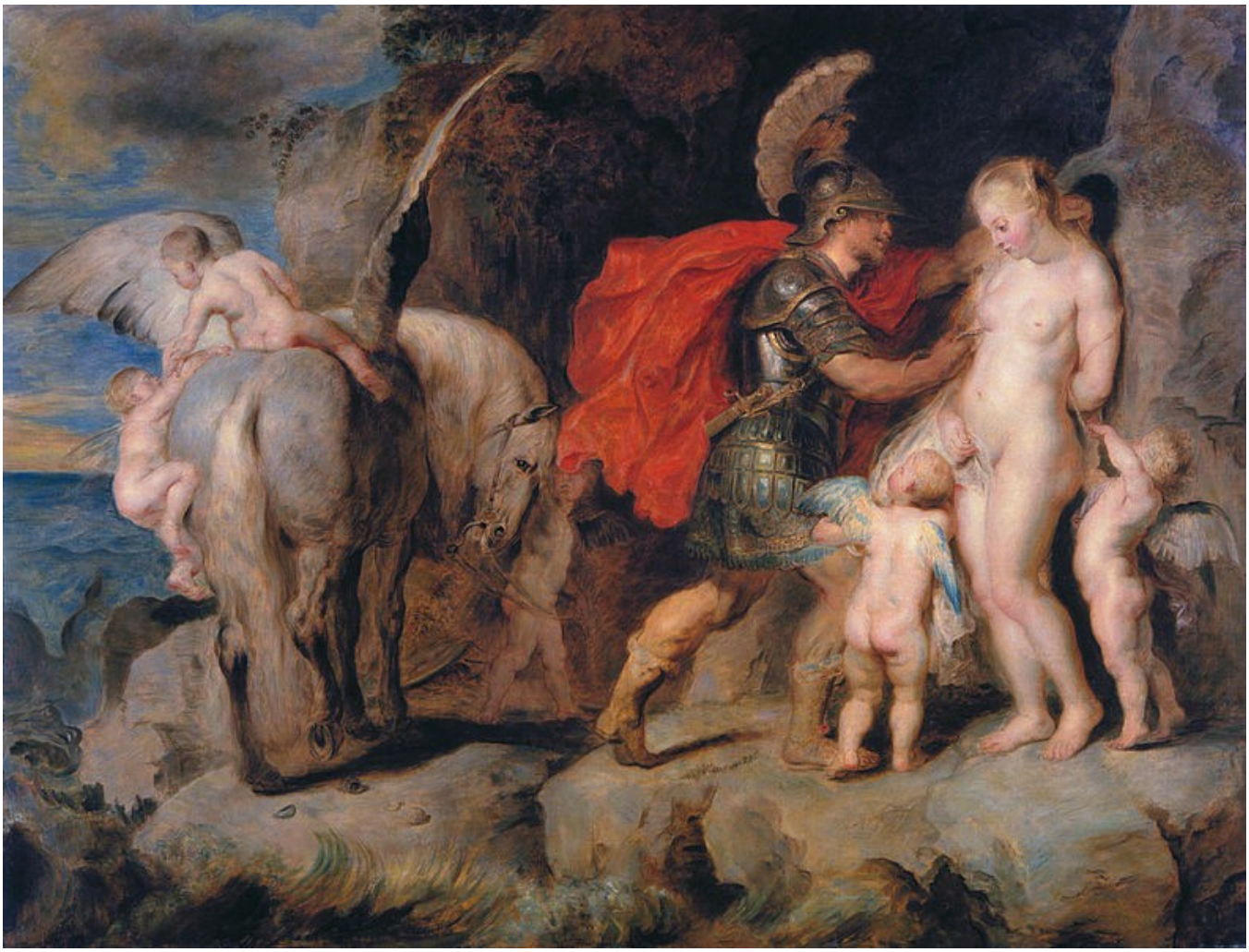
Certificate Chains, And How They Work

Craig Godden-Payne
Apr 19 · 3 min read ★



Certificate chains are used to be able to verify an end user certificate against a list of intermediaries and a root authority. We are going to explain this in a bit more detail.

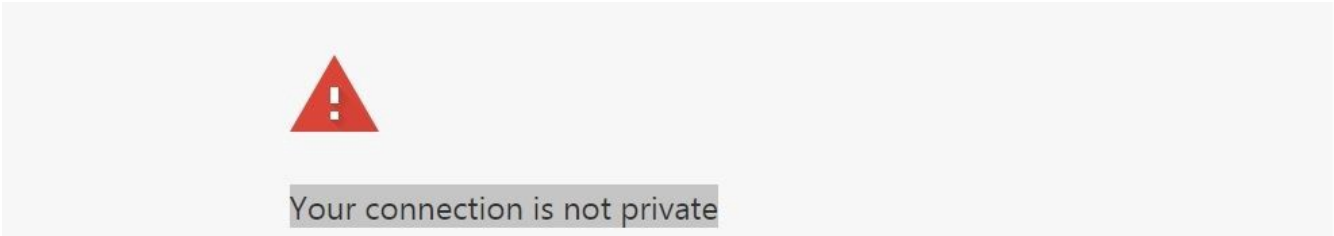
The Certificate Authority

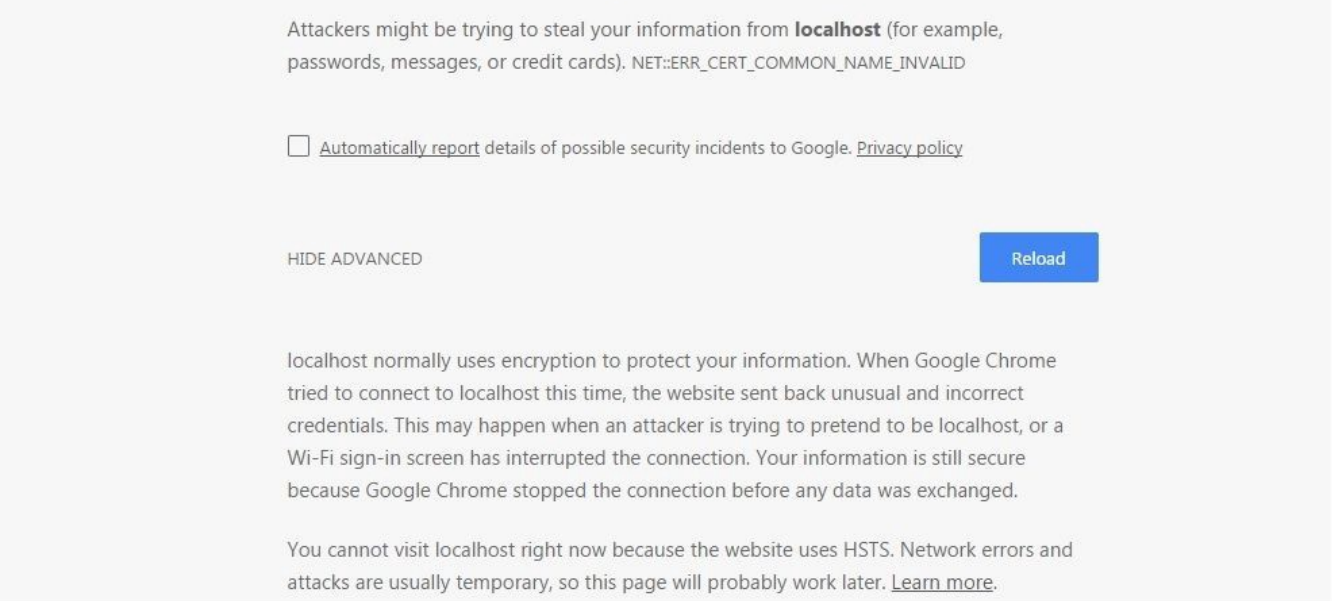
In order for an SSL certificate to be trusted, a certificate must have been issued by a certificate authority (CA) that is included in the trusted store of the device that is connecting.

If the certificate was not issued by a trusted CA, the connecting device will then check to see if the certificate of the issuing CA was issued by a trusted CA, and so on until either a trusted CA is found or no trusted CA can be found.

Common certificate authorities

Commonly used certificate authorities, such as Verisign, DigiCert, and Entrust, are automatically trusted by most browsers. However, if you use an untrusted internal certificate authority to generate SSL certificates for internal resources, you will be nagged by your browser when you attempt to connect.





Example of when an SSL certificate is not trusted.

How a Certificate Chain Works

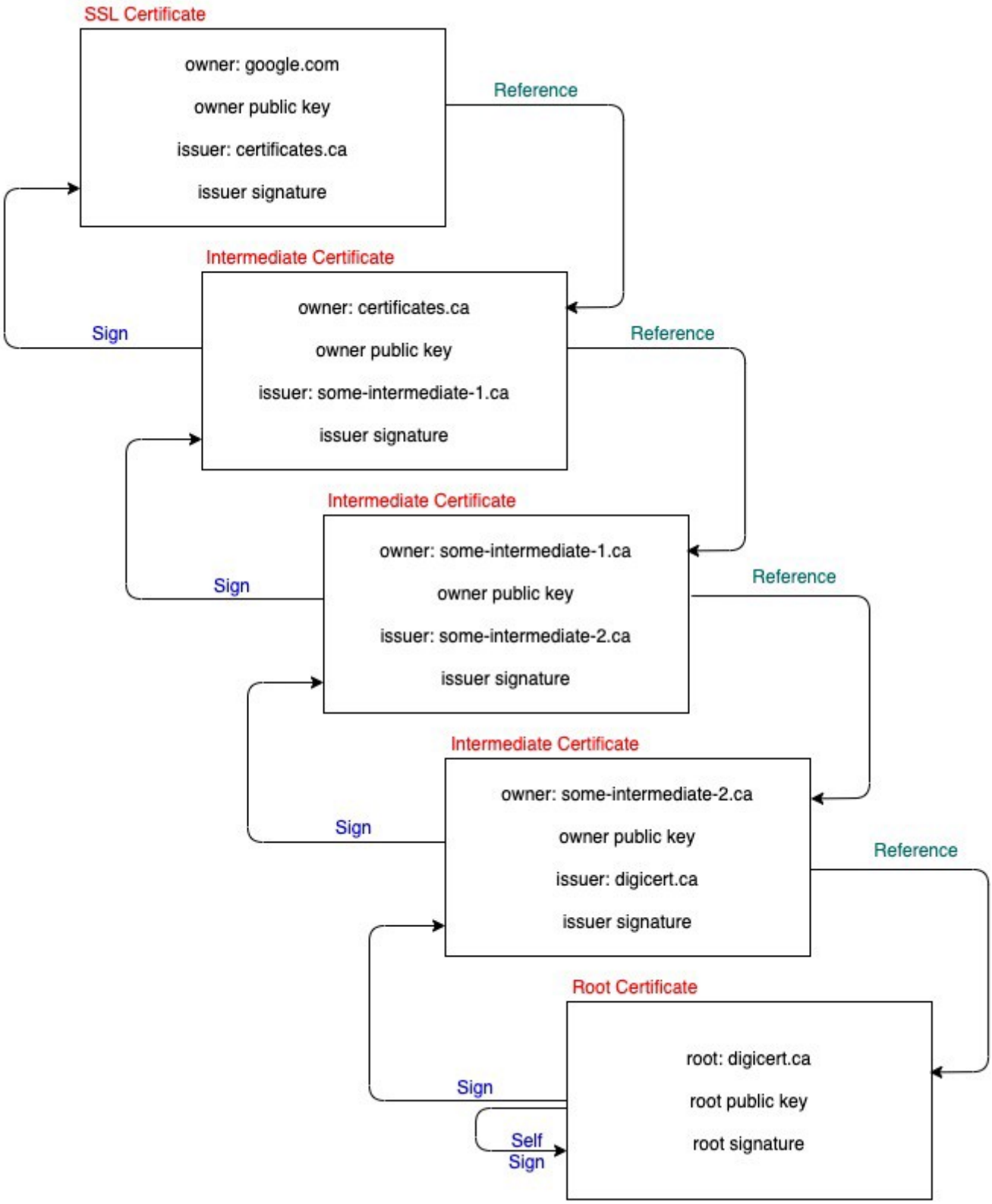
You decide to purchase a certificate for the domain *google.com* from a certificate supplier called *certificates.ca*. It's important to note, that certficates.ca is not a root authority, and therefore cannot be explicitly trusted.

A chain of trust must be built, by certificates.ca having intermediate certificates issue certificates up the chain all the way to a root CA.

Here is an example of a 5 chain certificate:

1. google.com — issued by certificates.ca (end user certificate)

2. intermediate certificate — issued to certificates.ca, issued by some-intermediate-1.ca
3. intermediate certificate — issued to some-intermediate-1.ca, issued by some-intermediate-2.ca
4. intermediate certificate — issued to some-intermediate-2.ca, issued digicert.ca
5. root certificate — issued to digicert.ca, by digicert.ca



-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

Installing a certificate

When you install an end-user certificate, such as the one in the example above bought from certificates.ca, you have to bundle the intermediate certificates and install them also.

This certificate chain enables the receiver to verify that the sender, and all certificates in the chain are trustworthy, but if the SSL certificate chain is invalid or broken, your certificate will not be trusted by some devices.

Certificate Keys Security Software Development

About Help Legal