

Tal Saraf, Senior Systems Engineer and Internet Technologies Expert, Microsoft Corporation

Interactive Internet sites require secure methods for transferring data and financial transactions. The solutions include encryption and digital signature technology and policy initiatives such as Certificate Authorities and SET.

The new paradigm of the Internet is the "active" interactive page. This increases the risk to users of encountering malicious code (viruses), tampered code, unknown authors and impersonations. Authentication and encryption are the key to secure data transmission, whether code, Email, or financial transactions.

One initiative to ensure data authentication is the Certificate Authority (CA) system. CAs are established organizations that verify a software publisher's identity. To apply for a certificate, a software publisher agrees to meet the CA's policies and submits the public key of its public/private key encryption. The CA publishes the public key and issues an identifying certificate that can be applied to an unlimited amount of code or other electronic items until it expires or is revoked. Verisign was the first CA. GTE, AT&T and the United State Postal Service are in the process of becoming CAs.

By allowing commercial or personal certification and various trust levels, the CA system lets code recipients know the risk level of any item. Automated systems could be designed to accept or reject transmission based on the information specified in a certificate.

As indicated, public/private key encryption plays an important role in authentication. In this form of encryption, a sender uses a private key to encrypt data. The recipient uses the sender's public key. By comparing a hash of the original code with a hash of decrypted code, a recipient can verify data integrity. Encryption is also used for digital signatures. Like a handwritten signature, digital signatures identify a software or data publisher. It guarantees that an item has not been altered from the time it was digitally "signed."

In addition to ensuring secure transmission of code, major financial and software companies (Microsoft, Visa, Mastercard) are designing means to ensure financial transmissions. The SET standard (a merging of STT and SEPP) is a universal comprehensive bankcard payment protocol. SET uses message-based encryption to allow multi-party transactions, multiple transports (Email), and secure interaction.