**MakeCert**

The MakeCert tool creates an [*X.509*](http://msdn.microsoft.com/en-us/library/ms721636(VS.85).aspx#_security_x.509_gly#_security_x.509_gly) certificate, signed by the test root key or other specified key, that binds your name to the public part of the key pair. The certificate is saved to a file, a system certificate store, or both. The tool is installed in the \Bin folder of the Microsoft Windows Software Development Kit (SDK) installation path.

MakeCert is available as part of the Windows SDK, which you can download from <http://go.microsoft.com/fwlink/?linkid=84091>.

The MakeCert tool uses the following command syntax:

**MakeCert** [*BasicOptions*|*ExtendedOptions*]*OutputFile*

*OutputFile* is the name of the file where the certificate will be written. You can omit *OutputFile* if the certificate is not to be written to a file.

**Options**

MakeCert includes basic and extended options. Basic options are those most commonly used to create a certificate. Extended options provide more flexibility.

The options for MakeCert are also divided into three functional groups:

* Basic options specific to certificate store technology only.
* Extended options specific to SPC-file and private key technology only.
* Extended options applicable to SPC-file, private key, and certificate store technology.

Options given in the following tables can be used only with Internet Explorer 4.0 or later.

|  |  |
| --- | --- |
| **Basic option** | **Description** |
| **-a** *Algorithm* | [*Hash*](http://msdn.microsoft.com/en-us/library/ms721586(VS.85).aspx#_security_hash_gly#_security_hash_gly) algorithm. Must be set to either **SHA-1** or **MD5** (default). For information about MD5, see [*MD5*](http://msdn.microsoft.com/en-us/library/ms721594(VS.85).aspx#_security_md5_gly#_security_md5_gly). |
| **-b** *DateStart* | Date the certificate first becomes valid. The default is when the certificate is created. The format of *DateStart* is mm/dd/yyyy. |
| **-cy** *CertificateTypes* | Certificate type. *CertificateTypes* can be **end** for end-entity, or **authority** for [*certification authority*](http://msdn.microsoft.com/en-us/library/ms721572(VS.85).aspx#_security_certification_authority_gly#_security_certification_authority_gly). |
| **-e** *DateEnd* | Date when the validity period ends. The default is the year 2039. |
| **-eku** *OID1***,** *OID2* … | Inserts a list of one or more comma-separated, [*enhanced key usage*](http://msdn.microsoft.com/en-us/library/ms721575(VS.85).aspx#_security_enhanced_key_usage_gly#_security_enhanced_key_usage_gly) [*object identifiers*](http://msdn.microsoft.com/en-us/library/ms721599(VS.85).aspx#_security_oid_gly#_security_oid_gly) (OIDs) into the certificate. For example, **-eku 1.3.6.1.5.5.7.3.2** inserts the client authentication OID. For definitions of allowable OIDs, see the Wincrypt.h file in CryptoAPI 2.0. |
| **-h** *NumChildren* | Maximum height of the tree below this certificate. |
| **-l** *PolicyLink* | Link to SPC agency policy information (for example, a URL). |
| **-m** *nMonths* | Duration of the validity period. |
| **-n "***Name***"** | Name for the publisher's certificate. This name must conform to the [*X.500*](http://msdn.microsoft.com/en-us/library/ms721636(VS.85).aspx#_security_x.500_gly#_security_x.500_gly) standard. The simplest method is to use the "CN=*MyName*" format. For example: **-n "CN=Test"**. |
| **-nscp** | The Netscape client authentication extension should be included. |
| **-pe** | Marks the private key as exportable. |
| **-r** | Creates a self-signed certificate. |
| **-sc** *SubjectCertFile* | Certificate file name with the existing subject public key to be used. |
| **-sk** *SubjectKey* | Location of the subject's key container which holds the [*private key*](http://msdn.microsoft.com/en-us/library/ms721603(VS.85).aspx#_security_private_key_gly#_security_private_key_gly). If a key container does not exist, one is created. If neither the **-sk** or **-sv** option is used, a default key container is created and used by default. |
| **-sky** *SubjectKeySpec* | Subject's key specification.  *SubjectKeySpec* must be one of three possible values:   * **Signature** (AT\_SIGNATURE key specification) * **Exchange** (AT\_KEYEXCHANGE key specification) * An integer, such as **3**   For more information, see the Note that follows this table. |
| **-sp** *SubjectProviderName* | CryptoAPI provider for subject. The default is the user's provider. For information about CryptoAPI providers, see the CryptoAPI 2.0 documentation. |
| **-sr** *SubjectCertStoreLocation* | Registry location of the subject's certificate store. *SubjectCertStoreLocation* must be either **LocalMachine** (registry key HKEY\_LOCAL\_MACHINE) or **CurrentUser** (registry key HKEY\_CURRENT\_USER). **CurrentUser** is the default. |
| **-ss** *SubjectCertStoreName* | Name of the subject's certificate store where the generated certificate will be stored. |
| **-sv** *SubjectKeyFile* | Name of the subject's .pvk file. If neither the **-sk** or **-sv** option is used, a default key container is created and used by default. |
| **-sy** *nSubjectProviderType* | CryptoAPI provider type for subject. The default is [*PROV\_RSA\_FULL*](http://msdn.microsoft.com/en-us/library/ms721603(VS.85).aspx#_security_prov_rsa_full_provider_type_gly#_security_prov_rsa_full_provider_type_gly). For information about CryptoAPI provider types, see the CryptoAPI 2.0 documentation. |
| **-#** *SerialNumber* | Serial number of the certificate. The maximum value is 2^31. The default is a value generated by the tool that is guaranteed to be unique. |
| **-$** *CertificateAuthority* | Type of certification authority. *CertificateAuthority* must be set to either **commercial** (for certificates to be used by commercial software publishers) or **individual** (for certificates to be used by individual software publishers). |
| **-?** | Displays the basic options. |
| **-!** | Displays the extended options. |

**Note**  If the **-sky** key specification option is used in Internet Explorer version 4.0 or later, the specification must match the key specification indicated by the private key file or private [*key container*](http://msdn.microsoft.com/en-us/library/ms721590(VS.85).aspx#_security_key_container_gly#_security_key_container_gly). If the key specification option is not used, the key specification indicated by the private key file or private key container will be used. If there is more than one key specification in the key container, MakeCert will first attempt to use the AT\_SIGNATURE key specification. If that fails, MakeCert will try to use AT\_KEYEXCHANGE. Because most users have either an AT\_SIGNATURE key or an AT\_KEYEXCHANGE key, this option does not need to be used in most cases.

The following options are only for [*software publisher certificate*](http://msdn.microsoft.com/en-us/library/ms721625(VS.85).aspx#_security_software_publishing_certificate_gly#_security_software_publishing_certificate_gly) (SPC) files and private key technology.

|  |  |
| --- | --- |
| **SPC and private key option** | **Description** |
| **-ic** *IssuerCertFile* | Location of the issuer's certificate. |
| **-ik** *IssuerKey* | Location of the issuer's key container. The default is the test root key. |
| **-iky** *IssuerKeySpec* | Issuer's key specification, which must be one of three possible values:   * **Signature** (AT\_SIGNATURE key specification) * **Exchange** (AT\_KEYEXCHANGE key specification) * An integer, such as **3**   For more information, see the Note that follows this table. |
| **-ip** *IssuerProviderName* | CryptoAPI provider for issuer. The default is the user's provider. For information about CryptoAPI providers, see the CryptoAPI 2.0 documentation. |
| **-iv** *IssuerKeyFile* | Issuer's private key file. The default is the test root. |
| **-iy** *nIssuerProviderType* | CryptoAPI provider type for issuer. The default is PROV\_RSA\_FULL. For information about CryptoAPI provider types, see the CryptoAPI 2.0 documentation. |

**Note**  If the **-iky** key specification option is used in Internet Explorer 4.0 or later, the specification must match the key specification indicated by the private key file or private key container. If the key specification option is not used, the key specification indicated by the private key file or private key container will be used. If there is more than one key specification in the key container, MakeCert will first attempt to use the AT\_SIGNATURE key specification. If that fails, MakeCert will try to use AT\_KEYEXCHANGE. Because most users have either an AT\_SIGNATURE key or an AT\_KEYEXCHANGE key, this option does not need to be used in most cases.

The following options are for [*certificate store*](http://msdn.microsoft.com/en-us/library/ms721572(VS.85).aspx#_security_certificate_store_gly#_security_certificate_store_gly) technology only.

|  |  |
| --- | --- |
| **Certificate store option** | **Description** |
| **-ic** *IssuerCertFile* | File that contains the issuer's certificate. MakeCert will search in the certificate store for a certificate with an exact match. |
| **-in** *IssuerNameString* | Common name of the issuer's certificate. MakeCert will search in the certificate store for a certificate whose common name includes *IssuerNameString*. |
| **-ir** *IssuerCertStoreLocation* | Registry location of the issuer's certificate store. *IssuerCertStoreLocation* must be either **LocalMachine** (registry key HKEY\_LOCAL\_MACHINE) or **CurrentUser** (registry key HKEY\_CURRENT\_USER). **CurrentUser** is the default. |
| **-is** *IssuerCertStoreName* | Issuer's certificate store that includes the issuer's certificate and its associated private key information. If there is more than one certificate in the store, the user must uniquely identify it by using the **-ic** or **-in** option. If the certificate in the certificate store is not uniquely identified, MakeCert will fail. |