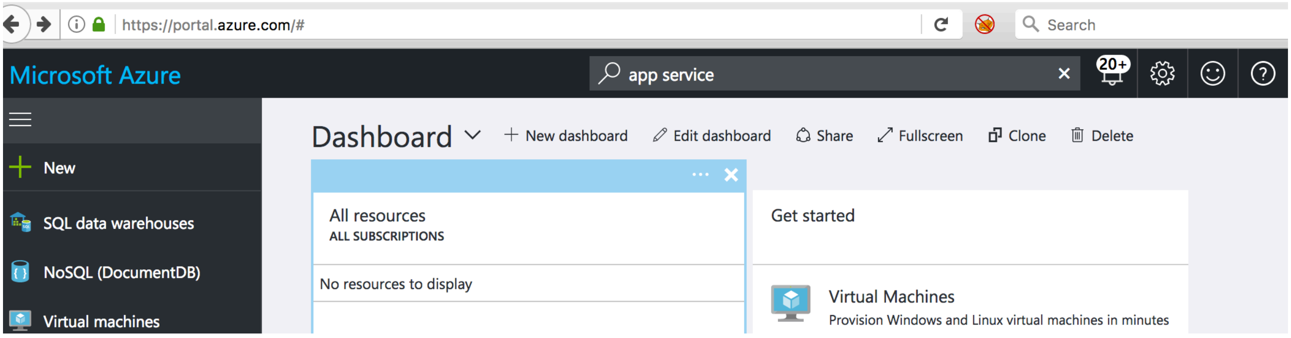
Creating a secure website using Let´s Encrypt: step-by-step

Creating a secure https website can be tricky, but once the site is set up correctly it´s security will increase dramatically. This tutorial will take you through the steps required to do this. The tools we will be using to create a secure website, Let´s Encrypt and Azure, are a hassle to use but the results are awesome and this tutorial will walk you through it step-by-step. Note that this process is only needed once, since after your website is setup with a Let´s Encrypt certificate the process of renewal will happen automatically.

Before you begin you will need:

- Microsoft Azure account
- Own a domain (if you don´t own one, you can always buy one on Azure)

When you logon to your Azure account, https://portal.azure.com you will be presented with the wonders of the Microsoft Azure Dashboard which is crammed with lots of stuff, but not the easiest site to navigate. Your way out of it is the “Search” box - trust me on this!

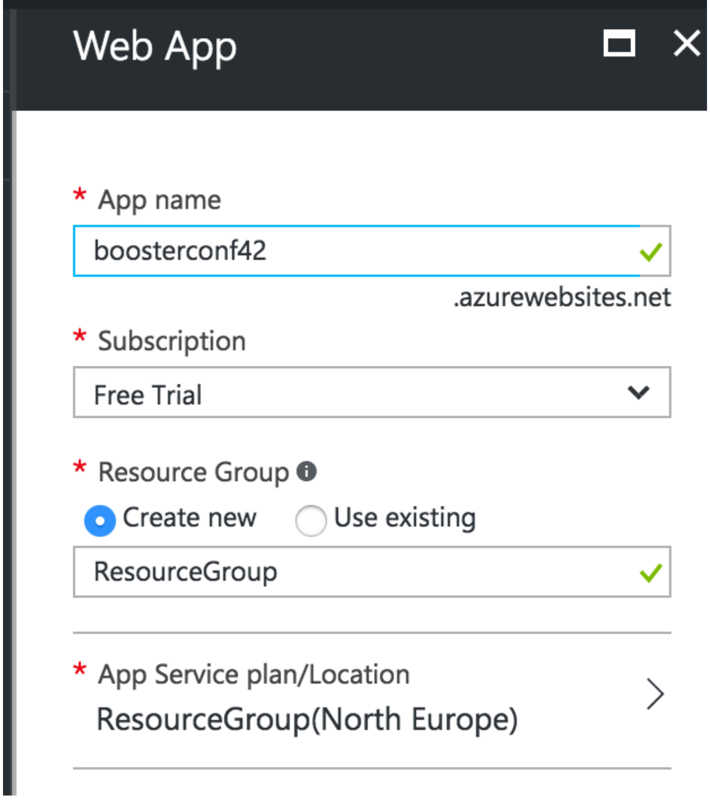


In this tutorial you will need to install a extension called “Lets Encrypt Extension”. In order to setup it up you will need a lot of information from different resources in your Azure portal. To avoid constantly going backwards and forwards in the wonders of Azure portal, I recommend that you have a text editor open so whenever this information is available you can copy and paste it so that you can find it easily when you need it in the final step of the tutorial. Whenever information needs to be copied it will be mentioned in the steps below.

Creating an Azure App Service

To create a web site, search for “App Services”, select it and then click “Add”. There are several web app templates to choose from. For this tutorial I chose the simplest one, which is called “Web App”. After selecting “Web App” click on “Create”.

Choose the name for your webpage. In this example we choose “boosterconf42”. In this example a Free Trial subscription is being used. In order to have the location setup correct chose “Create New” Resource Group.



Web App

* App name

boosterconf42 ✓

.azurewebsites.net

* Subscription

Free Trial

* Resource Group

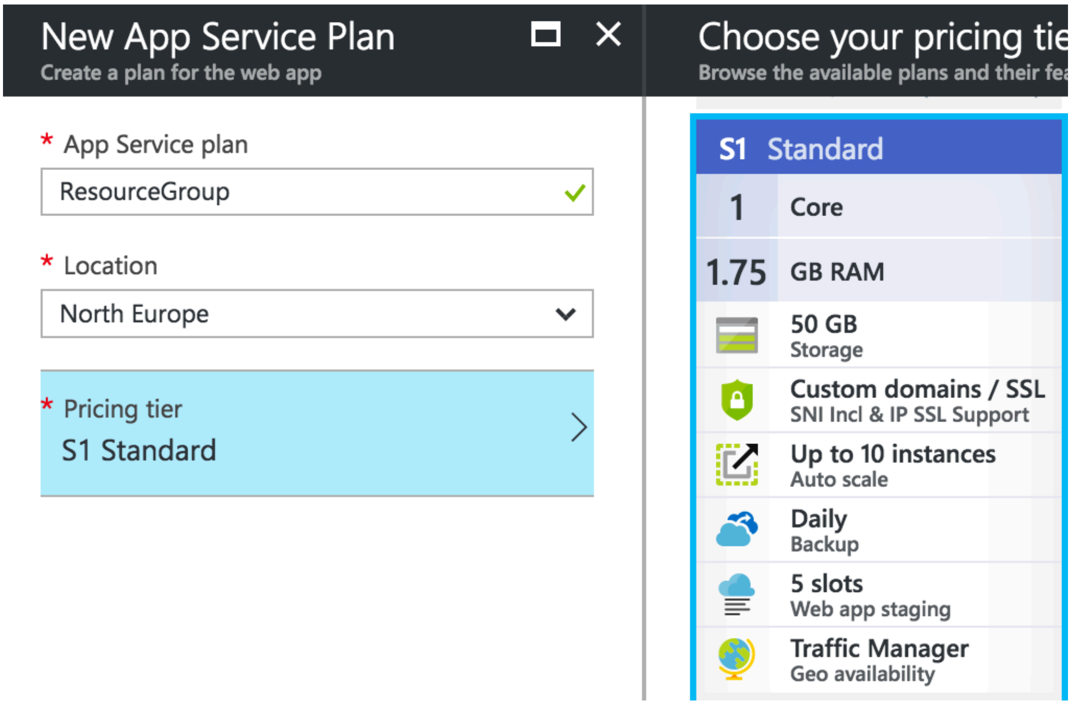
● Create new ○ Use existing

ResourceGroup ✓

* App Service plan/Location

ResourceGroup(North Europe)

Select “App Service Plan” and then “Create New”. It is important to check that your “Pricing tier” has “Custom domains/SSL” included. Sites created on Azure are setup by default with a Microsoft “*.azurewebsite.net” SSL certificate which cannot be changed. This would restrict you to hosting sites at azurewebsite.net, rather than on your preferred domain. For this example I am choosing “S1 Standard”. Our “boosterconf42” website will be registered with a Custom Domain and that custom domain will need a SSL certificate. I recommend that you choose the name of your “App Service plan” to be equal to the name of your “Resource Group”. The Let´s Encrypt Extension used here seems to have a bug and only works when these names are the same. In this example both are named “ResouceGroup”.



New App Service Plan

Create a plan for the web app

* App Service plan

ResourceGroup ✓

* Location

North Europe

* Pricing tier

S1 Standard

Choose your pricing tie

Browse the available plans and their fea

S1 Standard

1 Core

1.75 GB RAM

50 GB Storage

Custom domains / SSL SNI Incl & IP SSL Support

Up to 10 instances Auto scale

Daily Backup

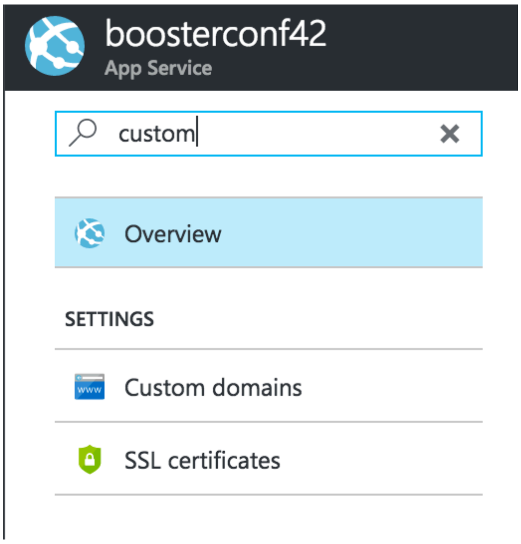
5 slots Web app staging

Traffic Manager Geo availability

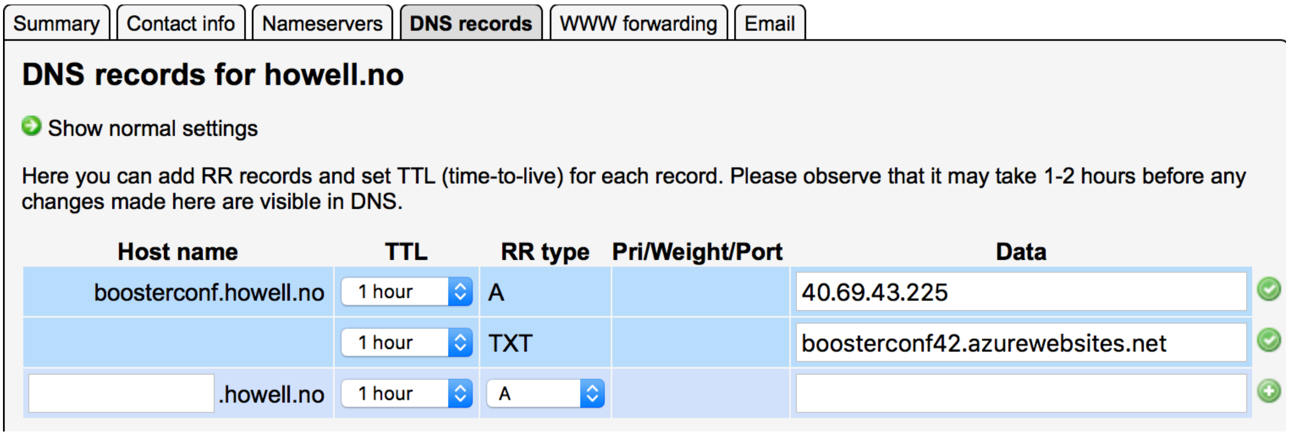
After the registration is finished click on the newly created application and then overview. There you will find your “Subscription ID”. This value is later needed when setting up your Let´s Encrypt Extension.

Registering a Custom Domain

In a different search box, the one for your app service, search for Custom Domain and then select it. The following steps are needed in order to prove that the domain you are registering is really yours.



Take note of your “External IP Address” (no - for some reason you cannot simply copy your IP address, you need to type it). The IP address is needed when registering our DNS record. In this example a domain from https://domainnameshop.com is used. In the domainnameshop portal, register RR Type “A” with your IP address and RR type “TXT”, with your application name at .azurewebsite.net (see the figure below).



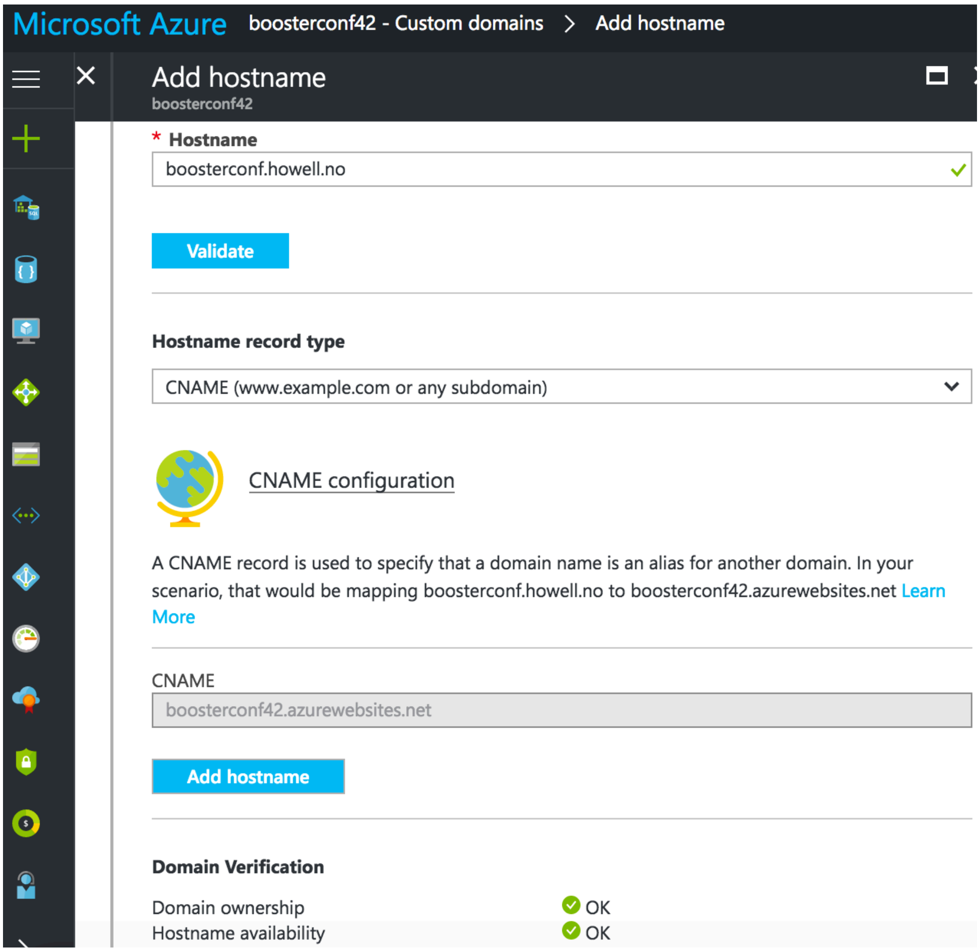
DNS records for howell.no

Show normal settings

Here you can add RR records and set TTL (time-to-live) for each record. Please observe that it may take 1-2 hours before any changes made here are visible in DNS.

Host name	TTL	RR type	Pri/Weight/Port	Data
boosterconf.howell.no	1 hour	A		40.69.43.225
	1 hour	TXT		boosterconf42.azurewebsites.net
.howell.no	1 hour	A		

After your DNS records are updated with your Azure website details, you can click on “Add hostname” and then click on “Validate”. Decrease TTL if you don´t want to wait too long for the changes to be available. The minimum TTL available on domainnameshop is 5 min. After you



Microsoft Azure boosterconf42 - Custom domains > Add hostname

Add hostname
boosterconf42

* Hostname
boosterconf.howell.no ✓

Validate

Hostname record type
CNAME (www.example.com or any subdomain)

CNAME configuration

A CNAME record is used to specify that a domain name is an alias for another domain. In your scenario, that would be mapping boosterconf.howell.no to boosterconf42.azurewebsites.net Learn More

CNAME
boosterconf42.azurewebsites.net

Add hostname

Domain Verification

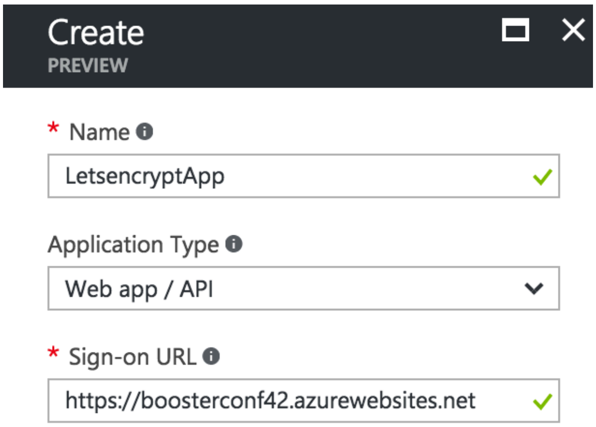
Domain ownership ✓ OK
Hostname availability ✓ OK

finished with your DNS registration, go back to Azure and click “Validate”. If domain verifications are OK then click on “Add hostname”.

Setting up an Azure Active Directory Application to be able to renew a Let´s Encrypt certificate

In your Azure dashboard find a link to “Azure Active Directory”. Do I need to mention that the easiest way to find this is to search it for it? Most accounts already come with a built in Azure AD. If yours doesn´t, you can simply create one. After selecting Azure Active Directory click “Domain names”. Take a note of your “Domain name”, this information is required later when setting up your Let´s Encrypt Extension. Your domain name is most likely something like your email address without the @, for example: usernamegmail.onmicrosoft.com.

Now choose the menu option “App Registrations” and then “Add”.



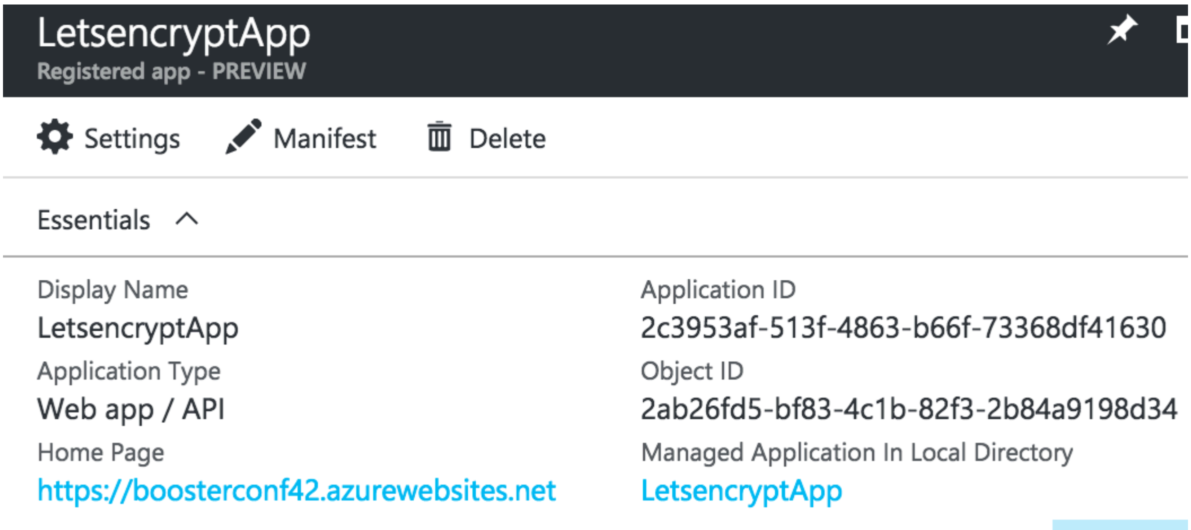
Create
PREVIEW

* Name
LetsencryptApp ✓

Application Type
Web app / API

* Sign-on URL
https://boosterconf42.azurewebsites.net ✓

Now select the newly created app registration. Take note of the “Application ID”. As always, this will be needed later on when setting up the Let´s Encrypt Extension.



Display Name
LetsencryptApp

Application Type
Web app / API

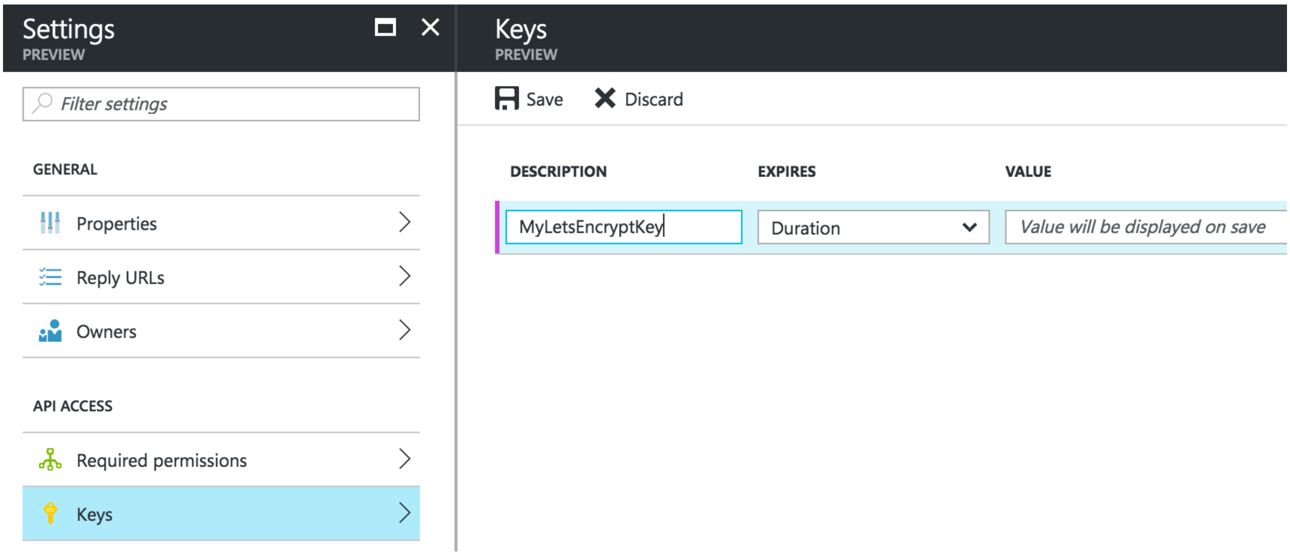
Home Page
https://boosterconf42.azurewebsites.net

Application ID
2c3953af-513f-4863-b66f-73368df41630

Object ID
2ab26fd5-bf83-4c1b-82f3-2b84a9198d34

Managed Application In Local Directory
LetsencryptApp

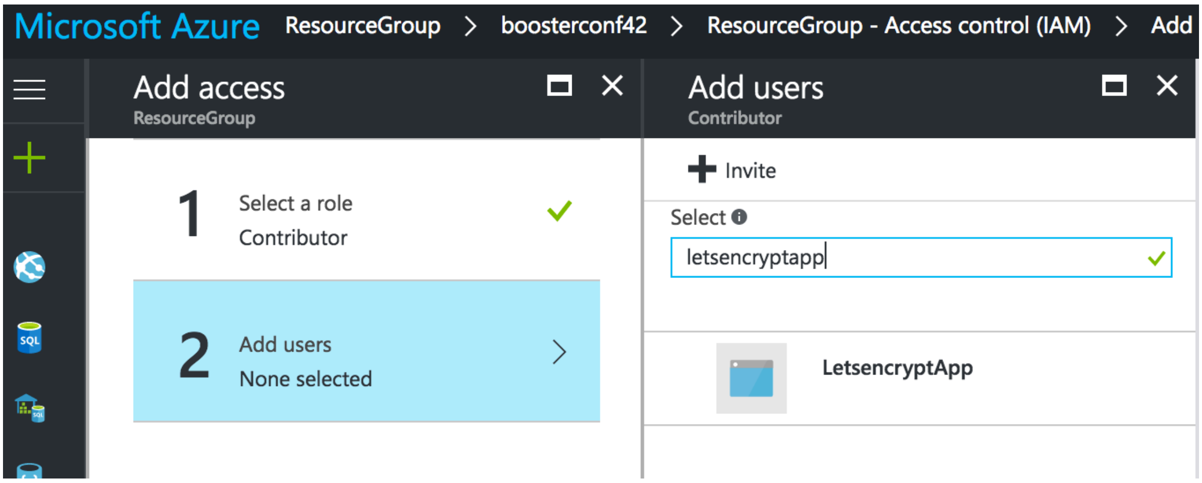
At the lower left, you will find a menu “Keys”. Select it and then create a new key. This key will be used by Let´s Encrypt Extension further in this tutorial. Choose a duration, in this example I chose “never expires”. The key value, as the dashboard says, will appear after you click on the “Save” button. Please take a copy of the key. This key is only visible once and it will be needed later on. Note that If you miss your chance to copy the key after you will be able to create a new one later.



DESCRIPTION	EXPIRES	VALUE
MyLetsEncryptKey	Duration	Value will be displayed on save

Giving the Azure AD app access to your Resource Group

Now, let´s go back to our app service and find our resource group. There are many ways to get there. One way is to select your app service, in this example it is called “boosterconf42”, and then “Overview”. There you will find a link to your resource group. Click on it and select “Access control IAM”. There you will see a button “Add”, select it and choose the role “Contributor”. Enter the name of the application registered on Azure AD. In this case it was named “LetsEncryptApp”.


Microsoft Azure
ResourceGroup > boosterconf42 > ResourceGroup - Access control (IAM) > Add
Add access
ResourceGroup
Add users
Contributor
Invite

1 Select a role: Contributor ✓

2 Add users: None selected

Select: letsencryptapp ✓

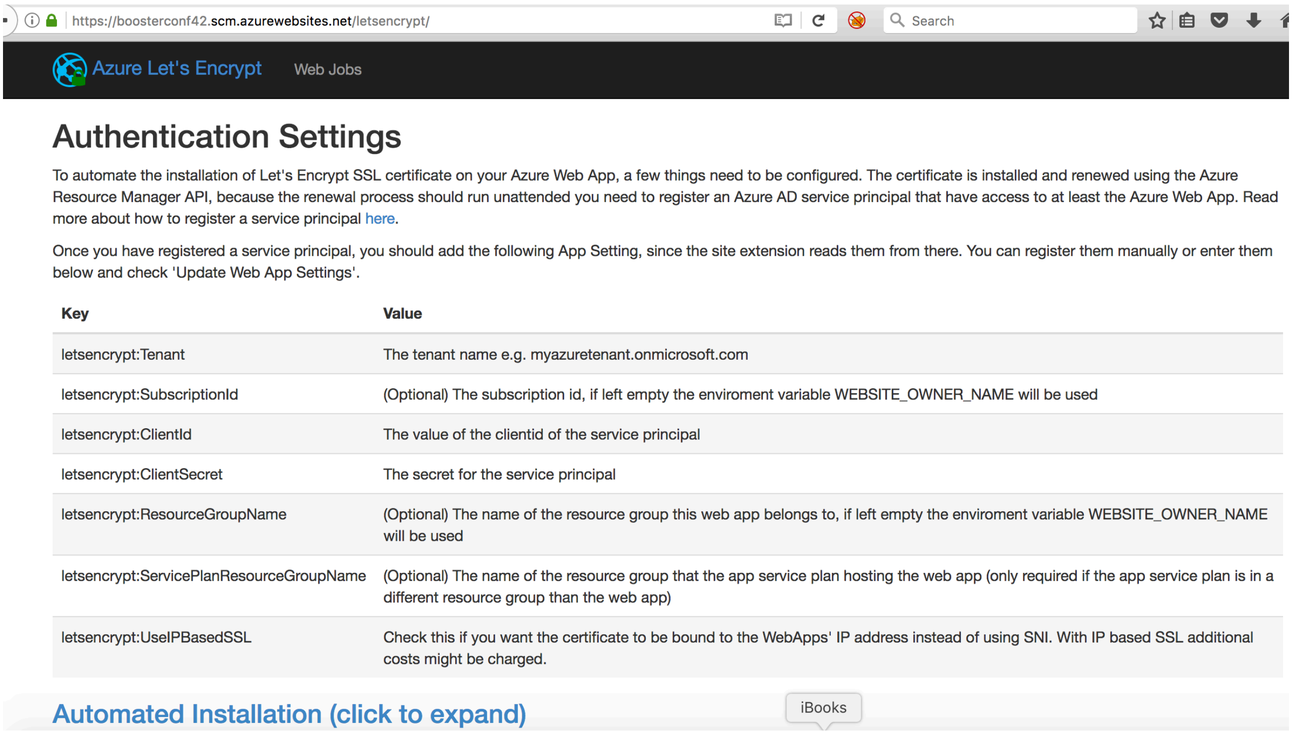
LetsencryptApp

Installing the Let´s Encrypt Extension

Select your app service and then search for “Extension”. Select it and then click on “Add extension”. Choose “Azure Let´s Encrypt (x86)” if you are using 32-bits or “Azure Let´s Encrypt (x64)” if you are using 64-bits. In this example x86 is chosen. Note that is possible to change your Resource Group to either 32-bits or 64-bits later if necessary.

After the extension is installed, select it and then click on the “Browse” option that is well hidden in the top left hand corner.

The “Browse” button will take you in the site below with lots of information. Remember all those IDs and names that you took note along the way? They are needed now.



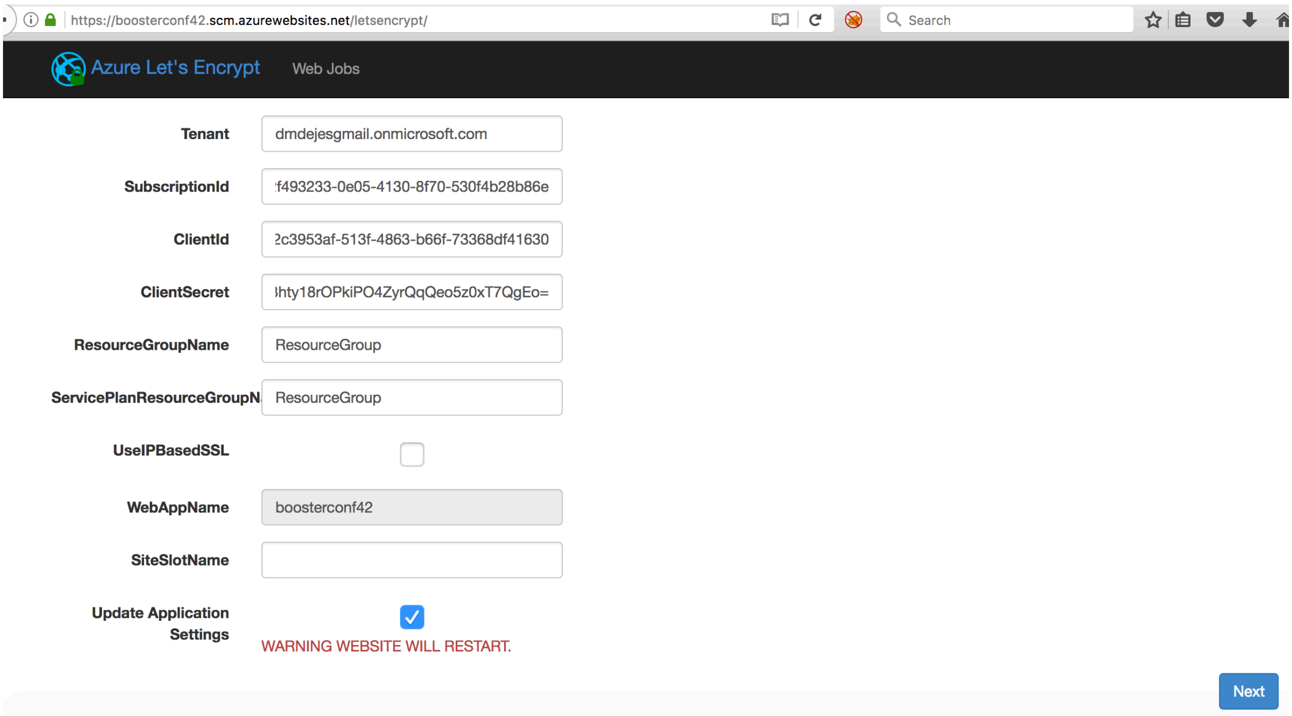
Authentication Settings

To automate the installation of Let's Encrypt SSL certificate on your Azure Web App, a few things need to be configured. The certificate is installed and renewed using the Azure Resource Manager API, because the renewal process should run unattended you need to register an Azure AD service principal that have access to at least the Azure Web App. Read more about how to register a service principal here.

Once you have registered a service principal, you should add the following App Setting, since the site extension reads them from there. You can register them manually or enter them below and check 'Update Web App Settings'.

Key	Value
letsencrypt:Tenant	The tenant name e.g. myazuretenant.onmicrosoft.com
letsencrypt:SubscriptionId	(Optional) The subscription id, if left empty the enviroment variable WEBSITE_OWNER_NAME will be used
letsencrypt:ClientId	The value of the clientid of the service principal
letsencrypt:ClientSecret	The secret for the service principal
letsencrypt:ResourceGroupName	(Optional) The name of the resource group this web app belongs to, if left empty the enviroment variable WEBSITE_OWNER_NAME will be used
letsencrypt:ServicePlanResourceGroupName	(Optional) The name of the resource group that the app service plan hosting the web app (only required if the app service plan is in a different resource group than the web app)
letsencrypt:UseIPBasedSSL	Check this if you want the certificate to be bound to the WebApps' IP address instead of using SNI. With IP based SSL additional costs might be charged.

Automated Installation (click to expand)



Tenant	dmdejesgmail.onmicrosoft.com
SubscriptionId	f493233-0e05-4130-8f70-530f4b28b86e
ClientId	2c3953af-513f-4863-b66f-73368df41630
ClientSecret	hty18rOPkiPO4ZyrQqQeo5z0xT7QgEo=
ResourceGroupName	ResourceGroup
ServicePlanResourceGroupN	ResourceGroup
UseIPBasedSSL	□
WebAppName	boosterconf42
SiteSlotName	
Update Application Settings	☑ WARNING WEBSITE WILL RESTART.

Now is time to find your text editor and just fill in all the information you have gathered along the way. But if you missed something check out the instructions below to find out where you can find them again.

Tenant:
Go to your Azure AD and choose Domain names

SubscriptionId:
Go to App service, select your app, and then overview

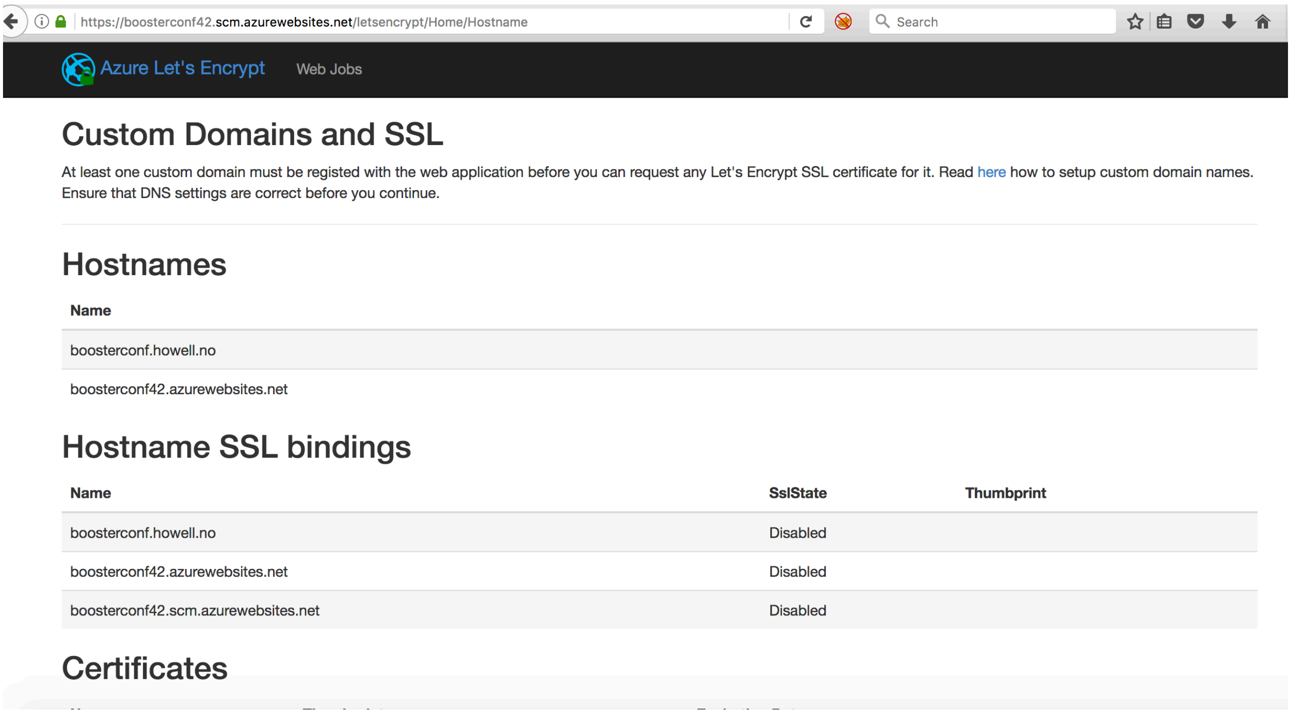
ClientId:
Go to Azure AD and click on App Registration. There you will find the application you registered, click on Overview. The value that Let´s Encrypt Extension calls “ClientId” you will find here as “Application id”

ClientSecret (key): Go to Azure AD, select “App Registration”. Choose the app you created and then click on “keys”. If you have not copied over the value of you key to your text editor you will need to create a new key.

ResourceGroupName
Your Resource Group Name. You will find this in your application Overview

ServicePlanResourceGroupName
If you follow the tutorial then your ServicePlan name should be the same as your ResourceGroupName. This information is available on your application Overview. Note: this is where Let´s Encrypt Extension appears to requires ResourceGroup and App Service Plan to have the same name.

When you finished filling in all the information I mentioned above, click on the button “Next”.


https://boosterconf42.scm.azurewebsites.net/letsencrypt/Home/Hostname
Search
Azure Let's Encrypt
Web Jobs

Custom Domains and SSL

At least one custom domain must be registed with the web application before you can request any Let's Encrypt SSL certificate for it. Read here how to setup custom domain names. Ensure that DNS settings are correct before you continue.

Hostnames

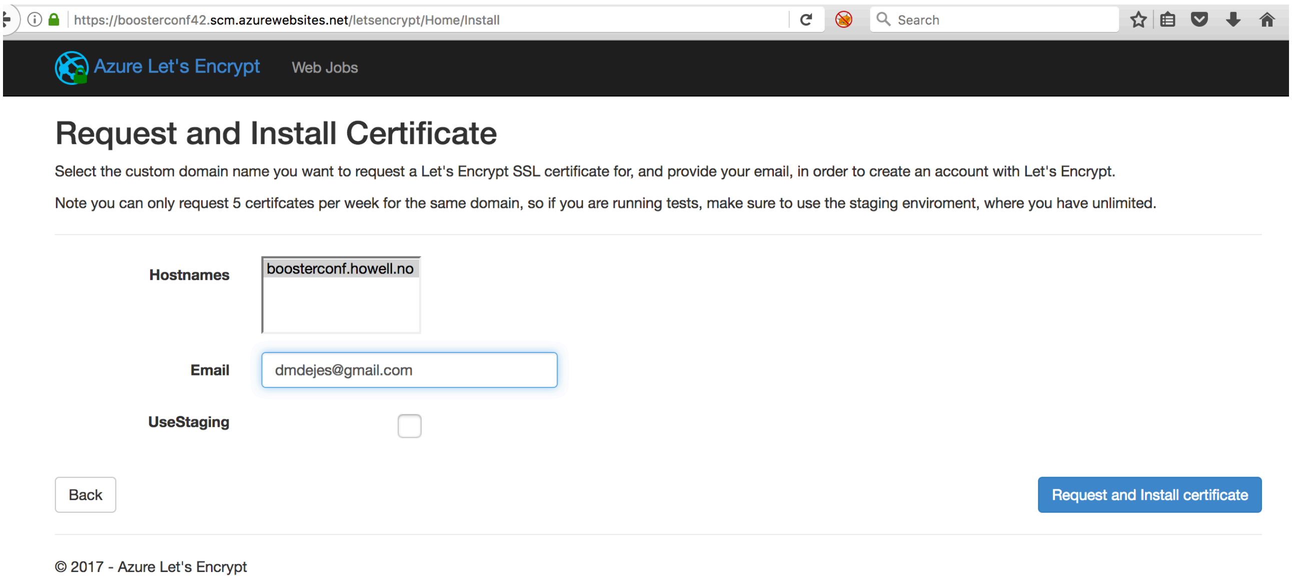
Name
boosterconf.howell.no
boosterconf42.azurewebsites.net

Hostname SSL bindings

Name	SslState	Thumbprint
boosterconf.howell.no	Disabled	
boosterconf42.azurewebsites.net	Disabled	
boosterconf42.scm.azurewebsites.net	Disabled	

Certificates

You will be presented with a summary. There you will be able to see the Hostname and SSL bindings. Click “Next” again to select a domain.


https://boosterconf42.scm.azurewebsites.net/letsencrypt/Home/Install
Search
Azure Let's Encrypt
Web Jobs
Back
Request and Install certificate

Request and Install Certificate

Select the custom domain name you want to request a Let's Encrypt SSL certificate for, and provide your email, in order to create an account with Let's Encrypt.

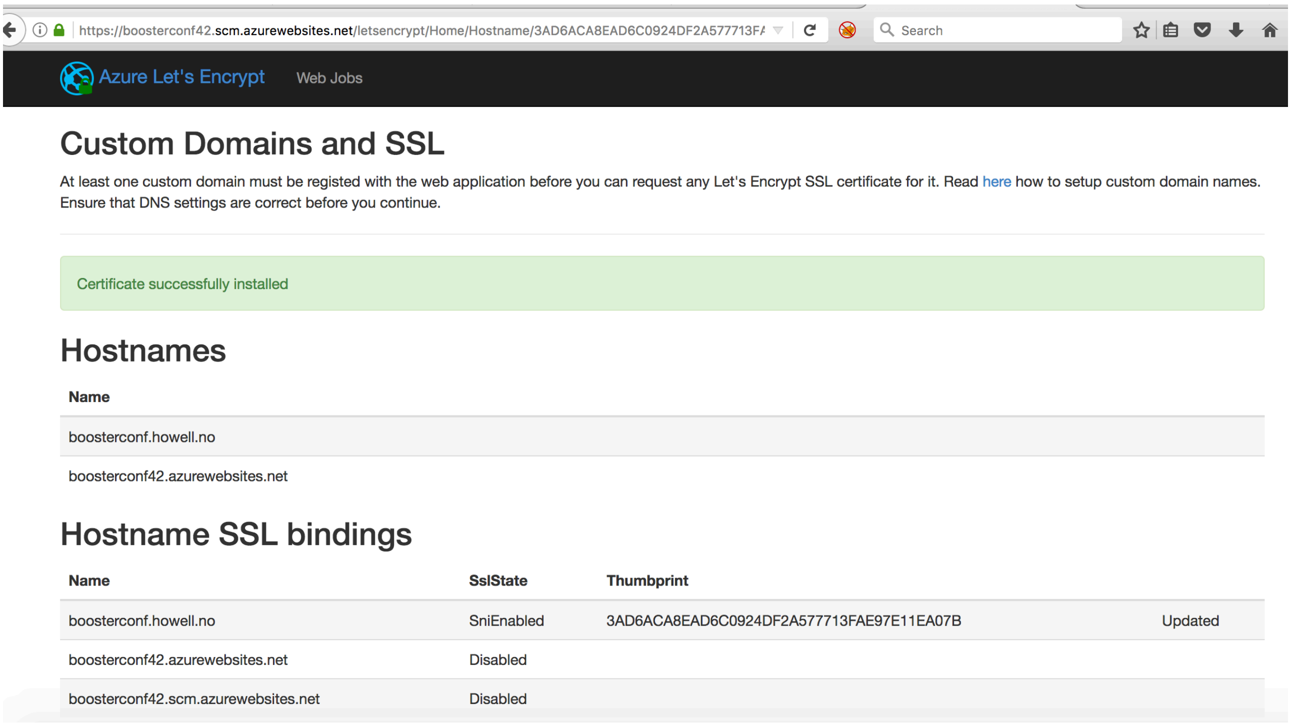
Note you can only request 5 certifcates per week for the same domain, so if you are running tests, make sure to use the staging enviroment, where you have unlimited.

Hostnames	boosterconf.howell.no
Email	dmdejes@gmail.com
UseStaging	□

© 2017 - Azure Let's Encrypt

And we are almost there. Click on “Request and install certificate”. After a few seconds your certificate will be ready.

Check that the certificate is working


https://boosterconf42.scm.azurewebsites.net/letsencrypt/Home/Hostname/3AD6ACA8EAD6C0924DF2A577713FA
Search
Azure Let's Encrypt
Web Jobs

Custom Domains and SSL

At least one custom domain must be registed with the web application before you can request any Let's Encrypt SSL certificate for it. Read here how to setup custom domain names. Ensure that DNS settings are correct before you continue.

Certificate successfully installed

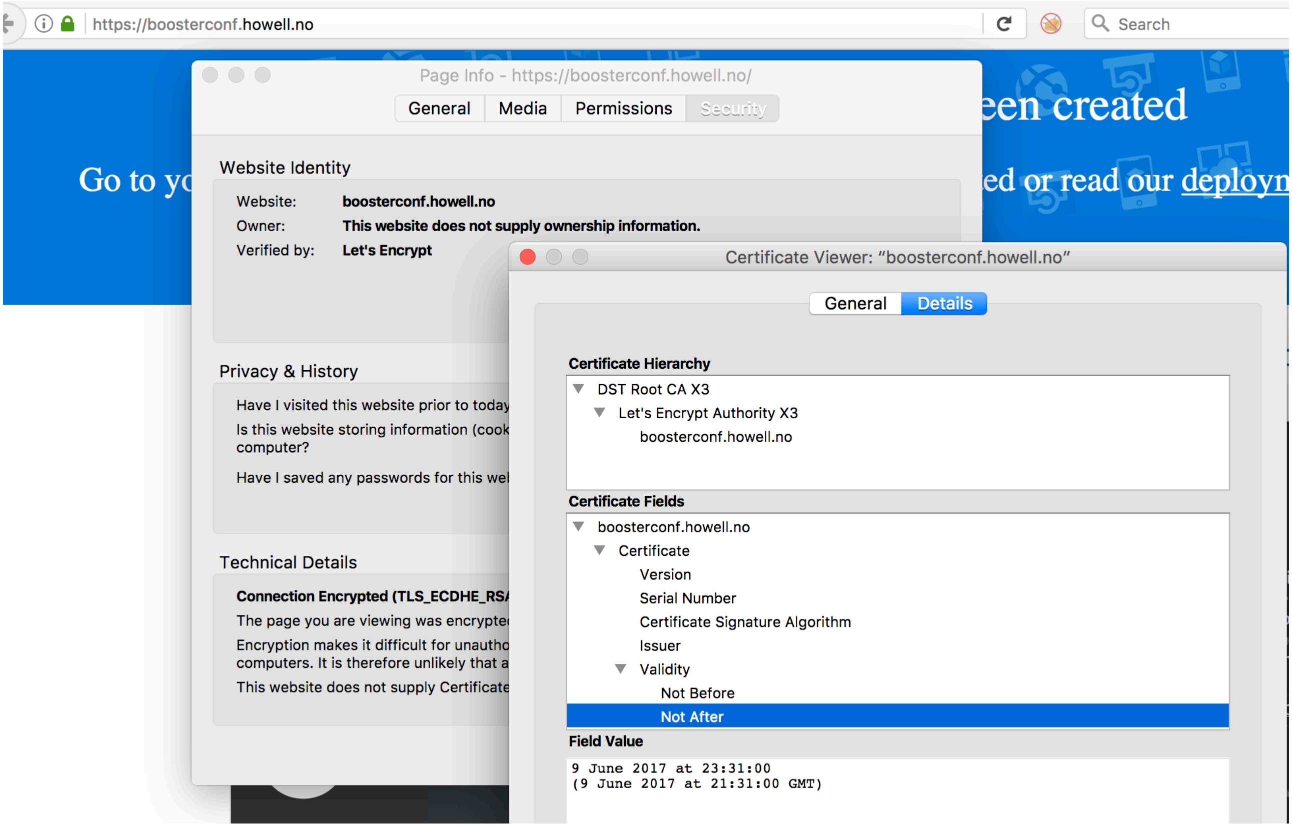
Hostnames

Name
boosterconf.howell.no
boosterconf42.azurewebsites.net

Hostname SSL bindings

Name	SslState	Thumbprint	
boosterconf.howell.no	SniEnabled	3AD6ACA8EAD6C0924DF2A577713FAE97E11EA07B	Updated
boosterconf42.azurewebsites.net	Disabled		
boosterconf42.scm.azurewebsites.net	Disabled		

Open your domain in a web browser, and verify that you now have a Let´s Encrypt SSL certificate attached to it. In this example go to https://boosterconf42.howell.no


https://boosterconf.howell.no
Search
een created
Go to yo
ed or read our deployn
Page Info - https://boosterconf.howell.no/
General
Media
Permissions
Security
Certificate Viewer: "boosterconf.howell.no"
General
Details

Website Identity

Website: **boosterconf.howell.no**
Owner: **This website does not supply ownership information.**
Verified by: **Let's Encrypt**

Privacy & History

Have I visited this website prior to today

Is this website storing information (cook computer?

Have I saved any passwords for this wel

Technical Details

Connection Encrypted (TLS_ECDHE_RSA

The page you are viewing was encrypte

Encryption makes it difficult for unautho computers. It is therefore unlikely that a

This website does not supply Certificate

Certificate Hierarchy

- DST Root CA X3
  - Let's Encrypt Authority X3
    - boosterconf.howell.no

Certificate Fields

- boosterconf.howell.no
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After

Field Value

```
9 June 2017 at 23:31:00
(9 June 2017 at 21:31:00 GMT)
```