

Запомните

Сертификат mTLS выглядит, как и обычный сертификат TLS. Он также содержит такую информацию, как:

- Субъект — кому выдан сертификат. Это может быть человек, организация или устройство.
- Эмитент — центр сертификации (ЦС), который проверил и выдал сертификат.
- Срок действия — дата выдачи и дата истечения срока действия сертификата.
- Открытый ключ — ключ, связанный с субъектом сертификата, используемый для шифрования и цифровой подписи.
- Алгоритм подписи — криптографический алгоритм, используемый для подписи сертификата эмитентом.
- Серийный номер — уникальный номер, присваиваемый эмитентом для отличия сертификата от других.
- Расширения — дополнительная информация о сертификате и его использовании, например, альтернативные имена субъектов (SAN) или ограничения на использование ключей.

Вот пример того, как может выглядеть сертификат в виде обычного текста (формат PEM, это текст в base64):

```
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIJAJC1HiIAZAiIMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRIMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwMzEwMTg1OTM3WhcNMTgwMzEwMTg1OTM3WjBF
.....
-----END CERTIFICATE-----
```