South Carolina

Electronic Signatures
Analysis and Implementation Guide

March 28, 2007

Proposed by the UETA Task Force,
to the
South Carolina Architecture Oversight Committee

South Carolina

Table of Contents

1. Revision History

First Draft	January 11, 2007	George Felix
Revision	January 31, 2007	Terry Garber
Revision	February 6, 2007	Terry Garber
Revision	February 26, 2007	Terry Garber
Revision	March 6, 2007	Terry Garber

2. Document Overview

This Analysis and Implementation Guide for electronic signatures is intended to assist South Carolina state agencies wishing to implement an electronic commerce program for which signatures are required or desired. It expands upon the foundation of the South Carolina Uniform Electronic Transactions Act provided in the UETA Standards for Electronic Signatures document, hereafter referred to as "the Standards." (UETA SC Standards for Electronic Signatures.doc). For definitions of terms used in this document, please refer to the Standards.

The Standards propose that the validity of an electronic signature is dependent upon four factors:

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 that the electronic sound, symbol, or action will be accepted as serving as a signature for the electronic document or record.

Intent to sign: The application of the electronic signature to the electronic record must be a deliberate act. It cannot be implied or inferred.

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.

This document expands on each of these four factors, and explores some of the implementation considerations in each of the four areas.

3. Purpose of a Signature

Signatures are intended to be used to attest:

a. the identity of the person,
b. to the truth and accuracy of information provided, often under penalty of law, and/or
c. to the terms of an agreement (e.g., a contract).

Depending on the circumstances, the signature can be attesting to only one of the above, a combination of any two of the above, or all three.

In the context of an electronic transaction, an electronic signature may be used to attest:

a) the identity of one or more parties to the transaction,
b) to the truth and accuracy of information provided, often under penalty of law,

c) to the terms of an agreement (e.g., a contract) being established by the transaction, and/or
d) to approval to proceed with the transaction (e.g. to file a tax return or charge a credit card).

An electronic signature does not exist in a vacuum; there must be an electronic record which is signed by the electronic signature. This record may exist prior to the transaction, for example, an electronic tax return transmitted to the Department of Revenue by the IRS. It may be created by the transaction, for example, a tax return created by a South Carolina electronic filing application. Or, it may simply be the log or audit record of the transaction itself. In any case, the effectiveness of the signature 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
- **Integrity:** the assurance that neither the record nor the signature has been altered since the moment of signing.

Before using this Analysis and Implementation Guide, the first logical question that agencies must ask is whether their electronic records must be signed at all. As stated in South Carolina's version of the Uniform Electronic Transactions Act and in the South Carolina Standards for Electronic Signatures, state government entities are not required to utilize electronic records or electronic signatures. Three primary determinants of the need for electronic signatures are:

- Is there a legal need for a signature? If the current paper version of the process in question does not require a signature, then the electronic version probably does not require an electronic signature.
- Will there be a need to verify the authentication, non-repudiation, or integrity of an electronic record created by the transaction, independently of the transaction itself, over the life of the electronic record? If not, the agency may need security and authentication processes at the time of the transaction, but may not need the creation of electronic signatures.
- Does the frequency, volume, or complexity of the paper process justify the work to build an electronic process at all, with or without electronic signatures?

To the extent that state government entities do need or choose to utilize electronic records or signatures, they are subject to the standards. Before embarking on new initiatives, agencies should study their requirements and options carefully to ensure that there is a clear business need and that any proposed solution utilizing electronic signatures is appropriate, feasible, and represents a practical trade-off between benefits, costs, and risks. Once a decision has been made to move forward, agencies will find this guide useful and instructive in choosing and implementing the appropriate technology to meet their needs.

4. Risk Assessment Approach

Some or all of the implementation decisions for an agency utilizing electronic signatures may be dictated by legislation, regulation, or the parameters of a national program such as HIPAA. To the extent that the agency is free to design the implementation, key decisions include

- The technology utilized to create the electronic signature
- The method of authenticating the signer and/or the user of the electronic transaction

- The security measures surrounding the execution of the transaction, including the transmission of data, and
- The security measures surrounding the subsequent storage of the signed electronic record.

The recommended approach to making these implementation decisions is a **Risk Assessment** of the entire program and its participants. This assessment should take into consideration issues such as the following:

- 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 consequences of successful fraud for participants, their organizations and the system(s).
- The implications for the program and its participants if the signature is repudiated.
- 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 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 of all intended participants, and the cost of technology.
- The required level of confidence in establishing the signer's and/or users' identity.
- The implications for the program and its participants if the electronic record is altered; the required level of communication integrity and the required level of record integrity.
- The length of time the electronically-signed records must be retained and made accessible.
- The cost of managing, preserving, and providing access to the signed electronic records during the time period they must be retained.

Risk Management Plan: After the possible risks have been identified, a risk management plan must be created. This plan will examine each dimension of the proposed electronic signature in light of the identified risks. Action may be taken to resolve the risk, mitigate the risk, have a contingency for the risk, or the risk may simply be accepted. Critical risks should be resolved fully prior to proceeding with the implementation. The risk management process should be fully documented.

The remainder of this document discusses each of the four factors of the electronic signature Standards, some of the risks associated with each of the factors, and some of the implementation considerations that may be used to mitigate the associated risk. Examples are then provided of various electronic signature technologies, and of uses of electronic signatures in South Carolina state government.

Please reference the Architecture Oversight Committee's Security Domain, Risk Analysis Discipline.

5. Use of Signature Unique to the Signer

The most fundamental determination regarding this factor of the electronic signature is the nature of the signer. If the signer is a specific human person, then the electronic signature must be reasonably unique to that person. The most unique electronic signatures involve the physical characteristics of the individual. Such "biometric" signatures depend on the digitization of a physical characteristic, such as a finger or thumbprint or retinal scan. The resulting electronic pattern is compared to known patterns to authenticate the signer. A digitized paper signature, although less precise, is still based on physical characteristics of an individual signer.

Alternatively, the signer may in fact be a computer system or server. In the case of a business to government transaction, or agency to agency, the concern may be that the transaction was originated by the proper business or agency, rather than a specific individual. In this case, the appropriate form of signature may utilize a digital certificate issued to the business or agency by a valid certificate authority and installed on a server under control of the business or agency. An application system may generate the proper signature without human intervention.

Other forms of electronic signature may be appropriate to either a human individual or to a business or government entity. A user-id and password, for example, may be thought up by an individual, or they may be randomly generated by a password server application. In either case, in order to be verifiable as an electronic signature, the user-id and password must be registered with, or made known to, the party intended to receive the electronic signature.

Risk assessment concerning this factor of the electronic signature in any program implementation focuses on two areas'

- Failure of authentication – what is the risk to the participants or the program if the signer was not the party that the signer represented himself to be, and
- Repudiation – what is the risk to the participants or the program if the signer denies that he signed the electronic record?

There are two general types of electronic transactions involving electronic signatures. The first is the transmission of a previously created electronic document or record containing an electronic signature. Examples include the retrieval of medical records, or the receipt by the Department of Revenue of a taxpayer return from the IRS. Formats of the electronic signature itself can include the digitized image of a paper signature, the inclusion in the record of a code or PIN assigned to the signer, or a digital signature created from the electronic record by means of a private encryption key, and can represent either an individual or a business or agency. Considerations for this type of electronic transaction include:

- Whether associated risk dictates that every electronic signature must be verified at the time of the transaction, or whether the signature is only verified if the electronic record is contested or repudiated. For example, a digitized paper signature would be impractical if large volumes of electronic transactions required that the signature be verified at the time of the transaction.
- Whether the transmitter of the signed electronic record is a trusted party that has itself verified the electronic signature. For example, the IRS may only transmit valid tax returns to the state.

The second type of electronic transaction is one where the signer is in fact the user of an electronic service such as an online transaction system. In this case, generally some form of authentication of the user takes place when the user logs onto the electronic service or transaction system. The electronic signature is created by some action of the user during the electronic transaction. Considerations for this type of electronic transaction include:

- What is the probability that an unauthorized user can "spoof" the authorized user by logging onto the electronic service or transaction system in place of the authorized user
- What assurance is there that the creator of the electronic signature is the same party who logged onto the electronic service or transaction system? For example, what can happen if the authorized individual human user steps away from the workstation during the transaction. Requiring the user to re-submit the same credentials used to log onto the electronic service or transaction system as the act of signing can reduce the risk that an unauthorized party has taken over the user's access.

Considerations common to both types of electronic transaction involving electronic signatures include:

- What is the level of technology available to the population of signers? For example, if the application is internal to a state agency or group of agencies, it is feasible to issue some form of electronic token to this limited set of signers, or to require the use of digital certificates installed on servers within the agency infrastructure. If this is an application intended for use by the general public, however, then either the issuance of electronic tokens or the requirement for digital certificates is probably neither cost justifiable nor manageable.
- What are reasonable steps that can be taken to increase the probability that the signature is unique to the signer? For example, if cost and availability considerations dictate the use of Personal Identification Numbers (PINs) or passwords, what complexity can be required such as the use of special characters and combinations of alpha and numeric?
- What is the risk that the electronic signature or the electronic record could be accessed during the transaction, providing an unauthorized party with the means to create future invalid electronic signatures? Measures for mitigating this risk include security measures for telecommunications, such as the encryption of the transmitted record or online transaction.

There are several recommended resources that provide guidance in the area of security and authentication of data transmissions and online transactions. This document is not intended to reproduce that guidance, but only to show how these concepts apply to the assurance that the electronic signature was in fact created undeniably by the intended signer. **The reader is referred to the AOC Security Domain for standards in the area of security for South Carolina state agencies.**

6. Agreement by the Parties

The second requirement for use of electronic signatures is an agreement by all parties to transact business electronically. For example, a citizen may not be able to e-mail to a state agency information normally contained in a notarized paper document and assume that the agency will accept the email contents as a signed document.

In the commercial world, businesses enter into peer-to-peer Trading Partner Agreements to spell out the legal, technical, and logistical requirements for the business to conduct electronic commerce. Governmental agencies may execute a similar Memorandum of Understanding to establish agreement. The situation changes, however, in a program offered by a governmental agency to the general public. Clearly it is not feasible to execute separate agreements with a large populace.

In this case, the agreement between the parties may be implicit rather than explicit. The governmental agency offers the electronic program, thereby indicating its willingness to conduct the transaction by electronic means. If the program is voluntary, the citizen indicates his agreement to conduct the transaction electronically by his participation in the program itself. The program may in fact be mandated by law or regulation. In this case the issue of agreement becomes moot.

The risk, in terms of impact on the use of electronic signatures, is that one or both parties will repudiate the transaction. Either the supposed signer will claim that the supposed signing party never agreed that the transaction would represent a signed document or record – for example, that the party never understood that the results of the transaction would be taken as acceptance of contractual conditions – or the recipient will claim that the receiving party never agreed to accept the electronic transaction as a signed document or record. Mitigation of this risk is generally procedural, and may include clear and unequivocal statement in the presentation of an electronic transaction that the completion of the transaction will be considered to be a signed document or record.

7. Intent to Sign

Agreement between the parties refers to a program in general, or a capability to conduct business by electronic means. Intent to sign refers to a specific transaction. There must be clear evidence that the signer intended to complete this particular transaction.

Several forms of electronic signature inherently indicate intent to sign. A paper and ink signature takes a deliberate act to create, so a digitization of that paper signature inherits that intent. A digital signature takes programmatic action to create the encrypted mathematical reduction of the electronic document or record being signed. Electronic transactions that transmit or retrieve documents or records previously signed in either of these manners obtain an intentionally created signature which may be verified if necessary or desired.

Intent to sign becomes more open to question with online transactions. If the user of an online service is properly authenticated at logon to the service, and provides the necessary data for an electronic transaction, it is easy to infer that the user intended to complete the transaction, and to utilize the user's logon credentials as a signature to the transaction. But what if the user enters all of the data, but then shuts down the browser? Did the user intend to complete the transaction, or to cancel it? To assume intent to sign without clear indication of that intent may incur risk that the user may later repudiate the transaction. To mitigate this risk, it is recommended that any online transaction conclude by requiring some affirmative action by the user to indicate clear intent to complete the transaction. This may take the form of a simple "click through," where the user clicks on a button that states "I agree," "I hereby sign," or other appropriate affirmation. However, as noted previously in this document, there may still be a slight risk that the party who

executed the click is not the same party who was authenticated at logon. If this risk is still unacceptable, then stronger risk mitigation is provided by requiring the user to present authentication credentials a second time to serve as an explicit electronic signature. As with Agreement Between the Parties, risk mitigation strategy for Intent to Sign is generally procedural.

8. Association of the Signature with the Signed Record

An electronic signature has no meaning apart from the electronic document or record which it signs. The record may be in the form of business data, such as a tax return or an application for a license; it may be a digitally signed logon request, a request for a medical record, or the retrieved medical record itself. Even though an individual or organization's credentials, such as a user-id and password, a fingerprint, or a physical token, are used for authentication of that individual or organization, unless those credentials are physically or logically associated with a record, with intent to sign the record, no electronic signature has been created. For example, an email that is created and sent is generally accepted as being signed; however, the act of opening and reading an email is generally not considered to have created a signature.

Some electronic signatures, such as the signature on a digitized paper document, cannot be physically separated from the document itself. In most cases, however, the signature is itself a piece of electronic data which can be logically, rather than physically, associated with the record. If a user's authentication credentials are used as an electronic signature on repeated transactions, for example, it would not be sound security practice to store an increasing number of copies of those credentials, increasing the risk of unauthorized use. In this case, some more public form of identification of the party, such as an account number, is used to link the electronic record to the party, with the properly secured credentials available only on an as-needed basis.

Risks associated with this factor of electronic signature implementation include:

- Risk that the signature may be disassociated from the document or record, increasing the possibility of repudiation
- Risk that a signature could be fraudulently associated with an unauthorized document or record
- Risk that a document or record could be modified without authorization after it has been electronically signed.

The form of electronic signature that best addresses these risks is the digital signature. Because a digital signature can only be created using the signer's private encryption key, it is a secure from fraud as the measures that the signer takes to protect that private key. Because the digital signature is created from a mathematical reduction of the electronic record or document, it can be used to detect whether the document has been altered since the digital signature was created. However, it is again noted that digital signature technology, while becoming more commonplace, is still not practical for the general South Carolina public. Moreover, as noted previously, a digital certificate, used to create the digital signature, generally identifies a system or server, rather than an individual. If the identification of an individual person is critical to the validity of an electronic program, then an additional form of authentication and/or electronic signature may be needed to authorize the creation of the digital signature (see Example 5 – SCDPPPS - Offender Supervision - Use of Biometrics).

Whether or not digital signatures are used, reasonable security measures should be taken by all parties to an electronically signed transaction, in order to protect both the electronic signature and

the signed electronic record or document, both during the transaction (in flight) and during their subsequent storage (at rest). This document does not attempt to discuss all of the security measures available; again the reader is referred to the AOC Security Domain standards. However, it must be noted that many electronically signed documents in governmental programs are in fact public records which must be managed in accordance with legally-established record retention schedules and which must be made available on demand, often for extended periods of time. The challenges then becomes ensuring that these records are not altered, forged, or counterfeited and that they are adequately preserved and remain accessible for the full amount of time they must be retained. For additional information on managing, preserving, and providing access to electronic records, refer to the *Electronic Records Management Guidelines* developed by the South Carolina Department of Archives and History (http://www.state.sc.us/scdah/erg/erg.htm), in particular the section on Electronic and Digital Signatures (http://www.state.sc.us/scdah/erg/ermEDS.pdf).

9. Independent Features of an Electronic Signature

An electronic signature is valid if it meets the four characteristics presented in section 2. Beyond these characteristics, however, a specific implementation of electronic signatures may need or wish to provide one or more of the following capabilities. Both business application requirements and risk assessment should be utilized to determine the utility of these features.

- **Continuity of signature capability:** The ability to ensure that public verification or revelation of a signature, encryption method or element of an electronic signature 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.

10. Examples of Electronic Signatures

Example 1 - Digitized Signature

A digitized signature is a graphical image of a handwritten signature.

Some business processes 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 handwritten 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.

See Example 3 – South Carolina Business One Stop below.

Example 2 – Biometric Signature

Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. Among these are voice patterns (where an individual's spoken words are converted into a special electronic representation), fingerprints, and the blood vessel patterns present on the retina (or rear) of one or both eyes. In this technology, the physical characteristic is measured (by a microphone, optical reader, or some other device), converted into digital form, and then compared with a copy of that characteristic stored in the computer and authenticated beforehand as belonging to a particular person. If the test pattern and the previously stored patterns are sufficiently close (to a degree which is usually selectable by the authenticating application, then the pattern can be verified as the signature of the particular person. Biometric authentication is best suited for access to devices, e.g. to access a computer hard drive or smart card, and less suited as a signature transmitted to a software system over an open network. However, it is an excellent approach when the need to authenticate a signature to a particular individual, as opposed to an organization or computer system, is required.

See Example 5 – SCDPPPS - Use of Biometrics below.

Example 3 – PIN/Password

A password or Personal Identification Number (PIN) is an example of a "shared secret," called "shared" because it is known to both the user and the receiving computer system. The system checks the password or PIN against data in a database to ensure its correctness and thereby

authenticates the user. Passwords and PINs may be entered into a computer system by the user to serve as a signature, in addition to their use to gain access to the system. Unless security is maintained concerning the PIN or password, however, an unauthorized party gaining access to the PIN or password may use it to impersonate the authorized party. Computer applications utilizing PINs and passwords should use security technologies such as encryption both when transmitting and when storing the PIN or password. These measures, however, are meaningless if the user does not also take reasonable precautions.

See Example 1 – EIP Employee Online Benefits Administration and Example 2 – Filing of Sales Tax via Web below.

Example 4 – Digital Signature

To produce a digital signature, a user must obtain or generate by computer two mathematically linked encryption keys – a private signing key that is kept private, and a public validation key that is made available to the public. Neither key can be derived from the other. The use of the public/private key pair is known as Public Key Infrastructure, or PKI. A digital signature must be related to a specific electronic record, such as a document, a data record, or a logon request. To create the digital signature, the computer creates a mathematical digest, or "hash," of the record to be signed. The digest is then encrypted by means of the user's private key. Since the recipient of the digital signature can only encrypt it by means of the user's public key, they recipient can verify that the user created the signature. If the private key has been properly protected from compromise or loss, the signature is unique to the individual or organization that owns it, and the owner cannot repudiate the signature. Moreover, because the digital signature is derived from a mathematical digest of the original electronic record, the record cannot be altered without invalidating the digital signature. The reliability of the digital signature is proportional to the degree of confidence one has in the link between the owner's identity and the digital certificate containing the owner's public and private keys. Note that because PKI relies on computer technology, a digital signature identifies a computer system rather than a particular human individual. For this reason, it is generally used to identify organizations rather than individuals.

See Example 4 – Tax returns between SC Department of Revenue and the IRS below.

Example 5 – Physical Token

A potentially more secure means of entering data to be used both for authentication and as an electronic signature is the use of a physical token, such as a smart card or one-time password device. The signer must be in physical possession of the device, so that it cannot be used by an unauthorized party unless it is lost or shared by the authorized signer. A smart card is a plastic card the size of a credit card containing an embedded integrated circuit or chip that can generate, store, and/or process data. A user inserts the smart card into a card reader attached to a computer. The smart card provides the data for authentication purposes and/or to serve as an electronic signature when the user also enters a PIN, password, or biometric identifier recognized by the card. A one-time password (OTP) device contains an integrated circuit or chip with both a date/time clock and password generation software. The device, which is synchronized with similar software in possession of the intended recipient, continuously generates new passwords at regular time intervals, such as a minute or even a second. When the OTP device is connected to a computer, the generated password may be used either for authentication or to serve as an

electronic signature. Because the password is continuously changing, an unauthorized party cannot reuse a previously used password that the party may be able to acquire.

11. Examples of SC Applications using Electronic Signatures

Example 1 – EIP Employee Online Benefits Administration

Description of Program
The State of South Carolina Employee Insurance Program (EIP) has introduced an internet-based Electronic Benefits System (EBS) to allow eligible employees to access their benefit information and to submit changes electronically to EIP in a total secure environment. Eligible South Carolina Employees will be able to make insurance benefit changes using the online EBS. Upon initial use of the EBS, employees will register online by providing personal information along with their Benefits Identification Number (BIN). This information will be verified against employee data within a master database. Once the employee has successfully registered online, he can view his account or perform direct data entry in the system such as annual / open enrollment or updates such as beneficiary changes or change of address. This program has been developed using industry standard practices and in conformance with regulatory requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Unique Identification of the Party
The employee logs into the system by providing a Benefits Identification Number (BIN) and a password. The BIN has been assigned by the state agency. At the time of registration, employees are required to select a password that must meet certain guidelines that have been established by the Employee Insurance Program and are best practices for security. Such requirements include mixing letters, numbers, and special characters, as well as, a minimum string length.

Agreement by the Parties
The State of South Carolina EIP provides the online EBS for employees to update their insurance benefit options, indicating EIP's agreement to conduct business in this manner. Employees indicate their agreement to make changes to their insurance benefits electronically by registering within and usage of the online EBS. This voluntary act of registering and making online changes constitutes the agreement of parties.

Intent to Sign
Once a state employee has completed changes to the benefits system online, there is a series of explicit actions to accept the changes representing the employee's "intent to sign". There are certain benefit changes that require documents that have a traditional handwritten signature. Such documents are imaged, securely stored and indexed in a relational database.

Association with the Record
The employee's BIN is kept by the Employee Insurance Program along with any associated imaged documents and the subscriber's insurance benefits record.

Security Considerations
In order to insure that a human is making the request within EBS, the subscriber (employee) will be required to repeat a string of characters (i.e., CAPTCHA) displayed within the first screen of the registration routine. Upon successfully entering the string, the subscriber will then be required to enter his/her full name and BIN (Benefits Identification Number). Since the nature of this

transaction involves PHI (protected health information), the system uses a PKI (Public Key Infrastructure) framework in which all transactions are performed over an SSL (Secure Sockets Layer) connection.

References
See **References** on page 18 for the key references used in developing the EIP system architecture and security program.

Example 2 – SCnetFile – Online Individual Income Tax

Description of Program
A South Carolina taxpayer wishes to file and, if necessary, pay Individual Income Tax online. The taxpayer logs onto the system using primary and possibly secondary Social Security Numbers, and a Personal Identification Number (PIN) that was mailed to the taxpayer by the Department of Revenue. The taxpayer then is guided through the submission of tax return data, including W-2 data from employers, and the system computes either the refund due to the taxpayer or else the balance due that the taxpayer must pay the State. If there is a balance due, the taxpayer selects either credit card or direct bank account debit as a payment method. When the taxpayer has entered all data, the taxpayer is shown a page with a "jurat" – a statement that the data that was entered is true and accurate – and is asked to re-enter the PIN to serve as signature.

Unique Identification of the Party
The taxpayer logs onto the system utilizing a PIN that was randomly assigned by the Department of Revenue, and was mailed to the taxpayer's address of record. While the PIN could conceivably be stolen from the mail, the thief would have to know the taxpayer's Social Security Number. There is reasonable assumption that the combination of SSN and PIN would uniquely identify the taxpayer and be known only to the taxpayer.

Agreement by the Parties
The South Carolina Department of Revenue provides the "SCnetFile" online application for filing and paying Individual Income Tax, indicating its agreement to conduct business in this manner. The taxpayer indicates agreement to conduct his personal business of income tax filing electronically by participating in the program. The voluntary act of filing, and if necessary paying, online is all the agreement that is required.

Intent to Sign
The SCnetFile program explicitly instructs the taxpayer to re-enter the PIN to sign the tax return. By re-entering the correct PIN, the taxpayer is again authenticated and performs a deliberate act of signing.

Association with the Record
The electronic Individual Income Tax return is indexed by the Department of Revenue using the taxpayer's primary Social Security Number. This SSN is stored as part of the taxpayer's account record with the Department of Revenue, and all tax returns are associated with the account. The PINs are associated with the SSNs via a separate, and highly secured, file. This file serves to link the PIN to the tax return as needed.

Security Considerations
The taxpayer is authenticated using a PIN that has been previously established. The PIN is transmitted to the taxpayer by US mail in a sealed mailer, and is not provided online or over the telephone, even if requested by the taxpayer. Although fraud is possible, the risk of an unauthorized party filing the return is considered to be only moderate. SSL is used to encrypt all data exchange between the taxpayer and the Department of Revenue. The resulting electronic Individual Income Tax return is stored in a database with controlled, limited access.

NOTE: By contrast, the Department of Revenue e-Sales application for online filing and payment of Sales Tax does not present a jurat or request that any data be entered for the purpose of signing the return. The application is otherwise similar to SCnetFile. While the e-Sales application creates a legally filed tax return, it is not considered by the Department of Revenue to have been signed. There is no legal requirement for a Sales Tax return to be signed.

Example 3 – South Carolina Business One Stop

Description of Program
South Carolina law requires that the Secretary of State receive a signed copy of certain documents. One example is the Articles of Incorporation for a corporation registering to do business in the state. The South Carolina Business One Stop (SCBOS) program is an online application to allow businesses to register electronically with a number of South Carolina agencies, including the Secretary of State. Although registration data is provided in electronic format, SCBOS also supports the ability for the business to upload a scanned pdf copy of the business's Articles of Incorporation.

Unique Identification of the Party
The Articles of Incorporation is a paper document signed in ink by an officer of the corporation and an attorney. These signatures, even when digitized, are provably unique to the signer as described above.

Agreement by the Parties
By providing the capability to upload a digitized copy of the Articles of Incorporation through the SCBOS program, the Office of the Secretary of State indicates its agreement to accept this as a signed document. By completing the action of uploading the digitized Articles, the business indicates its agreement to provide this electronic signature and to conduct this electronic transaction.

Intent to Sign
The business is asked to demonstrate intent to sign twice – first, by applying an ink signature in the appropriate place on the paper Articles of Incorporation, and secondly by uploading the signed document in pdf format. The SCBOS program asks the user to provide this signature, which is an intentional act.

Association with the Record
Because the ink signature is an integral part of the paper Articles of Incorporation, the digitized signature is an integral part of the digitized Articles of Incorporation in pdf format. As long as the pdf file is preserved intact, the signature will remain a part of the record.

Security Considerations
The signature on the pdf Articles of Incorporation is assumed to be valid with low risk, the same as if the paper version were brought to the Secretary of State. Self-selected user-id and password are used to register and authenticate the business user. Secure Socket Layer (SSL) encryption is used to secure SCBOS data exchange, to protect sensitive information such as Social Security Numbers during the transaction.

Example 4 – Tax returns between SC Department of Revenue and the IRS

Description of Program
An individual files an electronic Individual Income Tax return using a preparer such as H&R Block, or a third party software such as TurboTax™. The individual is asked to enter a self-selected PIN to serve as signature. Both federal and state returns are transmitted to the IRS. IRS splits out and batches the state returns and makes them available to the state for download. IRS is in the process of implementing a process where the state digitally signs its logon request to the IRS using a previously registered digital certificate.

Unique Identification of the Party
The taxpayer's PIN is self-selected, so it can be assumed to be under the unique control of the taxpayer. However, duplication across millions of taxpayers is possible, so the PIN is used in combination with the filer's Social Security Number for taxpayer identification. The state must obtain a unique digital certificate from a commercial certificate authority. The private key used to encrypt the state's logon uniquely identifies the trusted computer system used to communicate with the IRS.

Agreement by the Parties
The IRS sanctions electronic filing of Individual Income Tax by use of approved third parties. Its acceptance of electronically filed returns from these parties indicates IRS agreement to transact business in this manner. Electronic filing is voluntary, so the taxpayer's use of an electronic filing program, either through a paid preparer or through third party software, indicates the taxpayer's agreement to transact business electronically.

Intent to Sign
All electronic filing software approved by the IRS explicitly asks the taxpayer to enter the self-selected PIN to sign the return. The use of the PIN is therefore a deliberate act of signing. The state's communications gateway with IRS creates a digital signature from the electronic record created as its logon request. Although this is an automated function, the fact that this program was created and implemented by the state makes this an intentional act of signing.

Association with the Record
The taxpayer PIN is retained by IRS in association with the taxpayer's return. The digital signature of the state's logon request to IRS is created from the logon request record itself, and is logically associated in that the logon record cannot be altered without invalidating the electronic signature.

Security Considerations
Although there is known to be some amount of fraud associated with electronic tax filing, it generally does not involve misrepresentation of the identity of the filer. For that reason, the self-

selected PIN is accepted by IRS as electronic signature. The state assumes that IRS has validated this signature, and does not re-authenticate the signature. The transmission of batches of tax returns from the IRS to the state, however, contains highly sensitive information. For that reason, the IRS requires the digitally signed logon to ensure that the state's tax returns are transmitted only to the state. The data is encrypted during transmission. The state then stores these electronic returns using controlled limited access storage.

Example 5 – SCDPPPS - Offender Supervision - Use of Biometrics

Description of Program
The South Carolina Department of Probation, Pardon and Parole Service (SCDPPPS) has a future example of the use of biometrics. Future Department offender supervision business processes conducted by agents will be enhanced through the use of biometrics. This will afford real-time offender data capture and information storage through the agent's issued tablet PCs. Agents will be able to effect data collection, signature, and immediate information storage on the tablet for subsequent synchronization with the Department's main database.

Unique Identification of the Party
Currently, agents are required to register in person, and only with authorization from their manager to obtain their tablet PC. The future registration process will involve setting up agents' logins and passwords and recording their fingerprints for biometric identification. This information will be recorded as a Credential in both the Department's main information system as well as on agent PCs.

Additionally, supervised offenders are also required to register a fingerprint through use of a biometric identification device.

Agreement by the Parties
As a matter of Department business practice and processes inherent with offender supervision, agents agree to the use of biometrics to register their digital signatures.

Intent to Sign
When an agent is required to certify who created a business transaction, the ultimate goal will be to use the registered fingerprint, plus an issued PIN, as the certification mechanism.

Longer term, the use of kiosks to conduct some business transactions will also be facilitated by the same process.

Association with the Record
This two-part authentication activates a standard digital certificate and will be used to apply the digital signature from the agent's machine to the offender case supervision business processes and is retained with the record(s).

Security Considerations
The agent is authenticated by both the fingerprint and their login user id and password. The password requires a mix of numbers, letters, and special characters to make it more difficult to

guess. The use of the finger print is more secure for authentication due to the high risk of this application. The use of the digital signature securely identifies the source of the transaction and allows the recipient to determine if the document has been altered.

12. References

South Carolina UETA act (In S.C. Code Ann. 26-6-10 et seq.)
http://www.scstatehouse.net/code/titl26.htm

The State of Texas: Guidelines for the Management of Electronic Transactions and Signed Records Prepared by the UETA Task Force of the Department of Information Resources and the Texas State Library and Archives Commission
http://www.dir.state.tx.us/standards/UETA_Guideline.htm

An online dictionary and search engine for computer and Internet technology definitions.
http://www.webopedia.com/

Risk Assessment
United States General Accounting Office Information Security Risk Assessment Practices of Leading Organizations: http://www.gao.gov/special.pubs/ai00033.pdf

A copy of the UETA document with embedded comments:
http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

National Conference of Commissioners on Uniform State Laws
Home Page
http://www.nccusl.org/Update/
Summary of UETA
http://www.nccusl.org/Update/uniformact_summaries/uniformacts-s-ueta.asp
Why States should adopt UETA
http://www.nccusl.org/Update/uniformact_why/uniformacts-why-ueta.asp
A few facts about UETA
http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-ueta.asp

United States Postal Service – Electronic Postmark (EPM) and its use of auditable time stamps, digital signatures and hash codes.
http://www.usps.com/electronicpostmark/welcome.htm

South Carolina Department of Archives and History
Electronic Records Management Guidelines http://www.state.sc.us/scdah/erg/erg.htm
Electronic and Digital Signatures http://www.state.sc.us/scdah/erg/ermEDS.pdf

Security Links

Wireless Search - http://www.shmoo.com/gawd/

Cisco Security Page (good white papers on "Best Practices") -
http://www.cisco.com/go/security

CERT Web Page (Computer Emergency Response Team) - http://www.cert.org

Good Hacking Sites (shows exploits that you may want to be aware of):
http://packetstormsecurity.com/
http://www.securityfocus.com/

More Security Best Practices References:
• An Introduction to Computer Security: The NIST Handbook
- http://csrc.nist.gov/publications/nistpubs/800-12/
• Federal Agency Security Practices
- http://csrc.nist.gov/fasp/
• CERT Guide to System and Network Security Practices
- http://www.cert.org/security-improvement/#practices
• Security Self-Assessment Guide for IT Systems: NIST Special Publication 800-26
- http://csrc.nist.gov/publications/nistpubs/index.html

Key references used in developing the EIP system architecture and security program

Centers for Medicare and Medicaid Services (CMS). This government website provides the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules and regulations such as the Security Standard and the Transactions and Code Sets Standards**.**
http://www.cms.hhs.gov/home/regsguidance.asp
Directly to the document:
http://www.cms.hhs.gov/TransactionCodeSetsStands/Downloads/txfinal.pdf

National Institute of Standards and Technology's (NIST) Computer Security Resource Center (CSRC). The special publications 800 series presents the results of NIST studies, investigations, and research on information technology security issues. http://csrc.nist.gov/publications/

The Workgroup for Electronic Data Interchange (WEDI). Healthcare industry group focusing on development and implementation of healthcare industry standards, policies and regulations; http://wedi.org/

Health Level Seven (HL7) is an American National Standards Institute (ANSI) accredited Standards Developing Organization (SDO) operating in the healthcare arena. Health Level Seven's domain is clinical and administrative data. http://hl7.org/

The American National Standards Institute (ANSI) coordinates the development and use of voluntary consensus standards in the United States and represents the U.S. stakeholders in standardization forums around the globe. The ANSI X12 standards has been adopted for use in HIPAA financial transactions for health care (ex. 834 Benefit Enrollment and Maintenance and 837 Claims). http://www.ansi.org