GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

# Digital Certificates:
# A Secure Method for Digital Transfers

By: Stephen N. Williams

Electronic commerce is a strategic imperative for most competitive organizations today. It is a key to finding new customers, entering into new markets, cutting costs, and creating breakaway business strategies.

Electronic commerce is a very intriguing venture, but the risks involved are as great if not greater that than potential rewards. The infrastructure that supports electronic commerce can be susceptible to abuse, misuse, and failure, causing number of business problems--including financial loss due to fraud, lost business opportunities due to service disruption, a tarnished reputation for service, and loss of customer confidence.

Reports of attacks on computer networks or electronic services are abundant--from the 1995 hacking attack on Citibank's cash management system to the series of hacker attacks on U.S. military research facilities, Denial of Service attacks on major e-commerce venders, to the break-in at Microsoft that resulted in source code being stolen are all real world examples of the risks involved with the digital world.

Independent estimates of the extent of electronic fraud are staggering. For example:

- Online information theft, including pirated software, stolen credit card numbers, and unauthorized access to corporate secrets, is estimated to be in excess of $10 billion annually in the U.S. alone
- Nearly half of organizations suffered the consequences of an information-security-related financial loss in the last two years
- Credit card fraud is estimated at $5 billion annually

It is clear that businesses that conduct electronic commerce must protect themselves. It is not always clear how they should do so.

Digital authentication systems are becoming an essential part of doing business via the Internet and to protect corporate data form within. With the use of various encryption techniques, digital signature systems enable organizations to electronically confirm such features as their identity, their credit, or the legitimacy of an electronic document. A site certificate allows for secure sessions between a client and a server by providing authentication and confidentiality through digital signature technology and encryption thus insuring confidentiality, sincerity of data, authentication and non-repudiation. These are all key ingredients for the successful protection of data transmission..

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Digital certificates are electronic files that act like a kind of online passport. They are issued by a trusted third party, a Certificate Authority, which verifies the identity of the certificate's holder. A Certificate Authority 's role is analogous to that of a states Department of Public Safety, which issues driver's licenses and which is acknowledged and accepted as a trustworthy means of personal identification. The major Certificate Authorities offer a combination of cryptography technology, an infrastructure of highly secure facilities, and a specification of practices and liability that establish its ability to operate as a trusted third party. Certificate Authorities entrench an individual's or an organization's public key along with other identifying information into each digital certificate and then cryptographically sign it as a tamper-proof seal, verifying the integrity of the data within and validating its use. The Digital Certificate can not be copied or compromised. Thus Digital certificates are synonymous with an individuals fingerprints in the fact that they identify the individual without question. The certificate itself is simply a collection of information to which a digital signature is attached.

A digital signature is a piece of data that is sent with an encoded message to uniquely identify the originator and to verify that the message has not been altered since it was sent. A digital signature goes beyond other techniques such as integrity check-value mechanisms because it supports non-repudiation. In other words, it may legally be used to resolve disputes between parties in a transaction, should one party deny that the transaction occurred. Below is an example of a digital signature:

Integrity check-values cannot perform this function since the recipient knows the key used to generate the integrity check-value, and could therefore have created the value instead of the sender

Digital certificates do two things:

1. They authenticate that their holders - people, web sites, and even network resources such as routers - are truly who or what they claim to be.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. They protect data exchanged online from theft or tampering.

Digital certificates are part of the broader scope of Public Key Infrastucture (PKI), the same technology used to protect nuclear missile sites. PKI is the foundation for secure Internet applications. An enterprise's PKI constitutes the core of its Internet security infrastructure—the key to ensuring authenticated, private and non-repudiable communications. The success of an enterprise's PKI will have a major impact on its core business operations**.** Each key is like a unique encryption device. No two keys are ever identical, which is why a key can be used to identify its owner.

PKI protects your information assets in several essential ways:

- **Authenticate identity:** Digital certificates issued as part of your PKI allow individual users, organizations, and web site operators to confidently validate the identity of each party in an Internet transaction.
- **Verify integrity:** A digital certificate ensures that the message or document the certificate "signs" has not been changed or corrupted in transit online.
- **Ensure privacy:** Digital certificates protect information from interception during Internet transmission.
- **Authorize access:** PKI digital certificates replace easily guessed and frequently lost user IDs and passwords to streamline intranet log-in security - and reduce the Management Information Systems overhead.
- **Authorize transactions:** With PKI solutions, your enterprises can control access privileges for specified online transactions.
- **Support for non-repudiation:** Digital certificates validate their users' identities, making it nearly impossible to later repudiate a digitally "signed" transaction, such as a purchase made on a web site.

Digital Certificates automate the process of distributing public keys and exchanging secure information. Digital certificates may be distributed online--even through unsecure networks--because the certificates are self-protecting. Typical means of distributing certificates include:

- **Certificate accompanying signature:** The signer has a copy of its own certificate and can attach a copy of that certificate to the digital signature. If this is done, anyone who wants to verify a signature will have the certificate in hand.
- **Directory service:** When using public-key technology, the message originators must first obtain the certificates of the intended recipients. When multiple parties are involved, this can be a complex task. Directories provide an easy way to search for and find certificates on the Web.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

When you install a digital certificate on your computer or server, your computer or web site now has its own private key. Its matching public key is freely available as part of your digital certificate posted on your computer or web site.

Keys always work in pairs, one called the private key, and the other called the public key. What a public key encrypts, only the corresponding private key can decrypt, and vice versa. Public keys are distributed freely to anyone who wants to exchange secure information with you. The private key shows that the signature must have been made by the owner of that key. Your private key is never copied or distributed and remains secure on your computer or server.

When another computer wants to exchange information with your computer, it accesses your digital certificate, which contains your public key. The other computer uses your public key to validate your identity and to encrypt the information it wants to share with you using Secure Sockets Layer (SSL) technology. A secure hash, of the entire document is signed, so that any change to the document will invalidate the signature. Only your private key can decrypt this information, so it remains secure from interception or tampering while traveling across the Internet.

Secure Hash is a process which reduces a message of arbitrary length to a fixed length fingerprint which is very unlikely to be the same for any other message. The word "secure" indicates that the algorithm has been chosen so that it is not possible to forge a message which to have given hash value, nor to create two similar messages with the same hash value,

Digital Certificates are an integral part of an information security plan, and cryptography plays an important part. Cryptography is essential in today's information society. The establishment of a good infrastructure for information security that incorporates cryptography should be a organizations top priority. It safeguards the integrity and confidentiality of stored or transported data; it can also be used for non-repudiation of the sender. Indeed, for many purposes, cryptography is the only way to effectively shield information from unauthorized access or altering. For instance, cryptography protects billions of dollars of financial transactions that are processed daily over the global financial networks; it also provides for electronic payment, both in sending credit card numbers securely and with digital cash. Encrypted services, such as pay-TV or video-on-demand constitute a growing market. Likewise, the soaring market for mobile communications is enabled through cryptographic protection. E-mail can be encrypted to safeguard the confidentiality of privacy-related or sensitive company information; it also provides integrity, which is essential in electronic business transactions, online tax declaration, and government information publishing. Cryptography will enable new applications such as road pricing and electronic voting. A few of these applications are somewhat exotic, but many are everyday necessities.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The diagram below illustrates a typical electronic transaction using SET. Secure Electronic Transactions (SET) is a complete protocol and infrastructure specification for supporting bank card payments over the Internet. It was developed in 1995 by Visa, MasterCard, VeriSign, and many other organizations and technology vendors.

After the cardholder agrees to make a purchase from the merchant, the cardholder sends an online payment instruction to the merchant. The merchant then communicates with the appropriate financial institution (acquirer) via a payment gateway, forwarding the payment instruction, to authorize and capture the transaction. The capturing is done by the acquiring bank (leaving the merchant out of the transaction).

© SANS Institute 2000 - 2002, Author retains full rights.

The minimization of risk is imperative for business to survive the growing threats of a digital world. The transferring of documents and financial information and electronic funds must be protected for today's businesses to survive the highly competitive markets. A company must strive to protect their infrastructure and to defend their customers privacy and integrity. The Digital Certificate provides the most secure method of this type of data exchange. While doing business over the internet is essential for today's companies the Digital Certificates dramatically reduces the risk while facilitating the ease of customer access and the greatest protection for both entities.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

## Bibliography:


Jamie Lewis. "Digital-Signature Standard Gets Closer With Industry Support"
http://www.internetweek.com/columns00/lewis101100.htm (11 Oct 2000)

Eric Verheul, Bert-Jaap Koops, Hend van Tilborg. "Binding Cryptography A fraud detectible alternative to key-escrow proposals"
http://cwis.kub.nl/~frw/people/koops/bind-art.htm (Jan Feb 197)

"How Digital Certificates Work"
http://home.netscape.com/security/techbriefs/certificates/howcerts.html?cp=stbmid :

"Certificate Authority Program"
http://home.netscape.com/security/caprogram/index.html?cp=stbrt

"Introducing Enterprise PKI"
http://www.verisign.com/whitepaper/enterprise/difference/index.html :

"Encryption and Digital Certificates"
http://www.verisign.com/whitepaper/enterprise/overview/index.html:

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. "Handbook of Applied Cryptography"
http://www.cacr.math.uwaterloo.ca/hac/ (Oct 1996)


© SANS Institute 2000 - 2002, Author retains full rights.