

Electronic and Digital Signatures

Key issues to consider

No electronic signature technology in and of itself is sufficient to meet your legal needs. The evidentiary value of your signed records will ultimately rely on your ability to produce legally admissible documentation of your recordkeeping system. In addition, you will, of course, have to produce the electronic records themselves. Just preserving and providing access to electronic records present some daunting challenges (refer to the guideline *Electronic Records Management Strategy* for additional information). Adding electronic signatures to the equation can complicate the situation even further.

Every option available to you has its own advantages and disadvantages. Some issues are constant, though:

- Consider technology obsolescence: hardware and software become quickly outdated, often making it difficult, if not impossible, to preserve and provide access to older electronic records. If you are using two different technologies to create and to sign a record, they might “age” at different rates.
- Plan to document your decisions and transactions: understanding your legal needs and addressing them at the design phase of an application are keys to making this work. Keeping documentation up-to-date is an on-going responsibility, which could be complicated if you are relying on a third party. If you are using digital signatures, for example, you need to make sure that your certificate authority is managing its records and documentation adequately.
- Make sure that your electronic signature technology is interoperable with your and your constituencies’ other software applications: requiring complex or expensive solutions is probably not practical. It would be especially difficult to ask citizens to buy and maintain multiple signature technologies.
- Remember that the human side of the equation is critical: no technology will completely address your legal requirements. For example, despite all its attractive features as a technology, a digital signature is only as reliable as the certificate authority standing behind it.

Overall, selecting the appropriate electronic signature technology means defining the criteria you consider important and then determining if your system and proposed application meet those criteria. The criteria should give priority to legal concerns, since signatures are primarily valuable for evidentiary purposes. But your assessment should include the consideration of other factors, such as technology architectures, costs/benefits, your business practices, and all the policies, hardware, software, controls, and audit procedures that are pertinent.

For a model of and methodology for system development and assessment, refer to the *Trustworthy Information Systems Handbook*. For a specific example of the criteria pertinent to a digital signature application, see the American Bar Association's *PKI Assessment Guidelines* (See the *Annotated List of Resources* at the end of these guidelines).

Discussion Questions

- Why do you want to use electronic signatures? What business functions will the technology support?
- Who will have to use and rely on the electronic signature?
- How long will the signatures and the records to which the electronic signatures are affixed have to be preserved?
- Which state and federal statutes pertain to the functions and transactions that generate your signed records? What case law is there?
- How does the electronic signature technology fit into your overall technology architecture? What's the total cost of the technology? What's the cost per transaction?
- What sort of electronic signature technologies do your customers use? Will you have to share these records with any other organizations or agencies? What technologies do they use?
- What methodology will you use for documenting your information systems, policies, and practices?