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 <u>http://www.ipadresi.com/</u> You can also see your public IP address through TekCERT File / Get public IP address menu option.

TekCERT	х
Your public IP address is 176.43.62.191 (UPnP is enabled). Click OK to copy it to the clipboard.	
OK Cancel	

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.

AA) test Properties ? Host (A) Host (A) Host (uses parent domain if left blank): test test Eully qualified domain name (FQDN): test.kaplansoft.com IP address: 176.43.62.191 176.43.62.191				-	-
Host (A) Host (W) Hos	Host (A or AAAA)		test Properties	?	
Host (uses parent domain if left blank): test Eully qualified domain name (FQDN): test.kaplansoft.com IP address: 176.43.62.191 Update associated pointer (PTR) record	NAME)		Host (A)		
Eully qualified domain name (FQDN): Eully qualified domain name (FQDN): Est. Kaplansoft.com IP_address: I76.43.62.191 Update associated pointer (PTR) record	ger (MX)		Host (uses parent domain if left blank):		
Image: Construction of the second	5				-
IP address: [176.43.62.191 Update associated pointer (PTR) record	on.		test.kaplansoft.com		
IT6.43.62.191 Update associated pointer (PTR) record	a consta		I <u>P</u> address:		
	cords		176.43.62.191		
>			Update associated pointer (PTR) record		
> >					
>		>			
		>			
			OK Cancel	App	ply

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.

e <u>H</u> elp														
Certificates 🔀 Per	nding Signing Requ	iests 🗹	Sign Requ	lest 🚽	Timestam	oing 👫	Convert	🎯 ocs	P/SCEP	ACM	IE			
sued to							Options							
Name :	test.kaplansoft.com	m					Key	Length :	2048					
Alternatives (SANs) :							Algorithm I P	umose ·	sha-1with	RSAEn \				
Organization						=								
organization :						- 11	Certificat	e Store :	Local Ma	chine				
Unit :							5	Serial # :	486f5ft	96ccff7f	6 Val	id for d	ay(s):	
									_					
E-mail :	info@kaplansoft.c	om					Self	Signed :	Let's	Encrypt				
E-mail : City State :	info@kaplansoft.c	om	NY			-	Self	Signed :	Let's	Encrypt				
E-mail : City State :	Info@kaplansoft.c	:om	NY				Self Operation	Signed :	Let's	Encrypt				
E-mail: City State: Country:	Info@kaplansoft.c New York	:om	NY			~ [Self Operation	Signed :	enerate Ce	Encrypt	1	Genera	ite Requ	Jest
E-mail : City State : Country : owse Certificates (Loc	Info@kaplansoft.c New York United States al Machine \Person	al)	NY			~ [Self Operation *	Signed :	enerate Ce	Encrypt	1	Genera	te Requ	Jes
E-mail : City State : Country : rowse Certificates (Loc earch certificate	Info@kaplansoft.c New York United States al Machine \Person	al)	NY	lssu	Not Before	Not Afte	Self Operation Compensation Purpose	Signed :	enerate Ce	tificate Key		Genera	te Requ	Jest
E-mail : City State : Country : rowse Certificates (Loc sarch certificate Windows Live ID	info@kaplansoft.c New York ☑ United States al Machine\Person Ill stores ∨ ♀ Token Issuer	al)	NY Issuer Kapla	Issu Den	Not Before 27.04.2020	Not Afte 31.12.20	Self Operation Contempose Purpose Purpose Server A	Signed :	enerate Ce P.Key ion Yes	Encrypt tificate Key 2048		Genera	ite Requ	Jest
E-mail : City State : Country : rowse Certificates (Loc earch certificate A	Info@kaplansoft.c New York ☑ United States al Machine \Person VI stores ✓ Q Token Issuer	al)	NY Issuer Kapia Go Da	lssu Den Go	Not Before 27.04.2020 1.09.2009	Not Afte 31.12.20 1.01.203	Self Operation Contempose Purpose Purpose Server A Server A Server A	Signed :	enerate Ce P.Key ion Yes No	tificate Key 2048 2048		Genera	ite Requ	ues
E-mail : City State : Country : rowse Certificates (Loc earch certificate A Windows Live ID TrustedPublisher FlightRoot	Iinfo@kaplansoft.c New York ☑ United States al Machine\Person VI stores ✓ ☑ Token Issuer	al) Certif De Go Go	NY Issuer Kapla Go Da Go Da	lssu Den Go Go	Not Before 27.04.2020 1.09.2009 3.05.2011	Not Afte 31.12.20 1.01.203 3.05.203	Self Operation Comperation Reset Purpose Purpose Server A Sa All All All	Signed :	enerate Ce P.Key ion Yes No No	Encrypt tificate Key 2048 2048 2048		Genera	ite Requ	uest
E-mail : City State : Country : rowse Certificates (Loc earch certificate A 	linfo@kaplansoft.c New York ☑ United States al Machine\Person Il stores ✓ ☑ Token Issuer	al) Certif De Go Go Ka	NY Issuer Kapla Go Da Go Da Go Da	Issu Den Go Go Kapl	Not Before 27.04.2020 1.09.2009 3.05.2011 29.04.2020	Not Afte 31.12.20 1.01.203 3.05.203 27.06.20	Self Operation Contempose Purpose Purpose Server A Server	Signed :	enerate Ce P.Key ion Yes No No Yes	Encrypt tificate Key 2048 2048 2048 2048 2048		Genera	ite Requ	uest
E-mail : City State : Country : rowse Certificates (Loc earch certificates / A Windows Live ID TrustedPublisher FlightRoot TrustedPeople ADDRESSBOOK Local NonRemov	info@kaplansoft.c New York ☑ United States al Machine\Person Il stores ✓ ☑ Token Issuer	al) Certif Boom Certif Certif Certif Certif Certif Certif Certif	NY Issuer Kapia Go Da Go Da Go Da Kapia	Issu Den Go Go Kapl Kapl	Not Before 27.04.2020 1.09.2009 3.05.2011 29.04.2020 31.01.2020	Not Afte 31.12.20 1.01.203 3.05.203 27.06.20 31.12.20	Self Operation Contempose Purpose Purpose Server A Server	Signed :	enerate Ce P.Key ion Yes No Yes Yes	Encrypt tificate Key 2048 2048 2048 2048 2048 2048		Genera	ite Requ	uest
E-mail : City State : Country : rowse Certificates (Loc earch certificates (Loc earch certificate / A Windows Live ID TrustedPublisher FlightRoot TrustedPeople ADRESBOOK Local NonRemov Personal	info@kaplansoft.c New York ☑ United States al Machine\Person Il stores ✓ ☑ Token Issuer able Certificates	al) Certif Go Go Ka Ka	NY Issuer Kapla Go Da Go Da Kapla LENO	Issu Den Go Go Kapl LEN	Not Before 27.04.2020 1.09.2009 3.05.2011 29.04.2020 31.01.2020 21.04.2020	Not Afte 31.12.20 1.01.203 3.05.203 27.06.20 31.12.20 22.04.20	Self Operation Paration Purpose Purpose Purpose Server A Sa All All Code Sig D21 Code Sig D21 All Code Sig D21 All Code Sig D21 All Code Sig	Signed :	enerate Ce P.Key ion Yes No No Yes Yes Yes	Encrypt ttificate 2048 2048 2048 2048 2048 2048 2048 2048		Genera	ite Requ	ues
E-mail : City State : Country : rowse Certificates (Loc earch certificates (Loc earch certificate A Windows Live ID 	info@kaplansoft.c New York ☑ United States al Machine\Person IJ stores ✓ ☑ Token Issuer able Certificates	al) Certif Go Go Ka Ka Ka	NY Issuer Kapla Go Da Go Da Go Da Kapla LENO	Issu Den Go Go Kapl LEN	Not Before 27.04.2020 1.09.2009 3.05.2011 29.04.2020 31.01.2020 21.04.2020 12.01.2020	Not Afte 31.12.20 1.01.203 3.05.203 27.06.20 31.12.20 21.4.20	Self Operation ** Purpose 201 Server A 38 All 31 All 31 All 201 Code Sig 201 All 202 All	Signed :	P.Key ion Yes No Yes Yes Yes	Encrypt ttificate 2048 2048 2048 2048 2048 2048 2048		Genera	te Requ	nea

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.

🔒 TekCERT - X.509 Certificate / CSR Generator a	nd Signing Tool	(Registered [SP])			_		×
<u>F</u> ile <u>H</u> elp								
🖼 Certificates 🔀 Pending Signing Requests 🛛	Sign Request	🕹 Timestamp	ing 👫 Convert	OCSP/SCE	ip 🔒 ACN	4E		
Contact E-mail : sales@kaplansoft.com				👩 Upda	ate Contact	💡 Updat	e Accoun	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	🗙 Delete	👩 Re	fresh
HTTP token file is saved to 'C:\Program Files (x86)	\TekCERT\CgUK	PbzqhdPuleFp7	7UEPjiUiYZHH6y	SV4AqsJedkw74'.	DNS challe	nge is copi	ed to the	clipb.;

Figure 4. - Pending ACME signing requests