Create Let's Encrypt Signed Certificate Using HTTP Challenge

TekCERT allows you to create Let's Encrypt signed certificates easily if you have access to DNS administration interface for your domain. DNS records for the selected domain are hosted on a Windows server and a certificate for test.kaplansoft.com will be created in this example.

You need to obtain your public IP address if the TekCERT running machine is behind a NAT gateway. You can skip this procedure if your TekCERT running machine is connected directly to the Internet and you know your public address.

You can obtain your public IP address through online IP lookup applications like http://www.ipadresi.com/
You can also see your public IP address through TekCERT File / Get public IP address menu option.

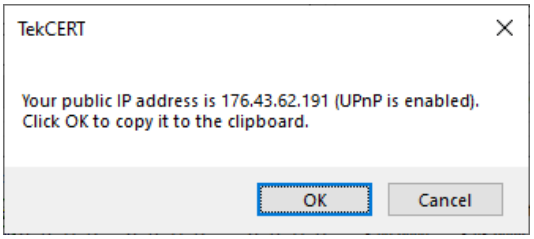

Figure 1. - Obtaining public IP address through TekCERT interface

You need to have a mapping for TCP port 80 on your TekCERT running machine. This is done by TekCERT automatically if your NAT gateway supports UPnP and it's enabled. You need to configure mapping for incoming connections to TCP 80 port if UPnP is not available. Please also make sure that there is not any IP filter or firewall policy blocking incoming TCP port 80 requests both in your machine and in the router which provides Internet connectivity.

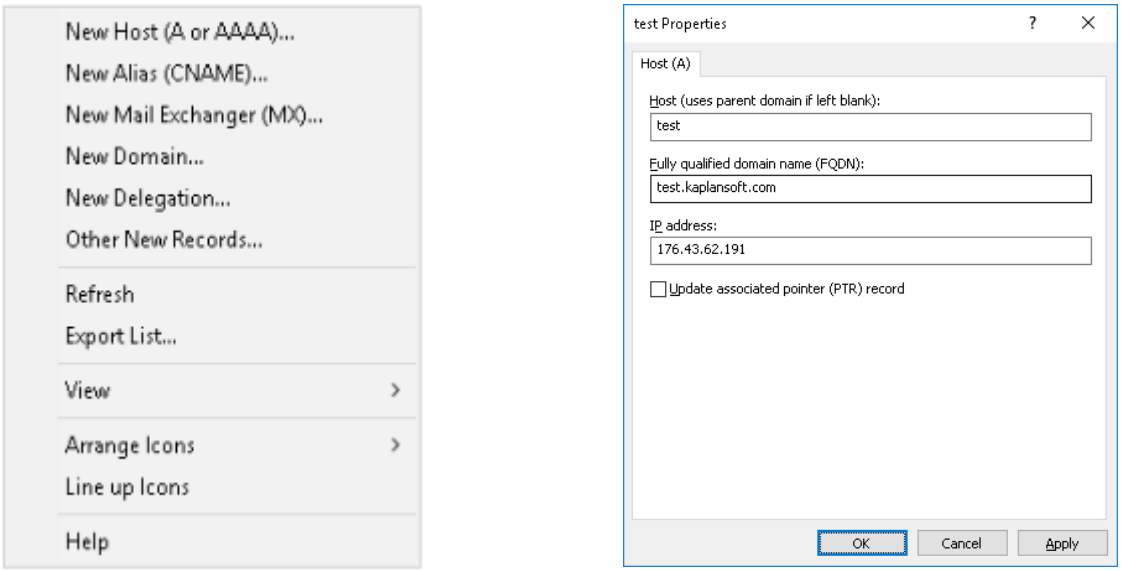

Figure 2. - DNS record creation options and new DNS A record entry

DNS Configuration

Connect to the Windows Server which hosts DNS server. Run DNS Manager and go to DNS / Server Instance / Forward Lookup Zones / Your domain (kaplansoft.com in this example). You need to create an A record for the host named test. Right click on the empty space on the right pane. Select New Host (A or AAAA)... Enter “test” as Host and enter obtained public IP address as “IP address” and click OK button. DNS configuration is ready after following this procedure.

Creating and Signing the Certificate

Run TekCERT and populate necessary certificate parameters in TekCERT certificates tab. Uncheck **Self Signed** option and select Let’s Encrypt as certificate authority. Click the Generate Certificate button when all necessary parameters are set.

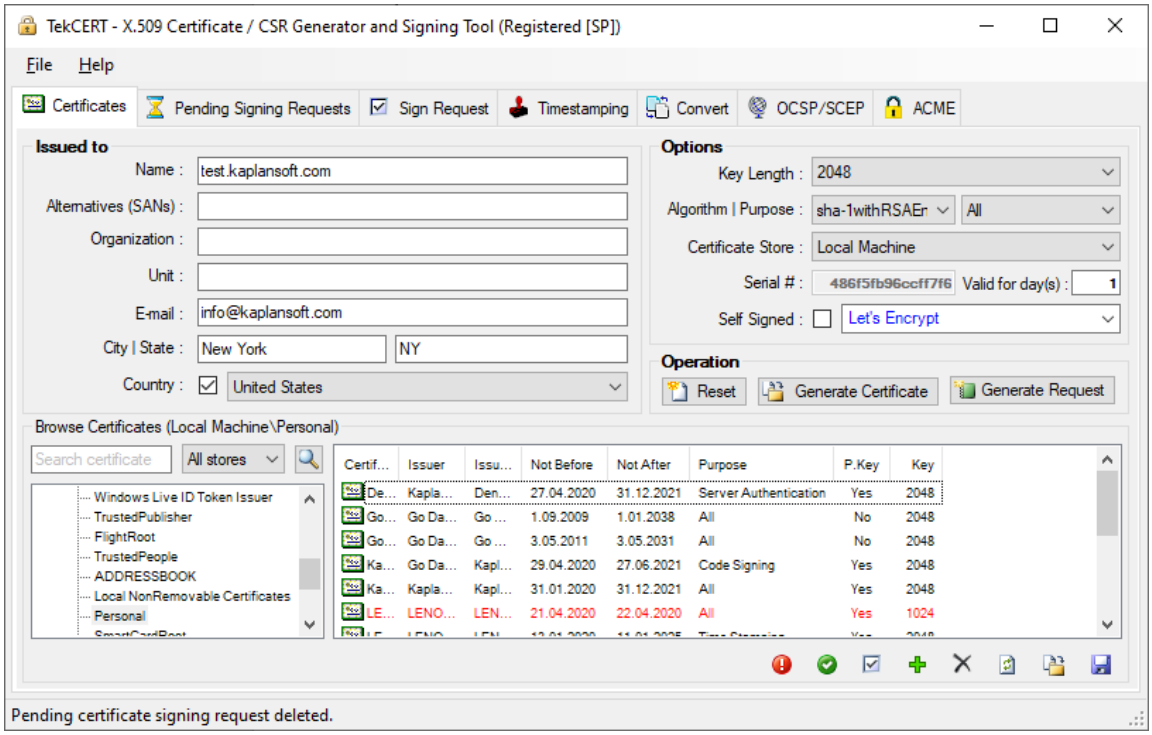

Figure 1. - Certificate Parameters

TekCERT will submit certificate signing requests and process received responses from Let’s Encrypt services and Certificate will be signed and copied to selected Windows certificate store if your configuration is correct.

When TekCERT is co-located with an IIS installation, TekCERT will automatically place ACME challenge file under root directory of the virtual server /.well-known\acme-challenge directory if a configured virtual server found for the domain name and automatically finalize certificate signing process.

TekCERT will display a file save dialog which allows you to save challenge file if configured DNS A record for the FQDN in the certificate points to another server. You must copy this file to the configured web server

root /.well-known/acme-challenge directory prior to complete signing process through ACME tab. TekCERT will create a pending signing request entry after saving challenge file. Select pending request in ACME tab and click Process Pending Request button to complete signing process.

Finalizing Signature Signing

Return to TekCERT and go to ACME tab. Select pending certificate signing request, Select HTTP-01 as “Challenge Type” and click Process Pending Request button. This will trigger Let’s Encrypt HTTP validation process to finalize signature signing process. The certificate will be signed and copied to selected Windows certificate store if your configuration is correct.

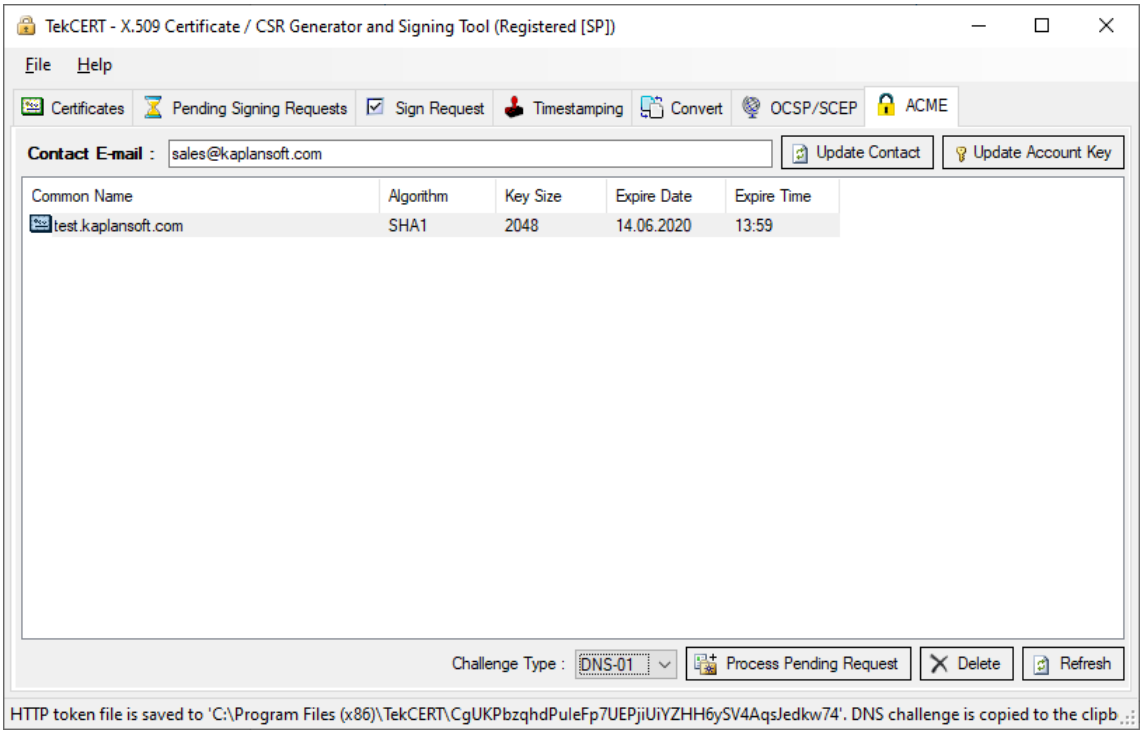

Figure 4. - Pending ACME signing requests