Pennsylvania Department of Public Welfare

Bureau of Information Systems

Guidelines for the Use of eSignatures

Version 1.0.5

September 28, 2005

Table of Contents

Use of Electronic Signatures (eSignatures)

Introduction

There is an ever-increasing use of the Internet to conduct business, both by commercial enterprises and by the government. Recognizing this and realizing the need for carrying over common, established business practices from the world of paperwork into the electronic world, the Federal and state governments have passed legislation enabling, among other things, the use of electronic signatures (eSignatures).

The U.S. Congress recognized the use of eSignatures in January, 2000, with the Electronic Signatures in Global and National Commerce Act (ESIGN). With the passage of the Electronic Transactions Act (Act 69 of 1999), the Pennsylvania General Assembly paved the way for entities in the Commonwealth to accept electronic signatures (eSignatures) in normal day-to-day business and legal transactions.

The purpose of this document is to outline general considerations in adopting e-signature policies and procedures.

Commonwealth Policy

The Pennsylvania Electronic Transactions Act broadly defines an eSignature 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." In the context of the legislation, the term "electronic" refers to "technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities." ESIGN provides an identical definition of "electronic" and a similar definition of "electronic signature."

The Commonwealth Policy regarding eSignatures is outlined in Management Directive 210.12 Electronic Commerce Initiatives and Security as follows:

c. Use of Electronic Signatures and Records.

1) As provided in the Act, executive agencies may send, accept, store, and use electronic records and signatures in conducting their operations following the criteria listed in subsection b.(2) and any other criteria the agency determines appropriate.

2) Consistent with the Electronic Commerce Security Assessment, executive agencies are authorized to specify the format in which electronic records are to be created, stored, accepted, and sent.

3) Executive agencies shall, to the greatest extent possible, adopt formats that are consistent and interoperable with other federal, state, and local agencies.

4) Executive agencies may require that a record submitted electronically contain an electronic signature. If the agency determines that an

electronic transaction requires an electronic signature, agencies shall specify the:

(a) manner and format in which the electronic signature must be affixed to the electronic record; and

(b) criteria that must be met by any third party used to facilitate the electronic signature process.

5) *Executive agencies may specify record retention requirements for entities regulated by or under the agency's jurisdiction, including the requirement that the record be retained and/or submitted in nonelectronic form.*

There are already examples of eSignatures use by Commonwealth agencies. PennDot's online registration and licensing renewal system and Revenue's online- and *telephone- filing of tax returns* are two major examples of such use. In each of these examples, there is a prior relationship between the agency and the citizen. There is more on this topic later in these guidelines.

Use of Signatures

A signature is generally attached to a document to satisfy one or more of the following purposes:

- *Demonstrate intent:* the signer understands what is contained in the document and agrees to fulfill his/her part of the agreement (e.g. a contract to perform services)
- *Authentication and approval:* the signature links the signer with the actual document and indicates his/her approval and authorization of the document and its contents (e.g. signing your income tax return or an application for welfare benefits)
- *Security:* the signature protects against fraud or impersonation (e.g. signing a check or a credit card charge slip)
- *Ceremony:* the signature warns the signer that he/she may be signing something with possible legal commitments and should give some thought or ask questions before doing so.

Depending on the degree of risk or the value of the transaction(s) being protected, varying types of signatures may be required. For example, ordering a box of paperclips at the office may simply require one's initials on the bottom of a memo. On the other hand, contracts in the hundreds of thousands or million dollar range generally require multiple approvals and signatures. In our daily lives, signing a check to pay a bill is a relatively low risk activity and requires a simple signature; signing a contract for a home purchase or other legal documents such as a will requires a high degree of identity authentication, generally calling for a notary public or witnesses.

When determining the need for a signature or the type of signature to be used, we must consider the following:

- *Legal requirements*: Are there laws or statutes requiring the signature? (There might be a statute or a regulation that is specific to a federal program.)
- *Business requirements*: Are there business needs for a signature? Such needs might include:

- Attesting to the accuracy of statements being made
- Agreement to certain conditions
- Understanding of the contents of the document
- Audit requirements

The processes behind the use of physical signatures may vary widely; however, they all have these common features:

- Establishment of the identity or bona fides of the signer (presentation of ID)
- Binding of the signer to the document (physical signature, notary, etc.)
- Assurance that the document, once signed, is not later altered (initialing of changes, archiving)
- Preservation of the document along with any related instruments (copy of ID, etc.) for however long is required by legal or business requirements (archiving)

As a general rule, there is little difference between physical signatures and eSignatures. The single biggest difference is in the technology (i.e. are we using a pen or are we typing on a computer screen?). For almost any given physical signature process we are familiar with, an eSignature process can be established.

Examples of eSignatures

Given the broad definition of eSignatures as established in the federal and state law, there are many possibilities for electronically signing a document. We will briefly discuss a few illustrative examples here. This is by no means a comprehensive list.

Check box / Click on

The signer of the document is asked to check off a box that's labeled "I accept," "Yes," "I agree," etc. or click a corresponding button. Generally he/she is given the option to make either a "Yes" or "No" choice. Sometimes the signer may be asked to type the words "I Agree" in a text box to ensure that there is no misunderstanding. Upon selecting the (usually) affirmative box, the signer is allowed to proceed with the action of the system.

A common example of this is the installation of a software package on a computer. Particularly with commercial software, the installer is asked to agree to terms and conditions before the software is actually installed on the system. Failing to click on the "I Agree" button or check the "Yes" box aborts the software installation process. Despite the lack of any real validation of the installer's or user's identity, many people have been successfully prosecuted for software piracy based on this eSignature.

There is little or no validation of the signer's identification in this type of eSignature. Generally it should only be used for low-risk or low-value transactions.

Personal Identification Number (PIN) or Password

The signer is asked to provide identifying information (userID, Social Security Number, etc.) and a shared secret (something that both parties know) such as a PIN or password.

Once the information is entered, the system authenticates the signer by checking that the shared secret is indeed the one that was established for the claimed identity. Generally there needs to be a pre-existing relationship between the entities.

The process for validating a user and subsequently issuing a shared secret can vary widely and may be as strong or as weak as deemed necessary for the transaction. For example, a customer may establish an account with an online retailer simply by entering some basic information (name, address, phone number, email account) and supplying their own choice of userID and password. This is sufficient to enter the site, browse the online catalog and even put items into a shopping cart. However, when it comes time for checkout, a higher level of authentication is required in the form of verifiable and valid credit card in the user's name and with the appropriate billing address, etc. Once this higher level of identity has been established, subsequent transactions of the sort may rely only on the userID and password and stored information.

An example of such a system being used within the Commonwealth is the online filing of state income tax returns. Here there is a pre-existing relationship between the user and the Commonwealth. The userID is the user's Social Security Number and the validating information or shared secret is information off of the user's previous year's state income tax return or the user's PA Drivers License or Identification Card number.

As noted above, the validation of the user's identity can vary widely and the process should be tailored to the risk/value of the transaction.

Digitized Signatures

The signer is asked to sign their name on a digital input device. The signature is recorded and stored with the document. For a higher level of identity validation, software may be used to compare the signature with a pre-existing sample. This is a form of biometrics.

A common example of this is the use of electronic signature pads for credit card transactions in retail establishments.

Digital Signatures (PKI)

A digital signature (not a *digitized* signature) makes use of public key infrastructure (PKI). A trusted (third party) certification authority validates the identity of a user and issues a two-piece digital key. One is the private key and is held by the user. The other is a public key and is made available to the world. The two keys are mathematically linked to each other and can be used to encrypt and to sign documents. Without going too in depth into the details, a document encrypted with one of the two keys (generally the public key) can only be decrypted with the other one of the pair. A document signed by one of the keys (generally the private one) can have the signature validated by the other key of the pair.

This type of eSignature provides a high level of security and validation of a document, depending on the rigor applied in the registration process. It is correspondingly costly. Also the key pairs must be preserved for the lifetime of the document; without them the signature cannot be validated and if the document is encrypted, it cannot be decrypted. Generally this type of signature is reserved for high risk/high value transactions such as high value bank transfers or corporate orders.

Biometrics

Personal characteristics (fingerprints, iris or retinal patterns, DNA, voice, handwriting) can provide a very high level of identity validation when used as or as a part of an eSignature process. These are not widely used at this point in time, however, examples include the comparison of a digitized signature with a previous sample (as mentioned above) or the recording of a signer's voice as he/she makes a required statement.

Hardware Tokens

While not necessarily an eSignature in itself, hardware tokens such as smart cards, single use PIN generators (e.g., RSA SecureID) can be used to augment an eSignature process. A smart card, for example, can be used to hold the user's private key in a digital signature solution or a user's biometric characteristics. A PIN generator can provide a higher level of security for a shared secret eSignature.

Hybrid Approaches

In many cases, the eSignature approach that is taken is a combination of various techniques. This provides a flexible experience and can meet the needs of transactions with varying security requirements. For example, a variation of the shared secret approach may be to enter both a userID and password to access an online shopping site for browsing. A number located on some form of physical document or ID is then required to complete the actual purchase. Most credit cards have a 3- or 4- digit code (in addition to the account number) that is printed somewhere on the physical card, but NOT on any other documents such as a statement. Requiring the use of this additional information provides a higher level of security when an online payment or purchase transaction is being made as it requires the physical possession of the credit card.

Security of eSignature Solutions

There are three main factors inherent in any eSignature system. These are:

- Identification or registration of the signer
- Authentication of the signer
- Integrity of the signed document

Identification or registration of the signer

One of the first requirements in transacting business between two or more parties is the establishment of each party's identity. If someone fills out a benefits application claiming to be George Washington and then signs the document (physically or electronically) with George Washington's name, do we just assume that this is a valid application from George Washington? The registration process or the establishment of the signer's identity is the key first step. The following table summarizes various types of identification practices with the level of risk they can support:

Identification Methods	Level of Risk
No registration, only self-identification as part of the signing process	Very low
Comparison of user supplied information with a trusted data source before authorization	Low
Acceptance of a previously conducted and trusted identification and registration process where the individuals personally presented themselves and proof of their identities	Medium
A separate identification process to authorize the use of an e-signature where the individuals personally present themselves and proof of their identities	High

Authentication of the signer

Once we have identified the signer, we must now ensure that the person we have identified is actually the one involved in this transaction. For example, John Doe opens a checking account with a bank and deposits money into that account. Weeks later, the bank is presented with a check signed "John Doe" drawn again that account in the amount of $1000.00. The bank knows that John Doe is a customer, but how does it know that John Doe actually signed this particular check? The following table summarizes various types of authentication methods and the level of risk they support:

Authentication Method	**Level of Risk**
No method of authentication beyond user identification as part of the signing process	Very low
User selected PIN or password	Very low
PIN or password assigned by the governmental entity	Low
PIN or password assigned by the governmental entity along with user supplied verifiable personal information	Low to medium
Cryptographic key or biometric (often includes two factor authentication through the use of a password or PIN)	Medium to high
Two factor authentication including the use of hardware device such as a smart card	High

Integrity of the signed document

Now that the document has been signed, how do we know that the document has not been subsequently modified by any of the involved parties? In our last example, how does the bank know that John Doe intended to pay $1000.00 and that the recipient of the check didn't change the amount from $100.00 to $1000.00? The following table summarizes some types of eSignature practices for document integrity and the level of risk they support:

Record Integrity Security Options	Level of Risk
System reasonably ensures the integrity of the record and the signature and record link	Low
The above plus use of a secure network or secure cryptographic method (e.g., secure socket layer (SSL) or VPN) to transfer the electronically signed record	Low to medium
All of the above plus use of a cryptographic method with hashing techniques to ensure record integrity and the link between the record and the signature (e.g., PKI)	Medium to high

Business Process Assessment

The selection and implementation of an eSignature system is primarily a business decision rather than a technical one. This section will discuss some of the considerations of both business requirements, as well as risk assessment that should be taken into account prior to deciding on an eSignature system. The business analysis and risk assessment should be considered jointly, not in isolation of each other.

Business Analysis

As noted above, the business process should be the primary determining factor in the selection of an eSignature system. Understanding the business process will drive both the risk analysis as well as the selection of an eSignature solution or solutions. In conducting a business analysis, the following steps should be followed:

- Perform a review of the business process, considering:
  - The transaction's purpose and origins.
  - Its place within the larger business process
  - What services will be delivered and their value to the governmental entity.
  - The various parties to the transaction, including stakeholders who are not directly involved in the transaction, and their business relationships to each other.
  - The transaction's workflow
- Analyze of legal and regulatory requirements, including:
  - How the transaction must be conducted, including timeframes.
  - Signature requirements (e.g., are they specifically required, what records need to be signed, who must or can sign, do they need to be notarized, etc.).
  - Any records-related requirements including:
    - What records must be produced.
    - How long do they need to be retained.
    - Who must or can have access to the records.
    - Specific formats prescribed for the creation, filing or retention of the records.
    - Confidentiality requirements.
  - The degree of importance that the identity of parties to the transaction has to conducting the transaction.

- Identify industry standards or generally accepted practices related to the transaction.
- Analyze those who will use electronically signed records and related requirements.
- Determine interoperability requirements, including those of business partners.
- Determine the cost of alternative approaches.

Risk Assessment

Once you understand the business process you must consider the associated risks. Basically, risk is the *likelihood* that a process or system will be breached in comparison with the degree of *impact* or loss that will be suffered due to said breach. This is usually illustrated as the following matrix:

Risk Assessment Matrix		Impact		
		Low	Medium	High
Likelihood	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Threats

In performing a risk assessment you must identify possible threats and vulnerabilities. Important items to consider include:

- Repudiation – the signer denying having signed the document or denying their intent in signing the document or claiming the document was altered at some time after they signed it
- Fraud – the signer misrepresenting information or forging the signature of another party
- Intrusion – an unauthorized third party gaining access to information in the transaction and exploiting it for personal gain or making other unauthorized use of it
- Loss of records or documentation – electronic documents being lost because they were not preserved or the systems they reside on are unavailable.

Once you have identified the potential threats, you must assess how likely an occurrence each threat is and then further assess the overall likelihood that any threat will occur. Some considerations in determining likelihood include:

- Motivation and capability of the source of the threat.
- Nature of the vulnerability.
- Existence and effectiveness of current controls.

Impact

The impact is the consequence or possible loss of a breach of the system. Some possible impacts include:

- Financial – monetary loss either to the agency, business partners, or the citizen.

- Reputation – public exposure damaging the agency's reputation or the trust the citizens have in the agency. There may also be political repercussions.
- Productivity – inability of agency employees or business partners to complete their work in a timely manner, if at all. Additional and otherwise productive time may be spent in addressing the breach and its impact.

Cost-Benefit Analysis

Now that you have completed the business analysis and risk assessment and identified potential eSignature solutions, you must consider the cost-benefit (or return on investment) of the proposed solution. You must then contrast the benefits of implementing the proposed solution with the costs of doing so. The benefits may include improved productivity of staff and business partners, faster or more convenient delivery of services to our constituents, or possibly reduction in fraudulent claims. Factors to consider include:

- The impact of implementing the solution.
- The impact of not implementing it.
- The costs of the implementation.
- The importance of implementing the solution, weighing the expected costs and benefits against the criticality of the business process and its underlying data.

Document Change Log

Change Date	Version	CR #	Change Description	Author and Organization
09/28/2005	1.0	N/A	Initial Creation	Frank Morrow, DPW