## 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 the Generate Certificate button when all necessary parameters are set.

TekCERT - X.509 Certificate / CSR Generator and Signing Tool (Registered [SP])	– 🗆 X
<u>E</u> ile <u>H</u> elp	
🖼 Certificates 🔀 Pending Signing Requests 🗹 Sign Request 🕹 Timestamping 🛱 Convert 🧶 OCSP/	P/SCEP 🔒 ACME
Issued to       Options         Name :       test kaplansoft.com         Alternatives (SANs) :	2048  sha-1withRSAEn  All  Local Machine  486f5fb96ccff7f6 Valid for day(s) : 1 Let's Encrypt
Browse Certificates (Local Machine \Personal)	
Search certificate All stores Q Certif Issuer Issu Not Before Not After Purpose	P.Key Key
Windows Live ID Token Issuer     TrustedPublisher     Go Go Da Go 1.09.2009 1.01.2038 All	on Yes 2048 No 2048
FlightRoot         FlightRoot           TrustedPeople         Go Da Go Da Kapl 29.04.2020         27.06.2021         Code Signing           ADDRESSBOOK         Kapl Sapl 31.01.2020         31.01.2020         31.01.2020         All	No 2048 Yes 2048 Yes 2048
Personal  Separt Card Poot	Yes 1024
Pending certificate signing request deleted.	🛛 🗕 🕇 🖄 📑 🛃

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 the test. Right click on the empty space on the right pane. Select New Domain.

New Host (A or AAAA) New Alias (CNAME) New Mail Exchanger (MX) New Domain		New DNS Domain	×
New Delegation Other New Records Refresh		Type the new DNS domain name:	
Export List View	>	OK Canc	əl
Arrange Icons Line up Icons	>		
Help			

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

Image: State of testEnter test as new DNS domain name and click OK. Double click on created sub domain.Image: State of testRight click on a empty space on right pane and click Other New Records.

Resource Record Type	×	New Resource Record	×
Select a resource record type:		Text(TXT)	
Renamed Mailbox (MR)	~	<u>R</u> ecord name (uses parent domain if left blank):	
Responsible Person (RP) Route Through (RT)		_acme-challenge	
Service Location (SRV)		Eully qualified domain name (FQDN):	
Text (TXT)	×	_acme-challenge.test.kaplansoft.com.	
		T <u>e</u> xt:	
Description: Text (TXT) record. Holds a string of characters that serves as descriptive text to be associated with a specific DNS domain name. The semantics of the actual descriptive text used as data with this record type depends on the DNS domain where these records are located. (RFC 1035)	*	MHjUzxwbgsUmeaNR3mFkLNUYUS48kzSb2lYpbWjulw4	
Create Record Cano	el	OK Cancel	

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 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. The certificate will be signed and copied to selected Windows certificate store if your configuration is correct.

🔒 TekCERT - X.509 Certificate / CSR Generator and Signing Tool (Registered [SP])				-		×		
<u>F</u> ile <u>H</u> elp								
🖼 Certificates 🔀 Pending Signing Requests 🔽	Sign Request	🕹 Timestampi	ing 👫 Convert	OCSP/SCE	P 🔒 ACN	1E		
Contact E-mail : sales@kaplansoft.com				🛃 Upda	ate Contact	💡 Update	e Account	t Key
Common Name	Algorithm	Key Size	Expire Date	Expire Time				
🔤 test.kaplansoft.com	SHA1	2048	14.06.2020	13:59				
	Challe	nge Type : DN	S-01 🗸 👪	Process Pending F	Request	X Delete	👩 Re	fresh
HTTP token file is saved to 'C:\Program Files (x86)'	\TekCERT\CgUK	PbzqhdPuleFp7	UEPjiUiYZHH6y	SV4AqsJedkw74'.	DNS challe	nge is copie	ed to the	clipb_;

Figure 4. - Pending ACME signing requests