ELECTRONIC SIGNATURES FOR FORMS

INFORMATIONAL ARTICLE

Electronic Signatures for Forms

Many forms require signatures. At the same time, many forms are signed when they don't really need to be. Signatures are a workflow conundrum, slowing down business processes and preventing many forms from being converted to enterprise-enabled forms.

In many ways, signature requirements are vestiges of old, out-of-date workflows. Managers require signatures on forms when the signature really doesn't add anything significant to the result. I think sometimes signature requirements merely feed the egos of the managers involved.

Now, this is **NOT** to suggest that all signatures are not important or not needed. In many cases, they add an important element to the transaction and are legally required. There is a large body of knowledge surrounding signatures. However, I am suggesting that many signature requirements should be reviewed and revised because they do not substantially contribute to the transaction. We see ample evidence in many credit card transactions today, where signatures have been eliminated.

Paper forms have supported signatures for centuries. It is easy to design a form for a wet signature and the form can be signed without delay. The use of proper zoning techniques provides an area for affixing signatures such that it is known what the signer is attesting to, enough space is provided for a signature, and a properly printed name, date signed, and affirmation statement can be provided if necessary. Validation of the signer is assumed and confirmed via handwriting analysis or notarization.

Electronic signatures present a different problem. The Electronic Signatures in Global and National Commerce Act (E-Sign), enacted June 30, 2000, made electronic signatures legal, but there is an obvious difference between being "legal" and being accepted as evidence in court.

Because the argument for the conversion of paper forms to truly electronic transactions is compelling, the requirement to print and sign just isn't acceptable anymore. Many solutions have been developed to solve the signature problem, yet, thirty years into electronic forms, many, if not most, forms are printed if they must be signed and the form enters a manual workflow. Avoiding this requirement to print and sign has become the focus.

As a standard part of the forms development workflow, we always challenge the need for a signature first. The question is - what does the signature add to the solution and what happens if it is excluded? Generally, the answer to this question is a matter of risk - the risk that someone would actually want to counterfeit this transaction and the amount of loss if they actually did. For many internal transactions, we find this risk is minimal and standard technology such as password signing (a standard signature field) or system login to the device used to complete the form should be sufficient to authenticate the signer and establish intent to sign. Generally, for these low-risk transactions, there is no need for further signature requirements. However, old policies and procedures die slowly and even these low-risk transactions frequently must be signed, therefore minimizing the opportunity to automate the transaction. This leads to Electronic Signature Opportunity 1 - change the policies and procedures and eliminate the signature altogether or at least use a simple signing process. Both avoid unnecessary printing and manual processing.

Many transactions represent higher risk. User authentication is critical, as is validation of intent to agree to the conditions attested to in the form. In these instances, level 1 signatures (login and password systems) simply won't suffice. This is generally true of transactions of a high dollar value or that have a higher risk of ending up in court at some point in the future. It is also generally true for anonymous transactions on the web. This is where it gets interesting from a forms design perspective.

There are many technologies available to sign a form. Virtually all of them are proprietary. This fact makes them hard to implement because focusing on only one solution excludes many users from participating. For internal solutions, this is solvable because the organization controls the technologies used internally and one selected solution can be implemented. However, "outside the firewall", such control over user technology does not exist and a single solution doesn't work. In these instances, the specific transaction workflow can drive the solution. The forms analysts and forms designers need to be familiar with the signing options and the advantages and disadvantages of each.

The following two charts provide a brief discussion of the available options:

Technology	Definition
Certificate Authority	Entity authorized to issue a digital signature to an applicant which contains the applicant's public key and other identification information.
Digital Certificates	An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply." An individual wishing to send an encrypted message applies for a digital certificate from a *Certificate Authority* (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA, and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. The most widely used standard for digital certificates is X.509.
User ID & Password	Users register and are assigned a user id and password.
Keypad Capture	Hardware device attached to the computer for handwriting capture.
Fingerprint	A scanning device attached to a computer for fingerprint capture.
Retina Scan	Hardware device for retina scan and capture.
Voice Signature	Server-based process (software) for capturing a voice print that is tied to the particular transaction.

Advantages & Disadvantages		
Technology	Advantages	Disadvantages

Digital Certificates	"The benefits of certificates and CAs occur when two entities both trust the same CA. This allows them to learn each other's public key by exchanging certificates signed by that CA. Once they know each other's public key, they can use them to encrypt data and send it to one another, or to verify the signatures on documents. Use of certificates both authenticates the user and provides evidence of user intent since the certificate is encrypted and made a part of the transaction." ** From Microsoft	Requires individuals to pre-register with one or more CAs. Can be expensive to acquire and maintain (revocation, stolen computers, changes in user status, etc.). The process can be confusing for casual users.
User ID & Password	Understood by most users. Easy to use.	Managing the password system, forgotten passwords, etc. Passwords can be compromised. No guarantee the person entering the password is who they say they are. Do not provide for non-repudiation of the transaction.
Keypad Capture	Replica of a "wet" signature.	Expensive. Not practical for most Internet solutions.
Fingerprint	Stores fingerprint for later validation.	Does not provide for non-repudiation of the transaction. Expensive. Not practical for most Internet solutions.
Retina Scan	Difficult to counterfeit.	Does not provide for non-repudiation of the transaction. Expensive. Not practical for most Internet solutions.
Voice Signature	Relatively inexpensive to implement. Provides both validation and non-repudiation.	Can be perceived as cumbersome to users.

Signature capture technology and processes used can be based on the level of validation required. This is generally related to the risk of loss associated with an individual transaction. We classify this risk as follows:

Classification	Definition	Discussion
Inside the Firewall	Employees, suppliers, and others are provided with a user id and password allowing access to the internet.	Covers most people involved with the operation of an organization. These systems are well-established, with management and administrative processes in place.
Outside the Firewall:		
Registered Users	Suppliers, customers, and qualified prospects have been asked to register (and provide personal information) to the organization and are subsequently provided a user id and password.	Uses the same processes as Inside-the-Firewall.
Anonymous Users	Unknown, casual users that wish to enter a transaction with the organization.	Highest risk category; generally, requires biometric or signature pads.
All Transactions	Any existing transaction that currently requires a signature to be affixed to a form.	The first step in any process requiring a signature is to assess the purpose of the signature, the associated risks, and the potential loss if the signature is not captured. The recommendation is to eliminate any signature requirement that cannot be justified in terms of actual risk abatement. This generally requires changes to policies and processes.

Electronic signature technologies are constantly evolving, and it is a challenge to keep up. Forms designers need to: thoroughly understand the requirements of the workflow; challenge the need for a signature; understand the available solutions; and apply the appropriate solution within the form design. If all else fails, take it to paper.