



## BEST PRACTICE

### Using Electronic Signatures (2006) (TIM)

**Background.** Federal legislation enacted in 2000, the *Electronic Signatures in Global and National Commerce Act* (the E-Sign Law), made electronic signatures and electronic contracts just as legally enforceable as traditional paper contracts signed in ink. Therefore, a digital signature is to an electronic document what a handwritten signature is to a paper document. However, a digital signature can provide additional assurances and security in linking an electronic document with the signer. The recipient of a digitally signed document can verify that both the document originated from the person whose signature is attached and that the document has not been changed since it was signed. Additionally, the signer of the document cannot later claim his digital signature was forged.

The term “electronic signature” is a generic, technologically neutral term that refers to the variety of ways a person can indicate their connection with an electronic document. Examples include:

- a symbol – sound or voice print
- a name typed at the end of an email
- a digitized form of a handwritten signature
- a unique password, code, or PIN number
- biometrics (retina scans, fingerprints, etc.)
- a digital signature created using encryption technology

The E-Sign Law does not define what an electronic signature is or what technologies can or should be used to create one. The law establishes only that E-signatures in all their various forms qualify in the legal sense and leaves it up to the free market to determine which methods will be used.

Many kinds of E-signatures offer very little security. If someone uses an unsecure method (such as a scanned image of a handwritten signature), it could be stolen and used for fraudulent purposes. Stolen E-signatures have the potential to become as widespread a problem as credit card scams and stolen passwords.

**Recommendation.** The Government Finance Officers Association (GFOA) recommends that state and local governments continue to improve electronic access to their services and information by other government entities and the public. When the identity of contact and/or the contents of the information received must be authenticated, the use of a secure form of electronic signatures is encouraged.

Governments should look for solutions that accomplish the following:

- There is a permanent attachment of a signature to the related document (for example, via a PDF or similar document that cannot be altered or via appropriate encryption).
- There is a permanent audit trail of the electronic signature.
- If changes are made to the documents, it will automatically alert the reader of those changes.

Additionally, the government should consider the following when setting up their electronic signature policies:

- Assess the risk of fraud, error or misuse of the various types of electronic signatures.
- Assess the cost-benefit on different alternatives of electronic signatures.

- Consult your legal counsel on the implications of using electronic signatures.
- Develop plans for retaining and deleting electronic information and employee access to such information.
- Seek input from technology experts.
- Perform periodic review and re-evaluation as appropriate.

### **References**

- P.L.106-229, the *Electronic Signatures in Global and National Commerce Act* (E-SIGN).  
[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106\\_cong\\_public\\_laws&docid=f:publ229.106.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf)  
June 30, 2000.
- United States Government Office of Management and Budget. Appendix II to OMB Circular No. A-130, Implementation of the Governmental Paperwork Elimination Act, November 4, 2003.

Approved by the GFOA's Executive Board, October 6, 2006.