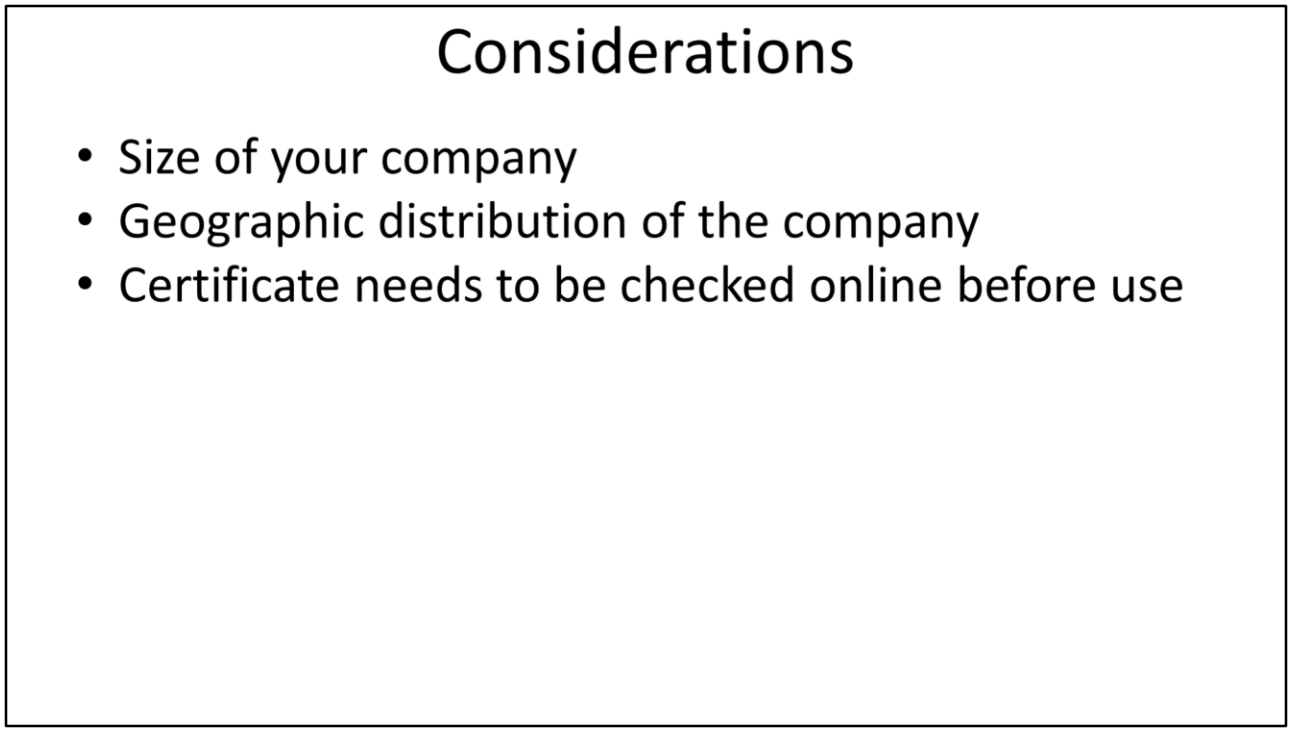
PKI Hierarchy

For the free video please see
http://itfreetraining.com/certificates/pki-hierarchy

PKI (Public Key Infrastructure) is a hierarchy of Certificate Authorities. This video looks at 3 different types of hierarchies that can be used to issue certificates.

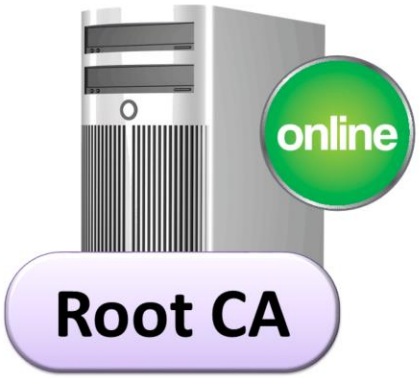


Considerations

When deploying Certificate Authorities (CA's) you should consider the size of your company, geographic distribution and the number of certificates that are required. Before a certificate can be used it needs to be checked that it has not been revoked. This can be done via a CA or online responder. When deploying CA's consider WAN links the users may need to travel over when obtaining new certificates and also checking that an existing certificate is still valid.

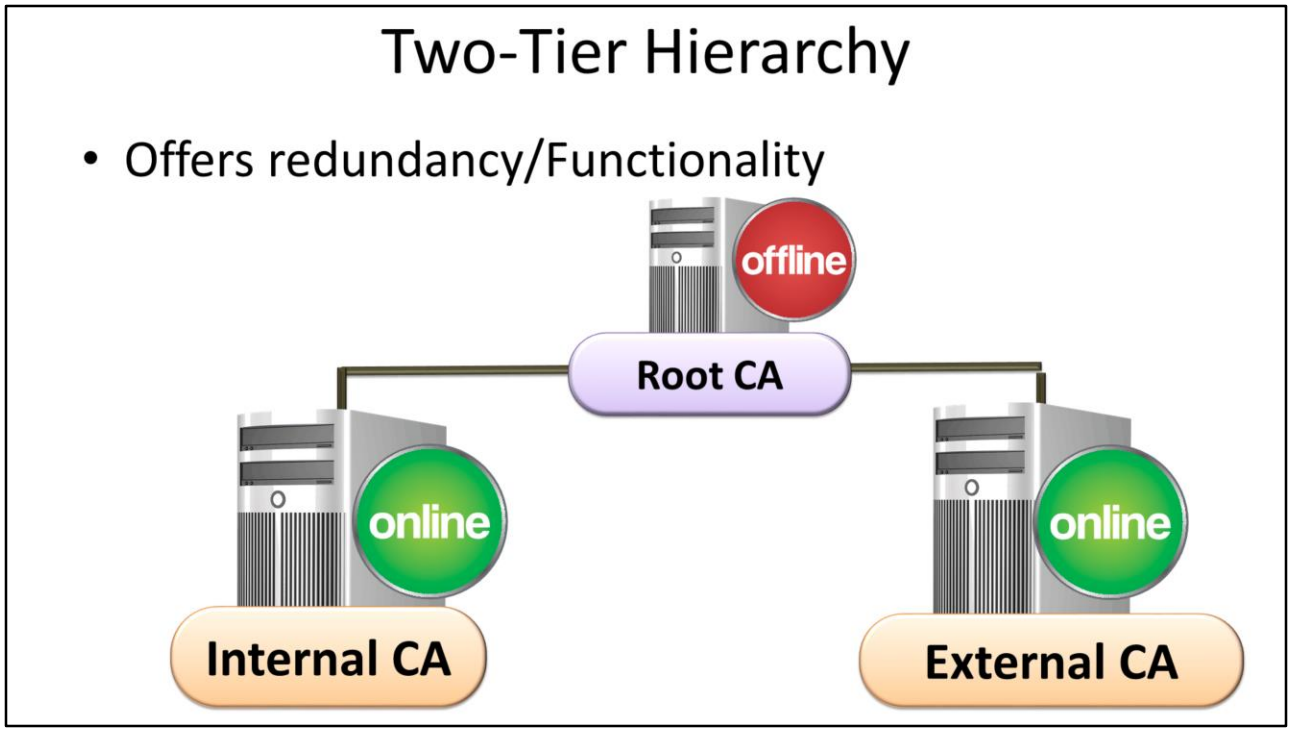
Single-Tier Hierarchy

- Suited for small organizations
- Always online
- Less administration
- No redundancy



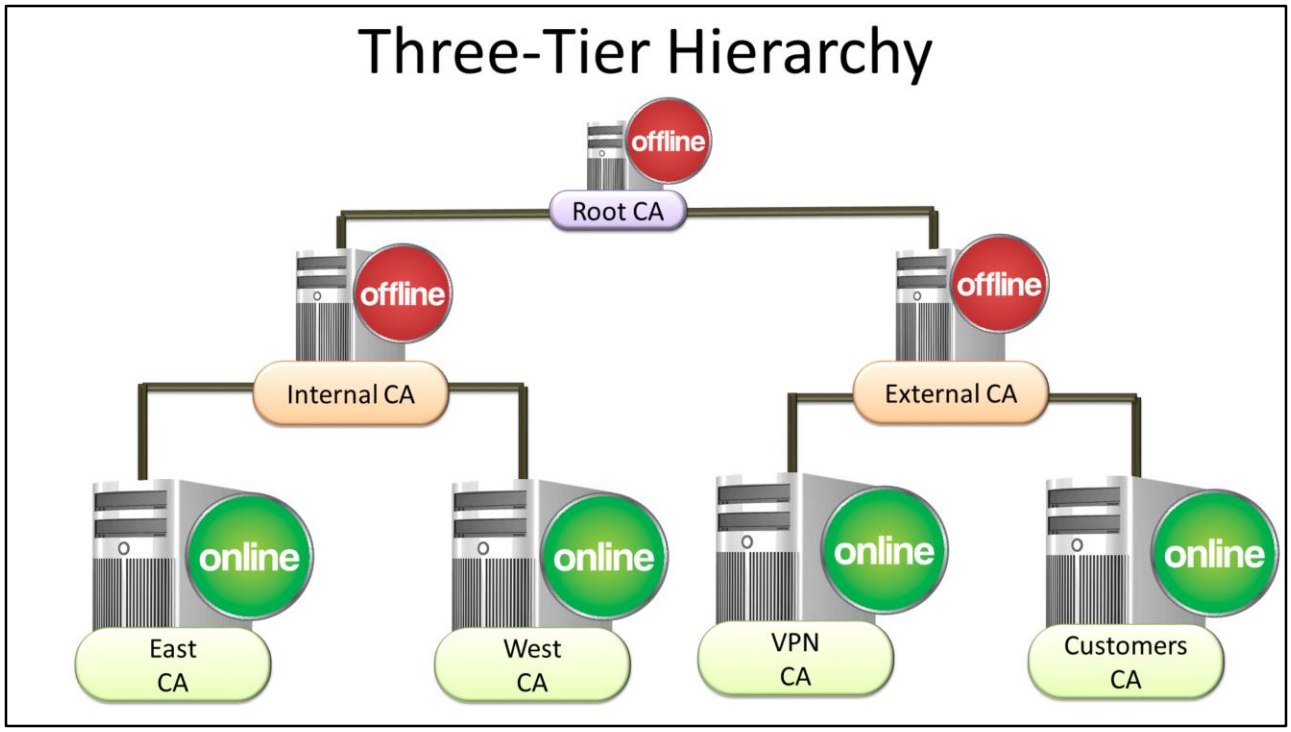
Single-Tier Hierarchy

This means that there is one CA on the network. This is suited for small networks. Having one server does mean less administration; however, it does not provide any fault tolerance. In order to issue certificates, the server must be online. The CA contains private keys and when there is only one CA on the network the server cannot be taken offline in order to protect these keys. If an attacker was to obtain these private keys, they could effectively create their own certificates or decrypt any traffic encrypted with any existing certificate.



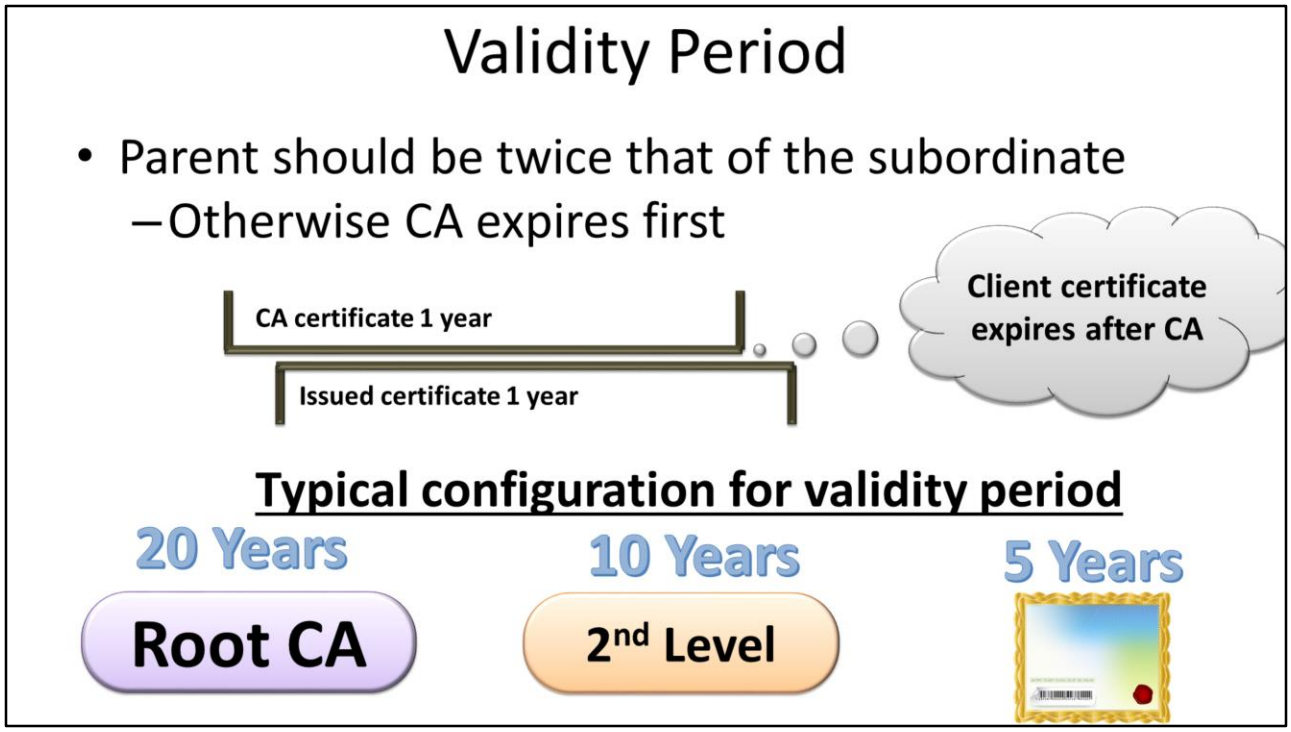
Two-Tier Hierarchy

This contains two levels of CA's. One Root CA and any number of child CA's. In order to improve security, the root CA is usually taken offline after the child CA's have been issued a certificate. The root CA only ever needs to be brought back online if another child CA is added to the network or a child CA needs to renew its certificate. Having a second level provides redundancy as multiple CA's can be created to issue certificates. Different CA's at the second level can be used for different reasons. For example, one CA may be for internal clients while another CA could be used for external customers or business partners.



Three-Tier Hierarchy

A three tier hierarchy adds another layer of CA's to the hierarchy. This improves security as the first 2 levels can be taken offline when not required. They can be brought back online only when new CA's need to be added to the network.



Validity Period

The validity period is how long a certificate is valid for before it cannot be used. The root CA certificate is the top of the hierarchy. Once the root CA certificate expires, all certificates in the hierarchy expire with it. For this reason, the root CA normally has a very high validly period like 20 years. A rule of thumb is that subordinate CA's have half the value of their parent CA. If they have the same validly period, this would mean that after the CA has been online for a day, it would be issuing certificates that expire after its parent CA.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.