

Digital Certificate

Today, digital certificates are a critical component of all online commercial transactions.

Secure communication over the Internet is paramount in importance. As concerns over Internet privacy and security have grown amid an increase in e-commerce transactions, knowing that we are communicating confidentially has become a top priority. Today, business and consumer relationships exist entirely online and parties must have the absolute assurance that they are communicating securely. PenTeleData Digital Certificates help fortify the communication of sensitive or private information online.

What is a Digital Certificate?

Technically, a digital certificate is an attachment to an electronic message used for security purposes. A digital certificate is used to verify that a user sending a message is who he or she claims to be. It also provides the receiver with the means to encode a reply.

Digital certificates give Internet and Extranet users two certainties:

Identity Confirmation — The party receiving the information (the party controlling the server) is the party to whom the communication is intended.

Non-interception — The user's information will not be intercepted, interpreted or corrupted between the user's browser and the server.

Who Needs a Digital Certificate?

Any company or individual wishing to send or collect private information to or from its users needs a Digital Certificate. This includes all e-commerce web-sites (for which SSL security has already become the standard) as well as sites which communicate private and personal information with its users. Any company or individual that wishes to communicate such important information should have their own digital certificate from PenTeleData.

PenTeleData Digital Certificates

PenTeleData currently offers three varieties of Digital Certificates: Shared, Private & Verisign digital certificates.

Shared — A Shared digital certificate provides customers with the first level of security. It is called "Shared" because a singular encryption signature is used by a number of clients. However, PenTeleData Shared digital certificate customers employ the same certificate encryption scheme as any other. Digital certificates are, in part, used to confirm identity, and the security provides commercial customers fundamental browser authentication. A user who visits a certificate-secured page does nothing special, and no changes to any system are needed (the client's machine must use a browser with 128-bit enabled encryption). Use of a Shared digital certificate ensures that the website is trusted, as a certificate is stored on the user's computer. PenTeleData recommends at least Shared certificate-level security to any business providing e-commerce transmission of sensitive information on a website to authenticate who your customers say they are. Also, by offering the first level in security for your online commercial transactions, a digital certificate wards against costing you and your customers money pursuing issues associated with various electronic frauds.

Private — A Private digital certificate provides vendors and customers the comfort of extraordinary security, since each Private digital certificate bears its own unique encryption signature. Used only one-per-entity, Private certificates offer a high level of Internet security. Although both Shared and Private digital certificates encrypt the data stream identically, only the Private digital certificate holder is the one who delivers that particular, specific key to its users.

There are two important benefits to having a Private certificate:

- **Liability For Stolen Data** — On-line privacy issues have become tremendously important. Privacy breaches result in embarrassment and loss of trust for on-line merchants and lead to costly and embarrassing litigation. Without a Private Digital Certificate, at some point in the data transfer process the possibility exists for information to get intercepted by another party using the same certificate.

- **Professionalism** — When the secure-session icon is visible in the browser's frame, it is indicating that the browser has entered into a secure session. Double-clicking on this icon will reveal information about the certificate. Among other items regarding the certificate (Certificate Authority, date of expiry, etc.), the information screen will identify to whom the certificate was issued. If the company to whom the certificate was issued is not the company with whom the user is intending to communicate then the level of professionalism is diminished and the trust is lost.

- **VeriSign** — PenTeleData also offers our customers the ability to purchase a full-serviced digital certificate from VeriSign, a third-party organization. This digital certificate works in the same way as a PenTeleData Private Certificate with the added benefit of insurance. Although an added feature, this type of digital certificate is more costly.

"The purchase of a Digital Certificate from PenTeleData ensures your customers receive the most trustworthy online security in the industry."

Jeff Reinhard
General Manager
- PenTeleData

How It Works

An individual wishing to send an encrypted message applies for a digital certificate from PenTeleData. PenTeleData issues an encrypted digital certificate containing the applicant’s public key and a variety of other identification information. PenTeleData makes its own public key readily available through print publicity or perhaps on the Internet. The recipient of an encrypted message uses the PenTeleData’s public key to decode the digital certificate attached to the message, verifies it as issued by PenTeleData and then obtains the sender’s public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

Secure Internet communication using Public Key Infrastructure PKI has four key components:

- **Private Key** — Each Private Key and Public Key is a mathematical algorithm through which a communication is passed and encrypted. A communication encrypted using a given Public Key may only be deciphered by the corresponding Private Key. Additionally, any communication encrypted with the Private Key can only be deciphered by the corresponding Public Key. The Private Key, as its name suggests, never leaves the server on which it was originally generated. Any individual using the Private Key to encrypt a message can rest assured that it can only be deciphered using the corresponding Public Key. The holder of the Public Key accepts communication with the confidence that the communication originated with the one and only holder of the Private Key.
- **Public Key** — The Public Key, as its name suggests, can be distributed publicly by the holder of the Private Key. Any individual encrypting a communication with the Public Key is assured that the communication can only be deciphered by the holder of the Private Key.
- **Trusted Third Party, TTP (a.k.a. Certificate Authority, CA)** — Sometimes in situations where a relationship is exclusively electronic, a user may obtain a Public Key from the holder of a Private Key but not have confidence that the holder of the Private Key is actually who they say they are. This is where the Trusted Third Party works. If the holder of the Private Key can show that their Public Key/Private Key pair has been certified by a TTP, then the user can have full confidence the Public Key they are using actually belongs to the party with whom they wish to communicate. A validated Public Key/Private Key pair in which the Private Key exists on a server is considered a Web Certificate.

In order to be useful, the Certificate Authority must be recognized by the major browsers as a Root Certification Authority. This means that when a browser sees the authentication it says “I trust that Authority’s judgment. Proceed”. This process is unseen to the user unless the CA is not recognized by the browser. If the key pair is not authenticated by a CA or the CA is not recognized by the browser the user will get a message stating that the identity of the server cannot be authenticated.

- **Secure Socket Layer Encryption (SSL Encryption)** — Once the identity of the server has been verified, the browser will open a SSL session with the server SSL encryption is used to encrypt information transfers from the user’s browser to the server with which the SSL session has been established. The browser encrypts the communication and the server deciphers the information. Internet browsers can enter into a secure communication at either 128-bit SSL encryption or 40-bit SSL encryption. 128-bit SSL provides a higher degree of protection than 40-bit. Although standard issue browsers are still 40-bit browsers, they can be easily upgraded.

The two key metrics by which a digital certificate can be evaluated are:

- **Browser Recognition** — In order for a Web Certificate to work without generating an error message it must be recognized by the browser. In order to be recognized the Web Certificate must have been issued by a CA that has root authority in the browser. This can be accomplished in two ways: 1) through an arrangement with the maker of the browser or 2) through an arrangement with a party that already has root authority in the browser. The list of CAs that have this authority is a static list in the browser. Therefore, for future revisions of the browser it is only possible for a new CA to get certification from the maker of the browser. In order to obtain certifications in existing versions of browsers, the only option is for the CA to get cross-certified by a CA that already has root certification in the browser. Therefore, depending upon with whom the CA has its cross-certification agreement and how it has managed its own root CA initiatives, each certificate will have varying degrees of recognition.
- **SSL Security Level** — Prior to January 2000 it was illegal for a North American company to export 128-bit technology outside of North America. That export restriction has since been lifted and none of the major Web Certificate suppliers sell 40-bit certificates any longer. A 128-bit SSL Web Certificate can support both 40-bit and 128-bit SSL sessions such that, if a web server is using a 128-bit web server certificate, the server will be able to securely communicate with any commercially available browser. The limitation on the level of security is the browser.

Digital Certificate Pricing:

PenTeleData Private Digital Certificate	\$10.00 per month (\$49.95 setup)
PenTeleData Shared Digital Certificate	\$5.00 per month (\$25.00 setup)
VeriSign Digital Certificate	\$349.00 per year (\$299.00 setup)

How Do I Get One?

PenTeleData makes it very simple to obtain a digital certificate. To begin the process of obtaining a Digital Certificate PenTeleData, prepare the following information before calling one of our friendly sales representatives:

- If your organization is a company, corporation, partnership, or proprietorship, you will need to submit the company registration document, or a copy of your article of incorporation or partnership stamped by the relevant authority to PenTeleData.
- If your organization is a government department or agency, you will need to submit an original letter signed by the department head on appropriate letterhead to PenTeleData. The letter must include contact information for the department and for the signer’s immediate superior.
- If your organization is a non-government organization (NGO), you will need to submit an original letter signed by the Chief Executive, Chairman, or Managing Director of the NGO on appropriate letterhead to PenTeleData.
- If your organization is a university, you will need to submit an original letter signed by the Dean or Vice-Chancellor of the requesting department on appropriate letterhead to PenTeleData. The letter must include contact information for the University.
- If your organization is A Doing Business As (DBA) organization, please submit a copy of the DBA registration papers for local levies and taxes or official correspondence indicating your right to use the name given.
- If your organization is a type of organization not listed here (such as the IETF) please contact PenTeleData to determine suitable documentation.

In order to complete the process, we will also need the following information:

Domain Name, Name of Owner, Company Name, Address, Name of Authorization Contact, Company Name, Phone Number, Title