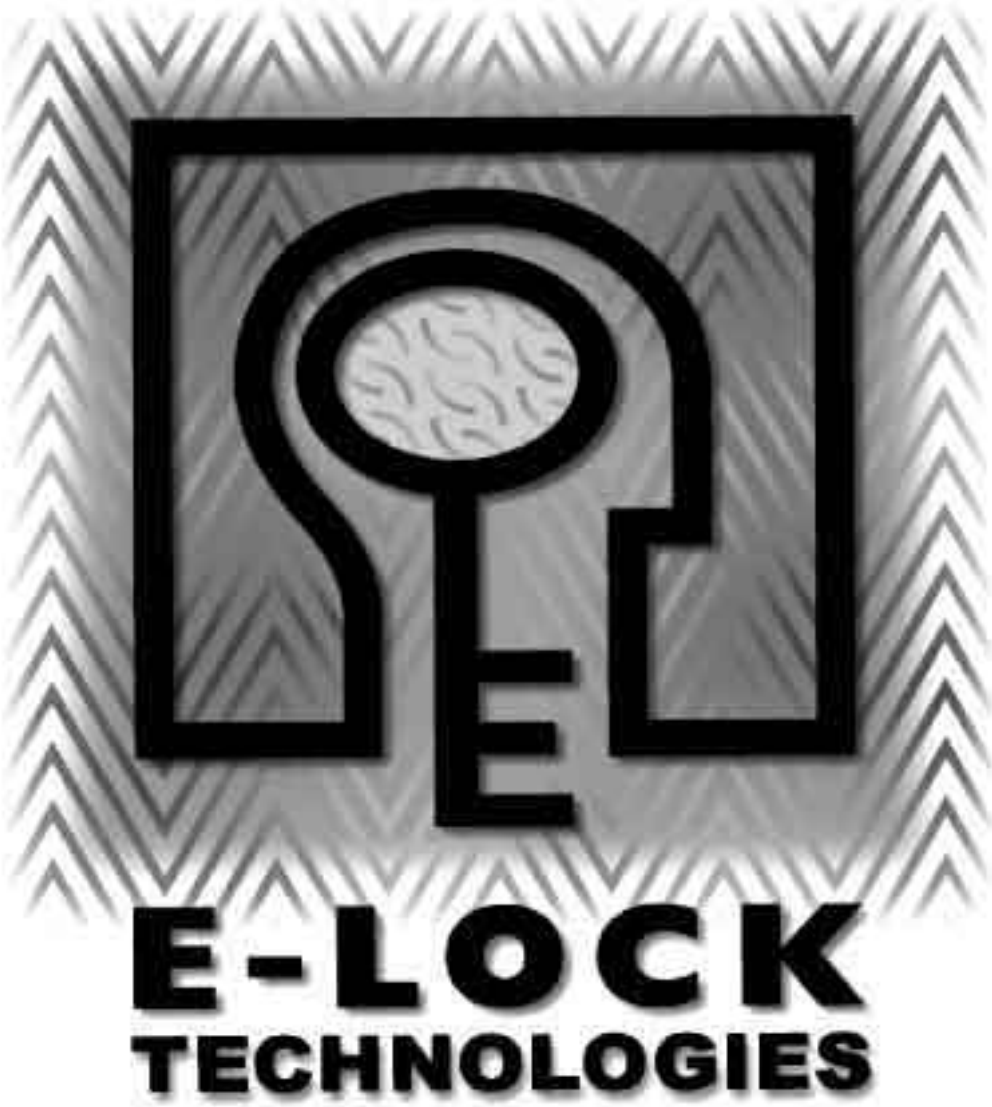


Business Issues in the implementation of **Digital signatures**

Much has been said about **e-commerce**, the growth of e-business and its advantages. The statistics are overwhelming and the advantages are so enormous that few companies can afford to not shift to this new digital economy.

E-Business breaks geographical, physical and time barriers and brings numerous time, cost, and efficiency related benefits to your business. Until recently, e-business was largely for retail or business to consumer transactions. Comparatively, organizations have shied away from conducting business-to-business transactions, due to the insecure nature of the Internet and because of the need of business trust in such transactions.

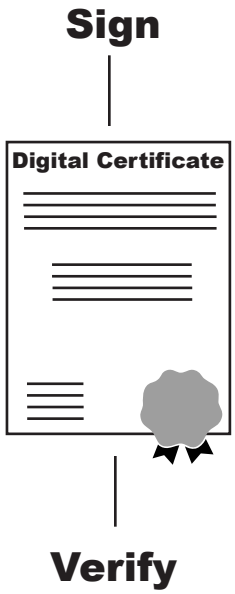
The arrival of **digital signatures**, and their legalization by Governments all over the world, has marked a new revolution in the world of electronic transactions. Digital Signatures will make business transactions over the Internet easier, and more reliable for businesses and consumers.

What are Digital Signatures?

Digital Signatures are based on Public Key Technology that uses asymmetric cryptography. Each person's identity is related to a key pair - a private key and a public key. These keys are nothing but mathematical codes generated on your computer.

The private key is under its owner's sole control and the public key is distributed to everyone without any risk to security. The private key is used for signing and the public key is used for verification. A Certifying Authority identifies and proofs individuals before issuing digital certificates to them.

This is very similar to credit cards, where you are proofed for identity before a card is issued to you, and this card is trusted by organizations in general since they trust the issuer. Credit cards are valid for a specific time period, and are renewed by the Credit card Authority after that time expires. It is exactly the same with digital certificates. The only difference is that in case of a credit card, the same card can be used for making payments and can be used by outside parties to verify your identity. In case of digital certificates, you use the private key for a transaction and other parties can verify your identity using the public key.



The significance of having ***two different keys*** in a PKI based transaction is that the public key, which is freely distributed, cannot be used for participating in a transaction, it can only be used for identification and verification. Only the private key, which is under the sole control of the owner can be used for participation in transactions.

What do Digital Signatures provide?

Specifically, Digital Signatures serve three business purposes: Authentication, Data Integrity, and Non-repudiation.

Authentication

Authentication refers to positively establishing an individual's identity in an electronic transaction. Since a digital certificate is issued on proofing by a trusted third party, it unquestionably identifies a person as who he claims to be.

Data integrity

In an electronic transaction, data flows through open networks. It is essential to ensure that data remains intact, and is not tampered with while it passes from the sender to the recipient. Data integrity refers to ensuring that data is in its original form and is not altered in any way en route to the recipient. When digital signatures are applied to data, they are glued in particular manner to the data. Any change in data will remove this binding and render the signature invalid.

Non-repudiation

Now that authentication and data integrity are established, the only thing that remains is to bind signers to the information that they sign. This is exactly like in a real-world business process where once your signature is on a document, you are legally bound to it and its content. Even at a later date, none of the participants in the transaction can deny their involvement.

Implementation of Digital Signatures

The real value of digital signatures is not in their application to transactions but in the level of security and trust they provide in a business process. They should be able to provide authentication of the sender and non-repudiation of the contents of a document. They should also be simple to use, secure, and meet all legal and regulatory requirements as laid down by the legislation.

In addition to signing and verification, there are various other factors that need to be considered for establishing business trust.

☑ Validating Digital Identities

Since digital identities can expire or be revoked by Certificate Authorities, it is important that the verification process involves verification of the Digital ID used to sign the data in addition to verification of the integrity of data content.

Certificate Authorities publish certificate revocation lists at regular intervals and revocation checking can be done against these lists. Newer technologies allow online checking of revocation status to provide the most recent status of the digital certificate being validated. This is similar to credit card systems where the validity of the card is checked at the time of the transaction.

☑ Time Stamping

One also needs to consider signature validity with reference to time. For instance, a document that is signed now should show as valid even if is verified years from now. The digital certificate used in signing may expire at a give date, say 1 yr or 2 yrs from now. But an expired certificate does not automatically mean that the signature is invalid. Digital Signature solutions should be intelligent enough to make this distinction and establish if the certificate was valid at the time of signing.

☑ Signing with valid digital identities

Signing should not be allowed with a digital identity or certificate that has been revoked or has expired. This not only binds the sender to the contents of the document but ensures that the individual's digital identity is trusted and valid.

☑ Multiple Signatures

A business process may involve two or more parties that need to be bound to the same data as in the case of a Non-Disclosure Agreement or an approval procedure. All involved parties need to sign the same digital content to indicate their consent. Each of the signatures on the document should also be capable of being verified independently.

☑ Policy based digital signing

Organizations should have the flexibility to centrally control and manage the use of digital signatures to ensure that their usage is in compliance with organizational policy. For instance, in an approval process, it is essential that documents be signed in a particular sequence - typically in order of hierarchy. This signing sequence needs to be enforced, so that all signatures needed on the document are received and also to ensure that no one signs out of turn.

☑ Confidentiality of high-value transactions

Certain high value documents such as financial reports or technical design documents need to kept confidential and their access should be restricted to only authorized people. Digital Signatures allow for the encryption of such sensitive documents so that only authorized and intended recipients can decrypt and view them. This allows for sensitive documents to be part of the workflow process while limiting and defining their accessibility.

Digital signatures offer a wide range of advantages for business processes. However, organizations need to carefully consider what features are best suited to their individual business needs and then work towards implementing a complete digital signature solution rather than buying different products in a piecemeal manner to address various issues. A complete solution should address **application interoperability**, **browser independence** and **ease of use.**

Lastly, it is important to distinguish between an electronic signature and a digital signature. An electronic signature is a very loosely defined term and is usually associated with a graphical image of a handwritten signature. Various technologies like biometrics, retinal scans, voice recognition, and hardware tokens also provide electronic signatures. However, PKI based digital signatures are the most popular and the most accepted form of electronic signatures. Most of the electronic signatures provide authentication but PKI based digital signatures provide other features that are essential for conducting business over the net.

For more information

Info@elock.com

E-Lock Technologies
10777 Main St., Suite 300, Fairfax, VA 22030, U.S.A.
Tel. (703) 383 9360 Fax.(703) 383 9366

www.elock.com