Initial eNotary Signature Candidate Profiles

John Messing

These are adapted from the Electronic Court Filing TC ECF 3.x profiles:

1. Null signature profile. This is essentially a click-wrap signature. A logical association is created between presented text, a signer's action in response to the text, and a database record of the action and a document's properties, such as a file name and/or hash value to establish the signature. Signer authentication may involve use of a username and password to logically associate a user's identity as signer with a signed document. This profile seems most closely to fit the notion of a notarial signature proposed by certain mortgage banking and title companies in connection with the ABA Best Practices document, with the additional step of creating a tamper-evident seal of the entire package of documents, including the notary's click-wrap signature, in connection with secure transmission of the relevant documents to a land recording office or note repository.

2. Digital Signature Profile. This profile enables use of conventional, commercially available PKI digital certificates for users to sign documents at a client computer workstation. This profile most closely fits the NNA-Verisign pilot project in Pennsylvania.

3. Application specific profile. This profile allows signers to use existing tools available within the applications themselves for signing Adobe Acrobat and Microsoft Word documents.

4. Proxy signature profile. A server makes its asymmetric key and digital certificate available to authenticated signers enabling them to sign uploaded documents or hashes of them electronically. This allows implementers to make use of another OASIS XML standard available through the Digital Signature Services (DSS) Technical Committee.

5. Symmetric signature profile. A server uses a symmetric key known only to itself. This method builds upon the null signature profile and effectively secures the hashes of the submitted documents against pre-imaging attacks while optionally binding the identity determination cryptographically to the hash. In addition, use of a symmetric key can prevent a known signature verification problem that can occur with conventional PKI digital certificates. Once the certificate expires (usually in one to two years from the date of issue) all signatures that were previously generated through using it may no longer properly validate, creating potential confusion in archived records.