

Repository

Introduction to Digital Certificates

Digital Certificates provide a means of proving your identity in electronic transactions, much like a driver license or a passport does in face-to-face interactions. With a Digital Certificate, you can assure friends, business associates, and online services that the electronic information they receive from you are authentic. This document introduces Digital Certificates and answers questions you might have about how Digital Certificates are used. For information about the cryptographic technologies used in Digital Certificates,

What is a Digital Certificate?

Digital Certificates are the electronic counterparts to driver licenses, passports and membership cards. You can present a Digital Certificate electronically to prove your identity or your right to access information or services online.

Digital Certificates, also known as digital certificates, bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information. A Digital Certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using phony keys to impersonate other users. Used in conjunction with encryption, Digital Certificates provide a more complete security solution, assuring the identity of all parties involved in a transaction.

A Digital Certificate is issued by a Certification Authority (CA) and signed with the CA's private key.

A Digital Certificate typically contains the:

Owner's public key

Owner's name

Expiration date of the public key

Name of the issuer (the CA that issued the Digital Certificate)

Serial number of the Digital Certificate

Digital signature of the issuer

The most widely accepted format for Digital Certificates is defined by the CCITT X.509 international standard; thus certificates can be read or written by any application complying with X.509. Further refinements are found in the PKCS standards and the PEM standard.

What are Digital Certificates used for?

Digital Certificates can be used for a variety of electronic transactions including e-mail, electronic commerce, groupware and electronic funds transfers. Netscape's popular Enterprise Server requires a Digital Certificate for each secure server.

For example, a customer shopping at an electronic mall run by Netscape's server software requests the Digital Certificate of the server to authenticate the identity of the mall operator and the content provided by the merchant. Without authenticating the server, the shopper should not trust the operator or merchant with sensitive information like a credit card number. The Digital Certificate is instrumental in establishing a secure channel for communicating any sensitive information back to the mall operator.

Why do I need a Digital Certificate?

Virtual malls, electronic banking, and other electronic services are becoming more commonplace, offering the convenience and flexibility of round-the-clock service direct from your home. However, your concerns about privacy and security might be preventing you from taking advantage of this new medium for your personal business. Encryption alone is not enough, as it provides no proof of the identity of the sender of the encrypted information. Without special safeguards, you risk being impersonated online. Digital Certificates address this problem, providing an electronic means of verifying someone's identity. Used in conjunction with encryption, Digital Certificates provide a more complete security solution, assuring the identity of all parties involved in a transaction.

Similarly, a secure server must have its own Digital Certificate to assure users that the server is run by the organisation it claims to be affiliated with and that the content provided is legitimate

What Digital Certificate Services do you offer?

We provide issuing, revocation, and status services for three types of Digital Certificates -- Server Certificates, Digital Certificates for companies, and personal Digital Certificates for use with Web Browsers and S/MIME applications.

Server Certificates enable Web servers to operate in a secure mode. A Server Certificate unambiguously identifies and authenticates your server and encrypts any information passed between the server and a Web browser.

Digital Certificates for companies are used by individuals but with their company information, when they exchange the data with other users or any online services (Tenders,Forms,etc.)

Personal Digital Certificates are used by individuals when they exchange messages with other users or online services.

We offer three classes of Digital Certificates. The classes are differentiated by their assurance level--the level of confidence that can be placed in the Digital Certificate based on knowledge of the process used to verify the owner's identity. The identification requirements are greater for higher numbered classes--for example, a Class 1 Digital Certificate verifies the owner's e-mail address, while a Class 2 Digital Certificate offers the additional assurance of verification of the owner's personal identity.

What is authentication?

Authentication allows the receiver of a digital message to be confident of both the identity of the sender and the integrity of the message.

What is a digital signature?

A digital signature functions for electronic documents like a handwritten signature does for printed documents. The signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming the signature was forged.

In other words, Digital Signatures enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message

How is a digital signature used for authentication?

Suppose Alice wants to send a signed message to Bob. She creates a message digest by using a hash function on the message. The message digest serves as a "digital fingerprint" of the message; if any part of the message is modified, the hash function returns a different result. Alice then encrypts the message digest with her private key. This encrypted message digest is the digital signature for the message.

Alice sends both the message and the digital signature to Bob. When Bob receives them, he decrypts the signature using Alice's public key, thus revealing the message digest. To verify the message, he then hashes the message with the same hash function Alice used and compares the result to the message digest he received from Alice. If they are exactly equal, Bob can be confident that the message did indeed come from Alice and has not changed since she signed it. If the message digests are not equal, the message either originated elsewhere or was altered after it was signed.

Note that using a digital signature does not encrypt the message itself. If Alice wants to ensure the privacy of the message, she must also encrypt it using Bob's public key. Then only Bob can read the message by decrypting it with his private key.

It is not feasible for anyone to either find a message that hashes to a given value or to find two messages that hash to the same value. If either were feasible, an intruder could attach a false message onto Alice's signature. Specific hash functions have been designed to have the property that finding a match is not feasible, and are therefore considered suitable for use in cryptography.

One or more Digital Certificates can accompany a digital signature. If a Digital Certificate is present, the recipient (or a third party) can check the authenticity of the public key

How long do digital signatures remain valid?

Normally, a key expires after some period of time, such as one year, and a document signed with an expired key should not be accepted. However, there are many cases where it is necessary for signed documents to be regarded as legally valid for much longer than two years; long-term leases and contracts are examples. By registering the contract with a digital time-stamping service at the time it is signed, the signature can be validated even after the key expires.

If all parties to the contract keep a copy of the time-stamp, each can prove that the contract was signed with

valid keys. In fact, the time-stamp can prove the validity of a contract even if one signer's key gets compromised at some point after the contract was signed. Any digitally signed document can be time-stamped, assuring that the validity of the signature can be verified after the key expires

What is the legal status of documents signed with digital signatures?

If digital signatures are to replace handwritten signatures they must have the same legal status as handwritten signatures, i.e., documents signed with digital signatures must be legally binding. The Australian Government and most states and territories in Australia have already enacted legislation that gives electronic communications the same status as written communications at law (both criminal and civil). These are known as the Electronic Transactions Acts. There are some limitations on when electronic communications are effective, but the basic principle is that transactions are not invalid because they took place electronically. However, since the validity of documents with digital signatures has never been challenged in court, their legal status is not yet well-defined. Through such challenges, the courts will issue rulings that collectively define which digital signature methods, key sizes, and security precautions are acceptable for a digital signature to be legally binding.

Digital signatures have the potential to possess greater legal authority than handwritten signatures. If a ten page contract is signed by hand on the tenth page, one cannot be sure that the first nine pages have not been altered. However, if the contract was signed with digital signatures, a third party can verify that not one byte of the contract has been altered.

Currently, if two people want to digitally sign a series of contracts, they might first sign a paper contract in which they agree to be bound in the future by any contracts digitally signed by them with a given signature method and minimum key size.

How do I use Digital Certificates?

When you receive digitally signed messages, you can verify the signer's Digital Certificate to determine that no forgery or false representation has occurred.

When you send messages, you can sign the messages and enclose your Digital Certificate to assure the recipient of the message that the message was actually sent by you. Multiple Digital Certificates can be enclosed with a message, forming a hierarchical chain, wherein one Digital Certificate testifies to the authenticity of the previous Digital Certificate. At the end of a Digital Certificate hierarchy is a top-level Certification Authority, which is trusted without a Digital Certificate from any other Certification Authority. The public key of the top-level Certification Authority must be independently known, for example by being widely published. The more familiar you are to the recipient of the message, the less need there is to enclose Digital Certificate.

You can also use a Digital Certificate to identify yourself to secure servers such as membership-based Web servers.

Generally, once you've obtained a Digital Certificate, you can set up your security-enhanced Web or e-mail application to use the Digital Certificate automatically.