



13th April 2021

SSL Certificates with Sectigo/ACME

DIAS

Institiúid Ard-Léinn | Dublin Institute for
Bhaile Átha Cliath | Advanced Studies

Jef Bucas
System Administrator
@itdiasie

DIAS

Institiúid Ard-Léinn | Dublin Institute for
Bhaile Átha Cliath | Advanced Studies

DIAS

Institiúid Ard-Léinn | Dublin Institute for
Bhaile Átha Cliath | Advanced Studies

= 100 SSL Certificates

DIAS

Institiúid Ard-Léinn | Dublin Institute for
Bhaile Átha Cliath | Advanced Studies

= 100 SSL Certificates

managed
manually

DIAS

Institiúid Ard-Léinn | Dublin Institute for
Bhaile Átha Cliath | Advanced Studies



= 100 SSL Certificates

managed manually

=



... when one morning in April 2020 ...

Subject [HEAnet #1730720] Access to SSL Certificate Service
From Eamonn Geoghegan via RT 
Reply-To noc@heanet.ie 
Date 2020-04-08 10:16

Hello,

HEAnet is writing to you as you have an Administrator account on our SSL Certificate Service [TCS], provided by Digicert. As the contract with Digicert is ending, a tender process to renew this service has been completed and in the new provider going forward is Sectigo.

The change over date is the 30th of April. You can still order SSL certificates with Digicert until this date. After this date you will no longer be able to order new certificates, but you will still have access to your account to manage and/or revoke existing certificates. Your account will remain available for the remainder of the life of any certificates in your account.

Over the next few weeks we will be on-boarding client administrators to the new Sectigo site, who will then manage users and certificates for their institution.

Kind regards,

Enters :

SECTIGO

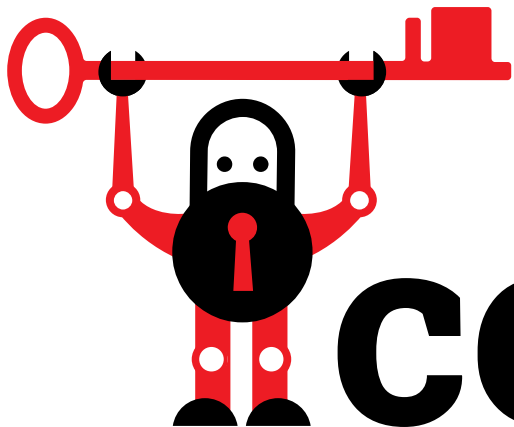
ACME protocol support



Automated Certificate Management Environment (ACME) Explained



Let's Encrypt

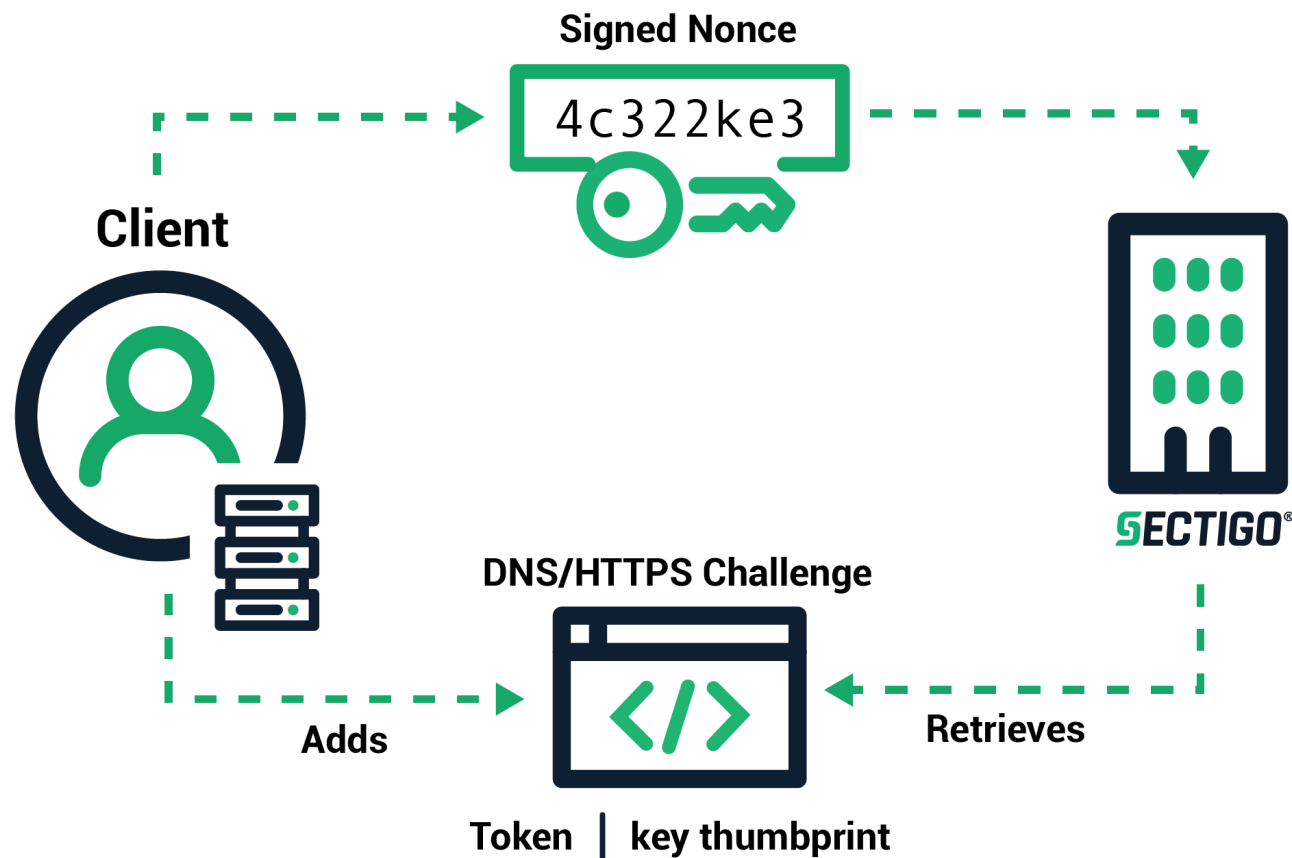


certbot

E ELECTRONIC
FRONTIER
FOUNDATION **FF**

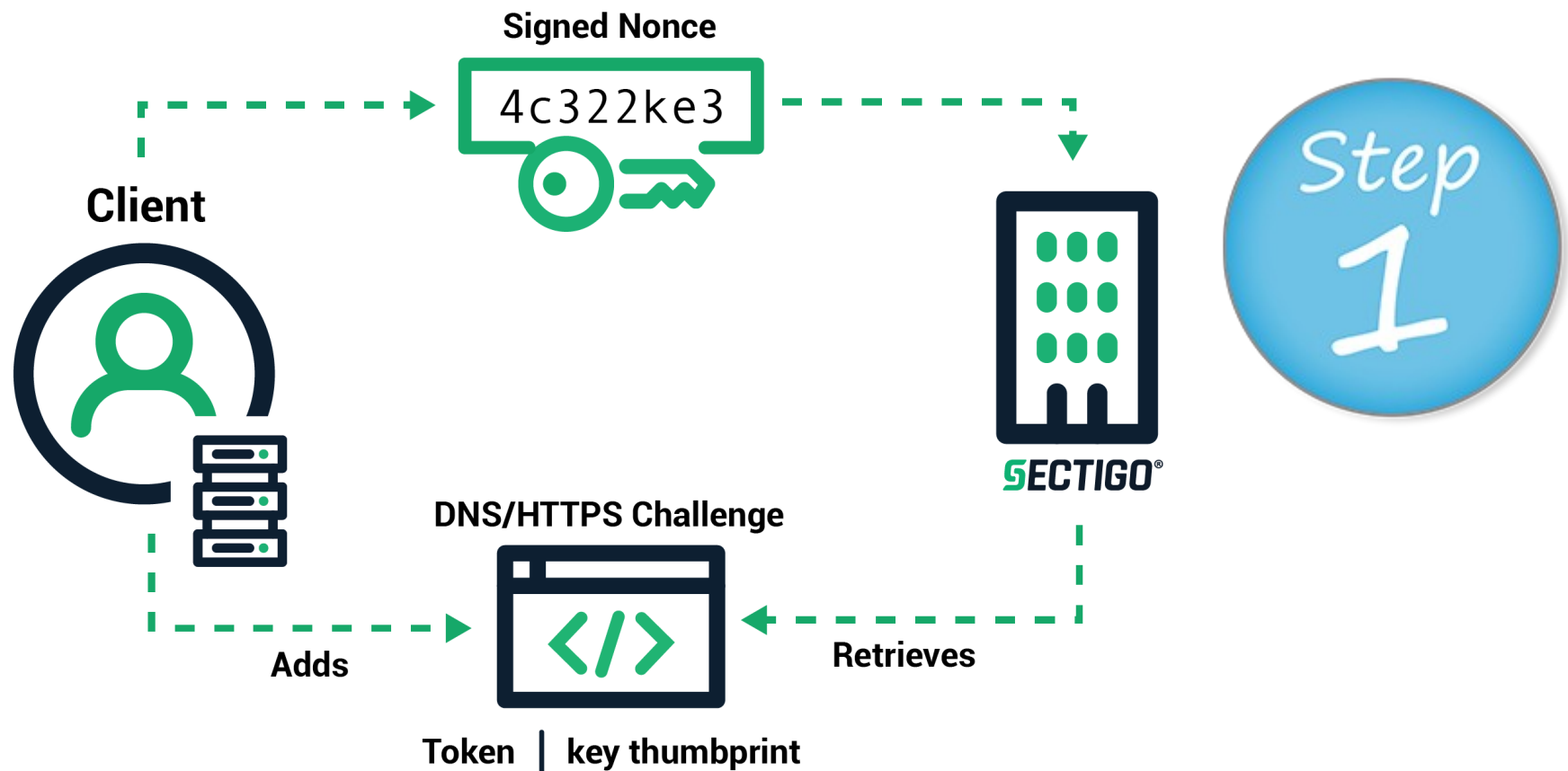
Automated Certificate Management Environment (ACME) Explained

How the ACME protocol works for automated PKI certificate management



Automated Certificate Management Environment (ACME) Explained

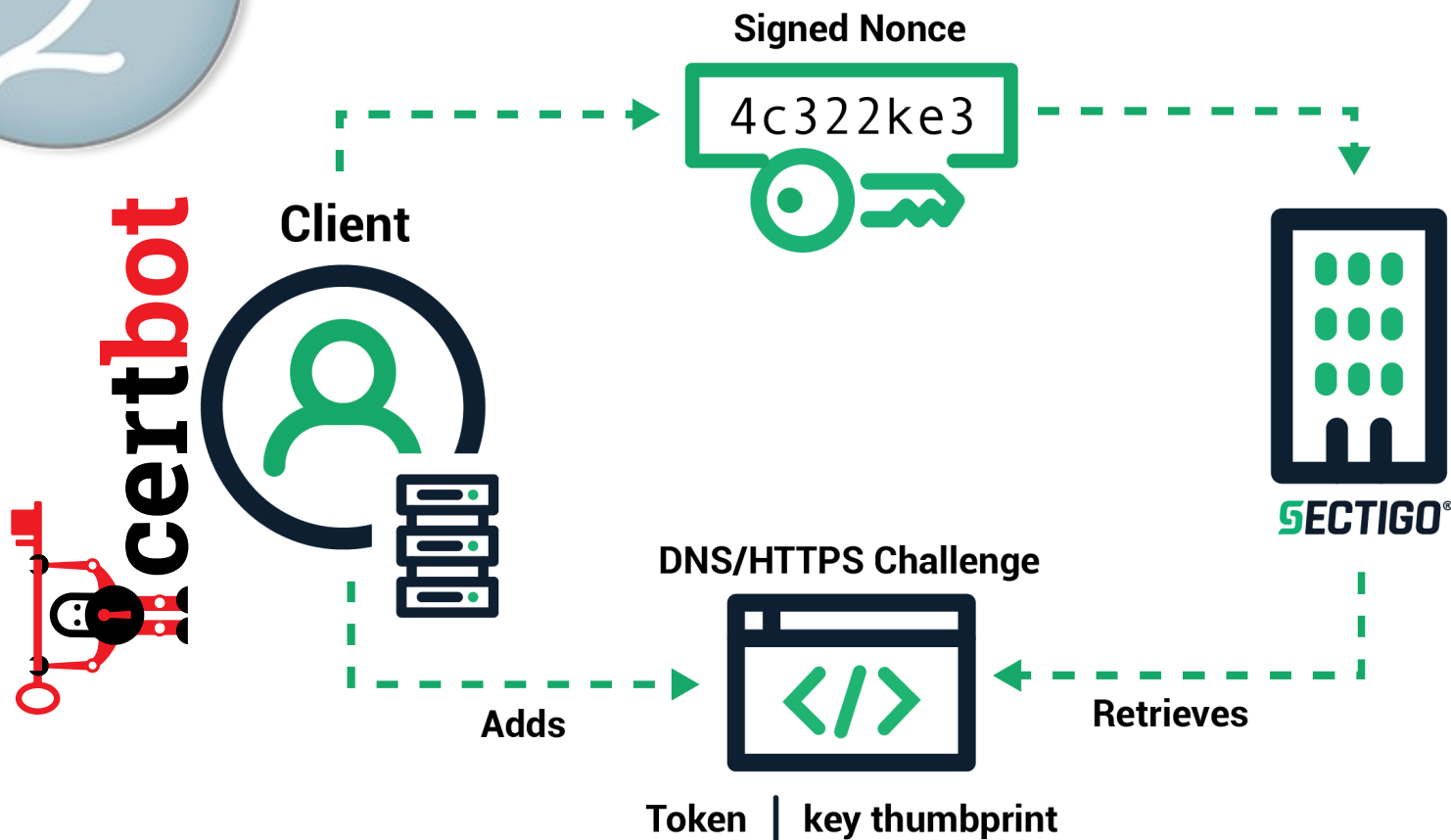
How the ACME protocol works for automated PKI certificate management



Automated Certificate Management Environment (ACME) Explained

Step
2

How the ACME protocol works for automated PKI certificate management

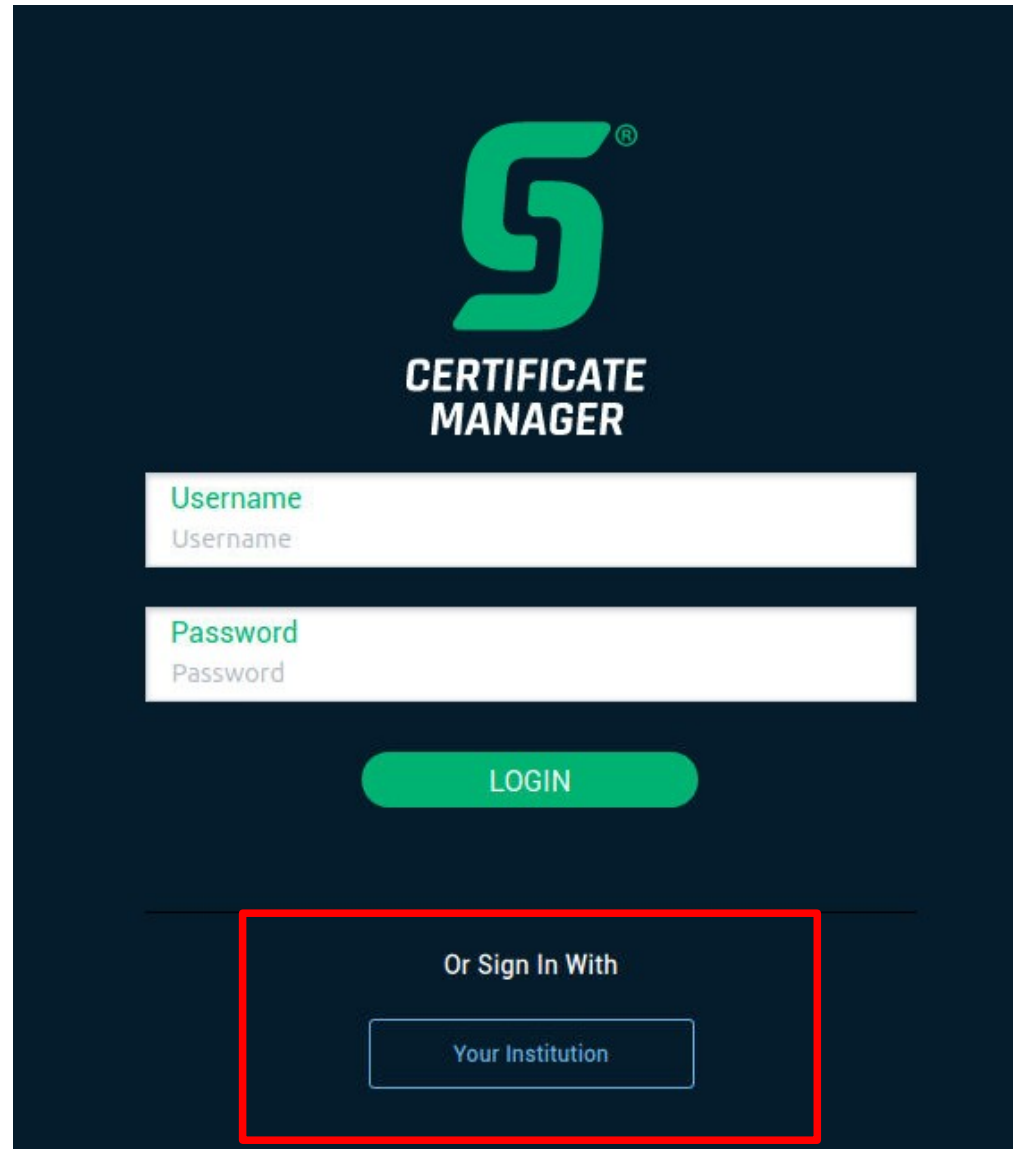




Configure

SECTIGO

<https://cert-manager.com/customer/HEAnet>



The image shows a login page for 'CERTIFICATE MANAGER'. At the top center is a green logo consisting of a stylized 'S' with a registered trademark symbol. Below the logo, the text 'CERTIFICATE MANAGER' is displayed in white, uppercase letters. There are two white input fields: the first is labeled 'Username' in green text with 'Username' in grey text below it; the second is labeled 'Password' in green text with 'Password' in grey text below it. Below these fields is a green rounded rectangular button with the text 'LOGIN' in white. At the bottom, there is a dark blue box with a red border containing the text 'Or Sign In With' and a white rounded rectangular button with the text 'Your Institution' in blue.

 Filter



Name	City	State	Country	Validation Status	Secondary Validation Sta
<input type="radio"/> Dublin Institute for Advanced Studies	Dublin	Leinster	IE	Validated	Not Validated

 Filter





Name	URL	Type
<input type="radio"/> https://acme.sectigo.com/v2/EV	https://acme.sectigo.com/v2/EV	Public ACME
<input type="radio"/> https://acme.sectigo.com/v2/OV	https://acme.sectigo.com/v2/OV	Public ACME





ADMIN SETTINGS ABOUT

ACME Accounts

Filter

 **Add** 

Name	Organization	Department	Validation Type	Status
<input type="radio"/> all	Dublin Institute for Advanced Studies		OV	valid

12 rows/page 1 - 1 out of 1    

[Close](#)

Create ACME Account



Name*

Organization*

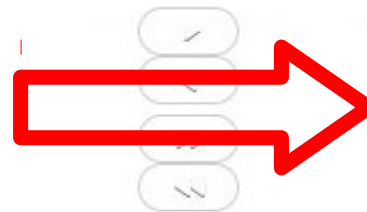
Department

Validation Type OV

DOMAINS

Available domains:

Assigned domains:



Cancel

OK

Step
1

Name

Organization

Department

Status

Account ID

ACME Account details: All



EXTERNAL ACCOUNT BINDING

ACME URL

Account ID

Key ID

HMAC Key

Ctrl-C

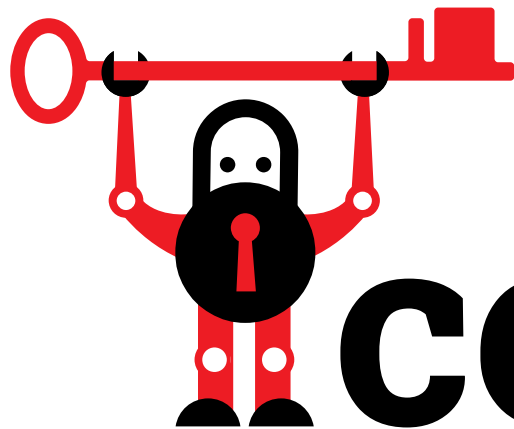
Instructions on how to use
account

```
When ACME client (certbot) is initialized, we specify  
ACME URL (--server), MAC Key (--eab-hmac-key), Mac ID  
(--eab-kid).
```

Close

Step
1

Step
2



certbot

```
1 #!/bin/bash
2
3 HOST="https://acme.sectigo.com/v2/0V"
4 KeyID=""
5 HMACKey=""
6
7 # From https://certbot.eff.org/docs/using.html#hooks
8 certbot certonly \
9     --manual \
10    -n \
11    --agree-tos --email \
12    --preferred-challenges=dns \
13    --manual-public-ip-logging-ok \
14    --manual-auth-hook defineDNS.sh \
15    --manual-cleanup-hook undefineDNS.sh \
16    --expand \
17    --force-renewal \
18    --server "$HOST" \
19    --eab-kid "$KeyID" \
20    --eab-hmac-key "$HMACKey" \
21    $FQDN $ALTNAME1 $ALTNAME2 $ALTNAME3 $ALTNAME4
22
23 # Deploy
24 ./deployCerts.sh $FQDN
25
```

```
1 #!/bin/bash
2
3 HOST="https://acme.sectigo.com/v2/0V"
4 KeyID=""
5 HMACKey=""
6
7 # From https://certbot.eff.org/docs/using.html#hooks
8 certbot certonly \
9     --manual \
10    -n \
11    --agree-tos --email \
12    --preferred-challenges=dns \
13    --manual-public-ip-logging-ok \
14    --manual-auth-hook defineDNS.sh \
15    --manual-cleanup-hook undefineDNS.sh \
16    --expand \
17    --force-renewal \
18    --server "$HOST" \
19    --eab-kid "$KeyID" \
20    --eab-hmac-key "$HMACKey" \
21    $FQDN $ALTNAME1 $ALTNAME2 $ALTNAME3 $ALTNAME4
22
23 # Deploy
24 ./deployCerts.sh $FQDN
25
```

Ctrl-V

```
1 #!/bin/bash
2
3 HOST="https://acme.sectigo.com/v2/0V"
4 KeyID=""
5 HMACKey=""
6
7 # From https://certbot.eff.org/docs/using.html#hooks
8 certbot certonly \
9     --manual \
10    -n \
11    --agree-tos --email \
12    --preferred-challenges=dns \
13    --manual-public-ip-logging-ok \
14    --manual-auth-hook defineDNS.sh \
15    --manual-cleanup-hook undefineDNS.sh \
16    --expand \
17    --force-renewal \
18    --server "$HOST" \
19    --eab-kid "$KeyID" \
20    --eab-hmac-key "$HMACKey" \
21    $FQDN $ALTNAME1 $ALTNAME2 $ALTNAME3 $ALTNAME4
22
23 # Deploy
24 ./deployCerts.sh $FQDN
25
```

```
1 #!/bin/bash
2
3 HOST="https://acme.sectigo.com/v2/0V"
4 KeyID=""
5 HMACKey=""
6
7 # From https://certbot.eff.org/docs/using.html#hooks
8 certbot certonly \
9     --manual \
10    -n \
11    --agree-tos --email \
12    --preferred-challenges=dns \
13    --manual-public-ip-logging-ok \
14    --manual-auth-hook defineDNS.sh \
15    --manual-cleanup-hook undefineDNS.sh \
16    --expand \
17    --force-renewal \
18    --server "$HOST" \
19    --eab-kid "$KeyID" \
20    --eab-hmac-key "$HMACKey" \
21    $FQDN $ALTNAME1 $ALTNAME2 $ALTNAME3 $ALTNAME4
22
23 # Deploy
24 ./deployCerts.sh $FQDN
25
```

```
1 #!/bin/bash
2
3 HOST="https://acme.sectigo.com/v2/0V"
4 KeyID=""
5 HMACKey=""
6
7 # From https://certbot.eff.org/docs/using.html#hooks
8 certbot certonly \
9     --manual \
10    -n \
11    --agree-tos --email \
12    --preferred-challenges=dns \
13    --manual-public-ip-logging-ok \
14    --manual-auth-hook defineDNS.sh \
15    --manual-cleanup-hook undefineDNS.sh \
16    --expand \
17    --force-renewal \
18    --server "$HOST" \
19    --eab-kid "$KeyID" \
20    --eab-hmac-key "$HMACKey" \
21    $FQDN $ALTNAME1 $ALTNAME2 $ALTNAME3 $ALTNAME4
22
23 # Deploy
24 ./deployCerts.sh $FQDN
25
```



```
1 #!/bin/bash
2
3 HOST="https://acme.sectigo.com/v2/0V"
4 KeyID=""
5 HMACKey=""
6
7 # From https://certbot.eff.org/docs/using.html#hooks
8 certbot certonly \
9     --manual \
10    -n \
11    --agree-tos --email \
12    --preferred-challenges=dns \
13    --manual-public-ip-logging-ok \
14    --manual-auth-hook defineDNS.sh \
15    --manual-cleanup-hook undefineDNS.sh \
16    --expand \
17    --force-renewal \
18    --server "$HOST" \
19    --eab-kid "$KeyID" \
20    --eab-hmac-key "$HMACKey" \
21    $FQDN $ALTNAME1 $ALTNAME2 $ALTNAME3 $ALTNAME4
22
23 # Deploy
24 ./deployCerts.sh $FQDN
25
```

DefineDNS.sh [hook script]

- `CERTBOT_DOMAIN`: The domain being authenticated
- `CERTBOT_VALIDATION`: The validation string
- `CERTBOT_TOKEN`: Resource name part of the HTTP-01 challenge (HTTP-01 only)
- `CERTBOT_REMAINING_CHALLENGES`: Number of challenges remaining after the current challenge
- `CERTBOT_ALL_DOMAINS`: A comma-separated list of all domains challenged for the current certificate

<https://certbot.eff.org/docs/using.html#hooks>

```
1 #!/bin/bash
2
3 TAGSTR="; Certificate for CERTBOT"
4 DNS="mydns.dias.ie"
5 FOLDER="/etc/bind/"
6
7 # [...] --> part where we find which $DNSFILE config file to modify
8
9 # Remove possible old definition line
10 ssh -x $DNS "cd $FOLDER; sed -i '/^_acme-challenge\.${CERTBOT_DOMAIN}\.* $TAGSTR$/d' '$DNSFILE'"
11
12 # Add new line
13 ssh -x $DNS "cd $FOLDER; echo '_acme-challenge.${CERTBOT_DOMAIN}. IN TXT \"${CERTBOT_VALIDATION}\" $TAGSTR' >> '$DNSFILE'"
14
15 # Reload config
16 ssh -x $DNS "cd $FOLDER; rndc reload"
17
```

DefineDNS.sh [hook script]

- `CERTBOT_DOMAIN`: The domain being authenticated
- `CERTBOT_VALIDATION`: The validation string
- `CERTBOT_TOKEN`: Resource name part of the HTTP-01 challenge (HTTP-01 only)
- `CERTBOT_REMAINING_CHALLENGES`: Number of challenges remaining after the current challenge
- `CERTBOT_ALL_DOMAINS`: A comma-separated list of all domains challenged for the current certificate

<https://certbot.eff.org/docs/using.html#hooks>

```
1 #!/bin/bash
2
3 TAGSTR="; Certificate for CERTBOT"
4 DNS="mydns.dias.ie"
5 FOLDER="/etc/bind/"
6
7 # [...] --> part where we find which $DNSFILE config file to modify
8
9 # Remove possible old definition line
10 ssh -x $DNS "cd $FOLDER; sed -i '/^_acme-challenge\.CERTBOT_DOMAIN\.* $TAGSTR$/d' '$DNSFILE'"
11
12 # Add new line
13 ssh -x $DNS "cd $FOLDER; echo '_acme-challenge.CERTBOT_DOMAIN. IN TXT \"$CERTBOT_VALIDATION\" $TAGSTR' >> '$DNSFILE'"
14
15 # Reload config
16 ssh -x $DNS "cd $FOLDER; rndc reload"
17
```

```
_acme-challenge.dias.ie. IN TXT " ; Certificate for CERTBOT
```

DefineDNS.sh [hook script]

- `CERTBOT_DOMAIN`: The domain being authenticated
- `CERTBOT_VALIDATION`: The validation string
- `CERTBOT_TOKEN`: Resource name part of the HTTP-01 challenge (HTTP-01 only)
- `CERTBOT_REMAINING_CHALLENGES`: Number of challenges remaining after the current challenge
- `CERTBOT_ALL_DOMAINS`: A comma-separated list of all domains challenged for the current certificate

<https://certbot.eff.org/docs/using.html#hooks>

```
1 #!/bin/bash
2
3 TAGSTR="; Certificate for CERTBOT"
4 DNS="mydns.dias.ie"
5 FOLDER="/etc/bind/"
6
7 # [...] --> part where we find which $DNSFILE config file to modify
8
9 # Remove possible old definition line
10 ssh -x $DNS "cd $FOLDER; sed -i '/^_acme-challenge\.$CERTBOT_DOMAIN\.* $TAGSTR$/d' '$DNSFILE'"
11
12 # Add new line
13 ssh -x $DNS "cd $FOLDER; echo '_acme-challenge.$CERTBOT_DOMAIN. IN TXT \"$CERTBOT_VALIDATION\" $TAGSTR' >> '$DNSFILE'"
14
15 # Reload config
16 ssh -x $DNS "cd $FOLDER; rndc reload"
17
```

```
_acme-challenge.dias.ie. IN TXT " "; Certificate for CERTBOT
```



Deploy.sh

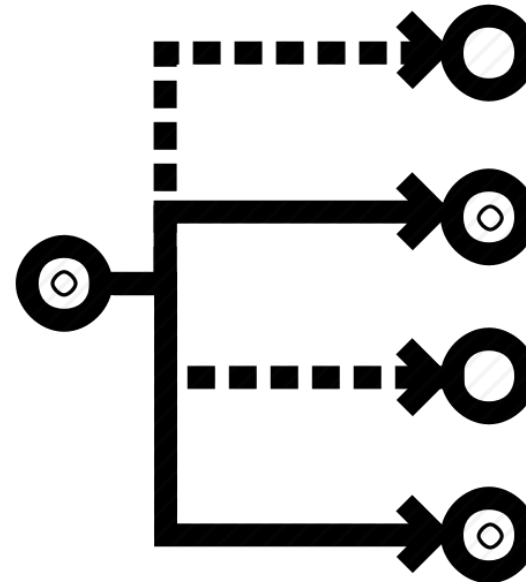
From:

/etc/letsencrypt/live/**\$FQDN**/*.{key,crt}



To:

- Apache
- Postfix
- LDAP
- Unify
- GitLab
- ...



Reload Daemon

```
# ./run.sh demo-heanet-conf-2020.dias.ie
```

“Live” pre-recorded demo, within the pre-recorded presentation



Why not just use Let's Encrypt?

Yes, you can

ACME Sectigo certificates can last up to 1 year

Auto-renew?

Definitely possible. Planned.



Why DNS rather than HTTP challenge?

Not blocked by Firewall for internal websites

Does it have to be shell script?

ACME supports all major languages.



Big thanks to

SECTIGO

GÉANT

