GOFF Concepts LLC
Intuitive Software

CertManEX 1.0 Series

Instruction Manual

document version: 1.0.0.2

Contents

Installing CertManEX

CertManEX was designed to be easy to use and install. The provided installer is merely a convenience to extract the bundled contents.

Using the provided installer

Run ***CertManEX_Install.exe*** by double clicking on it with a mouse. After agreeing to the EULA, the options are fairly generic. You also have the choice of creating *short cut folders* and where to install ***CertManEX.exe*** itself. Although CertManEX does not need administrator rights, the installer does as required by Microsoft Windows®.

Creating Certificates

CertManEX is a tool to enable you to create your own self-signed and issued certificates. These can be used in all your devices like NAS, ip camera, router, mobile phones, PBX, IoT, and other equipment that needs a certificate trusted when using a computer or phone.

Certificate Type

End Entity
By default the main program window shows an *End Entity Certificate* selected in the drop down. This is the certificate file that will be signed by your custom self-signed *Root* or *Intermediate* certificate. You will most likely create more of these than any other type. They will be installed to your equipment after you have exported them out.

Root Certificate
These issuing certificates are what prove *end entity* certificates as being valid. Generally, you will only create one root cert and use it to sign every other certificate you will ever create. Make the *valid start* and *valid end* times for as long as you want your maintenance period to be. Keep it secure and do not allow others to access it.

Intermediate Certificate
These certificates function similarly to root certificates but offer two useful characteristics: security and organization.

In order to sign an *end entity* certificate, the issuing certificate must naturally be present and accessible. If a *Root* certificate is being used, this could potentially expose it to unwanted access. How secure is the system being used to create certificates? If greater security is desired, you would create an *Intermediate* certificate, signed by a root. Then with the root locked away for safe keeping, the intermediate would do the majority of the work.

The other benefit of an intermediate certificate is when you create more than one of them. Some organizations might create one for each department. Then when a certificate is no longer valid, for whatever reason, only that department is effected. Another situation is when you are allowing others to use your intermediate cert to sign their own certificates. You would create one certificate for each group you want to give this ability to.

These two options are not something you would probably use in a home or small environment. But the option is made available nevertheless. A caveat to using an intermediate certificate is that some devices will need to have it available in addition to the end entity. This is just an extra step when exporting.

Exporting Certificates

Exporting certificates sounds simple but is actually quite complex. However, CertManEX makes this more intuitive for you. More options will be forth coming based on your feedback. For now, here are some typical options to export your certificate based on the intended usage.

X.509 v3

This is your standard certificate format output either in der (binary) or pem (base64) based encoding. For an Apache server, you would choose your favorite file extension, pem encoded, then the *Cert and Key separate file* option. If you issued this certificate by signing it with an *Intermediate* certificate, then you may also need to export the intermediate cert (without its private key). If your device supports it, you could make a single file by copying the contents of the two certificates into one. Let us know if you need this feature and why.

PKCS #7

Used for email based certificate signing. Useful when you want the full chain stored in one file (chain is the file cert itself along with intermediate or root certs). Does **not** contain the private key.

PKCS #12

A storage file for the certificate or chain of certificates. Does contain the private key. Use this when you want to export the key out of CertManEX to move to another system or to backup your certificates. The *Extended Properties* option stores items like the *Description* data and creation times. Only valid on Windows based systems.

Keyboard shortcuts

F1	Show the help file.
F3	Show Export window.
F4	Drop down focused combo box.
F5	Refresh list of certificates.
F10	Puts focus on the menu bar.
ALT	Puts focus on the menu bar.
ESC	Close a window.
DELETE	Delete selected item.
CTRL+A	Select all items.
CTRL+D	Delete selected items.
CTRL+W	Closes the application or window