to swearing the information represented is true and accurate.

Non-repudiation (or non-reputable records): A security feature under which the origin of data cannot be denied, and can be proven to an independent third party.

Password: The confidential authentication information composed of a string of alpha-numeric and / or special characters, whose specific requirements may vary by application, used during an authentication process.

PDA: Personal Digital Assistant (e.g., a Palm Pilot or other handheld electronic equivalent)

PDF: Portable Document Format. A electronic format to convey the image of a document. It is often viewed with Acrobat Reader.

PIN: Personal Identification Number

PKI: Public Key Infrastructure

Record: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

UETA: Uniform Electronic Transactions Act. (S.C. Code Ann. Section 26-6-10 et seq.)

http://www.scstatehouse.net/code/titl26.htm

WORM: Write Once Read Many. A type of data storage that when once the data is stored, the data cannot be changed.