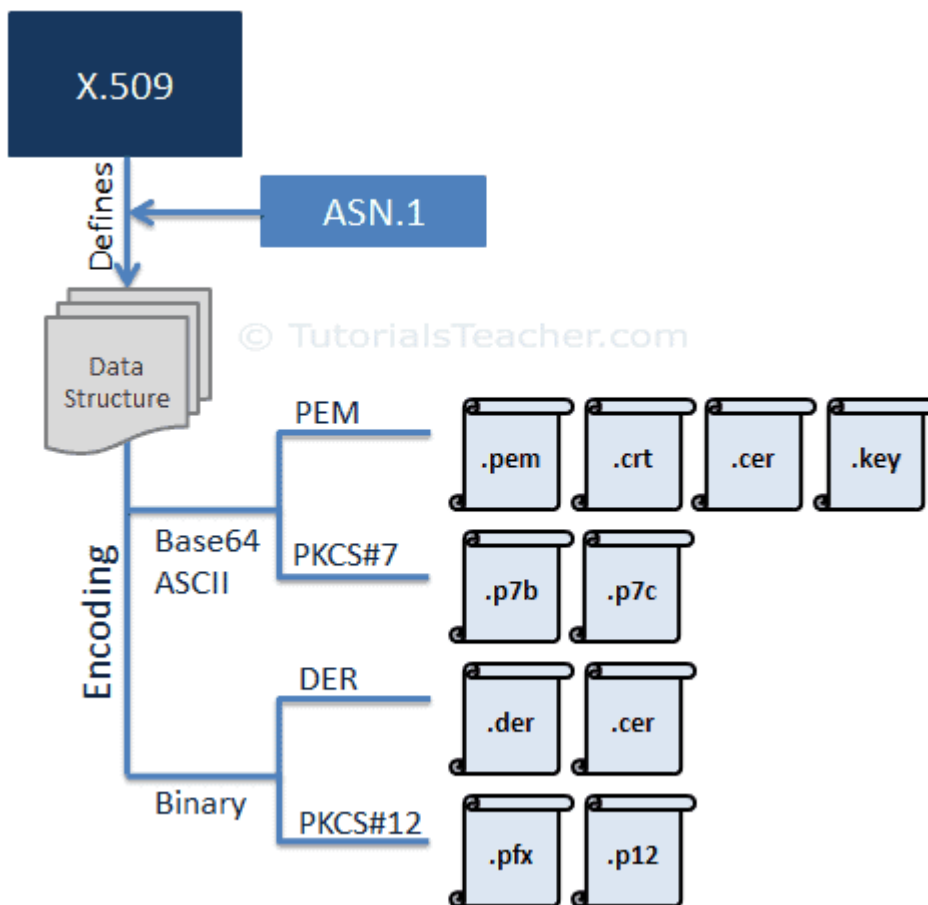


TLS/SSL	3
.....	3
Let's Encrypt / certbot	4
certbot	4
- (dhparam) 가?	4

TLS/SSL

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



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

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

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 dns . 가 http
--preferred-challenges dns 가
--preferred-challenges dns *.domain.com
--preferred-challenges dns
http my.domain.dom let's encrypt
--standalone . dns
--manual http dns
--manual http dns
```

- (dhparam) 가?

- (dhparam) SSL WAS SSL dhparam
 . SSL A .

OpenSSL dhparam .

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

dhparam 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=1623396786

Last update: **2021/06/11 07:33**

