SSL

SSL validation, installation, and verification

- SSL Validation
- SSL Checks
- Self Signed & Free Certificates

SSL Validation

==========

SSL Validation?

CNAME DNS VALIDATION

Add CNAME Records which are listed in ANS Portal SSL section:

Format:

```
Value.comodoca.com
SSLvalue
```

Example:

Email Validation

Verification email is sent to admin email for domain

File Upload? Validation

Validation information needs to be added onto the server in a text file, this needs to be available via the relevant domain.

http(s)://example.com/.well-known/pki-validation/<MD5 Hash>.txt

Example file contents:

6051E0C6B973EBC70926FD060D8EFA298BBDEBAB2ADF0A2CE23A43285A6B96AA
sectigo.com
63c554fc

SSL Checks

==========

Online Tools

There are various online tools which can be used for SSL validation, here are a few:

SSL Checker

WhyNoPadlock

QuaysSSL lab

CLI Tools

```
echo | openssl s_client -servername website.co.uk -connect website.com:443 2>/dev/null
| openssl x509 -noout –dates
```

==========

Self Signed & Free Certificates

==========

What are self-signed certificates (OpenSSL)?

- **Generated using OpenSSL:** You can generate these certificates yourself without any cost.
- **Not Trusted by Browsers:** Browsers and operating systems do not recognize self-signed certificates as trusted because they are not signed by a recognized Certificate Authority (CA). This results in security warnings when users visit your site.
- **Use Cases:** Self-signed certificates are typically used for internal testing, development environments, or intranets where trust can be manually configured.

What are Let'sEncrypt Certificates?

- **Generated using Let's Encrypt:** Let's Encrypt is a free, automated, and open CA that provides SSL/TLS certificates.
- **Trusted by Browsers:** Certificates from Let's Encrypt are recognized and trusted by all major browsers, ensuring that users won't see security warnings when visiting your site.
- **Automation:** The process can be automated using tools like Certbot, which handles the issuance and renewal of certificates.
- **Free:** These certificates are provided at no cost.

==========

OpenSSL

using OpenSSL, you can generate a private key and a CSR to either:

1. **Send to a Certificate Authority (CA)** to obtain a certificate that will be trusted by browsers and other clients.
2. **Generate a self-signed certificate** for your own use, which will not be trusted by browsers by default but can be useful in certain scenarios.

/etc/ssl

perms for SSL files needs to be 600

Generating a private key and CSR

Generate a private key:

generating a private key is a prerequisite for creating a Certificate Signing Request (CSR). The private key is essential because it is used to sign the CSR and is part of the SSL/TLS certificate generation process.

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out keyfilename.key
```

Generate a CSR:

A Certificate Signing Request (CSR) is a block of encoded text that is given to a Certificate Authority (CA) when applying for an SSL/TLS certificate. The CSR contains information about the organization and the public key that will be included in the certificate.

```
openssl req -new -key keyfilename.key -out csrfilename.csr
```

Generating a certificate

Using the steps above, you will generate a private key and CSR file. We can then use these files to generate a self-signed certificate.

```
openssl x509 -req -days 365 -in csrfilename.csr -signkey keyfilename.key -out crtfilename.crt
```

==========

LetsEncrypt

Apache

https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-centos-7

Running certbot for a single domain

```
sudo certbot --apache -d example.com
```

Running certbot for multiple domains (or subdomains)

```
sudo certbot --apache -d example.com -d www.example.com
```

Auto Renewal

Nginx

https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-ubuntu-20-04

```
sudo apt install certbot python3-certbot-nginx
```

```
sudo certbot --nginx -d example.com -d www.example.com
```

Generate a certificate to be manually installed

```
certbot certonly -manual -d example.com -d example.com --webroot -w /path/to/doc/root
```

Auto Renewal

```
systemctl status certbot.timer
```

test renewal:

```
certbot renew --dry-run
```