NAME

certmgr – Mono Certificate Manager (CLI version)

SYNOPSIS

certmgr [action] [object type] [options] store [filename] or **certmgr -ssl [options] url**

DESCRIPTION

This tool allows to list, add, remove or extract certificates, certificate revocation lists (CRL) or certificate trust lists (CTL) to/from a certificate store. Certificate stores are used to build and validate certificate chains for Authenticode(r) code signing validation and SSL server certificates.

STORES

The *store* represents the certificate store to use. It can be one of the following:

My This is the personal certificate store.

AddressBook
This is the store for other people.

CA This is a store for intermediate certificate authorities.

Trust This is for trusted roots.

Disallowed
This is for untrusted roots

ACTIONS

-list List the certificates, CTL or CTL in the specified store.

-add Add a certificate, CRL or CTL to specified store. If filename is a pkcs12 or pfx file, and it contains a private key, it will be imported to local key pair container.

-del Remove a certificate, CRL or CTL from specified store. You must specify the object to be removed with it's hash value (and not a filename). This hash value is shown when doing a **-list** on the store.

-put Copy a certificate, CRL or CTL from a store to a file.

-ssl Download and add the certificates from a SSL session. You'll be asked to confirm the addition of every certificate received from the server. Note that SSL/TLS protocols do not requires a server to send the root certificate. This action assumes a certificate (-c) object type and will import the certificates in appropriate stores (i.e. server certificate in the OtherPeople store, the root certificate in the Trust store and any other intermediate certificates in the IntermediateCA store).

-importKey
Allows importing a private key from a pkcs12 file into a local key pair store. (Useful when you already have the key's corresponding certificate installed at the specific store.)

OBJECT TYPES

-c , -cert , -certificate
Add, Delete or Put certificates. That is the specified file must/will contain X.509 certificates in DER binary encoding.

-crl Add, Delete or Put certificate revocation lists (CRL). That is the specified file must/will contain X.509 CRL in DER binary encoding.

-ctl Add, Delete or Put certificate trust lists (CRL). UNSUPPORTED.

OPTIONS

-m Use the machine's certificate stores (instead of the default user's stores).

-v More details displayed on the console.

-p password
Use the specified password when accessing a pkcs12 file.

-help , -h , -? , /?
Display help about this tool.

FILES

WARNING: This details the current behavior of Mono and could change between releases. The only safe way to interact with certificate stores is to use the certmgr tool. The current releases of Mono keeps all the user certificate stores in separates directories under *~/.config/.mono/certs/*

For example the trusted root certificates for a user would be kept under
~/.config/.mono/certs/Trust/

Certificates files are kept in DER (binary) format (extension .cer).

The filenames either start with
tbp (thumbprint) or *ski* (subject key identifier).

The rest of the filename is the base64-encoded value (tbp or ski).

Private key data is stored under
~/.config/.mono/keypairs/

EXAMPLES

mono certmgr.exe -list -c -m Trust
List all certificates in the machine Trust store. This will display the hash value for each certificate. This value can be used to identify uniquely a certificate for some operations (e.g. delete). E.g. **Unique Hash: FFA3AC0084DA1673B5A031EBB2156B3E8FBBF6D8**

mono certmgr.exe -del -c -m Trust FFA3AC0084DA1673B5A031EBB2156B3E8FBBF6D8
Remove the certificate, represented by the hash value, from the machine Trust store. Note that the machine store is normally restricted. The following error message will appear if the current user doesn't have the minimum access rights to remove the certificate: **Access to the machine 'Trust' certificate store has been denied.**

certmgr -ssl https://www.verisign.com
Import certificates from www.verisign.com used for HTTP over SSL. See KNOWN ISSUES (MD2) if you're downloading from www.verisign.com.

certmgr -ssl ldaps://www.nldap.com:636
Import the certificates from www.nldap.com used for secure LDAP. This works even if we don't know how to speak LDAP because we stop the communication shortly after the SSL handshake (which gives us the certificate).

KNOWN ISSUES

MD2 Some Certificate Authorities (CA) old root certificates use the MD2 hash algorithm. MD2 is old enough not to be part of the standard .NET framework. This makes it impossible to validate a digital signature made with MD2. For this reason MD2 is included in the Mono.Security.dll assembly. However the machine.config file must be updated so the OID for MD2 is known at runtime.

To correct this insert the following XML snippet inside the <configuration> element of your machine.config file.

```
 <mscorlib>
  <cryptographySettings>
   <cryptoNameMapping>
    <cryptoClasses>
     <cryptoClass monoMD2="Mono.Security.Cryptography.MD2Managed, Mono.Security,
Version=1.0.5000.0, Culture=neutral, PublicKeyToken=0738eb9f132ed756" />
```

```
      </cryptoClasses>
      <nameEntry name="MD2" class="monoMD2" />
    </cryptoNameMapping>
    <oidMap>
      <oidEntry OID="1.2.840.113549.2.2" name="MD2" />
    </oidMap>
  </cryptographySettings>
</mscorlib>
```

AUTHOR

Written by Sebastien Pouliot

Minor additions by Pablo Ruiz García

COPYRIGHT

MAILING LISTS

Visit http://lists.ximian.com/mailman/listinfo/mono-list for details.

WEB SITE

Visit http://www.mono-project.com for details

SEE ALSO

makecert(1),setreg(1)