Create Let's Encrypt Signed Certificate Using DNS Challenge

You can create a Let's Encrypt signed certificate using DNS Challenge. This requires you to 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.

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

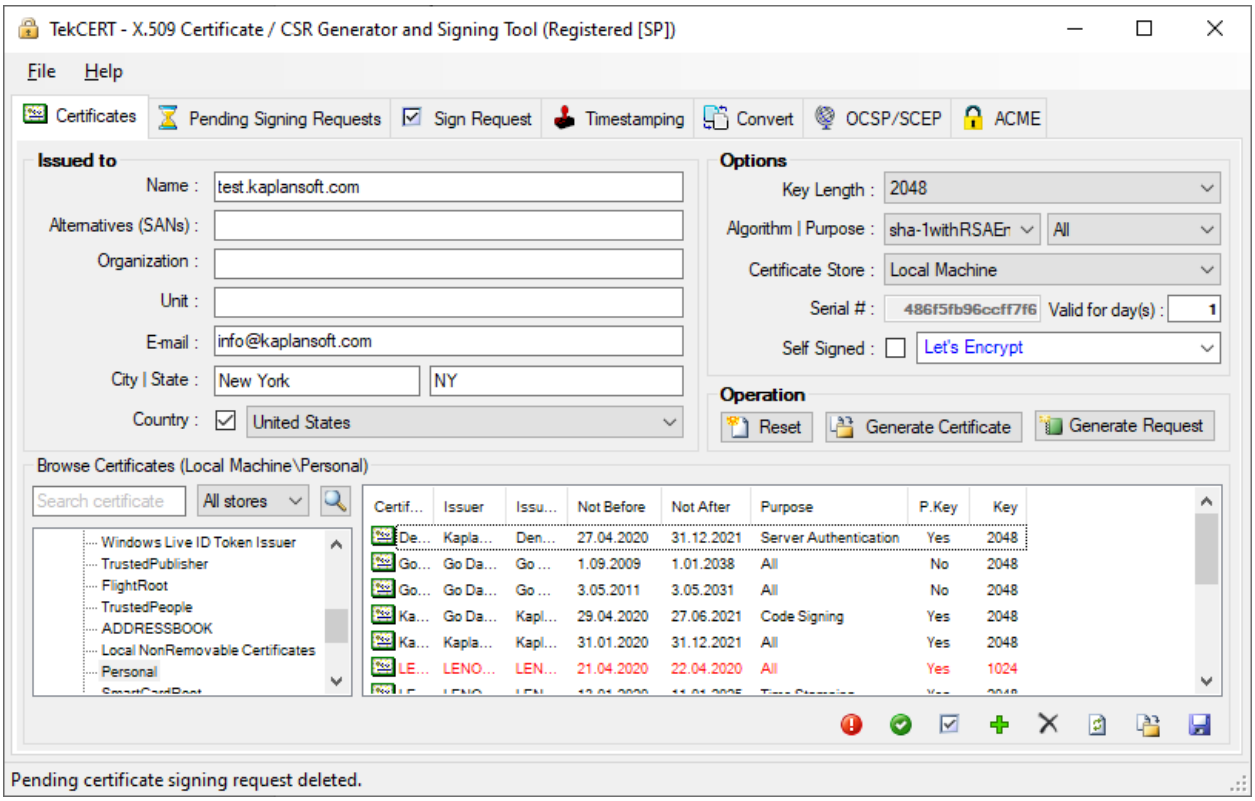


Figure 1. - Certificate Parameters

TekCERT will prompt a file save dialog when it receives challenges from Let's Encrypt service. HTTP challenge will be saved as a text file and DNS challenge is copied to the clipboard. Run Notepad file and copy it to a blank text file.

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 a sub domain for test. Right click on empty space on right pane. Select New Domain.

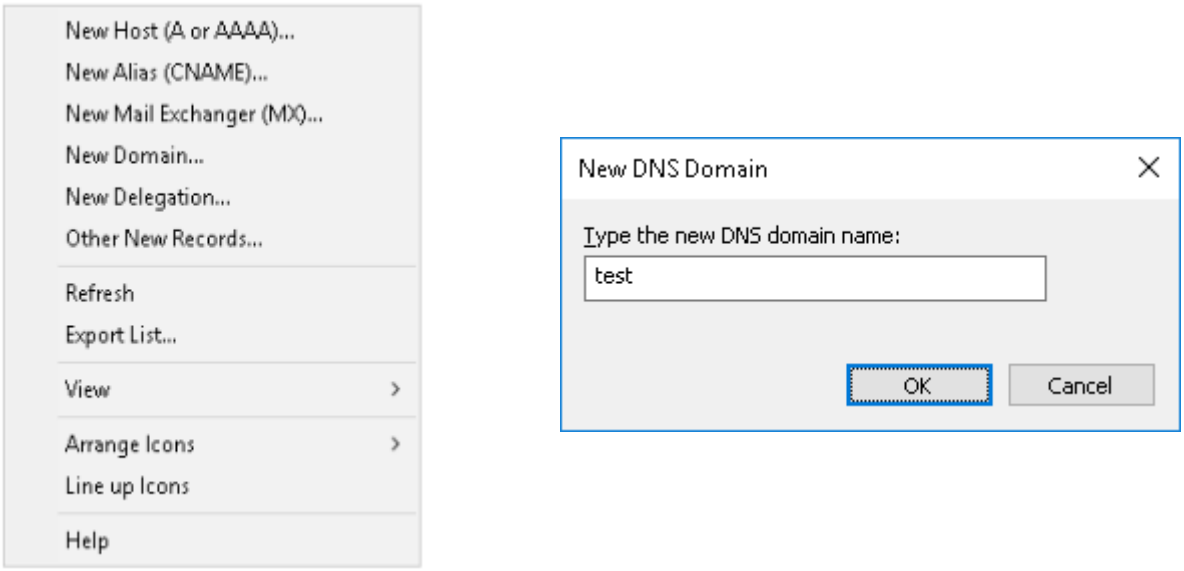
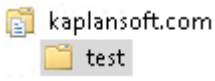


Figure 2. - DNS record creation options and new DNS sub domain name entry



Enter test as new DNS domain name and click OK. Double click on created sub domain. Right click on a empty space on right pane and click Other New Records.

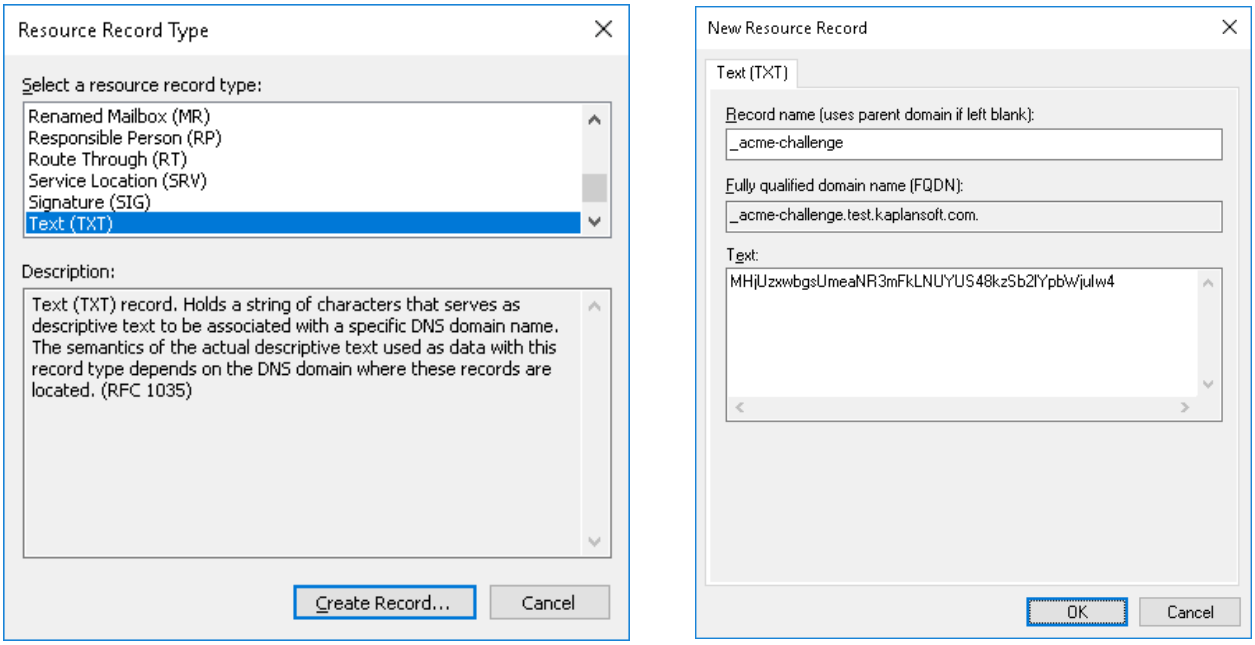


Figure 3. - DNS TXT record creation

Select “Text (TXT)” as “Resource Record Type” and click “Create Record” buton. Enter `_acme-challenge` as Record name and paste copied DNS challange to “Text” parameter and click OK button. Your DNS configuration is ready after following this procedure.

When TekCERT is co-located with a Microsoft DNS installation, and name server points to the local machine, TekCERT will automatically create TXT records for the DNS token and automatically finalize certificate signing process.

Finalizing Signature Signing

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

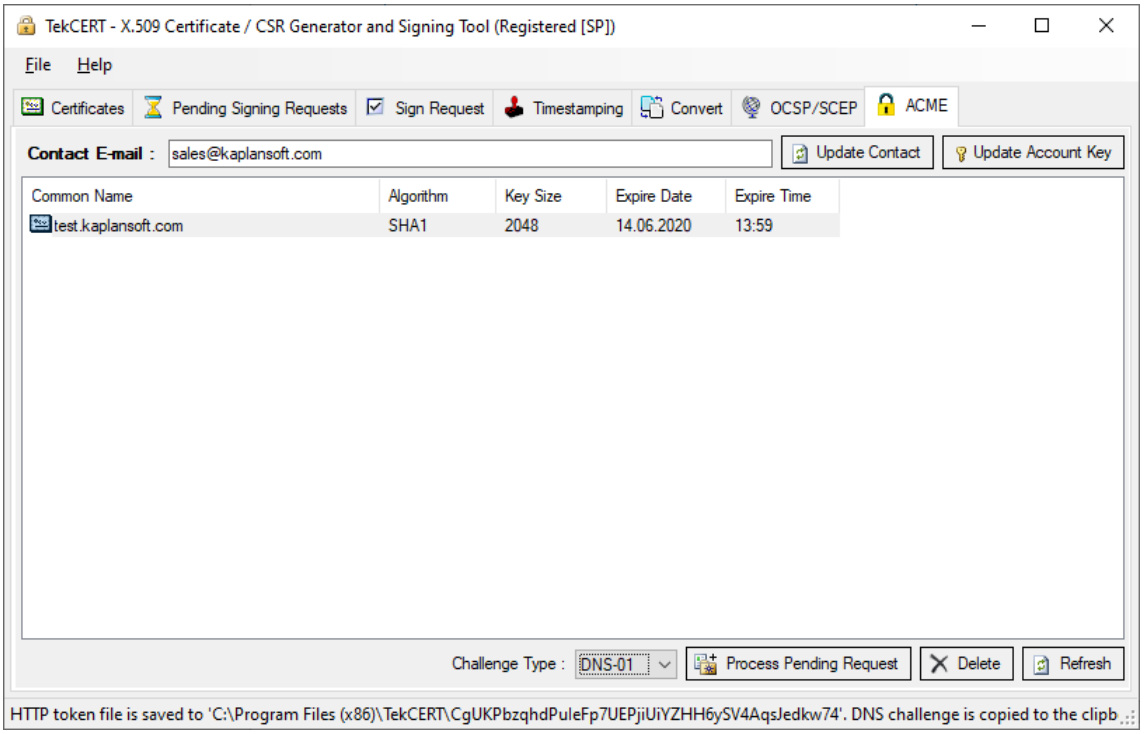


Figure 4. - Pending ACME signing requests