Only you can see this message

This story's distribution setting is on. You're in the Partner Program, so this story is eligible to earn money. Learn more

How Certificates Work On The Web

Craig Godden-Payne
Apr 18 · 4 min read ★

Certificate Encryption

In order for a web request to establish an encrypted network connection using secure socket layer (SSL) / transport layer security (TLS) protocol, you must use an SSL/TLS certificate. SSL/TLS is a protocol that operates directly on top of the TCP protocol. The reason for this is that higher layers, such as http can be left unchanged whilst still providing a secure connection. If you look underneath the SSL layer, http is identical to https.

Benefits of using certificates

1 — Encryption

Encrypting traffic should not only be used to process sensitive information, such as credit cards or banking details, it should be used everywhere it can. When you enter information on a website, that data will pass through multiple touch points before it reaches its final destination.

If you don't use SSL/TLS encryption, the data sent from client to server, is sent as plain text, and could be viewed or altered by anyone at any of the touch points before it reaches its destination.

Encryption

2 — Authentication

An SSL/TLS connection ensures that data is sent to and received from the correct server. This is because the data cannot be intercepted without knowing the key.

It helps to prevent malicious actors from falsely impersonating a site.

3 — Data Integrity

An SSL/TLS connection ensures that there's no loss or alteration of data during transport by including a message authentication code. This ensures that the data that gets sent is received without any changes or malicious alterations.

How a connection is established

- Client starts to establish a TCP connection to a server
- Client requests that the server should identify itself, which includes which version of SSL/TLS it is running, what cipher suites it wants to use, and what compression methods it wants to use.
- Server sends its certificate. This certificate must be trusted by either the client itself or a party that the client trusts.

An example of this, would be if the client trusts a certain certificate authority. The client can trust a certificate from google.com, because the certificate authority cryptographically signed google's certificate.

- The certificate is validated, and if valid a key is exchanged. This is dependent on the cipher suite.
- Both the server and the client can now compute the key. The client tells the server that from now on, all communication will be encrypted, and sends an encrypted and authenticated message to the server.
- The server verifies that the message can be decrypted, and then returns a message, which the client verifies as well
- The two entities can communicate securely.

What is a Certificate Authority

A certificate authority (CA) is an entity that issues digital certificates. Commercially, the most common type of digital certificate is based on the ISO X.509 standard. The CA issues signed digital certificates that affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate. A CA also typically manages certificate revocation.

Difference between Public and Private Certificates

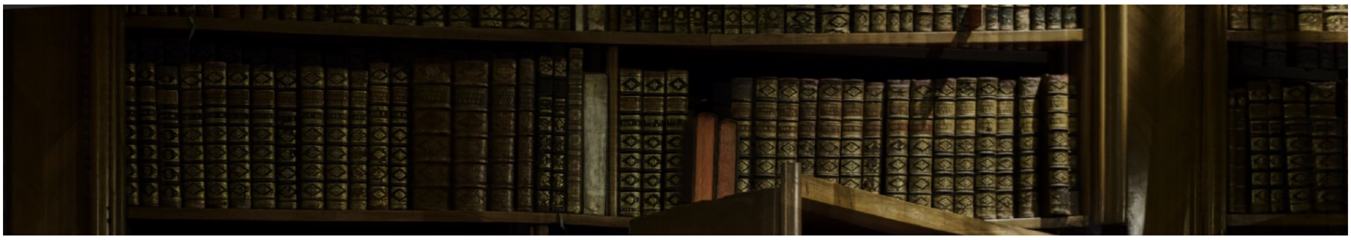
Public and private certificates identify resources on networks and secure communication between these resources.

Public certificates are used to identify resources on the public Internet, whereas private certificates do the same for private networks.

One key difference is that applications and browsers trust public certificates automatically by default, whereas an administrator must explicitly configure applications to trust private certificates.

Public certificate authorities must follow strict rules, provide operational visibility, and meet security standards imposed by browser and operating system vendors that decide which certificate authorities their browsers and operating systems trust automatically.

Private certificate authorities are managed by private organisations, and the administrators can make their own rules for issuing private certificates, including practices for issuing certificates and what information a certificate can include.



What can be seen by someone looking at your traffic?

If your traffic is encrypted using SSL/TLS, if someone were to sniff your traffic, all they would be able to see would be

- IP address and port it is connected to.
- How much data you are sending.
- Which encryption and compression are used.
- Potentially the hostname by making s reverse DNS lookup

They would not be able to see the content of the data being exchanged.

Digital Security Security Https Overview