# 15.2.2 Public Key Infrastructure Facts

The public key infrastructure (PKI) is an encryption and cybersecurity architecture that manages digital certifications and communication encryption. PKI ensures secure electronic transfer and provides authentication for communications, such as online banking, that require data integrity and stringent proof of identity.

This lesson covers the following topics:

- PKI componenets
- How PKI works
- Common certificate authorities
- Certificate signing

## PKI Components

Each component of PKI is an intricate part a security platform that makes communication secure. The following table describes the components of PKI.

| Component | Description |
|---|---|
| Certificate management system | The certificate management system is the primary component of PKI. It manages the certificate process and creates key pairs, which consist of public and private keys. It stores the private key for the host and helps to ensure private key safety. It distributes the public key to those who will access the system. PKI works to ensure the continued authenticity of the keys and verifies certificates. |
| Digital certificates | Digital certificates are electronic passwords. They associate the identity of a person or entity with a public/private key pair. |
| Validation authority (VA) | The validation authority is used to verify the validity of a digital certificate using the X.509 standard and RFC 5280. The VA also stores certificates with their public/private keys. |
| Certificate authority (CA) | The certificate authority is the organization that issues the digital certificate. The CA is also the controller of the PKI certificates. The CA, in a sense, mints the certificate and specifies critical pieces of information such as the organization name and the certificate expiration date. The private key certificate on the hosted website is checked against the CA to ensure it is valid and authentic. If the certificate is expired or the company name is different, the user will receive a warning stating the site failed the authenticity check. |
| Registration authority (RA) | The registration authority acts as the verifier for the CA. While, in many instances, the CA handles certificate registration, the CA may offload its registration and validation when an organization is geographically dispersed or PKI resources increase. |
| End user | The end user is the consumer who requests and uses certificates. Most of the activities involved in PKI are transparent to the user. For example, an individual might go to a website and completes a transaction, such as online banking or shopping, without being aware of the processes that take place to secure the transaction. |

## How PKI Works

PKI can be either an automated or manual process. Often, when a user visits a website, the website itself switches to a secure, encrypted mode using PKI. The steps to obtaining a digital certificate are as follows:

1. The user, company, or system intending to exchange information securely applies to an RA for a certificate.
2. The RA receives the request, verifies the subject's identity, and requests that the CA issue a certificate to the subject.
3. The CA issues the certificate, binding the subject's identity with the subject's public and private keys, and sends the updated information to the validation authority.

To initiate a transaction, the user sends the information and the digital certificate to the other party in the transaction. The other party then verifies the authenticity of the certificate with the validation authority. Finally, the validation authority compares the certificate of the user with the updated information provided by the CA and determines whether the certificate is valid. For a website to be trusted and enable secure communications using SSL and the PKI infrastructure, the certificate must come from a trusted source. A certificate is trusted because the information is verified by the trusted authority.

For example, a new business wants to create a secure website where consumers can shop and purchase goods. The website must protect a customer's information, including payment information, from being hijacked or intercepted. To do this, the merchant purchases a certificate from a trusted certificate provider. This is an arduous process since the merchant must prove identity. Merchants may have to provide corporate papers, business licenses, and other forms of evidence to corroborate and prove identify. Once satisfied, the trusted authority provides the business with its certificate and private/public keys and acts as the PKI CA, RA, and VA.

## Common Certificate Authorities

There are several CAs that issue PKI digital certificates and provide strong Secure Sockets Layer (SSL) encryption for secure communications such as email, banking, and trading. Some are well known, and others service more vertical markets that cater to the specific necessities requiring specialized services. The following table describes three very well-known CAs:

| Certificate Authority | Description |
|---|---|
| Comodo | Offers a wide range of PKI services including a strong SSL encryption available in either 128- or 256-bit encryption. |
| IdenTrust | Provides CA services for several vertical entities such as banks, corporations, government, and healthcare. |
| GoDaddy | Provides SSL certificates for both business and personal use. GoDaddy offers simple services with pricing to match and a complete range of certificates that comply with CA and internet browser forum guidelines. |

## Certificate Signing

While operating systems such as Windows and Linux can create their own public key infrastructure, it is much more common for organizations to use trusted authorities like the certificate authorities in the preceding table. Using SSL, an organization purchases the infrastructure to secure its websites. Web browsers recognize a trusted authority and will allow direct connection using SSL when browsing the website. If an untrusted authority, such as a local operating system, creates the keys, the user is generally warned that the site does not use a trusted authority and may not be safe.

Creating a self-signed certificate is an easy, straightforward task. In Linux, a user simply downloads and installs OpensSSL. The user answers a few simple questions such as the company name and how many bits should be used for the key. Then both a public and private key can be created and installed. This becomes a self-signed key and is untrusted. The user can also create public and private keys using tools like Adobe Reader, Java's keytool, or Apple's Keychain. These too will be untrusted.

Businesses or entities that don't use the internet for their business may choose to use self-signed certificates. These certificates provide secure communications; however, the certificate has not been vetted. A user accessing the website will get a warning message stating that the website is not untrusted. When this warning is issued, the user must be careful and continue only if the user knows, without a doubt, the website is safe. This is very common in internal websites and third-party tools where SSL is used.

---