

What is a self-signed root certificate?

A self-signed root certificate is a root certificate authority that someone makes for immediate use as a certificate. Such certificates do not benefit from the security of certificate chains and certificate policies. Most computers will not accept a self-signed certificate unless their owner first tells them to, and some computers will not accept them under any circumstances. They are however easy and quick to make, and are often used for testing purposes in place of certificates signed by proper certificate authorities.

What is a leaf certificate?

A leaf is a certificate signed by an intermediate or root Certificate Authority. A leaf certificate benefits from the security of certificate chains and certificate policies. A leaf is situated at the bottom of a certificate chain.