AMIDO

MakeCert Cheat sheet

Usage: MakeCert [basic|extended options] [outputCertificateFile]

Basic Options

Switch		Action
-sk	<keyName>	Subject's key container name; To be created if not present
-pe		Mark generated private key as exportable
-ss	<store>	Subject's certificate store name that stores the output certificate
-sr	<location>	Subject's certificate store location. <CurrentUser|LocalMachine>. Default to 'CurrentUser'
-#	<number>	Serial Number from 1 to 2^31-1. Default to be unique
-$	<authority>	The signing authority of the certificate <individual|commercial>
-n	<X509name>	Certificate subject X500 name (eg: CN=Fred Dews)

Extended Options

Switch		Action
-tbs	<file>	Certificate or CRL file to be signed
-sc	<file>	Subject's certificate file
-sv	<pvkFile>	Subject's PVK file; To be created if not present
-ic	<file>	Issuer's certificate file
-ik	<keyName>	Issuer's key container name
-iv	<pvkFile>	Issuer's PVK file
-is	<store>	Issuer's certificate store name.
-ir	<location>	Issuer's certificate store location <CurrentUser|LocalMachine>. Default to 'CurrentUser'
-in	<name>	Issuer's certificate common name.(eg: Fred Dews)
-a	<algorithm>	The signature's digest algorithm. <md5|sha1|sha256|sha384|sha512>. Default to 'sha1'
-ip	<provider>	Issuer's CryptoAPI provider's name
-iy	<type>	Issuer's CryptoAPI provider's type
-sp	<provider>	Subject's CryptoAPI provider's name
-sy	<type>	Subject's CryptoAPI provider's type
-iky	<keytype>	Issuer key type <signature|exchange|<integer>>.
-sky	<keytype>	Subject key type <signature|exchange|<integer>>.
-l	<link>	Link to the policy information (such as a URL)
-cy	<certType>	Certificate types <end|authority>
-b	<mm/dd/yyyy>	Start of the validity period; default to now.
-m	<number>	The number of months for the cert validity period
-e	<mm/dd/yyyy>	End of validity period; defaults to 2039
-h	<number>	Max height of the tree below this cert
-len	<number>	Generated Key Length (Bits) Default to '2048' for 'RSA' and '512' for 'DSS'
-r		Create a self-signed certificate
-nscp		Include Netscape client auth extension
-crl		Generate a CRL instead of a certificate
-eku	<oid[<,oid>]>	Comma separated enhanced key usage OIDs

Examples

Purpose	Command
Signing / Encryption	`makecert -r -pe -n "CN=Amido Encryption" -ss My -sky Exchange`
Certificate Authority	`makecert.exe -n "CN=My Root CA " -pe -ss my -sr LocalMachine -sky exchange -m 96 -a sha1 -len 2048 -cy authority -r My_Root_CA.cer`
SSL Certificate	`makecert -pe -n "CN=fqdn.of.server" -a sha1 -sky Exchange -eku 1.3.6.1.5.5.7.3.1 -ic CA.cer -iv CA.pvk -sp "Microsoft RSA SChannel Cryptographic Provider"  -sy 12 -sv server.pvk server.cer`

http://www.amido.com

MakeCert Cheat sheet

Usage: MakeCert [basic|extended options] [outputCertificateFile]

Other Utilities

Utility	Purpose
pvk2pfx	`pvk2pfx -pvk server.pvk -spc server.cer -pfx server.pfx` Combines the Private Key (server.pvk) and the Public Key (server.cer) into a single PKCS #12 (server.pfx) file.
Cert2spc	`cert2spc myX509.cer mySPC.spc` Convert the certificate (myX509.cer) to a Software Publisher Certificate (mySPC.spc) file.
SignTool	`signtool sign /f cert.pfx /p abc123 assembly.exe` Signs the Assembly (assembly.exe) with the certificate loaded from the PFX (cert.pfx) using the password (abc123) to access the certificate.
OpenSSL	`openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout mycert.pem -out mycert.pem` Creates a new X.509 certificate in PEM format that expires in a year.
Certmgr	`certmgr /add /c certificate.cer /s my` Imports the certificate (certificate.cer) into the My system store.
PowerShell (Get-ChildItem)	`Get-ChildItem -Recurse Cert:\` List all certificates on the Local system (CurrentUser and LocalMachine stores) and returns them a .NET X509Certificate2.

Common EKUs

OID	Action
1.3.6.1.5.5.7.3.1	Server authentication (i.e. Server SSL Certificate)
1.3.6.1.5.5.7.3.2	Client authentication (i.e. Client SSL Certificate)
1.3.6.1.5.5.7.3.3	Code signing (i.e. Authenticode)
1.3.6.1.5.5.7.3.4	Email Encryption and Signing
1.3.6.1.5.5.7.3.5	IPsec end system
1.3.6.1.5.5.7.3.6	IPsec tunnel
1.3.6.1.5.5.7.3.7	IPsec user
1.3.6.1.5.5.7.3.8	Timestamping
1.3.6.1.4.1.311.10.3.4	Encrypting File System (EFS)
1.3.6.1.4.1.311.10.3.12	Document Signing
1.3.6.1.5.5.8.2.2	Internet Key Exchange (IKE)
1.3.6.1.4.1.311.10.12.1	Any Application Policy

Further Reading:

- Manu Cohen-Yashar's Blog Post: Creating X.509 Certificates using Makecert.exe
- Stack Overflow: Using Makecert for Development SSL
- MSDN: Makecert.exe (Certificate Creation Tool)
- MSDN: SignTool.exe (Sign Tool)
- MSDN: Cert2spc (Software Publisher Certificate Test Tool)
- MSDN: Pvk2Pfx
- MSDN: Certmgr.exe (Certificate Manager Tool)
- Microsoft Support: Object IDs associated with Microsoft cryptography
- OpenSSL Command-Line HOWTO

http://www.amido.com