Bulletin on Digital Signatures

Federal Deposit Insurance Corporation

September 30, 2000

Bank Technology Bulletin

TO: Chief Executive Officers of All FDIC Insured Banks

SUBJECT: *Digital Signature Deployment Issues*

The future is increasingly pointing to the use of digital documents and digital signatures. The speed with which a bank adopts new technology is not as important as the quality of the solution that a bank adopts. Banks should thoughtfully consider the attributes of a new or augmented information system to be certain it will interoperate with their existing systems, and the solution vendor is capable of withstanding a changing marketplace.

The growth of e-commerce and the recent enactment of the Electronic Signatures in Global and National Commerce Act (E-Sign Act) have presented banks with a new set of technology-related issues to consider. The E-Sign Act provides for the legal validity of "electronic signatures"[1] on such documents as checks, loan applications and contracts. The term "electronic signature" encompasses a number of different technologies, including "digital signature" technology.

Digital signature technology is the electronic equivalent of a written signature on written documents. The e-commerce marketplace is generally focusing on digital signatures[2] as an essential component. This is, in large part, due to digital signatures addressing the issues of authentication, non-repudiation and message integrity.

Forecasted growth of online lending alone indicates that e-commerce and digital signatures are an area that many banks may explore. However, due to the complexities of digital signature technology, it is imperative that banks research the area and engage in careful planning before deployment.

This technology bulletin is informational in nature and outlines four of the most critical issues for financial institutions to consider when deploying digital signature technology

Banks considering deploying these technologies should exercise caution in selecting a vendor and adopting its solutions.

Owing to the initial and ongoing costs, it is unlikely that banks will opt to develop their own digital signature technology and, thus, they will be outsourcing this function or purchasing this capability for their existing infrastructures.

A number of new vendors have emerged as a result of the increased demand for digital signature technology. Unfortunately, a given vendor may be marketing a proprietary solution that may not be compatible with the bank's other systems. Interoperability, now and in the future, should be a primary consideration.

The lack of interoperability and too few standards may result in ultimate failure of the system purchased. According to the consulting firm GartnerGroup, "…30% to 40% of public key infrastructure deployments will fail within two years of launching because they fail to demonstrate value." This means banks that engage certificate authority (CA)[3] start-up organizations may find themselves using digital signatures that are unverifiable[4] or information systems that have no technical support. While standards and best-use policies[5] are being developed and integrated into information system products, banks should perform a thorough due diligence on any vendor marketing a digital signature solution.

Signing and Receiving Documents

When signing a document, the sender uses his or her private key and a numerical algorithm to create an encrypted image of the original document that is sent with the clear text document to a recipient.

When receiving a document and verifying the signature, the recipient uses the public portion of the sender's key. Together, both parts of the sender's key are used to verify the document was not altered and that it originated from the signer of the document.

Implementing the use of digital signatures requires adopting a new or augmented set of technologies, services and bank policies.

When a bank decides to implement digital signatures, the bank must also implement digital documents[6] and the associated requirements for, among other things, document management, storage, access security, periodic hardware upgrades, and disaster recovery facilities. Further, the implementing bank could incur additional expenses as a result of the need for more staff in the form of new technology-management positions.

Once the bank decides to implement digital signatures, the bank has made a strategic decision to maintain digital records and service digital documents. Maintaining digital documents will require new policies and procedures, and introduce new complexities pertaining to system upgrades and information conversions.

If digital documents are used, customers will need reasonable access to those documents. Additionally, if a bank chooses to implement remote access to digital documents, the bank may need to establish a secure information area that allows customers access.

Digital documents, such as mortgages, could have an active life of more than 30 years plus an additional three- to five-year retention life. Some banks never destroy old loan documents.

A bank can operate a CA service for its customers. However, becoming a CA may require different technical skills and may impose liabilities.

While banks routinely verify the identification of existing and new customers, the electronic authentication process is more complex, and the decision to operate a CA is more involved. The primary role of a CA is to issue and verify digital certificates. The CA issues certificates that are used, in part, to verify the authenticity of a user signing or encrypting a document.

There are advantages and disadvantages associated with a bank becoming a CA (see box). A thoughtful review of these items should be included in a bank's decision-making effort.

Operating a CA requires additional facilities for hardware, specific operational policies and procedures, disaster recovery systems, and diligent attention to security for managing revocation lists and monitoring for unauthorized access.

Liability could arise from a variety of scenarios. For example, consider a bank customer using a bank-issued digital certificate to authenticate a digital signature for contracts or other digital documents that are external[7] to the bank. If the bank's CA service issues incorrect certificate types or revokes a certificate erroneously and a customer is unable to use its digital signature, legal exposure could result.

Becoming a Certificate Authority

Advantages

- Establishes bank customer identity.
- Technology is relatively inexpensive.
- Adds potential for customer retention.
- Provides for community outreach.

Disadvantages

- Standards are still changing.
- Requires additional expenses to operate services.
- Requires more technical expertise.
- Creates potential new liabilities for bank.

Hardware and software in support of digital signatures and digital documents will become obsolete and require replacement. Conversion of the digital signature and digital document to newer, more capable platforms will likely result in some loss of data.

Hardware and software will inevitably become obsolete. The usable life of computer hardware is approximately three to five years. The functional life of software is shorter, often only six months to a year. If a bank does not upgrade and replace older equipment, the bank could operate at a disadvantage.

The E-Sign Act is serving as a catalyst to support the gathering and storage of digital documents and signatures. Given that a document will need to be converted to a new file format at least once and perhaps several times over the life of the document, banks can reasonably expect conversion failures. Careful implementation of safeguards during file conversions or upgrades is paramount to prevent or minimize loss of data.

Questions or comments regarding the contents of this bulletin should be directed to the Bank Technology Group by email: e-banking@fdic.gov.

Becoming a Certificate Authority

When hardware or software is replaced, there is always a risk of loss of data in the conversion. Problems can develop, such as faulty backup tapes, incompatible hardware, differing standards, file conversion errors, and file layout differences.

Christie A. Sciacca
Director, Bank Technology Group

[1]In the E-Sign Act, the term "electronic signature" is defined broadly as follows: "The term 'electronic signature' means an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Section 106(5).

[2]A digital signature is a unique sequence of data that is split into two parts that together form a complete encryption key. One part is publicly shared and the other part is kept private - known only by the owner.

[3]A certificate authority is an organization responsible for issuing and verifying digital certificates used, in part, for digital signatures.

[4]An unverifiable certificate is a certificate whose issuer cannot be verified - a fictitious certificate.

[5]Best-use policies are those policies adopted by the industry to cope with real or perceived shortcomings in a technology or hardware/software product.

[6]Digital documents are those documents that exist in electronic form and not on paper. Digitally signed documents are digital documents. The document cannot be separated from the digital signature.

[7]External transactions are those transactions to which the bank is not a party.

Last Updated 10/05/2000