A public key infrastructure (PKI) supports the distribution, revocation and verification of public keys used for public key encryption, and enables linking of identities with public key certificates. A PKI enables users and systems to securely exchange data over the internet and verify the legitimacy of certificate-holding entities, such as webservers, other authenticated servers and individuals. The PKI enables users to authenticate digital certificate holders, as well as to mediate the process of certificate revocation, using cryptographic algorithms to secure the process.

PKI certificates include a public key used for encryption and cryptographic authentication of data sent to or from the entity that was issued the certificate. Other information included in a PKI certificate includes identifying information about the certificate holder, about the PKI that issued the certificate, and other data including the certificate's creation date and validity period.

Without PKI, sensitive information can still be [encrypted](https://searchsecurity.techtarget.com/definition/encryption), ensuring confidentiality, and exchanged between two entities, but there would be no assurance of the identity of the other party. Any form of sensitive data exchanged over the internet is reliant on the PKI for enabling the use of [public key cryptography](https://searchsecurity.techtarget.com/definition/asymmetric-cryptography) because the PKI enables the authenticated exchange of [public keys](https://searchsecurity.techtarget.com/definition/public-key).

Elements of PKI

A typical PKI includes the following key elements:

A trusted party provides the root of trust for all PKI certificates and provides services that can be used to authenticate the identity of individuals, computers and other entities. Usually known as [certificate authorities (CA)](https://searchsecurity.techtarget.com/definition/certificate-authority), these entities provide assurance about the parties identified in a PKI certificate. Each CA maintains its own root CA, for use only by the CA.

A [registration authority](https://searchsecurity.techtarget.com/definition/registration-authority) (RA), often called a subordinate CA, issues PKI certificates. The RA is certified by a root CA and authorized to issue certificates for specific uses permitted by the root.

A certificate database stores information about issued certificates. In addition to the certificate itself, the database includes validity period and status of each PKI certificate. Certificate revocation is done by updating this database, which must be queried to authenticate any data digitally signed or encrypted with the [secret key](https://searchsecurity.techtarget.com/definition/secret-key-algorithm) of the certificate holder.

A certificate store, which is usually permanently stored on a computer, can also be maintained in memory for applications that do not require that certificates be stored permanently. The certificate store enables programs running on the system to access stored certificates, [certificate revocation lists](https://searchsecurity.techtarget.com/definition/Certificate-Revocation-List) and certificate trust lists.

A CA issues digital certificates to entities and individuals; applicants may be required to verify their identity with increasing degrees of assurance for certificates with increasing levels of validation. The issuing CA digitally signs certificates using its secret key; its public key and [digital signature](https://searchsecurity.techtarget.com/definition/digital-signature) are made available for authentication to all interested parties in a self-signed CA certificate. CAs use the trusted root certificate to create a "chain of trust;" many root certificates are embedded in web browsers so they have built-in trust of those CAs. Web servers, email clients, smartphones and many other types of hardware and software -- including IoT devices -- also support PKI and contain trusted root certificates from the major CAs.

PKI certificates

Along with an entity's or individual's public key, digital certificates contain information about the [algorithm](https://whatis.techtarget.com/definition/algorithm) used to create the signature, the person or entity identified, the digital signature of the CA that verified the subject data and issued the certificate, the purpose of the public key encryption, signature and certificate signing, as well as a date range during which the certificate can be considered valid.

While PKI certificates are used for implementing cryptography over web and other internet connections, they are also used for other applications, including individual certification for code signing applications, for authenticating digital transactions and more.

Problems with PKI

PKI provides a chain of trust so that identities on a network can be verified. However, like any chain, a PKI is only as strong as its weakest link. There are various standards that cover aspects of PKI -- such as the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527).

The Certification Authority Browser Forum, also known as CA/Browser Forum, is an industry consortium founded in 2005 and whose members include CAs, browser software publishers and other system providers who use X.509 digital certificates for encryption and authentication. The CA/Browser Forum publishes guidelines and best practices for CAs, browser and other parties involved in the PKI as it relates to the use of digital certificates.

Although a CA is often referred to as a "trusted third party," shortcomings in the security procedures of various CAs in recent years has jeopardized trust in the entire PKI on which the internet depends. If one CA is compromised, the security of the entire PKI is at risk. For example, in 2011, Web browser vendors were forced to [blacklist](https://whatis.techtarget.com/definition/blackhole-list-blacklist) all certificates issued by the Dutch CA DigiNotar after more than 500 fake certificates were discovered.

In 2017, Google engineers identified problems with certificates issued through Symantec's CA business, which led to subsequent distrust of all certificates issued by Symantec prior to the sale of its CA business to DigiCert last year.

A web of trust

An alternative approach to using a CA to authenticate public key information is a decentralized trust model called a "web of trust," a concept used in Pretty Good Privacy ([PGP](https://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy)) and other [OpenPGP](https://whatis.techtarget.com/definition/OpenPGP)-compatible systems. Instead of relying solely on a hierarchy of certificate authorities, certificates are signed by other users to endorse the association of that public key with the person or entity listed in the certificate.

One problem with this method is a user has to trust all those in the key chain to be honest, so it’s often best suited to small, user communities. For example, an enterprise could use a web of trust for authenticating the identity of its internal and remote users and devices. It could also act as its own CA, using software such as Microsoft Certificate Services to issue and revoke digital certificates.