NAME

signcode − Digitally sign an PE executable using an X.509 certificate.

SYNOPSIS

signcode [options] filename

DESCRIPTION

Digitally sign an PE executable (CLR assembly, Win32 EXE or DLL) using an X.509 certificate and it's associated private key. The signature is compatible with Authenticode(r) and can be validated with chktrust (either on Windows or on any platform supported by Mono).

OPTIONS

-spc spcfile

The Software Publisher File (spc) that contains the X.509 certificate chain used to digitally sign the PE executable.

-v pvkfile

The Private Key File (pvk) that contains the private key used to digitally sign the PE executable. This private key must match the public key inside the publisher X.509 certificate.

-a sha1 | md5 | sha2 | sha256 | sha384 | sha512

The hash algorithm used in the digital signature of the PE executable. The default algorithm is SHA1.

-$ individual | commercial

Add information about the publisher, i.e. if the signature is generated by an individual or a commercial entity.

-n description

Add a textual description of the signed file.

-i url Add a URL associated to the publisher or the signed file.

-t url URL to a timestamp service to countersign the PE executable. Countersignature is required if you want the PE executable signature to be valid after the publisher certificate expires. The countersignature proves that the publisher had a valid (non-expired) certificate when the PE executable was signed.

-tr # Number of retries to get a timestamp for the countersignature.

-tw # Delay (in seconds) between the retries to get a timestamp for the countersignature.

-k name

CryptoAPI key container name (when not using -v).

-p name

CryptoAPI provider name (when not using -v).

-y # CryptoAPI provider type (when not using -v or -p).

-ky signature | exchange | #

CryptoAPI key type (when not using -v).

-r localMachine | currentUser

CryptoAPI key location (when not using -v).

-help , -h , -? , /?

Display help about this tool.

OTHER CODE SIGNING TECHNOLOGIES

Assemblies are PE files that can also be strongnamed using the sn.exe tool. The order of code signature is important if a file requires both an Authenticode and a strongname signature. Strongname must be applied before the Authenticode signature. Applying a strongname after the Authenticode signature, like re-signing an assembly (e.g. delay-sign), will invalidate the Authenticode signature.

KNOWN RESTRICTIONS

signcode cannot generate Authenticode signatures for CAB files.

AUTHOR

Written by Sebastien Pouliot

COPYRIGHT

MAILING LISTS

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

WEB SITE

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

SEE ALSO

chktrust(1),makecert(1),**cert2spc(1)**