

TLS/SSL	3
.....	3
.....	3
.....	3
.....	3
.....	3
.....	4
.....	4
CA	4
.....	5
CSR()	5
Let's Encrypt / certbot	5
certbot	5
- (dhparam) 가?	6

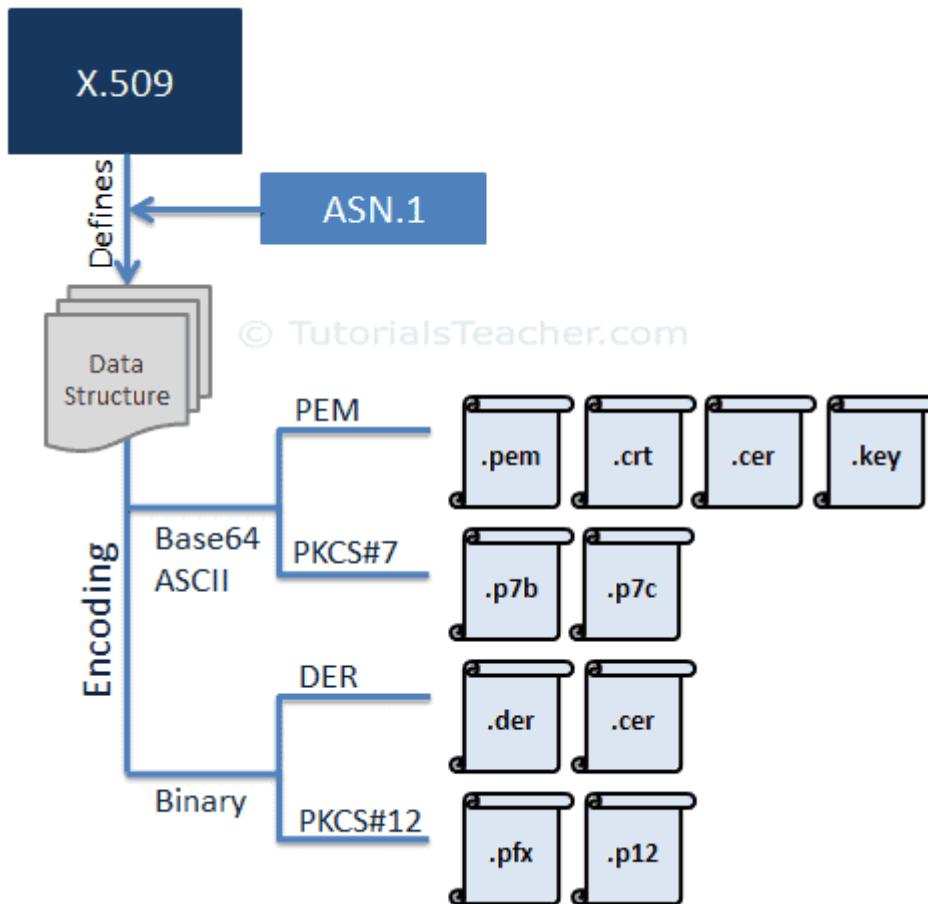
TLS/SSL

- <https://www.ssllabs.com/> -
- <https://sslmate.com/caa/> - CAA
- [DNS CAA](#) ?
- [Diffie-Hellman Key](#)
- [Cipher Suite](#)

- DES
- AES
- SEED
- ARIA

- RSA
- DSA
- Diffie-Hellman

- MD5
- SHA1
- SHA2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)
- SHA3



<https://www.tutorialsteacher.com/https/ssl-certificate-format>

- PEM(Privacy-enhanced Electronic Mail) : Base64 ASCII encode .pem, .cert, .key
가 .cert cer 가 key
- DER(Distinguished Encoding Rules) : binary .der .cer
Java web
- pfx, p12 ... : PKCS#12(Public Key Cryptography Standards #12)

```
openssl x509 -in cert.crt -outform der -out cert.der
```

CA

```
# key
openssl genrsa -out ca.key 4096
#
openssl req -x509 -new -nodes -sha512 -days 3650 \
-key ca.key \
```

```
-out ca.crt
```

```
# key
openssl genrsa -out ia.key 4096

# CSR( )
openssl req -sha512 -new \
    -key ia.key \
    -out ia.csr
```

CSR()

```
#
cat > v3.ext <<-EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
DNS.1=yourdomain.com
DNS.2=yourdomain
DNS.3=hostname
EOF

openssl x509 -req -sha512 -days 3650 \
    -extfile v3.ext \
    -CA ca.crt -CAkey ca.key -CAcreateserial \
    -in ia.csr \
    -out ia.crt
```

Let's Encrypt / certbot

- <https://certbot.eff.org/docs/using.html> Certbot Manual
- [Let's Encrypt\(CertBot\) SSL with HAProxy](#)
- [HAProxy SSL](#)
- [Let's Encrypt\(CertBot\) Wildcard Certificates](#)

certbot

certbot

가

http

dns

- http

*.domain.com

- dns

http

let's encrypt

my.domain.dom

--standalone

. dns

TXT

--preferred-challenges dns 가

--manual

--manual http dns

-

(dhparam)

가?

- (dhparam) SSL

WAS SSL

dhparam

dhparam

. SSL

A

OpenSSL dhparam

```
openssl dhparam -out dhparam.pem <KEY-SIZE>
# KEY-SIZE    2048    4096
```

dhparam

가

가

가

<https://ssl-config.mozilla.org/>

dhparam

- <https://ssl-config.mozilla.org/ffdhe2048.txt>
- <https://ssl-config.mozilla.org/ffdhe4096.txt>

- <https://rsec.kr/?p=242>
- <https://waspro.tistory.com/479>

From:

<https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link:

https://atl.kr/dokuwiki/doku.php/tls_ssl?rev=1623400153

Last update: **2021/06/11 08:29**

