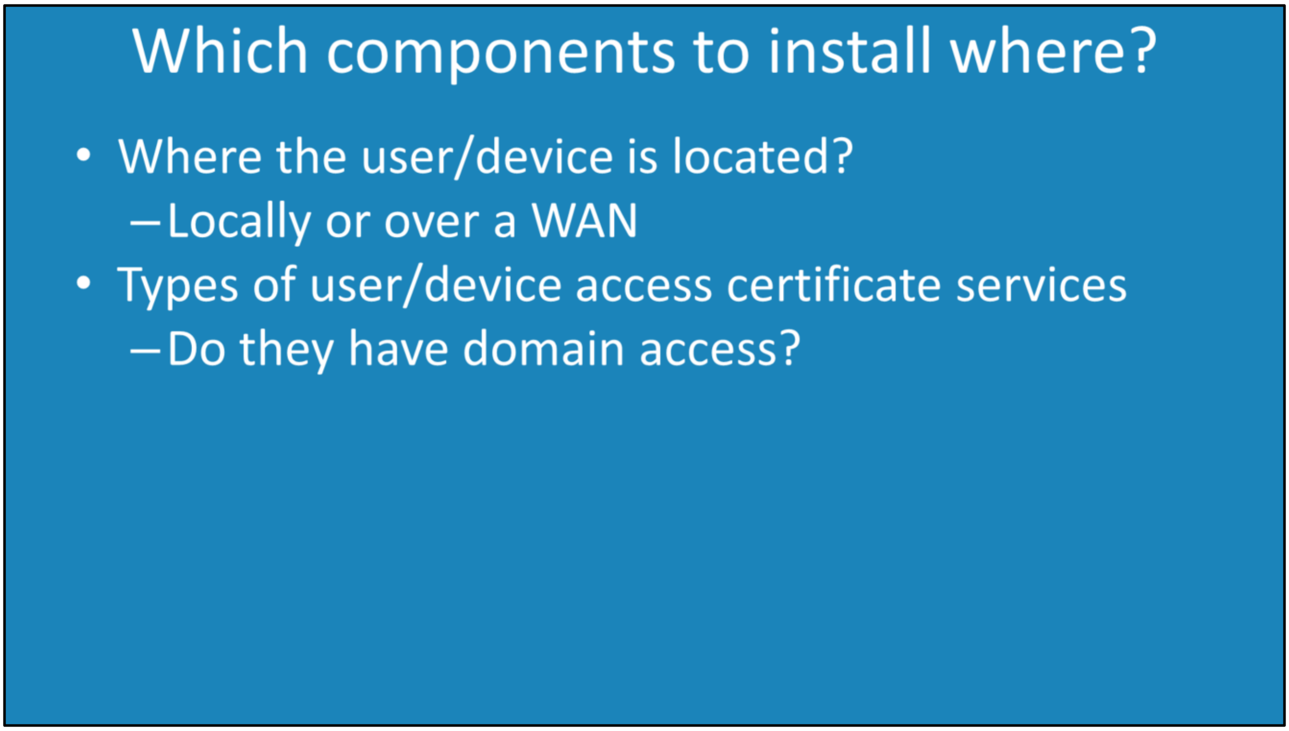
Components Of Certificate Services

For the free video please see
http://itfreetraining.com/certificates#components

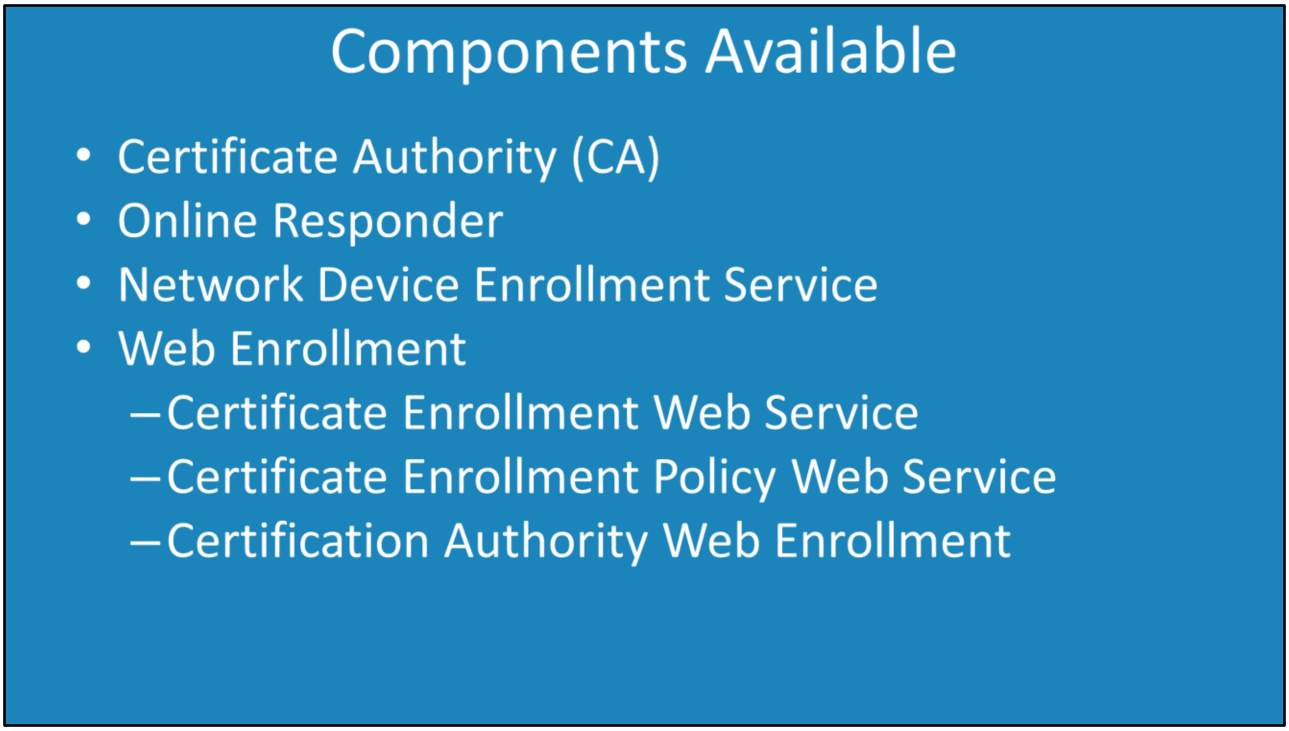
This video will look at the different components that make up Active Directory Certificate Services and which services you should look at installing these components on.



Which components to install where?

- Where the user/device is located?
  - Locally or over a WAN
- Types of user/device access certificate services
  - Do they have domain access?

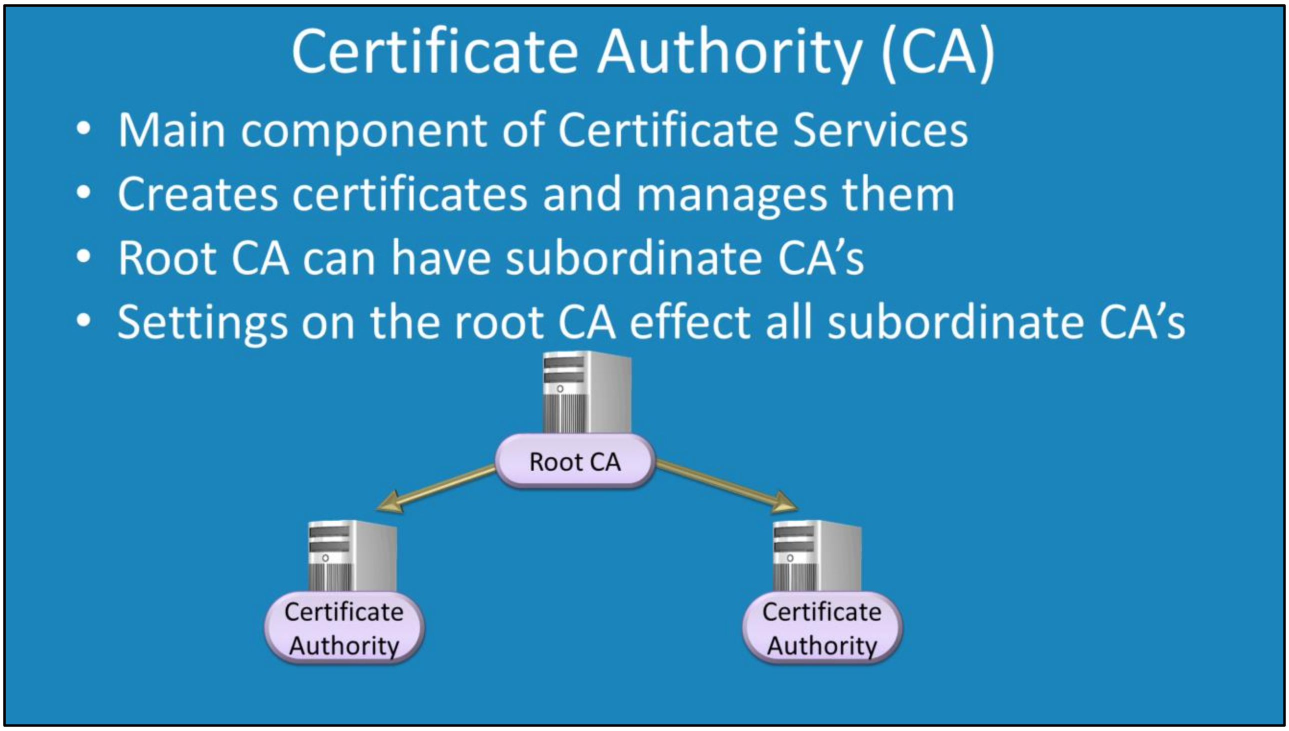
Which components to install where?
When looking at which components of certificate services to install where a few points need to be considered. First where is the user or device that is using the certificate located? If they are located over a WAN then additional components may need to be installed closer to the user or device. If the user or device is part of the domain this will make the process simpler. If not, additional components may be required to assist the user or device accessing the certificate infrastructure.



Components Available

- Certificate Authority (CA)
- Online Responder
- Network Device Enrollment Service
- Web Enrollment
  - Certificate Enrollment Web Service
  - Certificate Enrollment Policy Web Service
  - Certification Authority Web Enrollment

Components Available
There are 6 components in Active Directory Certificate Services.
Certificate Authority (CA): This is the core component which creates certificates for use. These certificates are issued to users or devices or to a subordinate CA.
Online Responder: This component provides a way for certificates to be checked that is uses a small amount of network traffic.
Network Device Enrollment Service: This component allows non-domain devices like switches and routers to obtain certificates.
Certificate Enrollment Web Service: This allows certificates to be obtained using the web.
Certificate Enrollment Policy Web Service: This component works with Certificate Enrollment Policy Web Service to provide certificates. It provides the policy that is used with Certificate Enrollment Web Service.
Certification Authority Web Enrollment: This component provides a web interface which end users can use to obtain certificates.



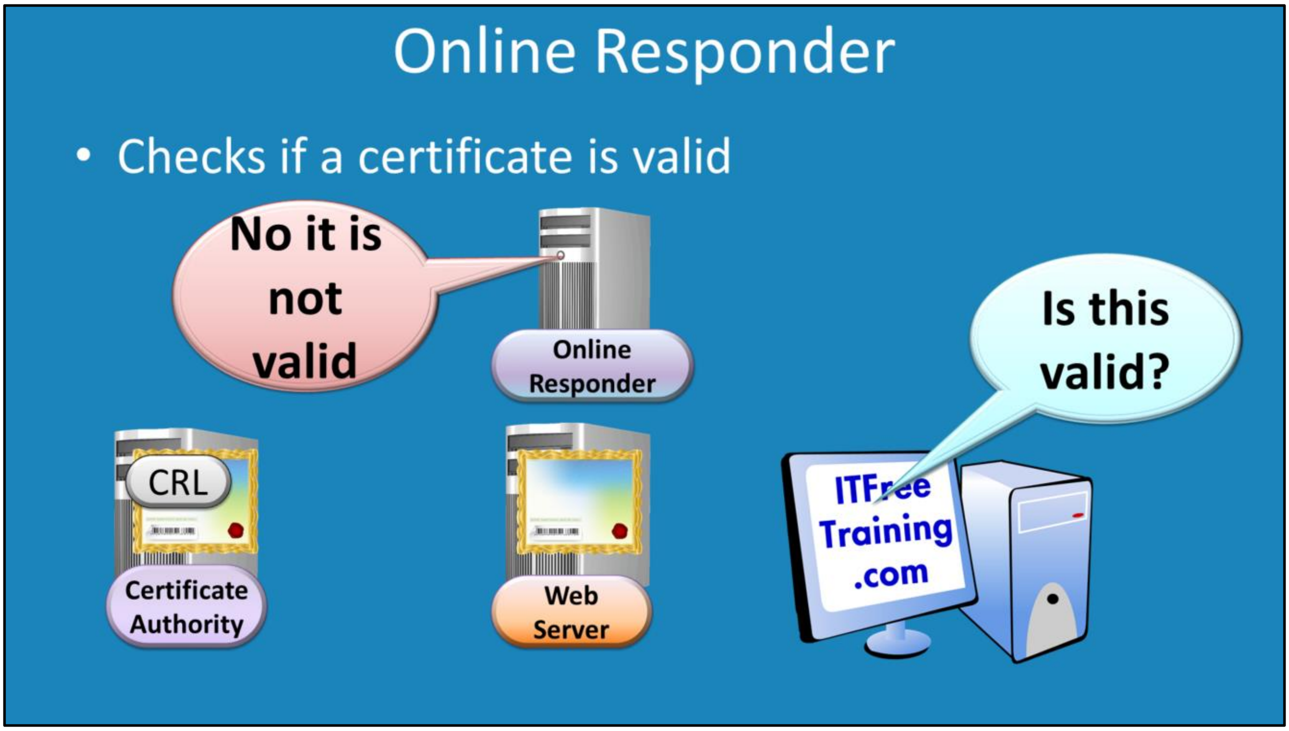
Certificate Authority (CA)

- Main component of Certificate Services
- Creates certificates and manages them
- Root CA can have subordinate CA's
- Settings on the root CA effect all subordinate CA's

Root CA
Certificate Authority
Certificate Authority

Certificate Authority (CA)

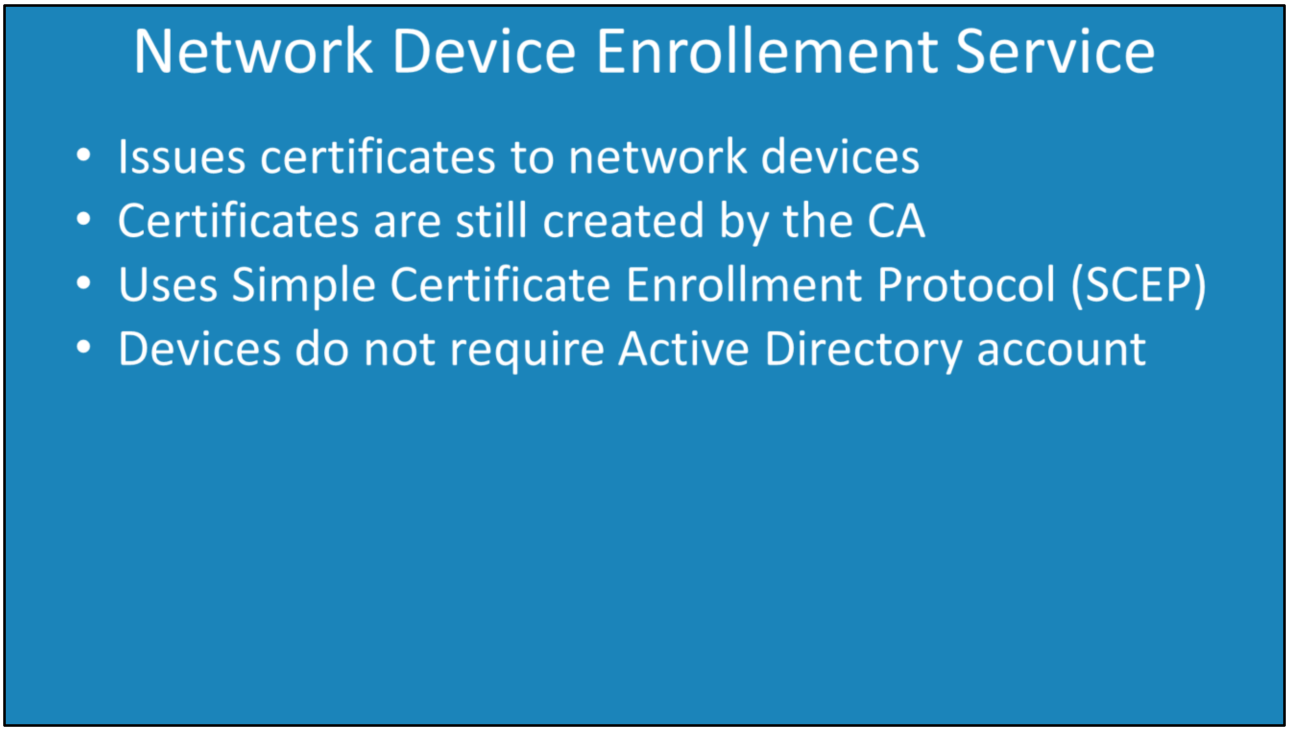
The Certificate Authority or CA is the main component of certificate services. It should be remembered that Active Directory Certificate Services is Microsoft's implementation of certificates. There are other 3rd party implementations of certificates. Microsoft CA can use certificates from these CA's or these certificates can be used with Microsoft CA's. A CA's job is to create and manage certificates. The certificates that it creates can be used by subordinate CA's or by clients. At the top of the certificate hierarchy is the root CA. If you decide to create your own root CA it is important to be careful which settings you use. The settings used on a CA effect all certificates created below it. This is because certificates form a chain. In order for a certificate to be validated, all certificates in the chain need to be checked.



Online Responder

- Checks if a certificate is valid

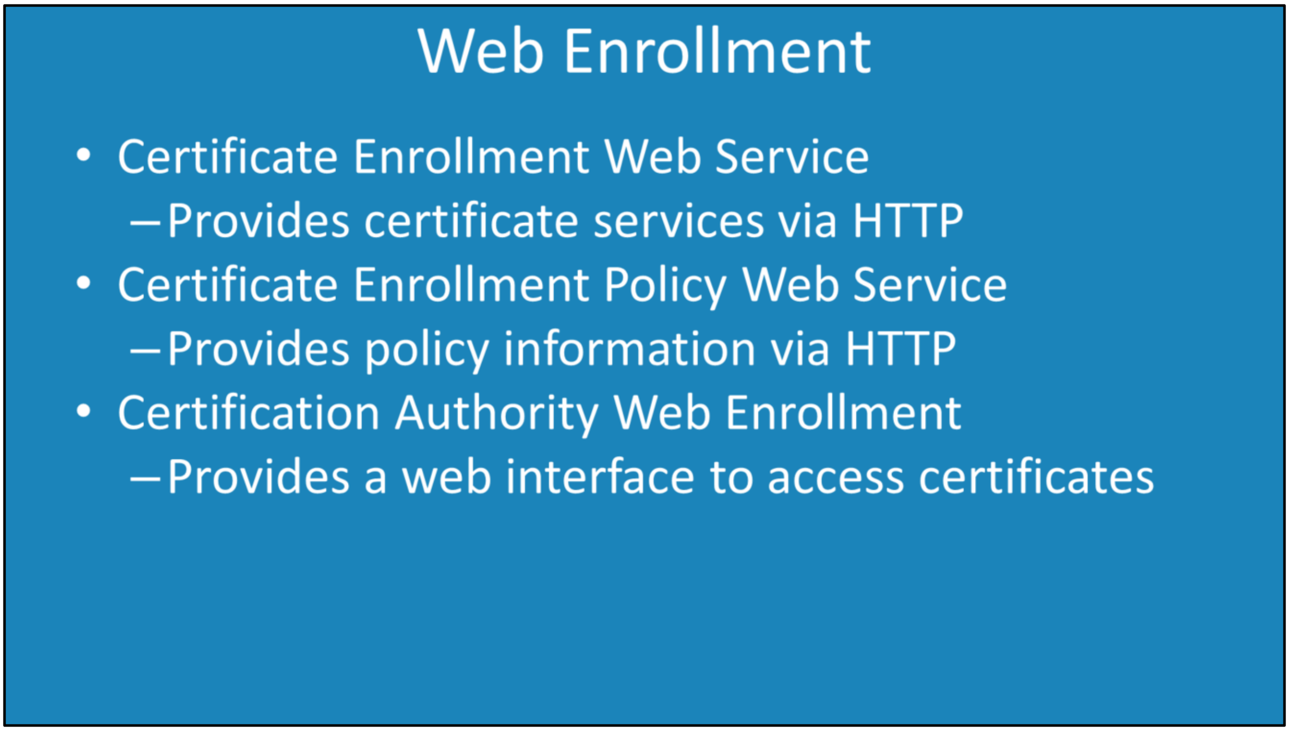
Online Responder
This component checks if a certificate is valid. The user or device using the certificate can send a query to the online responder and the online responder will send back a response either yes or no if the certificate is valid. The advantage of this is that the response message is always the same size. The other way of doing this is using what is called a Certificate Revocation List or CRL. The CRL contains all certificates that have been revoked so this can become quite large. In order to obtain the CRL the client also requires access to a CA. The second advantage of an online response is that it can talk to the CA on behalf of the client. This means that an online responder can be deployed in locations that you may not normally deploy a CA. For example an area that is accessible on the internet.



Network Device Enrollement Service

- Issues certificates to network devices
- Certificates are still created by the CA
- Uses Simple Certificate Enrollment Protocol (SCEP)
- Devices do not require Active Directory account

Network Device Enrollment Services
This component allows devices on the network to use the Simple Certificate Enrollment Protocol (SCEP). The device will request the certificate from this component. This component will then contact a Certificate Authority on the device's behalf to obtain a certificate. Network Device Enrollment Services using this method can allocate certificates to devices on the network that are not domain members.



Web Enrollment

- Certificate Enrollment Web Service
  - Provides certificate services via HTTP
- Certificate Enrollment Policy Web Service
  - Provides policy information via HTTP
- Certification Authority Web Enrollment
  - Provides a web interface to access certificates

Web Enrollment
There are 3 components that all relate to web enrollment, or obtaining certificates using HTTP.
Certificate Enrollment Web Services: This component provides certificates using HTTP, however it does not provide a web page to obtain the certificate. HTTP is only used as the communication protocol to obtain the certificate.
Certificate Enrollment Policy Web Service: This component provides policy information to clients for use with the Certificate Enrollment Web service.
Certification Authority Web Enrollment: This provides a web page that a user can use to request a certificate. This is often used when 3rd parties require certificates. The 3rd party can use this web site to request a certificate and the administrator will need to at some stage approve this certificate to be created.

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.

References
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 779 - 780
"Windows Server 2008 PKI and Certificate Security" pg 33 - 37
"Certificate Enrollment Web Services"
http://blogs.technet.com/b/askds/archive/2010/02/01/certificate-enrollment-web-services.aspx