

An Introduction to
Digital Signatures

By Clyde Hoadley
Metropolitan State College of Denver
<http://clem.mscd.edu/~hoadleyc/>
hoadleyc@mscd.edu

v1.0
May 30, 2002

WHY DO WE USE SIGNATURES?3

WHAT IS A DIGITAL SIGNATURE?3

WHY DO WE NEED DIGITAL SIGNATURES?.....4

WHAT IS PKI?5

HOW DO DIGITAL SIGNATURES WORK?5

ARE THERE STANDARDS AND LAWS THAT PERTAIN TO DIGITAL SIGNATURES? 8

ARE THERE ANY PROBLEMS WITH DIGITAL SIGNATURES?9

HOW CAN I GET A DIGITAL SIGNATURE?9

REFERENCES10

Why do we use signatures?

Signatures have been used in every society for thousands of years. A signature does not have to be a written name; it can be any mark that serves to authenticate a document. A signature may serve different purposes depending on the context in which it is used. The American Bar Association lists five such examples:

1. *“Evidence: A signature authenticates a writing by identifying the signer with the signed document.”*
2. *“Ceremony: The act of signing a document calls to the signer’s attention the legal significance of the signer’s act, and thereby helps prevent “inconsiderate engagements.”*
3. *“Approval: In certain contexts defined by law or custom, a signature expresses the signer’s approval or authorization of the writing, or the signer’s intention that it have legal effect.”*
4. *“Efficiency and logistics: A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.”¹*

What is a digital signature?

A digital signature is an electronic mark used to authenticate an electronic document. A digital signature is normally made in such a way that the identity of the signer can be verified and, it provides assurance that the document has not been altered. When used correctly, a digital signature is very difficult to falsify.

A digital signature should not be confused with a digital certificate. A digital signature can, and often is used by itself. A properly issued digital certificate is issued by a trusted impartial third party called a Certificate Authority. A digital certificate encapsulates the public key for the owner of the certificate, along with additional information that helps to support the authenticity of the certificate, and is digitally signed by the issuing Certificate Authority.

Both digital signatures and digital certificates make use of asymmetric cryptography (sometimes called public key private key cryptography).

Why do we need digital signatures?

The increasing reliance on the Internet, e-mail and on-line business brings an increase in the potential for fraud, misuse and theft when conducting business electronically. Digital signatures and digital certificates help to reduce those threats.

Ordinary e-mail can easily be forged and, under the right conditions, an e-mail message can be intercepted and read by others. It is also not uncommon for the sender to mistype an e-mail address and send private correspondence to the wrong person. Ordinary e-mail is not a safe and secure communication medium but it can be made more secure with the use of digital signatures.

When people engage in eBusiness over the World Wide Web, the customer needs some assurance that the Web site they are accessing is actually the Web site for the business they are transacting business with. It is not very difficult to hijack, misdirect or spoof a Web site and mislead customers into transacting business with a bogus web site. If the legitimate business has installed a valid and current Digital Certificate, issued by a trusted third party, the customer has strong assurance that they are using the correct Web site. Digital Certificates can also be used to provide confidentiality of the transaction by encrypting the data that is sent and received. If the customer has their own digital certificate, the business has assurance that the customer is who they claim to be.

If Jane sends Dick a digitally signed e-mail message, the digital signature provides the following assurances:

1. Authentication. When Dick receives the message, he can verify the digital signature to be certain that it was actually Jane that sent the message.
2. Integrity. If Dick is able to successfully verify Jane's digital signature, Dick knows that the message Jane sent has not been altered and what he received is what Jane sent.
3. Non-repudiation. Because Dick is in possession of a verified digitally signed message from Jane, Jane cannot deny that she sent the message nor can she dispute the contents of the message.
4. Confidentiality. Jane also has the option to encrypt her message before sending it so that only Dick would be able to decrypt the message and read it.

What is PKI?

PKI (public key infrastructure) is the technology and organizational structure used to support the issuance of digital certificates by a trusted third party. The trusted third party is called a Certificate Authority (CA). One of the responsibilities of the Certificate Authority is to authenticate the identity of the individual or business who requests a digital certificate. PKI also provides directory services to facilitate retrieving and verifying the public key for a digital certificate. PKI provides a certificate management system, which includes the ability to revoke a previously issued certificate. RFC-2459 is the primary document that describes the Public Key Infrastructure (PKI). Several different vendors have implemented PKI solutions, however these implementations are not always compatible with each other. The standard for PKI is still under development.

Asymmetric encryption is the cornerstone of PKI. Asymmetric encryption is a method of encrypting data which uses two mathematically related keys. One key is used when encrypting the data and the other key is used to decrypt the data. Unlike symmetric encryption, the same key cannot be used for both encrypting and decrypting the data. When PKI issues a digital certificate, it generates a unique pair of public and private keys for the certificate. The owner of the certificate keeps their private key a secret and never shares it with anyone else.

How do digital signatures work?

The process of creating and affixing a digital signature is usually done by software that is integrated into an application program. Many modern e-mail clients have this software built into them. This makes it very easy send and receive digitally signed e-mail or even encrypted mail. Some software used for signing or encrypting electronic documents can be used separately from other software; Pretty Good Privacy (PGP) is an example.

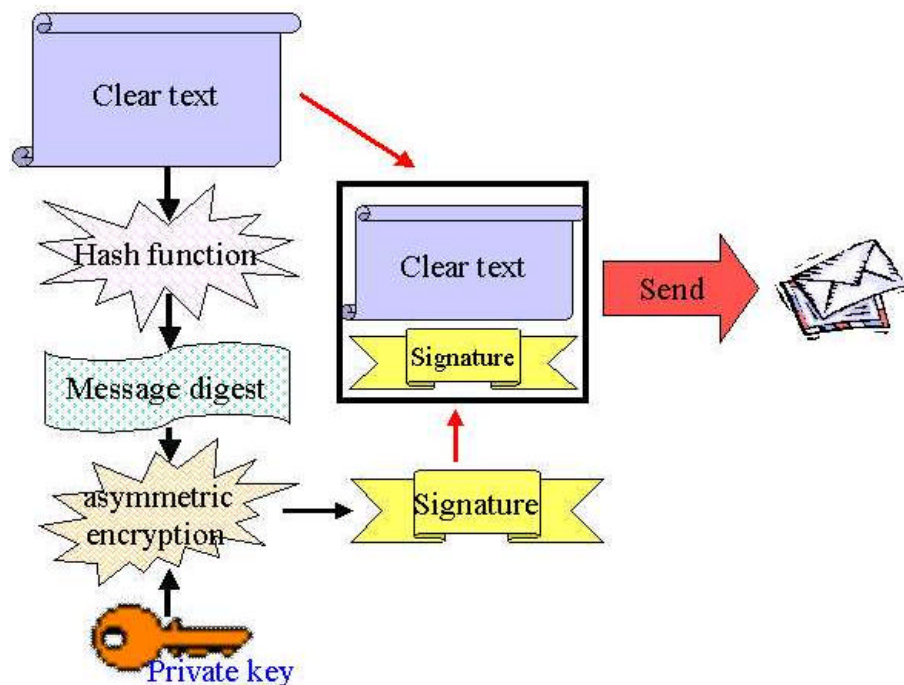
Before you can sign e-mail or other electronic documents with a digital signature, you must first obtain a unique public and private key pair. This would normally be done by obtaining a digital certificate from a PKI Certificate Authority. When using a digital certificate, you must install the certificate into your e-mail program. Regardless, you must protect and keep secret your private key. The private key is often protected with a password. You make your public key available to others; there are many different ways to do that, including adding it to a directory service.

Creating and sending a digitally signed e-mail message is a five step process:

1. Type in your message.
2. Calculate a message hash value (also called a message digest).

3. Use **your private** key to encrypt the hash value. This is your digital signature.
4. Attach or append the digital signature (the encrypted hash value) to the message.
5. Send your message, including the digital signature, to the recipient.

A hash value is a fixed length string of characters that has been mathematically derived from the input text, such as the text of an e-mail message. A hash function uses a one-way encryption algorithm which produces a unique hash value for a given text. It is mathematically difficult to duplicate a hash value or its original text. MD5 and SHA are common hashing programs.

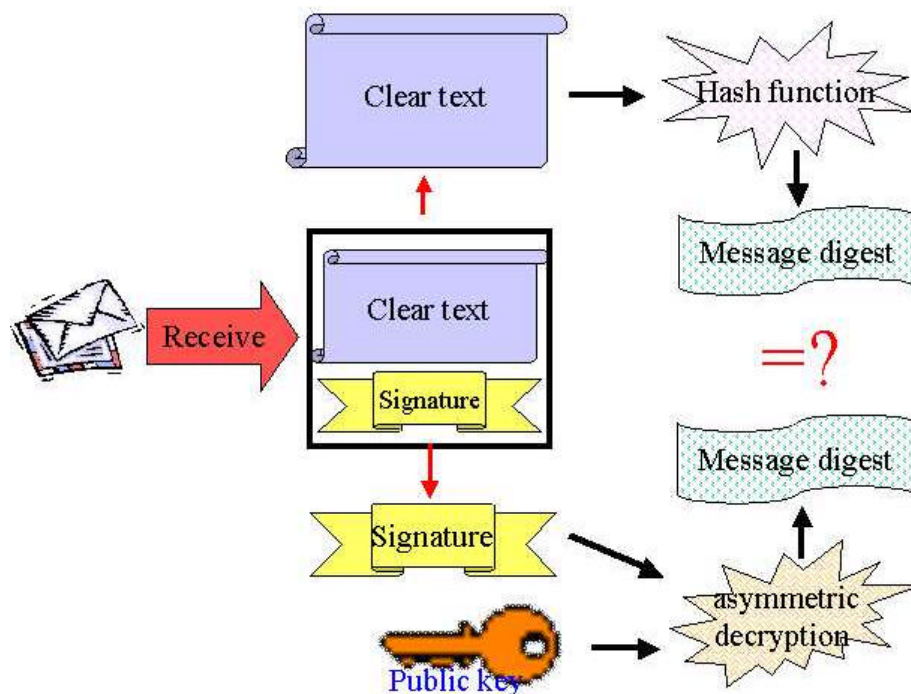


Signing and sending a digitally signed e-mail message

To read and verify the signature of a digitally signed message, the following steps are performed:

1. Open the digitally signed message.
2. Extract the digital signature.
3. Use the **senders public key** to decrypt the signature. This yields the hash value of the original message text.
4. Extract the message text.
5. Calculate the hash value of the extracted message text.

6. Compare the freshly calculated hash value against the hash value retrieved from the digital signature.
 - a. If the two hash values match then:
 - i. It was the senders "private key" that encrypted the attached hash value.
 - ii. The message that was received is the message that was sent.
 - b. If the two hash values do not match each other then:
 - i. The senders private key was not used when signing the message or,
 - ii. The message text has been altered.



Reading and verifying the signature of a digitally signed e-mail message

Notice that the receiver uses the **senders public key** to decrypt the senders digital signature. Decrypting the senders digital signature results in the hash value of the original message that was sent.

When the calculated hash value matches the decrypted hash value, it means that the senders public key successfully decrypted what had been encrypted. When the senders public key successfully decrypts what was encrypted, it means that only the **senders**

private key could have been used during the encryption process. And, since only the sender knows and has access to their private key then, it was indeed the sender who signed the message; this authenticates the sender. This also means that the sender can not deny having sent the message; this is called non-repudiation.

When the calculated hash value matches the decrypted hash value, it means that the message has not been altered. What was received is what was actually sent.

When the calculated hash value does not match the decrypted hash value, it means either the message was altered after it had been signed or, someone is attempting to impersonate the sender (the sender isn't who they claim to be).

Are there standards and laws that pertain to digital signatures?

The primary standards document for Digital Signatures is the Federal Information Processing Standards Publication 186-2, "Digital Signature Standard (DSS)" also called FIPS 186-2. The DSS establishes standards for the creation of Digital Signatures only. It does not apply to digital certificates or other file encryption. The DSS applies to all Federal departments and agencies for unclassified information. FIPS 186-1 established the Digital Signature Algorithm (DSA) as the Federal standard for the creation and use of Public and Private keys; it also established SHA-1 as the algorithm to be used for computing the hash value. The standard was updated in February of 2000 to permit the use of RSA encryption and Elliptic Curve encryption; SHA-1 remains the standard for computing the hash value. SHA-1 is defined in FIPS 180-1, "Secure Hash Standard (SHS)".

The Internet Engineering Task Force document RFC-2459, "Internet X.509 Public Key Infrastructure Certificate and CRL" provides the definition of PKI. Many different vendors have developed PKI solutions. However, each vendors PKI implementation differs slightly and therefore they are not compatible with each other.

In October 2000, Congresses passed the "Electronic Signatures in Global and National Commerce Act" and it was signed into law by President Clinton. searchSolaris.com provides the following description of the "Electronic Signatures in Global and National Commerce Act":

"The Electronic Signatures in Global and National Commerce Act (often referred to as the e-signature bill) specifies that in the United States, the use of a digital signature is as legally valid as a traditional signature written in ink on paper. In effect since October 1, 2000, the U.S. law is expected to save companies that use

e-signatures a significant amount of money by reducing the costs of mailing and handling hard-copy contracts and similar documents.

“The Act does not specify a single digital signature technology. Many e-signature advocates expect that the public key infrastructure (PKI), used for authenticating credit card transactions over the Web, will play an important role in the development of secure e-signatures. Several third-party companies are now exploring other methods to verify a person's legal identity, including the use of personal smart cards, PDA encryption devices, and biometric verifications (fingerprint, voice, or iris scans). Experts agree that until the legality of e-signatures has been tested in the courts, the routine use of e-signatures is likely to be several years away, primarily because businesses lack confidence in present security and verification procedures.”⁴

Are there any problems with digital signatures?

The problems associated with digital signatures are more accurately problems associated with the PKI. Some of the problems associated with PKI are:

1. Competition between standards.
2. Standards that are still in flux which have not been fully adopted.
3. What requirements should a Certificate Authority satisfy?
4. How do you select a Certificate Authority?
5. Can, should and how do Certificate Authorities cross certify?
6. Should you install your own PKI solution and be your own Certificate Authority or, should you outsource the role of Certificate Authority?
7. Interoperability of digital signatures and digital certificates issued by different Certificate Authorities.
8. Ease of use and key management.

How can I get a digital signature?

You can obtain a Digital signature (or Digital ID) for use with e-mail from VeriSign by visiting their web site at <http://www.verisign.com/products/class1/index.html>. It costs \$15 per year. The VeriSign digital signature works with both Netscape and Outlook e-mail clients, using either IMAP or POP and, can be used to digitally sign or encrypt your e-mail messages. VeriSign is just one of many PKI Certificate Authorities.

References

1. The American Bar Association. Digital Signature Guidelines Tutorial.
Online: <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. Chicago.
2. SANS Institute. "Security Essentials: Encryption I.", Version 1.11, 2001.
3. searchSecurity.com. "Digital signature.",
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html
4. searchSolaris.com . "Electronic Signatures in Global and National Commerce Act.",
http://searchsolaris.techtarget.com/sDefinition/0,,sid12_gci347233,00.html
5. Savage, David E. "A Digital Certificate Introduction". SANS Institute: 2001.
Online: <http://rr.sans.org/encryption/certificate.php>.
6. National Institute of Standards. "Digital Signature Standard (DSS).",
<http://csrc.nist.gov/cryptval/dss.htm>.
7. SANS Institute. "Security Essentials: Introduction to VNPs, PKI and PGP.",
Version 3.4, 2002.