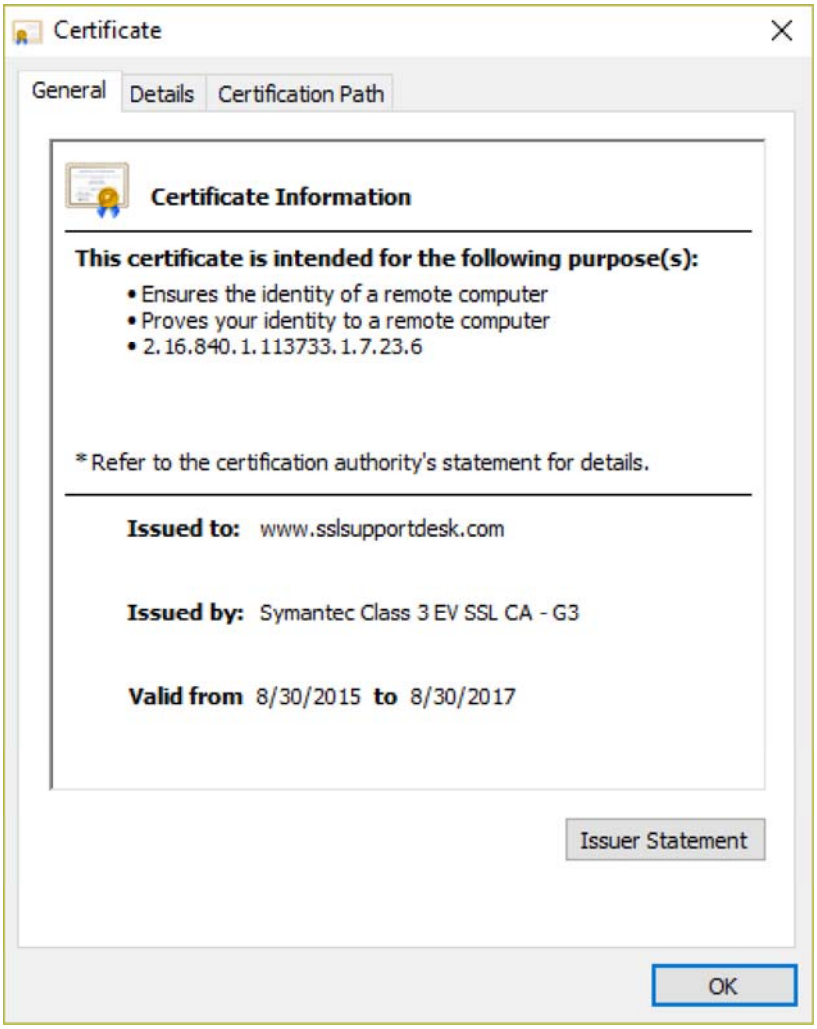


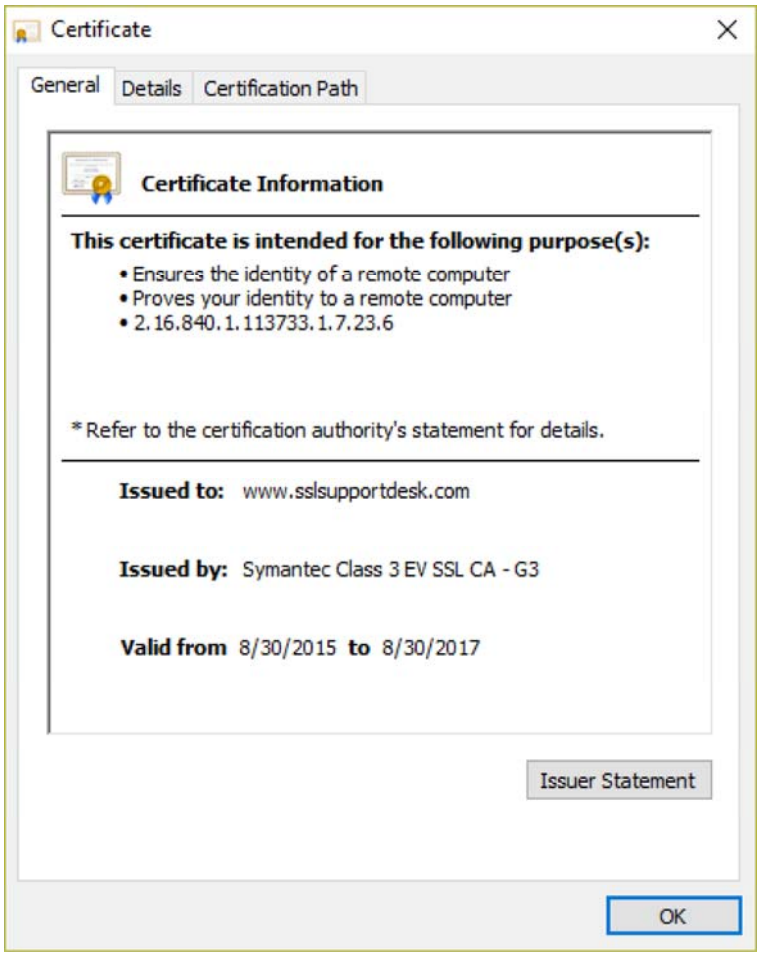
What Do The Details of a Digital Certificate Mean?

www.sslsupportdesk.com

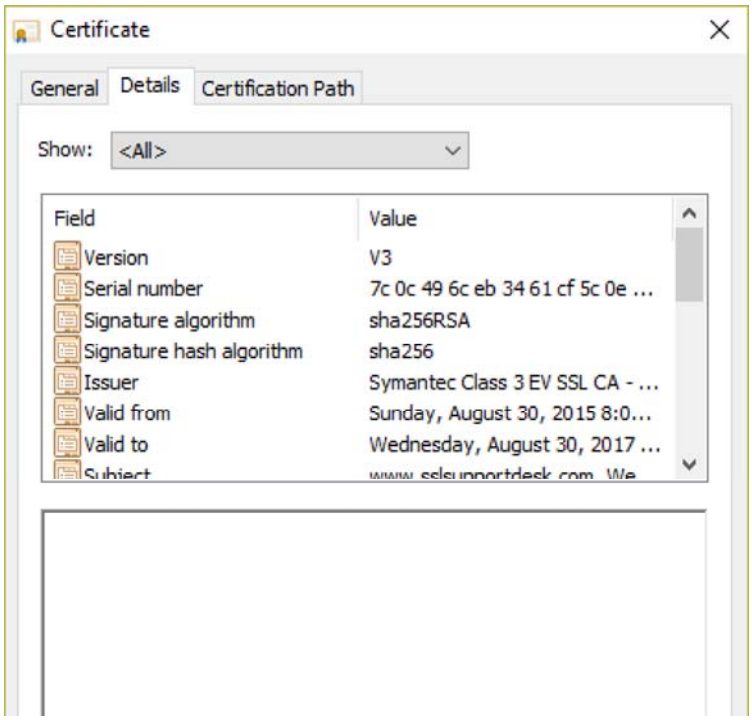
7 mins read

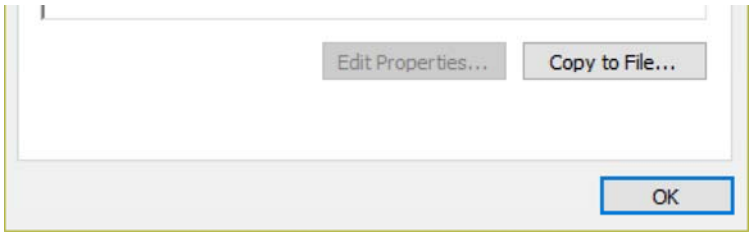
There is a lot of information that gets added to a digital certificate. The information within these fields under the details of a digital certificate state the parameters from its issuance. Some of these fields are just informational, but sometimes an application can be built around these specific fields.

With the standards of the security industry always changing these attributes may change at anytime to comply with [CAB Forum requirements](#).



To see the details of a digital certificate just click on the **Details** tab.

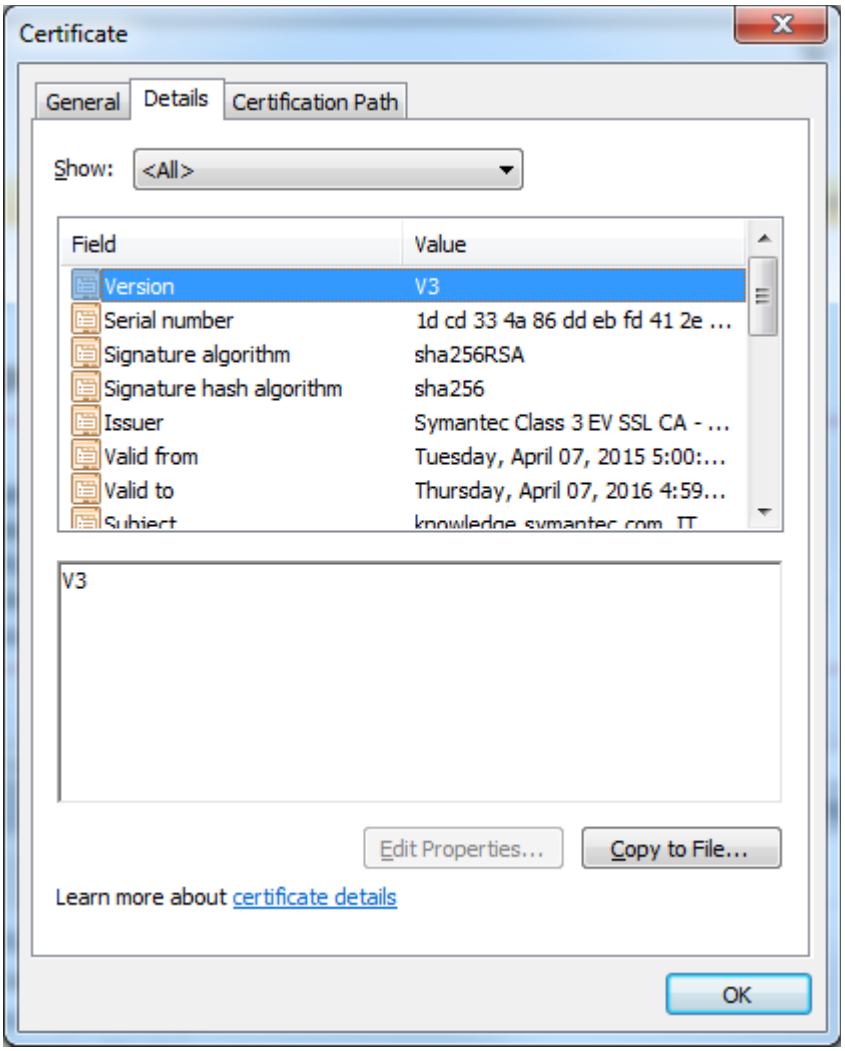




Below is a brief run down of each field displayed on a Digital certificate and what them mean.

Version:

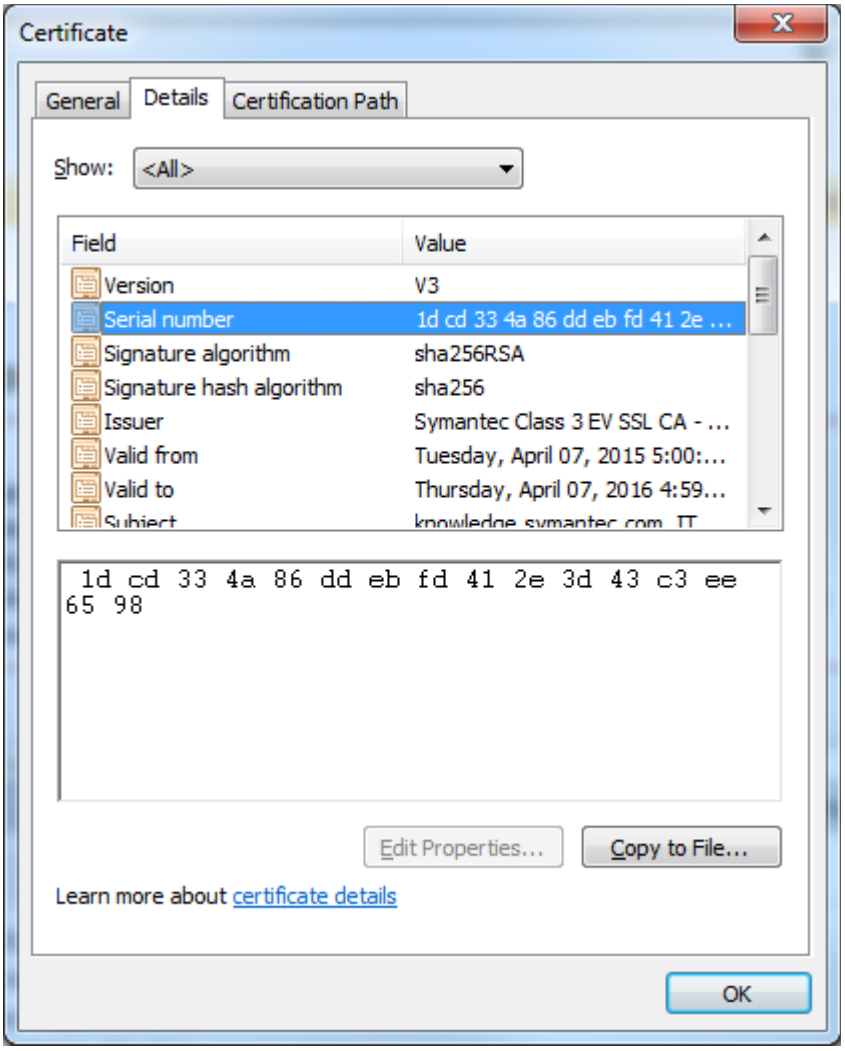
This field describes the version of the encoded certificate. For SSL certificates, the x509 version is 3 since certificate extensions are used. It's basically not important.



Serial Number:

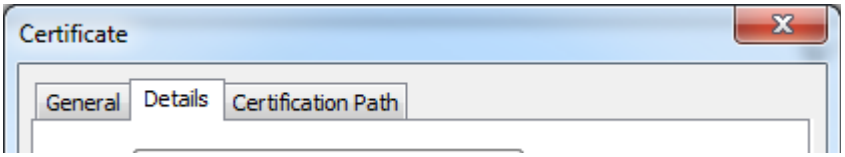
The Serial Number is a positive integer assigned by the Certificate Authority to each Digital Certificate. It is unique for each certificate

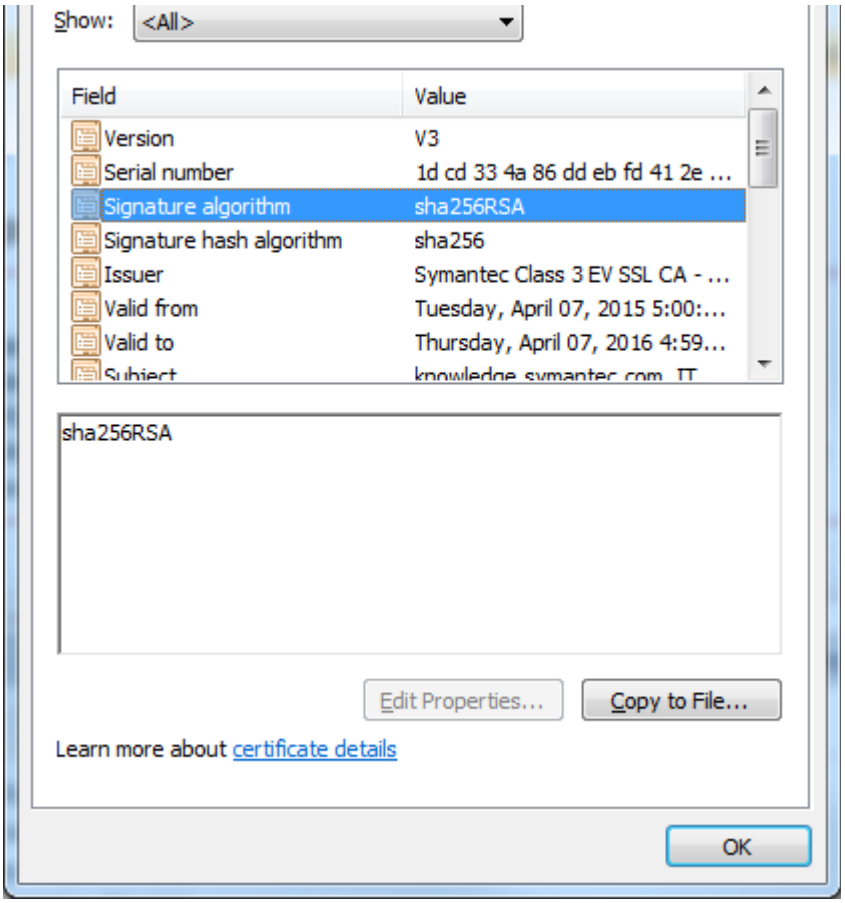
issued. This is good when you need to make sure you are referencing the correct certificate.



Signature Algorithm:

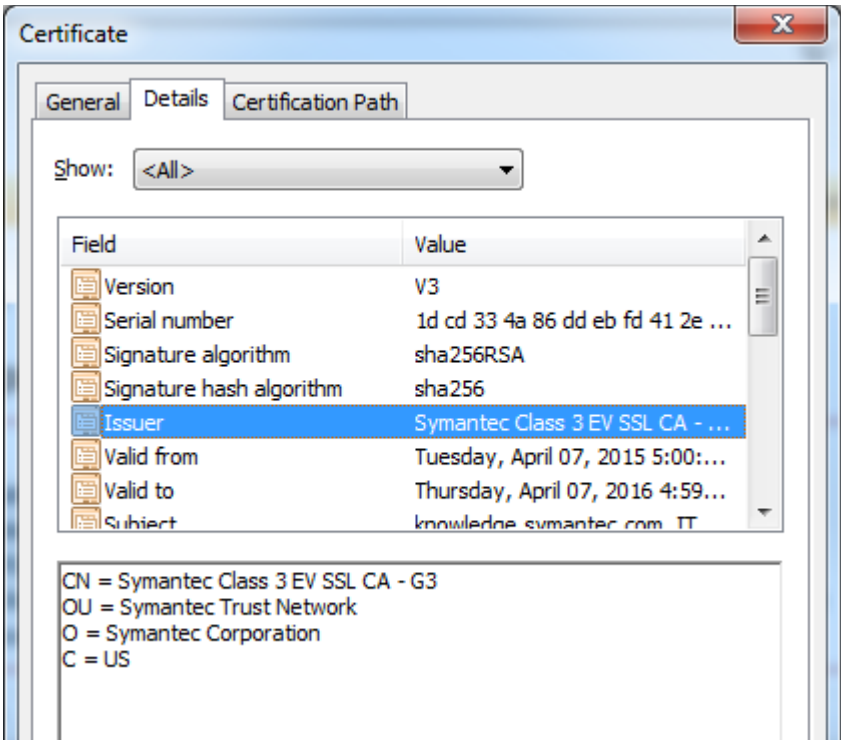
The Signature Algorithm identifies the cryptographic algorithm used by a certificate authority to sign the digital certificate. This is a important extension used to drive the security standards of the industry. Every so often this will change. As of 2016 all certificate authorities have to sign a digital certificate using the SHA2 algorithm. If you see a digital certificate other than a root stating SHA1 or MD5 it will be a older certificate. Browsers such as Firefox will want to see a digital certificate in SHA2 running on a website or it will give warning messages.

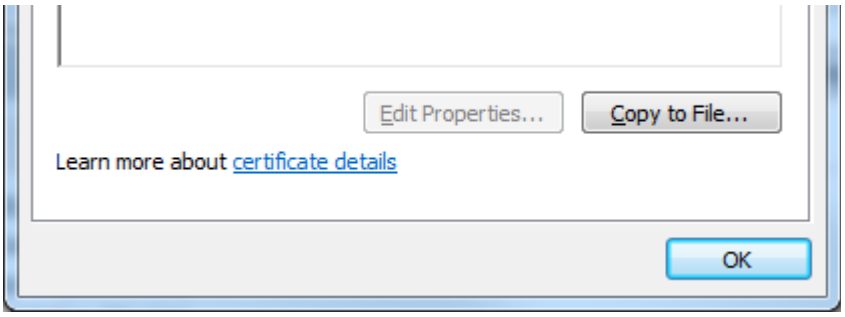




Issuer:

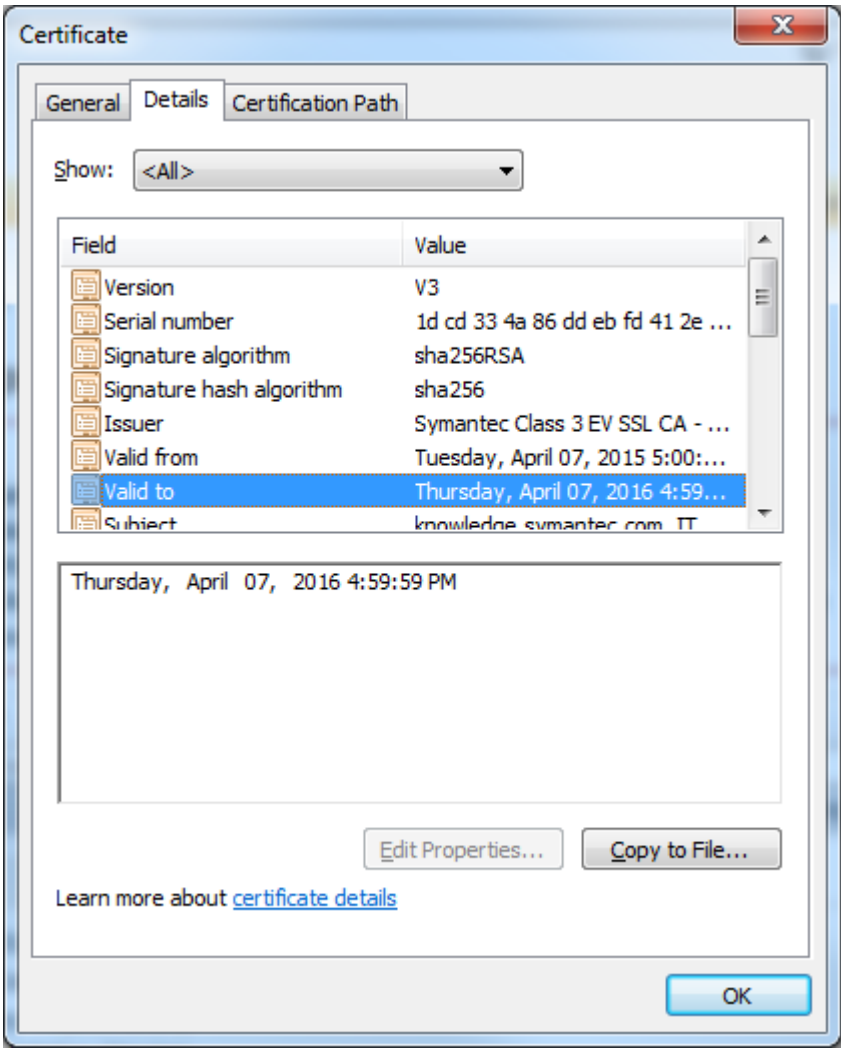
The Issuer field identifies the entity or Certificate Authority or self signing application that signed the certificate. This field is good at finding out who issued the certificate.





Valid From and Valid To:

These field indicate the validity period of the certificate. These dates cannot be changed magically after the certificate is issued. A renewal or a reissue of a certificate will always have a different start date at least. Keeping an eye out on the validity date of a certificate is a good way to troubleshoot installation or binding of a certificate.



Subject:

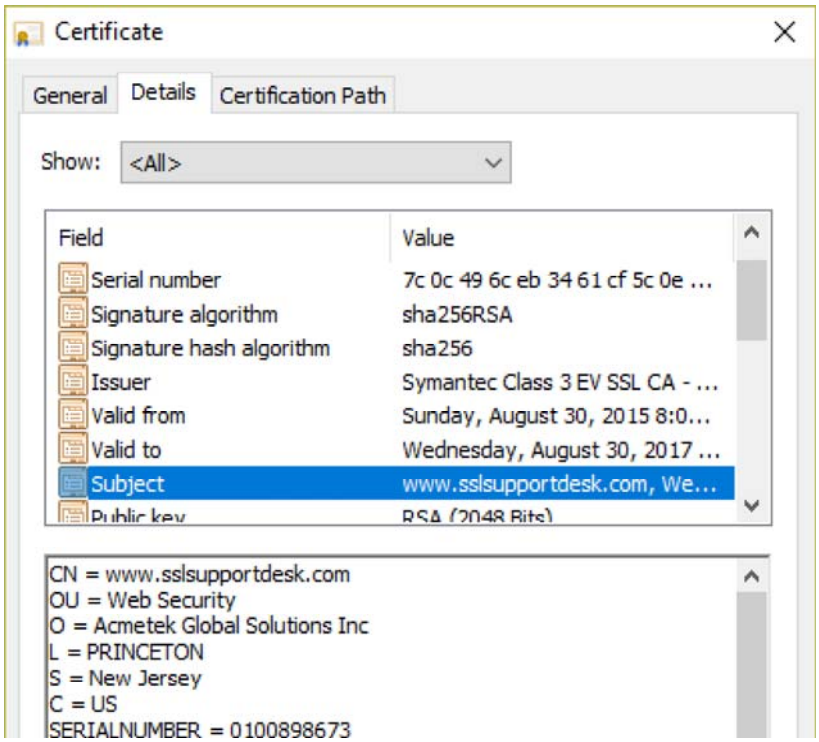
This field contains the Distinguished Name (DN) information for the certificate. Depending on the type of certificate will distinguish the information that gets displayed in this field.

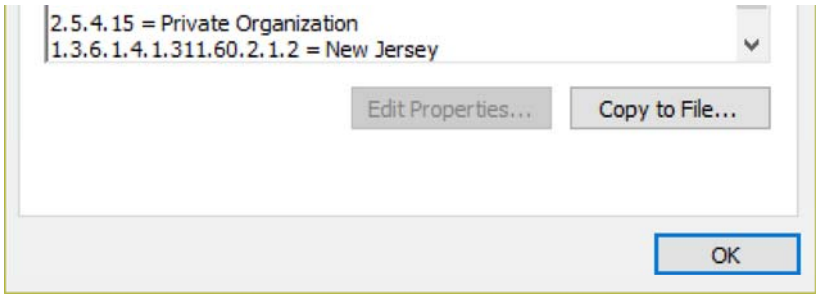
A Domain Validated certificate (DV) will only display the CN info. A Organization Validated certificate (OV):

- *Common Name (CN)*
- *Organization (O)*
- *Organizational Unit (OU)*
- *Locality or City (L)*
- *State or Province (S)*
- *Country Name (C)*

For Extended Validation (EV) SSL certificates, these additional fields are also included:

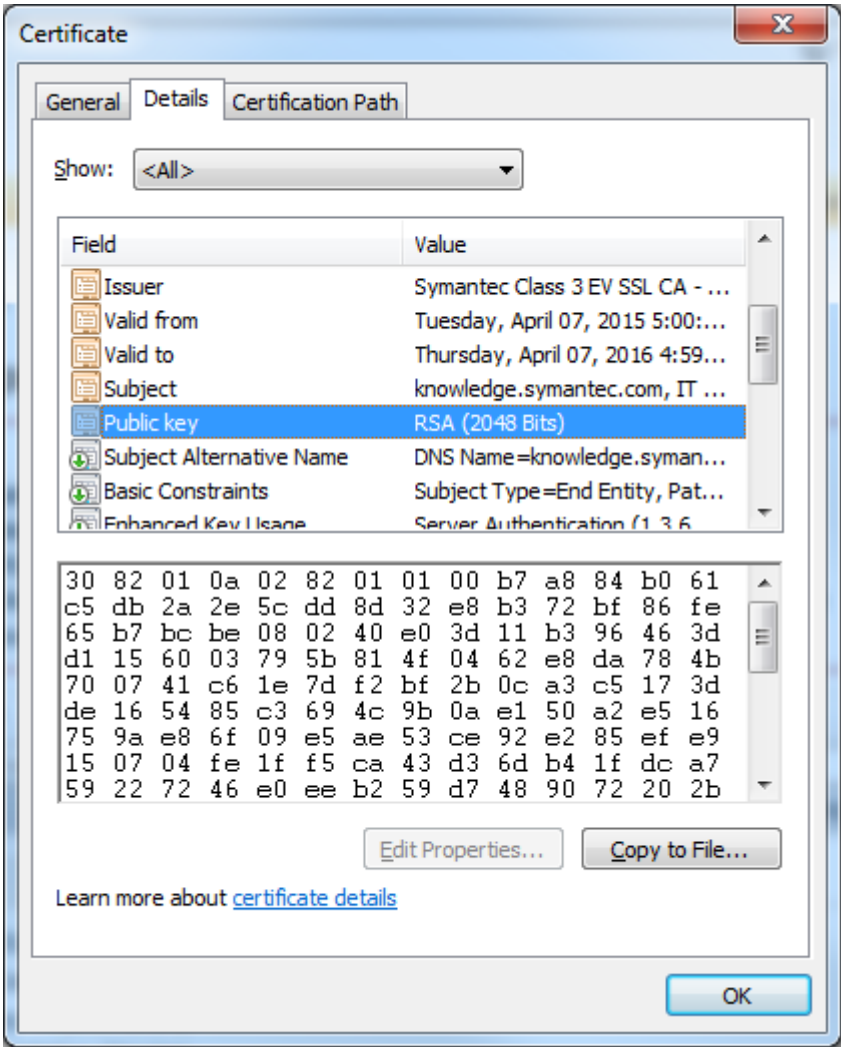
- *Company Street Address*
- *Postal Code*
- *Business Category*
- *Serial Number (Business Registration Number)*
- *Jurisdiction State*
- *Jurisdiction Locality*





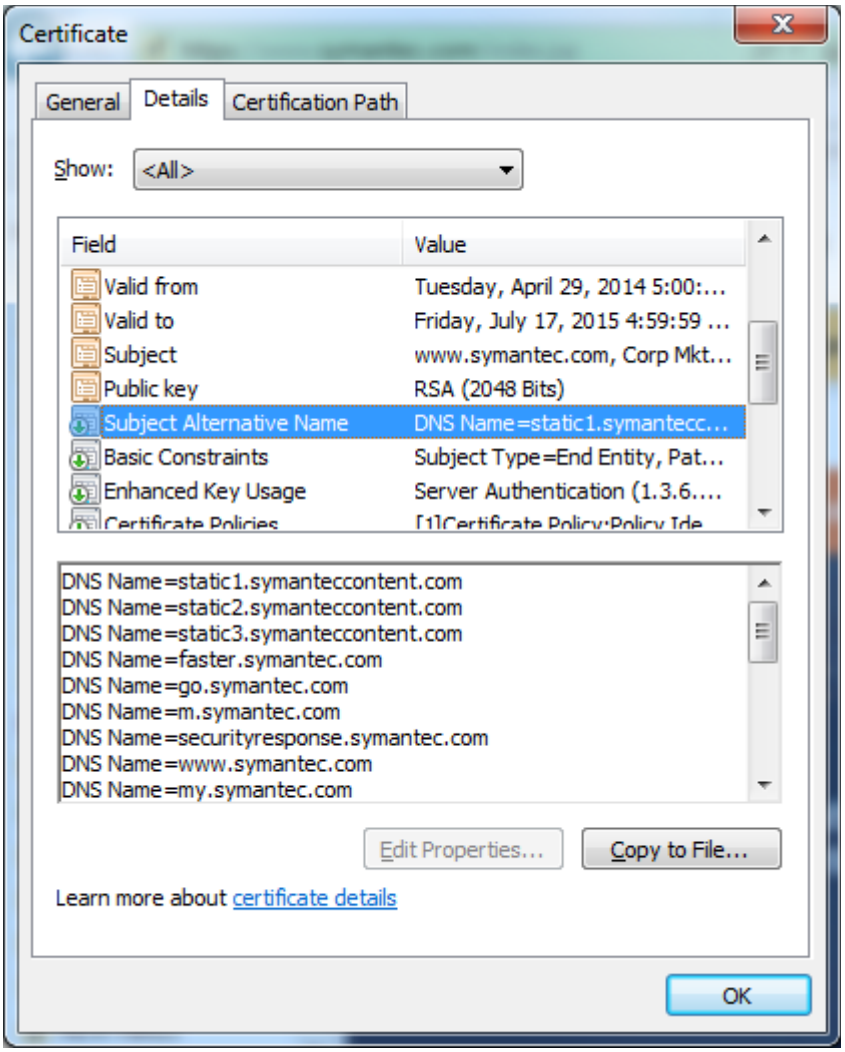
Public Key:

This field is used to identify the modules key bit length. Some applications require at least 2048 bits for a certificate. The more bits a certificate public key has the more randomization a server/applications protocols have to work with when encrypting information.



Subject Alternative Name (SAN):

The Subject Alternative Name extension allows additional identities to be bound to the **Subject** of the certificate. The DNS Name is used to add additional Fully Qualified Names to an SSL Certificate. Majority of all applications/web-browsers work with this field. It will list all the FQDN that the certificate can validate when bound to a website or application.

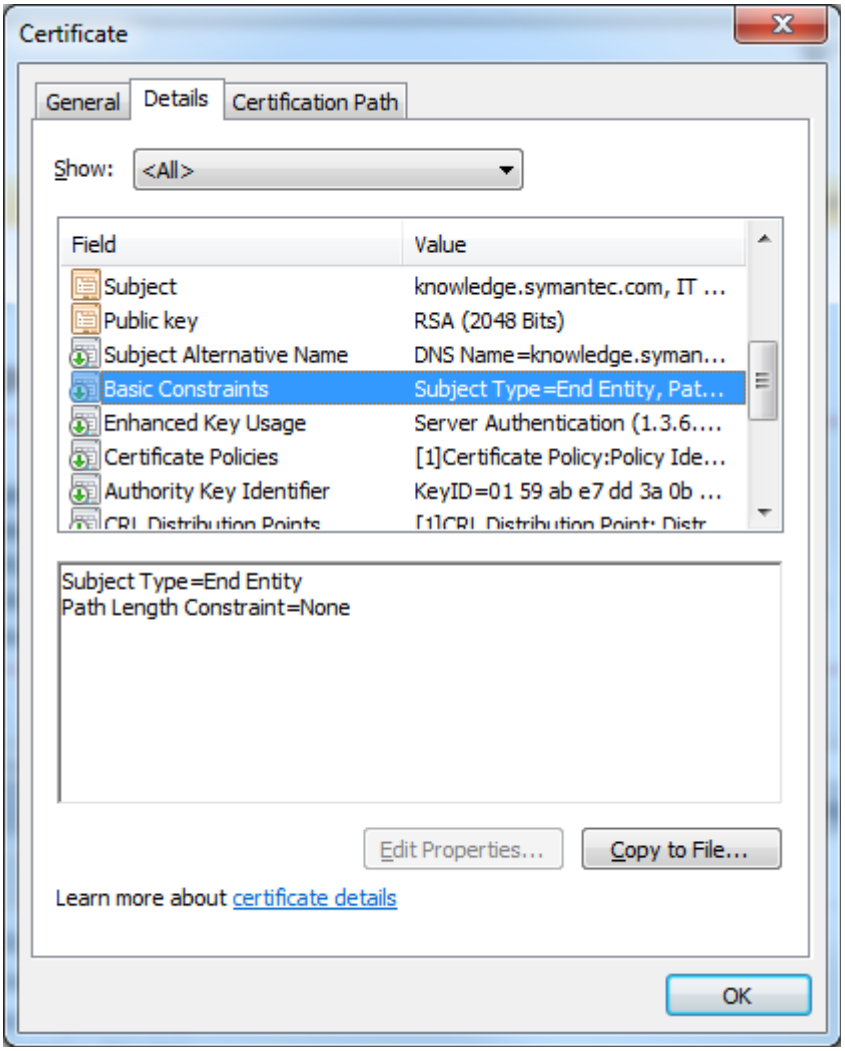


Basic Constraints:

This is an optional extension, it indicates what type of digital certificate this is.

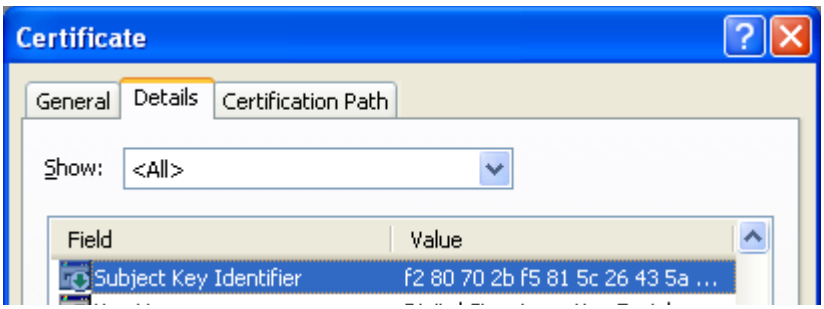
Subject = End Entity: Means that the certificate is a SSL Certificate or a User Certificate. used to actually authenticate websites or people. No other certificate can be build off this certificate. “It is the “End” of the Chain of certificates

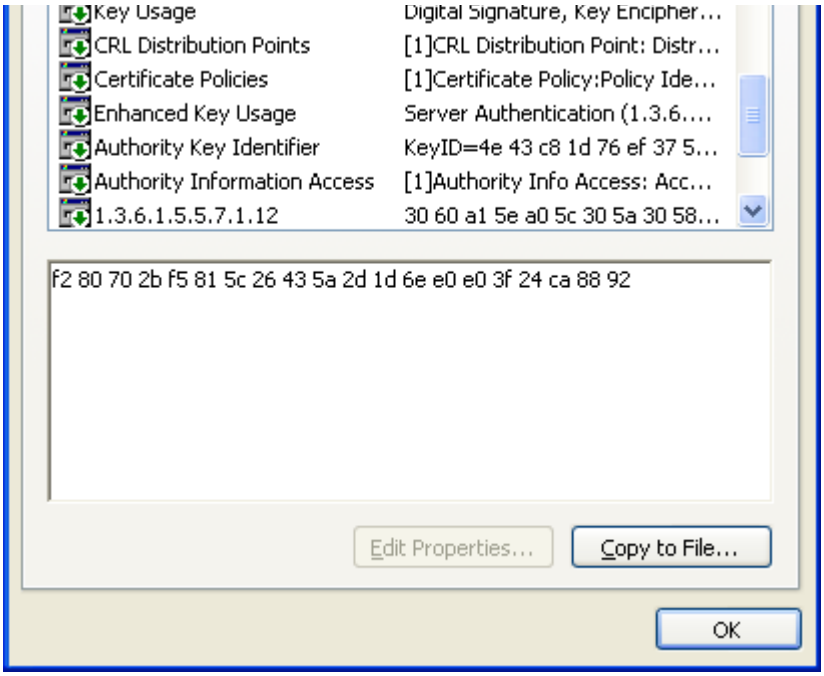
Subject = CA: Means that the certificate is a Intermediate or a Root certificate. Other certificate can be build from this type of constraint.



Subject Key Identifier (SKI):

The Subject Key Identifier extension provides a means of identifying certificate that contain a particular public key. This is a hash value of the SSL Certificate. A Digital certificate is built off a CSR/Public key. One CSR can be used to generate an SSL Certificate multiple times if necessary. Although an SSL Certificate will always be unique once it is issued this SKI will show the CSR it is derived from.





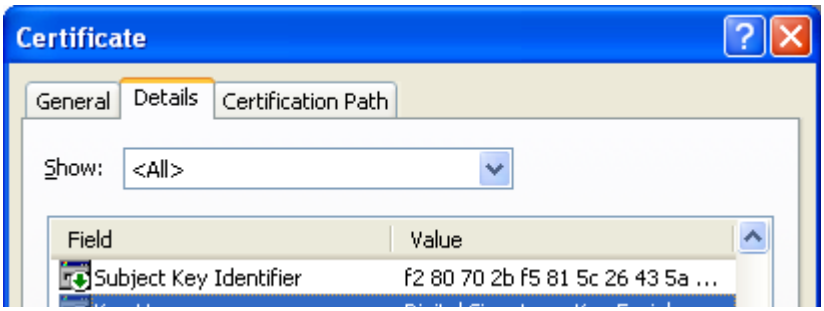
Key Usage:

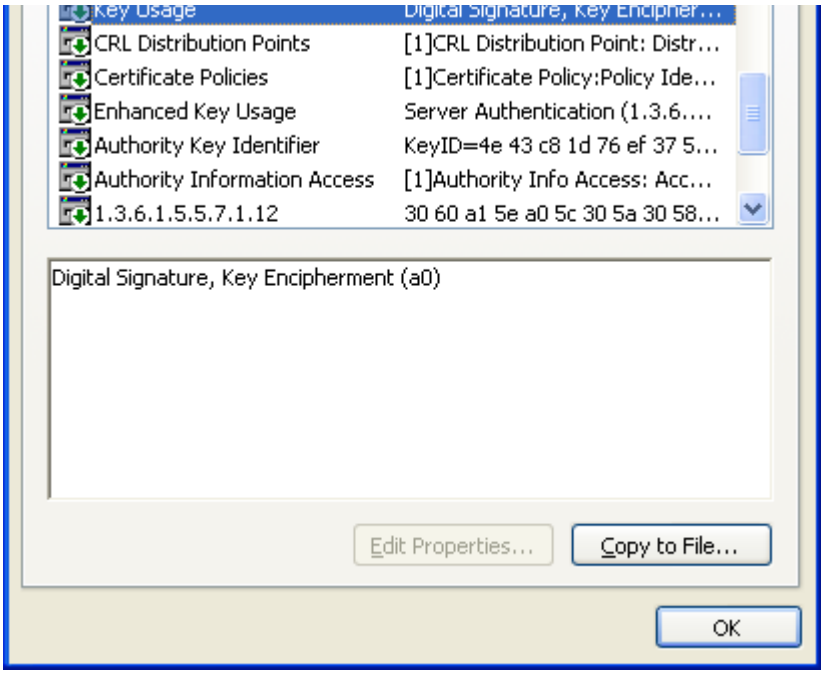
The Key Usage extension defines what a digital certificate can be used for (assuming the application/browser can use these extensions or are built around them).

The main usages for a End Entity (SSL Certificate) digital certificate are the following..

Digital Signature: A digital signature is often used for entity authentication and data origin authentication with integrity.

Key Encipherment: The key Encipherment asserted when the subject public key is used for key transport. An example of Key Encipherment is the SSL handshake, where the two applications use asymmetric encryption to wrap around the exchange of a secret key that is ultimately used for the session. To encrypt your information the public and private key are used to encrypt and decrypt the information.





Intermediate Root CAs have different key usage attributes that are unique to only them, they are the following...

You will pretty much never find the same key Usage attributes of an End Entity certificate and a Intermediate Root CA certificate in one certificate.

Certificate Signing: This attribute give the capability of signing other certificates, but does not have the ability to be used as an End Entity certificate to perform encryption.

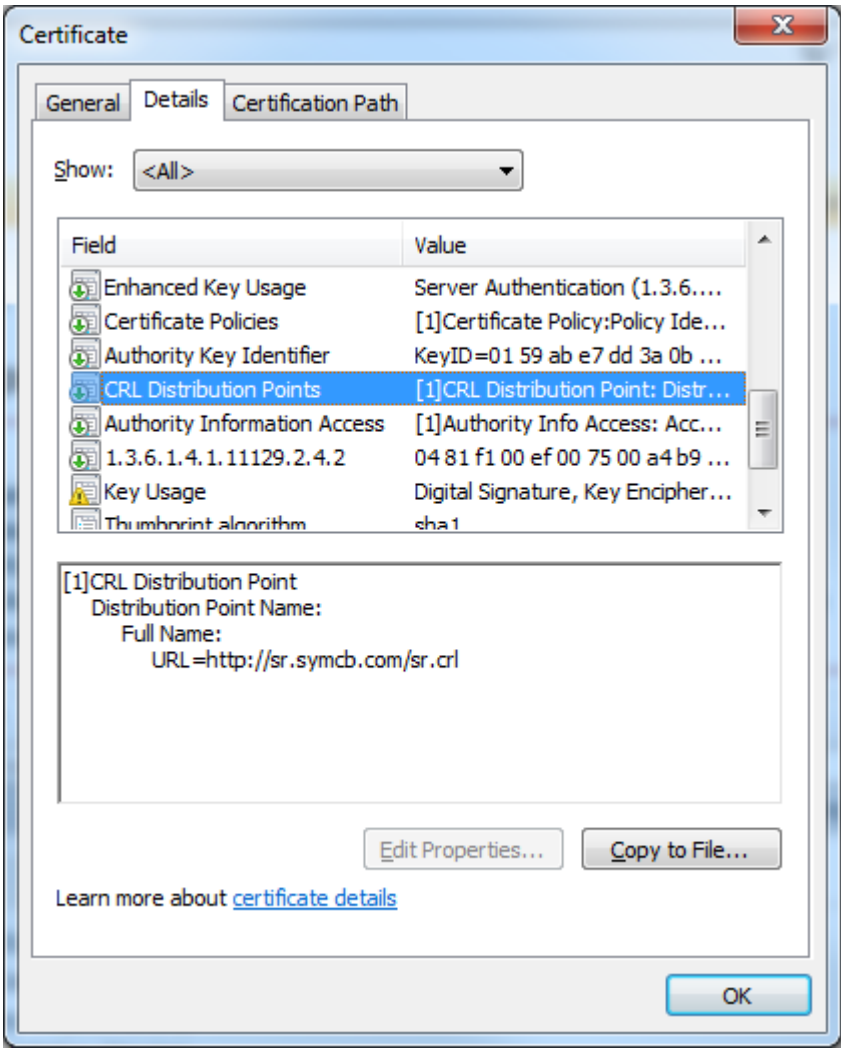
Off-line CRL Signing, CRL Signing (o6): This give the certificate the ability to sign certificates into a Certificate Revocation List.

CRL Distribution Points:

The CRL Distribution Points (Certificate Revocation List) extension provides the location of the corresponding Certificate Revocation List (CRL) for the SSL certificate. At the speed of light a web-browser will check the link that the certificate provides to check and see if the certificate has been revoked for ever non compliance or security reason. Firefox and IE will not allow you to access a website if the certificate running on it has been revoked.

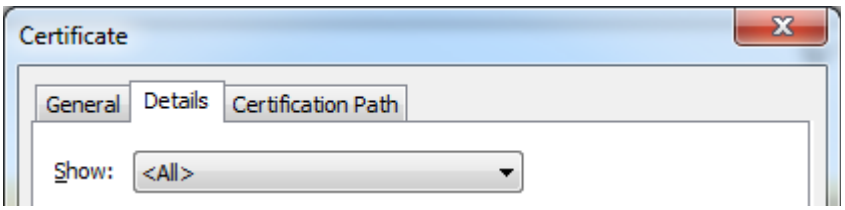
For some reason Google Chrome does not check this extension.... They do Something called CRL sets. Google gathers Certificate Revocation

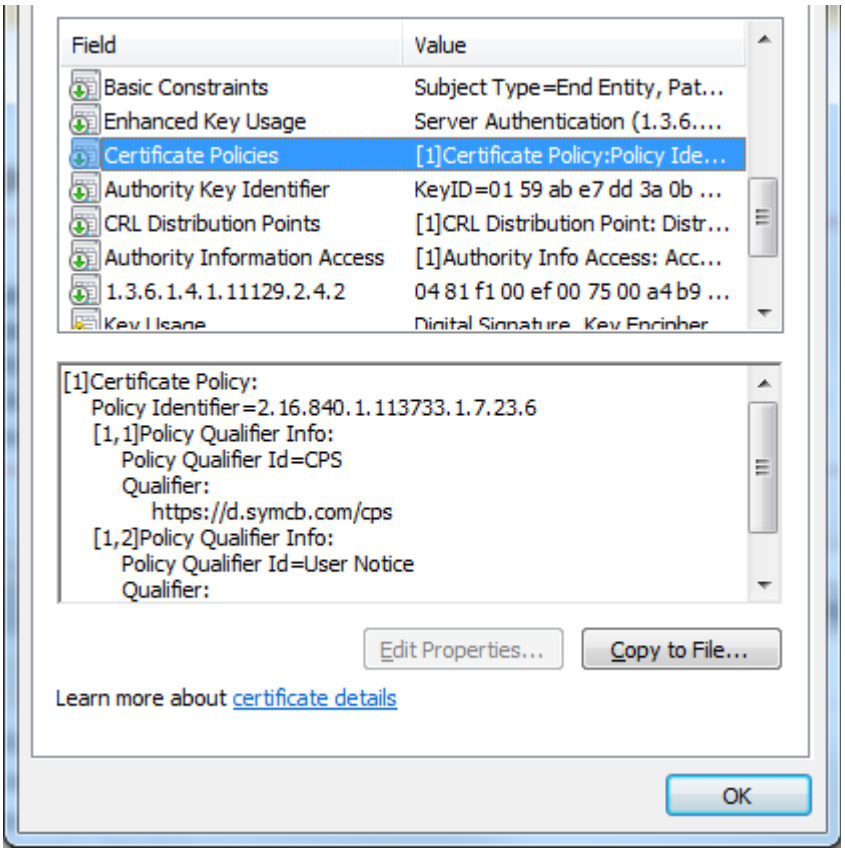
Lists from “participating” Certificate Authorities, trims the list down to include certificates that “they think are important” and then sends it out to Chrome. This means that the browser doesn’t need to contact the Certificate Authority itself and removes the performance and privacy overheads. The only problem here is that the list is not definitive. If Chrome doesn’t have a CRL for a particular CA, it will always trust certificates, even though they may have been revoked.



Certificate Policies:

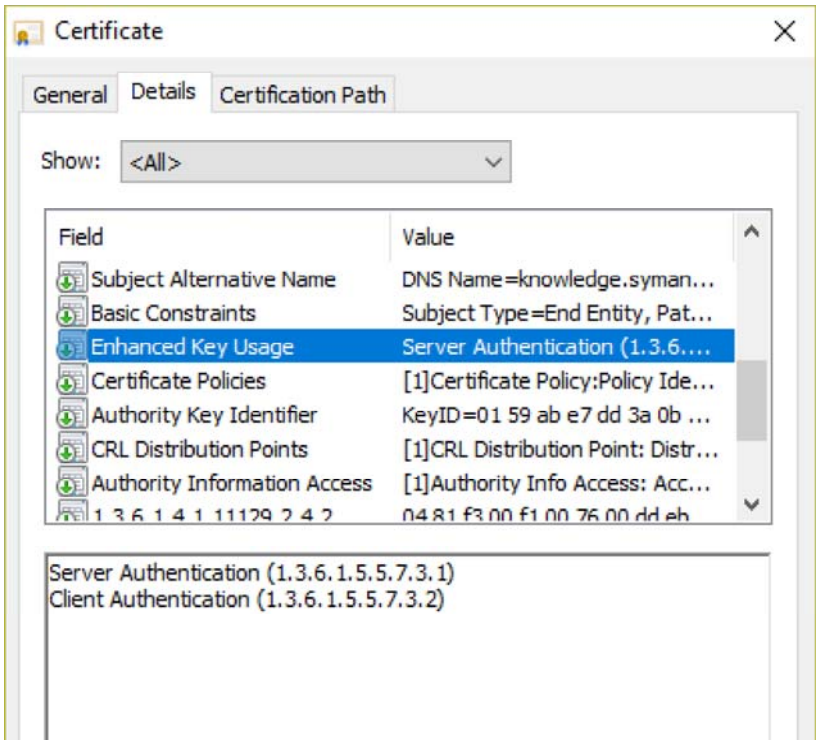
The Certificate Policies extension defines the legal rules associated with a particular certificate’s usage. Each CA has their own set of policies.

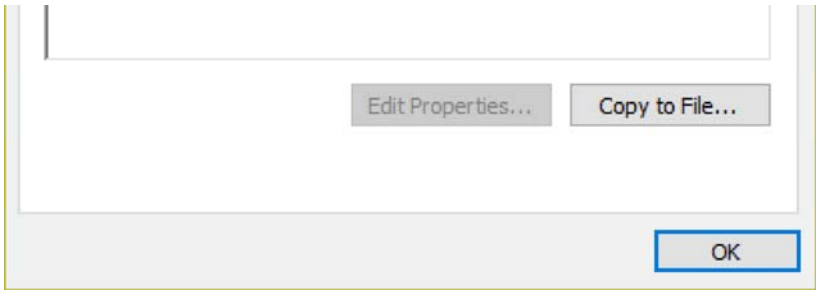




Enhanced Key Usage:

This is an important extension. A digital certificate performs the main function of Server Authentication, and Client Authentication. It pretty much tells users and servers “Hey I am who I am and this is the CA signed certificate that can prove it.”





The following Enhanced Key Usage extensions are not standard on a End Entity Certificate. If you require a certificate with one of these extensions then you may have to contact your CA for a special signing.

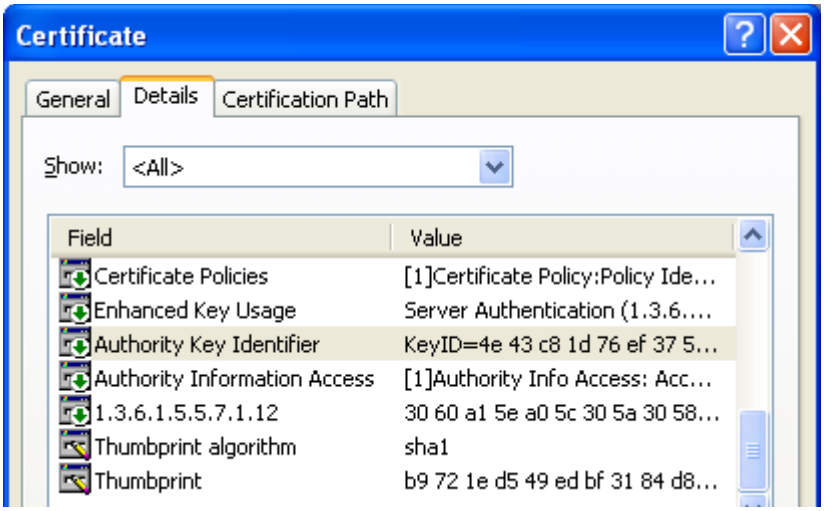
Non-repudiation: Use when the public key is used to verify digital signatures used to provide a non-repudiation service. Non-repudiation protects against the signing entity falsely denying some action (excluding certificate or CRL signing). This usage was once used by the banking industry, but of course now they do not want any liability for loosing your money with poor security practices on anyone's part.

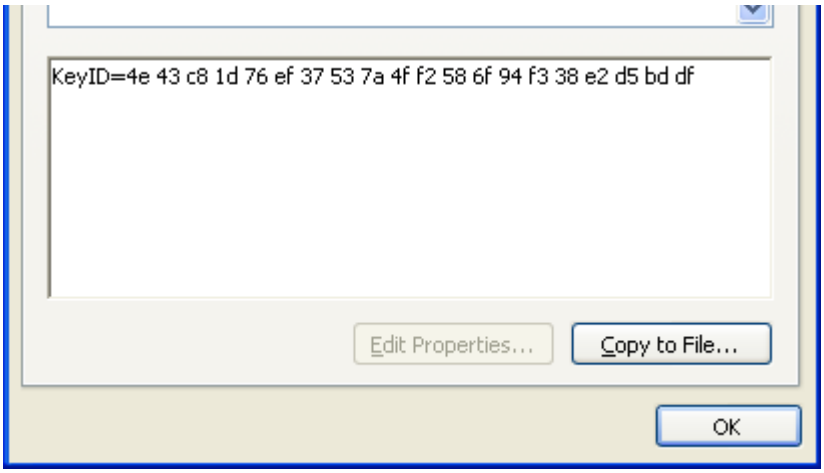
Data-encipherment: Use when the public key is used for encrypting user data, other than cryptographic keys. Usually server to server communications that transfer important data may require this.

For a list of other Key Usage extensions check out this link.

Authority Key Identifier (AKI):

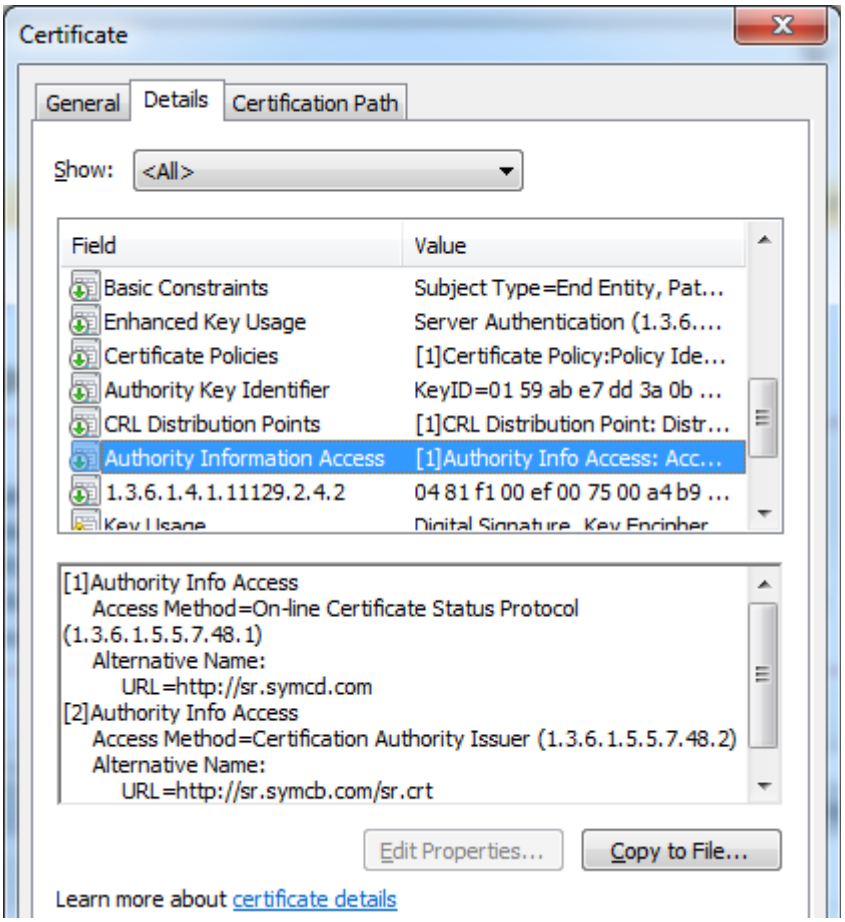
The Authority Key Identifier extension provides the key identifier of the Issuing CA certificate that signed the SSL certificate. This AKI value would match the SKI value of the Intermediate CA certificate.

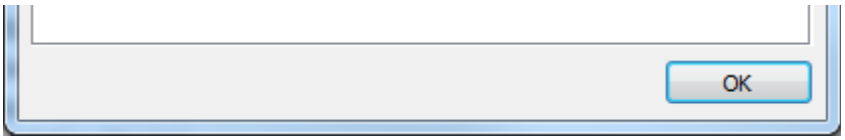




Authority Info Access:

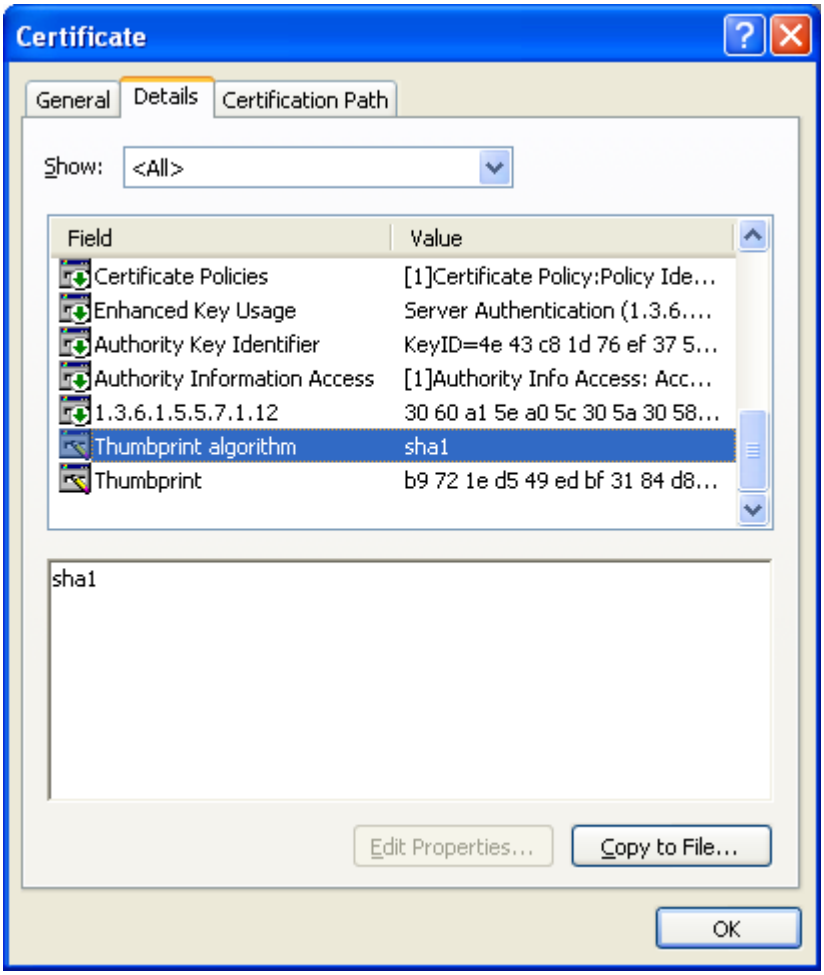
The Authority Info Access extension provides information about how to access information about a CA, such as OCSP validation and CA policy data. Some browsers are savvy enough to use this extension to fix the gaps in the "Chain of Trust." An Intermediate certificate helps the Chain of Trust from the End Entity Certificate to be trusted to all the different applications that may connect or use the End Entity Cert. Think of an intermediate as a wingman helping the End Entity Certificate.





Thumbprint algorithm:

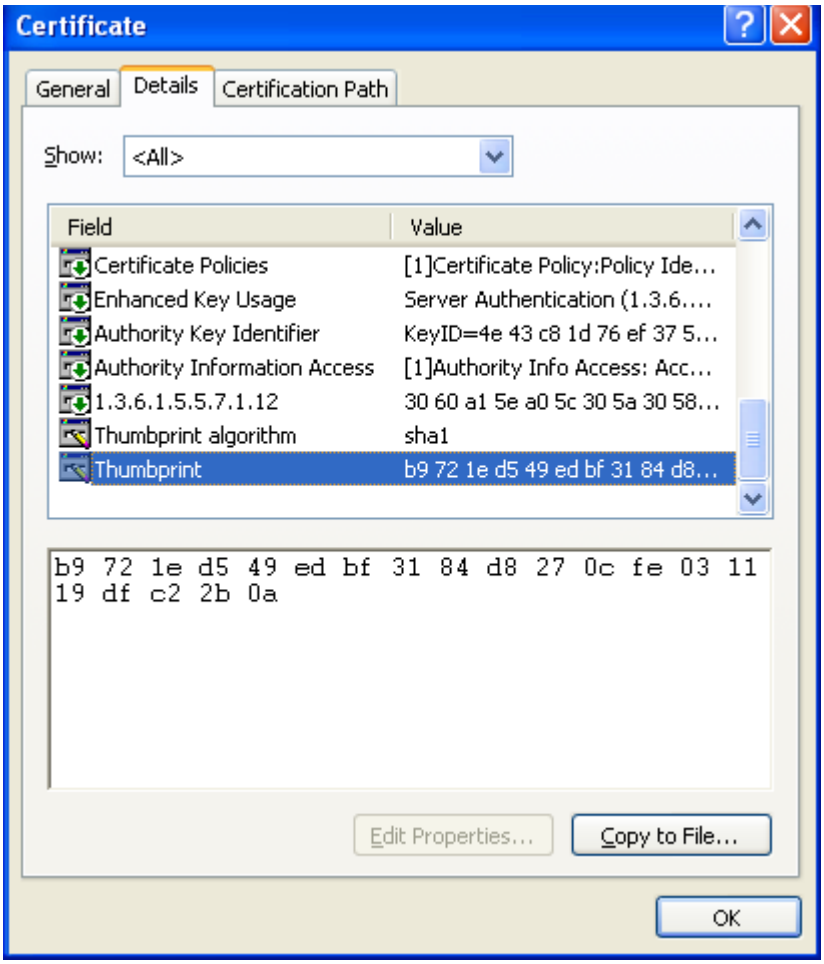
This extension indicates the algorithm used to hash the public/CSR key. It is not uncommon to have this be different then Signature Algorithm.



Thumbprint:

This extension provides the actual hash to ensure that the certificate has not been tampered with.

This Thumbprint can be used in Windows systems to recover or to troubleshoot private key related issues. Check out our article Troubleshooting: Missing Private Key on Windows Server Systems to learn more.



Add to favorites

About SSLSupportDesk:

SSLSupportDesk is part of Acmetek who is a trusted advisor of security solutions and services. They provide comprehensive security solutions that include Encryption & Authentication (SSL), Endpoint Protection, Multi-factor Authentication, PKI/Digital Signing Certificates, DDOS, WAF and Malware Removal. If you are looking for security look no further. Acmetek has it all covered!

Contact an SSL Specialist to get a consultation on the Website Security Solutions that can fit your needs.

Become a Partner and create additional revenue stream while the heavy lifting for you.