CLEARWAY INTEGRATION

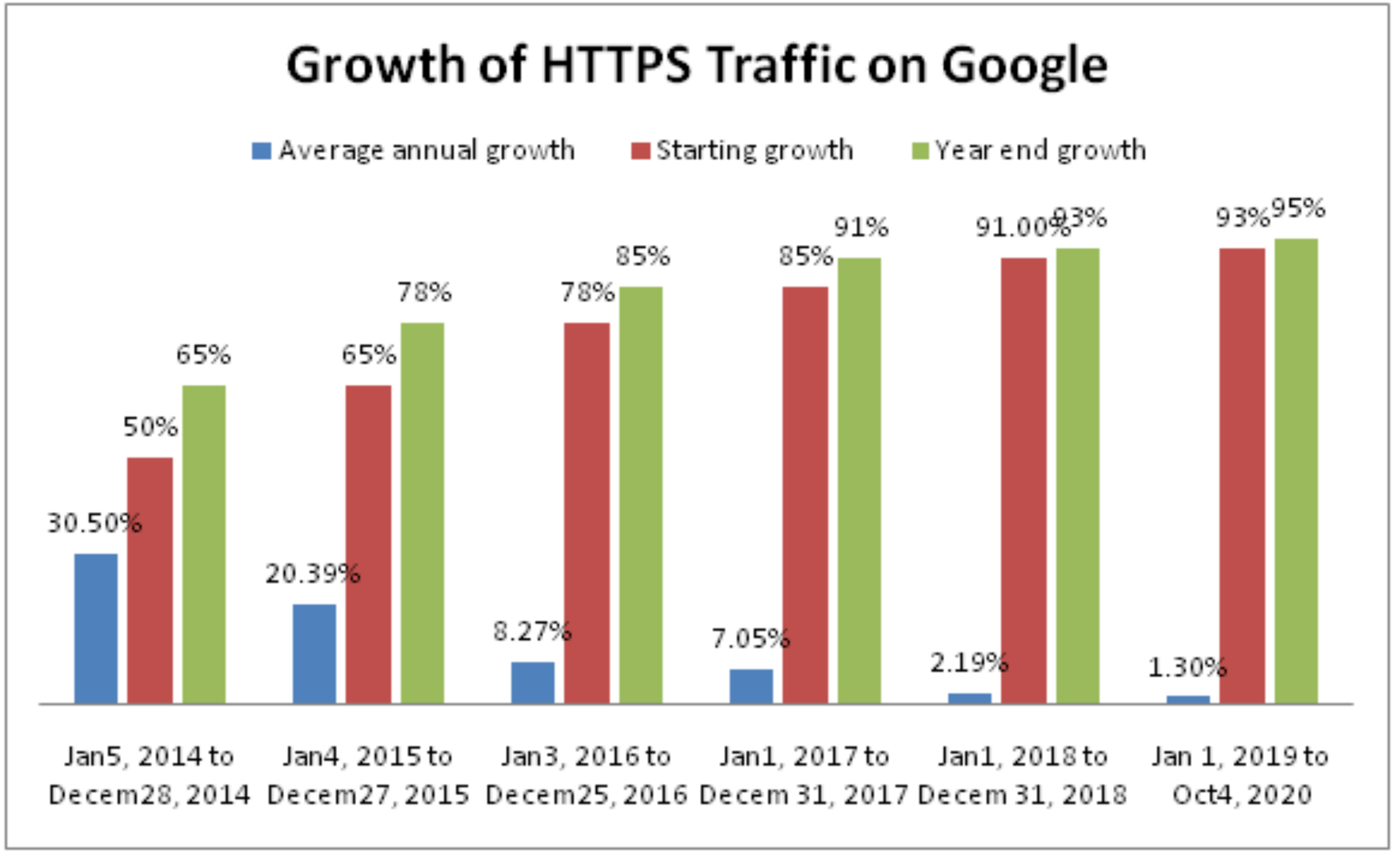
Back to Basics. Сертификаты, TLS и взаимная аутентификация сервисов

Лучник Анна

План

- Сертификаты: формат и проверка подлинности
- Основы криптографии, необходимые для понимания работы сертификатов
- TLS и mTLS
- Частые ошибки при настройке сертификатов
- И как ошибки избежать

Чем вызван такой рост HTTPS-трафика?



https://www.blowwager.com/what-is-https-importance-work-and-statistics/

HTTPS повышает SEO

В 2014 году

Google призвал к повсеместному использованию HTTPS для повышения безопасности во всем интернете.

Сайты использующие **HTTPS** получали **более высокий рейтинг в поисковой выдаче.**

В 2018 году

Google начала наказывать **HTTP-сайты**, помечая их как **«небезопасные» в браузере Chrome**.

https://www.digicert.com/news/google-chrome-update-labels-websites-using-http-as-not-secure/

А еще HTTPS обеспечивает

Аутентификацию

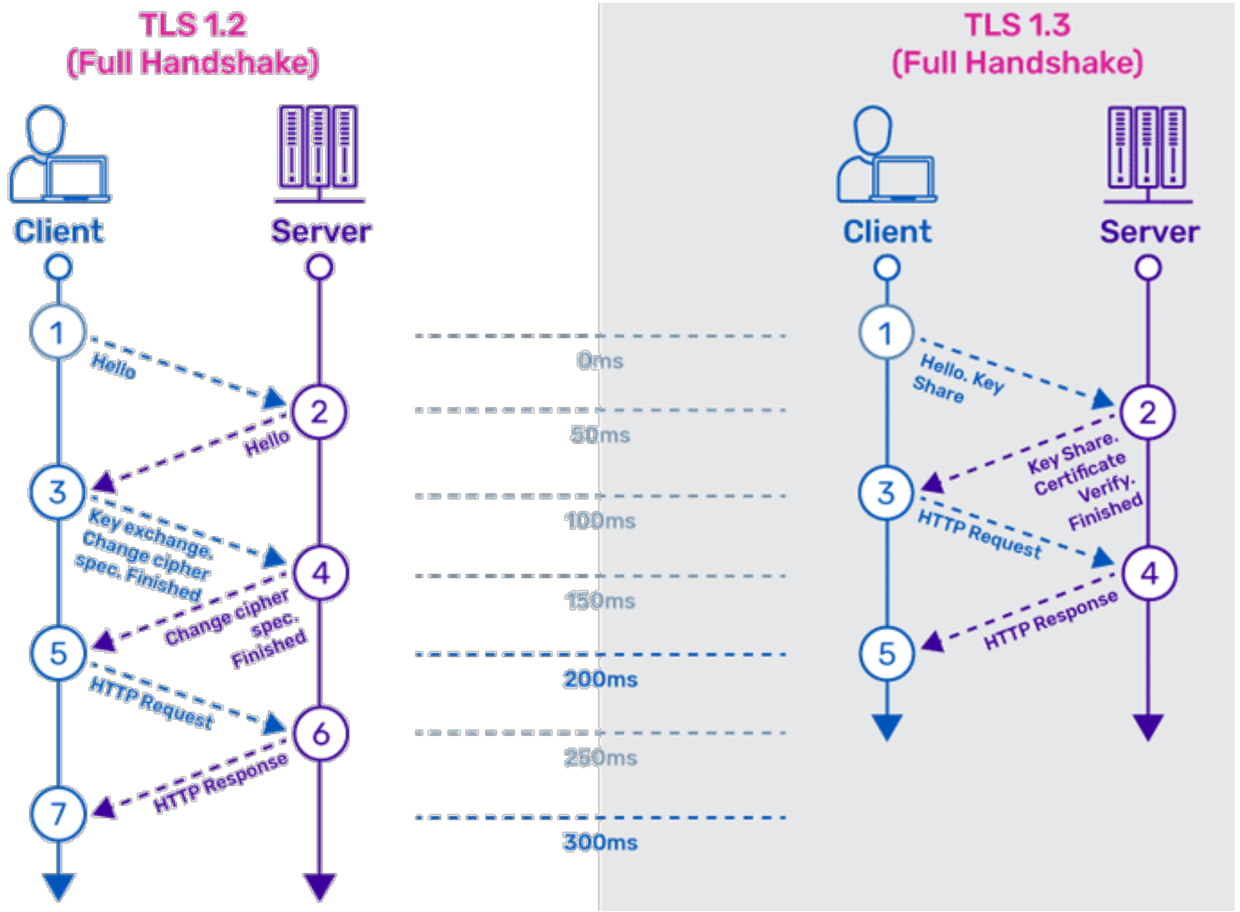
Шифрование

Контроль целостности

HTTPS = HTTP + TLS

TLS = Handshake Protocol
+ Record Protocol
+ Alert Protocol

TLS 1.2 vs TLS 1.3



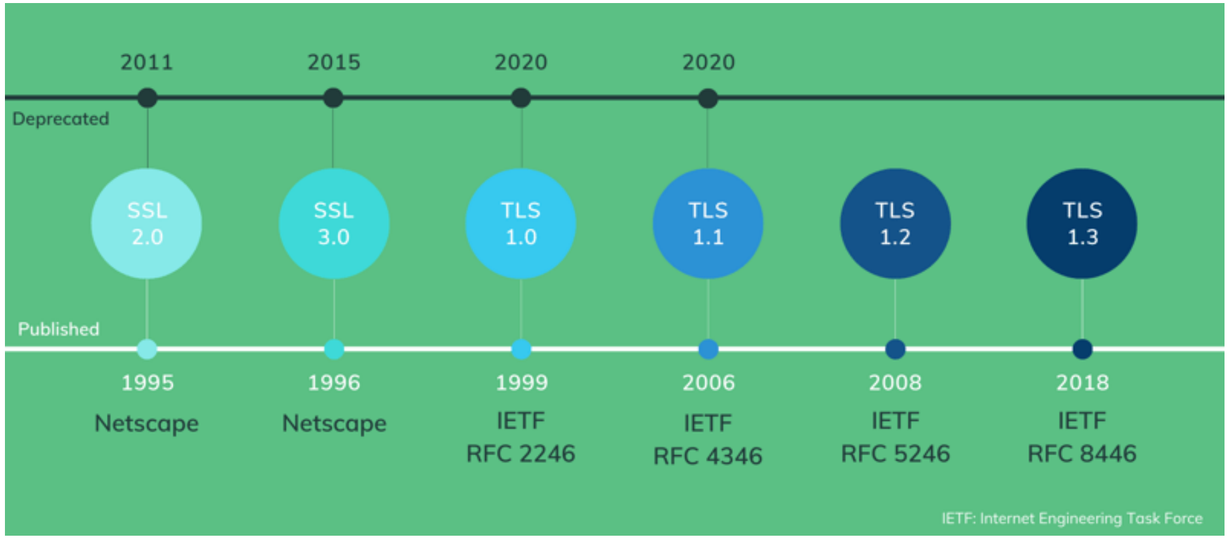
https://www.a10networks.com/glossary/key-differences-between-tls-1-2-and-tls-1-3/

Что такое SSL-сертификат?

Термин, который **устарел 10 лет назад**, но…

SSL certificate ~184,000,000 результатов в Google

TLS certificate ~56,400,000 результатов в Google

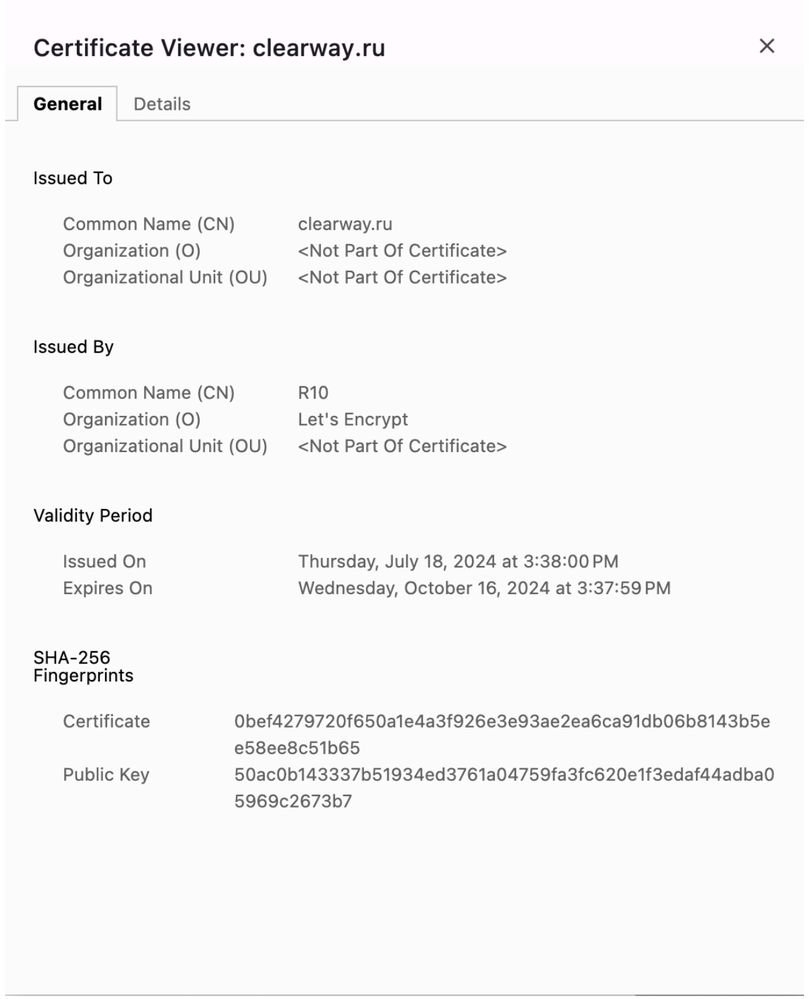


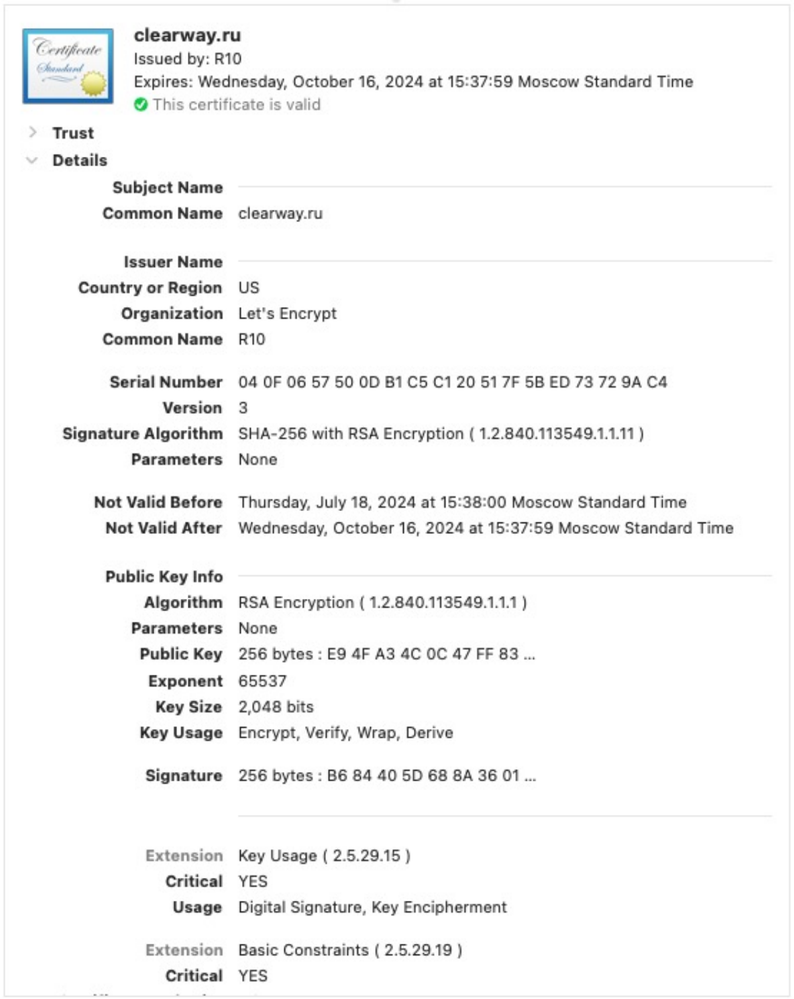
https://dev.to/techschoolguru/a-complete-overview-of-ssl-tls-and-its-cryptographic-system-36pd

Сертификат


```
-----BEGIN CERTIFICATE-----
MIIC7jCCAlegAwIBAgIBATANBgkqhkiG9w0BAQQFADCBqTELMAkGA1UEBhMCWFkx
FTATBgNVBAgTDFNuYWtlIERlc2VydDETMBEGA1UEBxMKU25ha2UgVG93bjEXMBUG
A1UEChMstOU25ha2UgT2lsLCBMdGQxHjAcBgNVBAsTFUNlcnRpZmljYXRlIEdGhv
cml0eTEVMBMGA1UEAxMMU25ha2UgT2lsIENBMR4wHAYJKoZIhvcNAQkBFg9jYUBz
bmFrZW9pbC5kb20wHhcNOTgxMDIxMDg1ODM2WhcNOTkxMDIxMDg1ODM2WjCBpzEL
MAkGA1UEBhMCWarFukxFTATBgNVBAgTDFNuYWtlIERlc2VydDETMBEGA1UEBxMKU
a2UgVG93bjEXMBUGA1UEChMOU25ha2UgT2lsLCBMdGQxFzAVBgNVBAsTDldlYnNl
cnZlciBUZWFtMRkwFwYDVQQDExB3d3cuc25ha2VvaWwuZG9tMR8wHQYJKoZIhvcN
AQkBFhB3d3dAc25ha2VvaWwuZG9tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDH9Ge/s2zcH+da+rPTx/DPRp3xGjHZ4GG6pCmvADIEtBtKBFAcZ64n+Dy7Np8b
vKR+yy5DGQiijsH1D/j8HlGE+q4TZ8OFk7BNBFazHxFbYI4OKMiCxdKzdif1yfaa
lWoANFlAzlSdbxeGVHoT0K+gT5w3UxwZKv2DLbCTzLZyPwIDAQABoyYwJDAPBgNV
HRMECDAGAQH/AgEAMBEGCWCGSAGG+EIBAQQEAwIAQDANBgkqhkiG9w0BAQQFAAOB
gQAZUIHAL4D09oE6Lv2k56Gp38OBDuILvwLg1v1KL8mQR+KFjghCrtpqaztZqcDt
2q2QoyulCgSzHbEGmi0EsdkPfg6mp0penssIFePYNI+/8u9HT4LuKMJX15hxBam7
dUHzICxBVC1lnHyYGjDuAMhe396lYAn8bCld1/L4NMGBCQ==
-----END CERTIFICATE-----
```

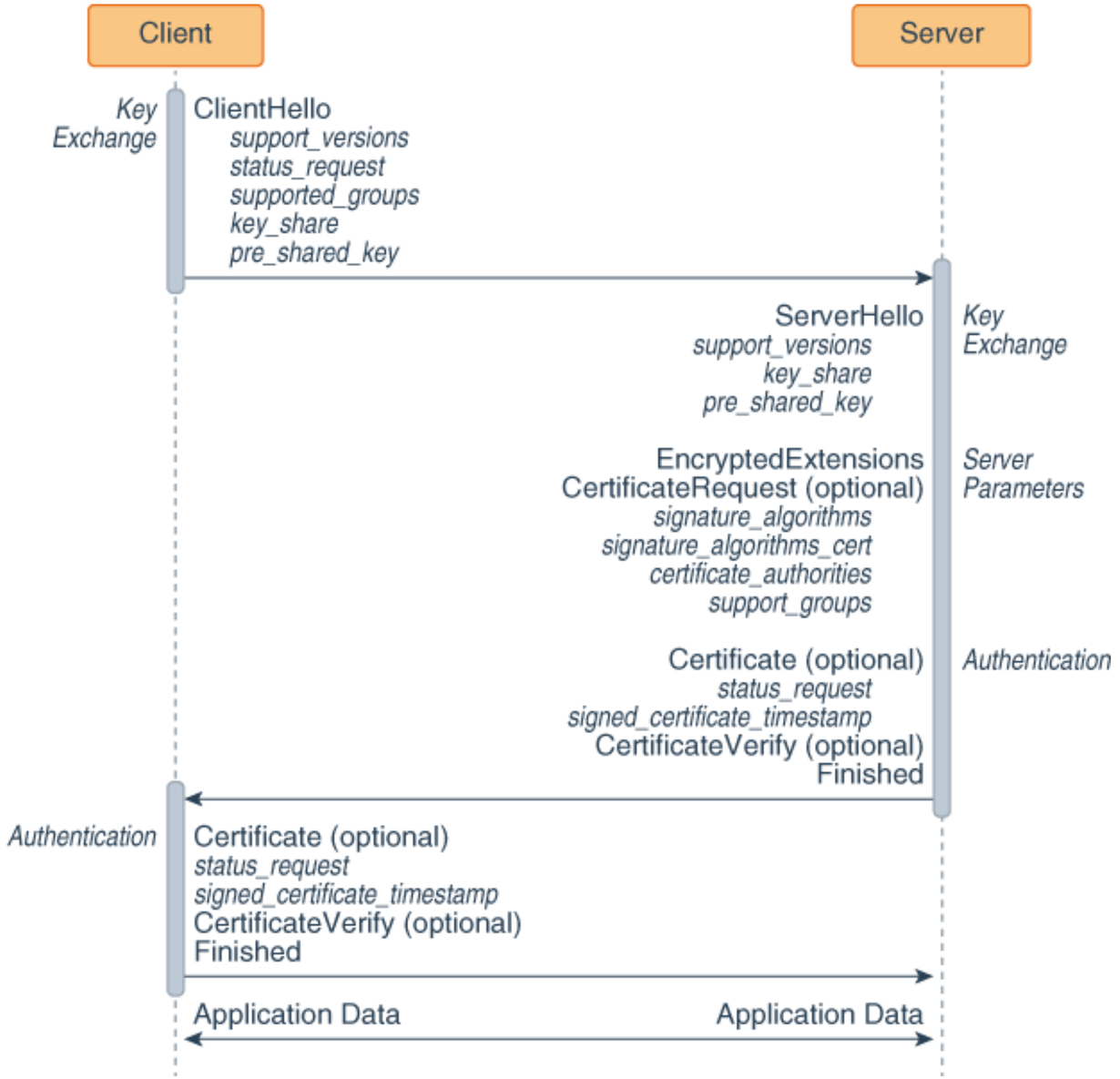
Сертификат


Certificate Viewer: clearway.ru
General
Details
Issued To
Common Name (CN) clearway.ru
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) R10
Organization (O) Let's Encrypt
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Thursday, July 18, 2024 at 3:38:00 PM
Expires On Wednesday, October 16, 2024 at 3:37:59 PM
SHA-256 Fingerprints
Certificate 0bef4279720f650a1e4a3f926e3e93ae2ea6ca91db06b8143b5ee58ee8c51b65
Public Key 50ac0b143337b51934ed3761a04759fa3fc620e1f3edaf44adba05969c2673b7


clearway.ru
Issued by: R10
Expires: Wednesday, October 16, 2024 at 15:37:59 Moscow Standard Time
This certificate is valid
Trust
Details
Subject Name
Common Name clearway.ru
Issuer Name
Country or Region US
Organization Let's Encrypt
Common Name R10
Serial Number 04 0F 06 57 50 0D B1 C5 C1 20 51 7F 5B ED 73 72 9A C4
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None
Not Valid Before Thursday, July 18, 2024 at 15:38:00 Moscow Standard Time
Not Valid After Wednesday, October 16, 2024 at 15:37:59 Moscow Standard Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 256 bytes : E9 4F A3 4C 0C 47 FF 83 ...
Exponent 65537
Key Size 2,048 bits
Key Usage Encrypt, Verify, Wrap, Derive
Signature 256 bytes : B6 84 40 5D 68 8A 36 01 ...
Extension Key Usage (2.5.29.15)
Critical YES
Usage Digital Signature, Key Encipherment
Extension Basic Constraints (2.5.29.19)
Critical YES

Нужны ли SSL сертификаты для установки TLS соединения?

Нужны ли SSL сертификаты для установки TLS соединения?



https://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/tls.html

DH Key Exchange

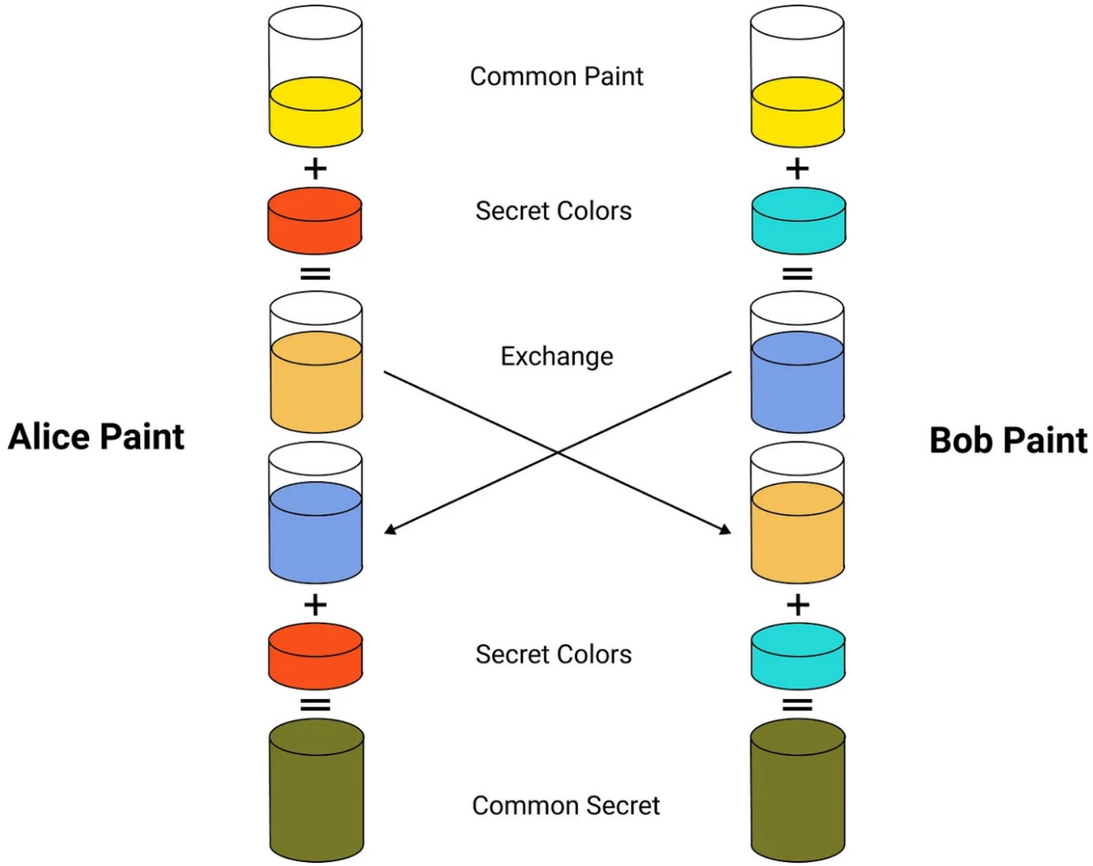
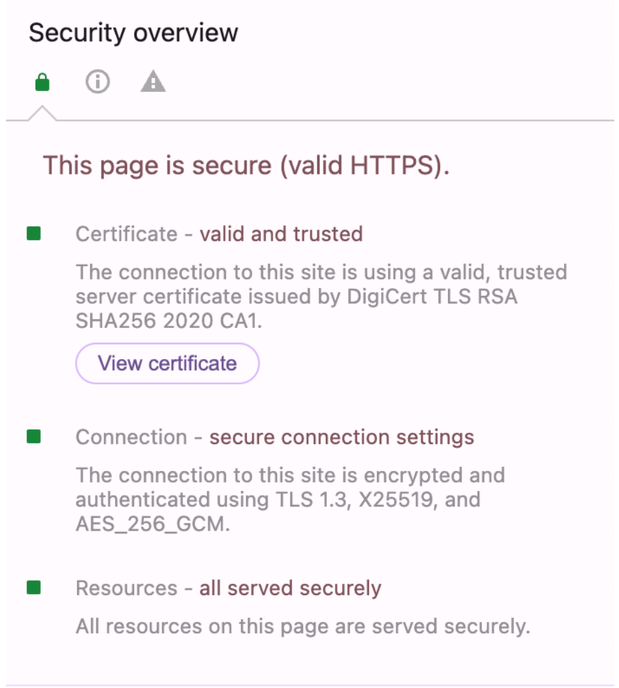
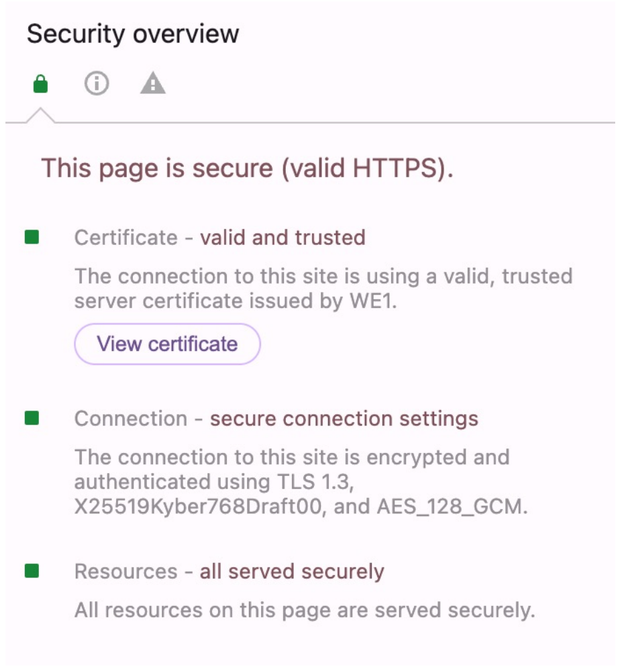


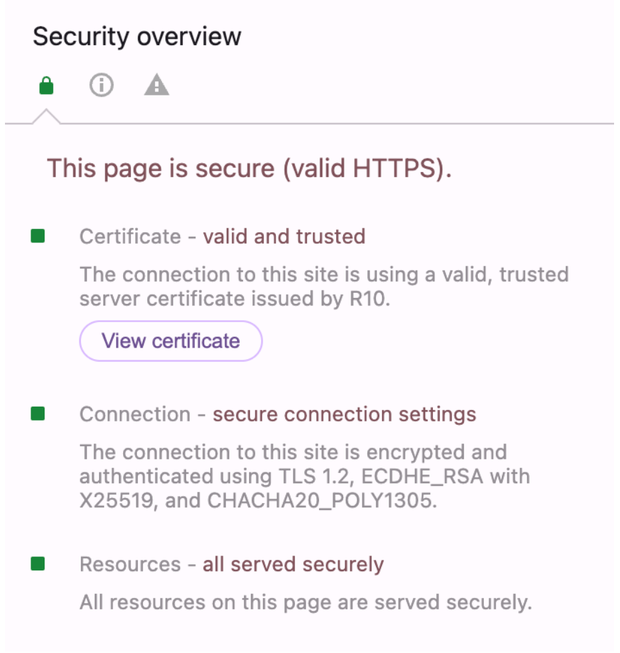
Figure 1. Diffie–Hellman key exchange concept diagram.

https://medium.com/@razumovsky_r/diffie-hellman-key-exchange-via-rest-b7a91c9df7b1

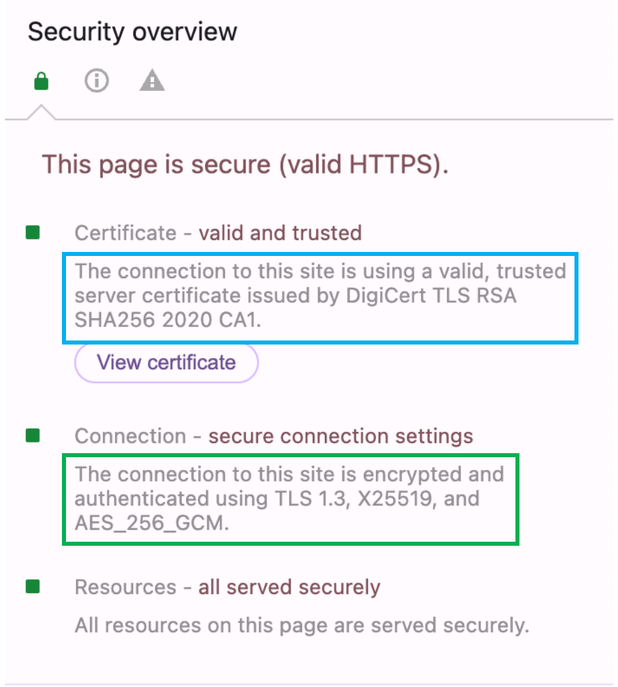
Алгоритмы TLS/SSL

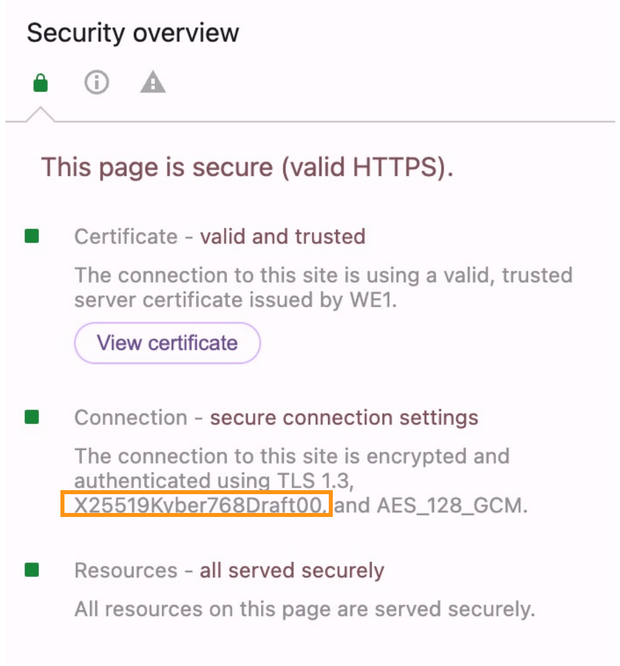


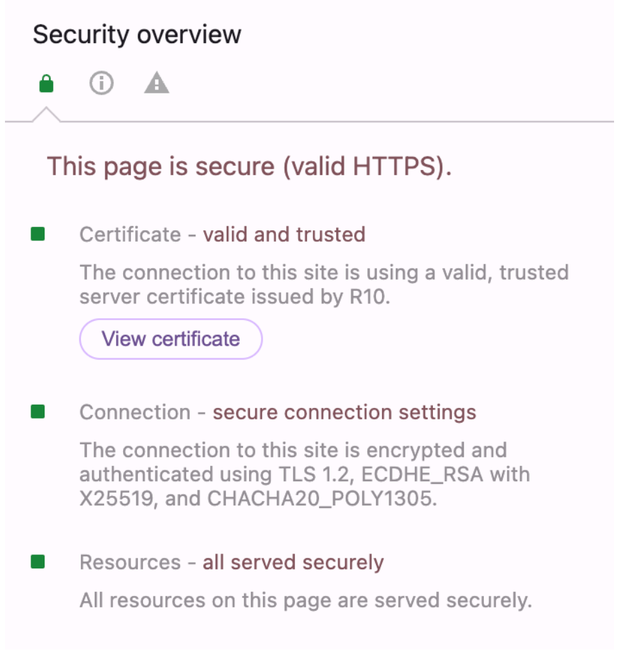




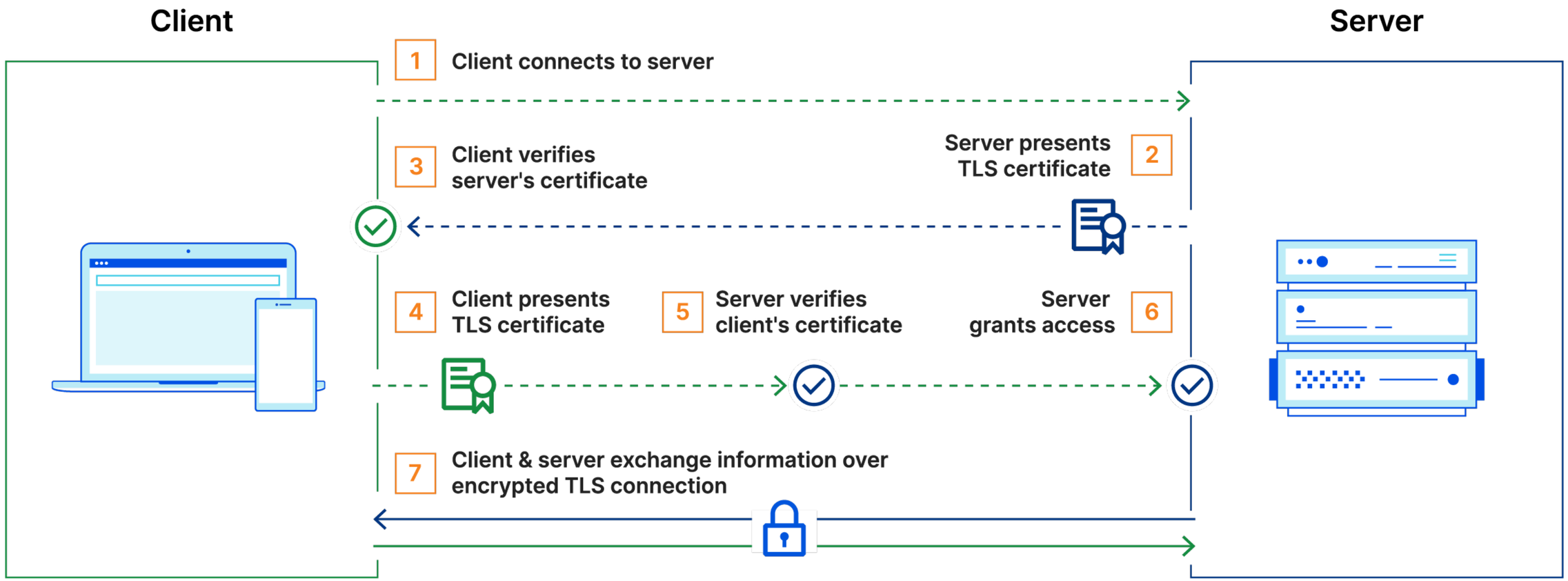
Алгоритмы TLS/SSL







mTLS



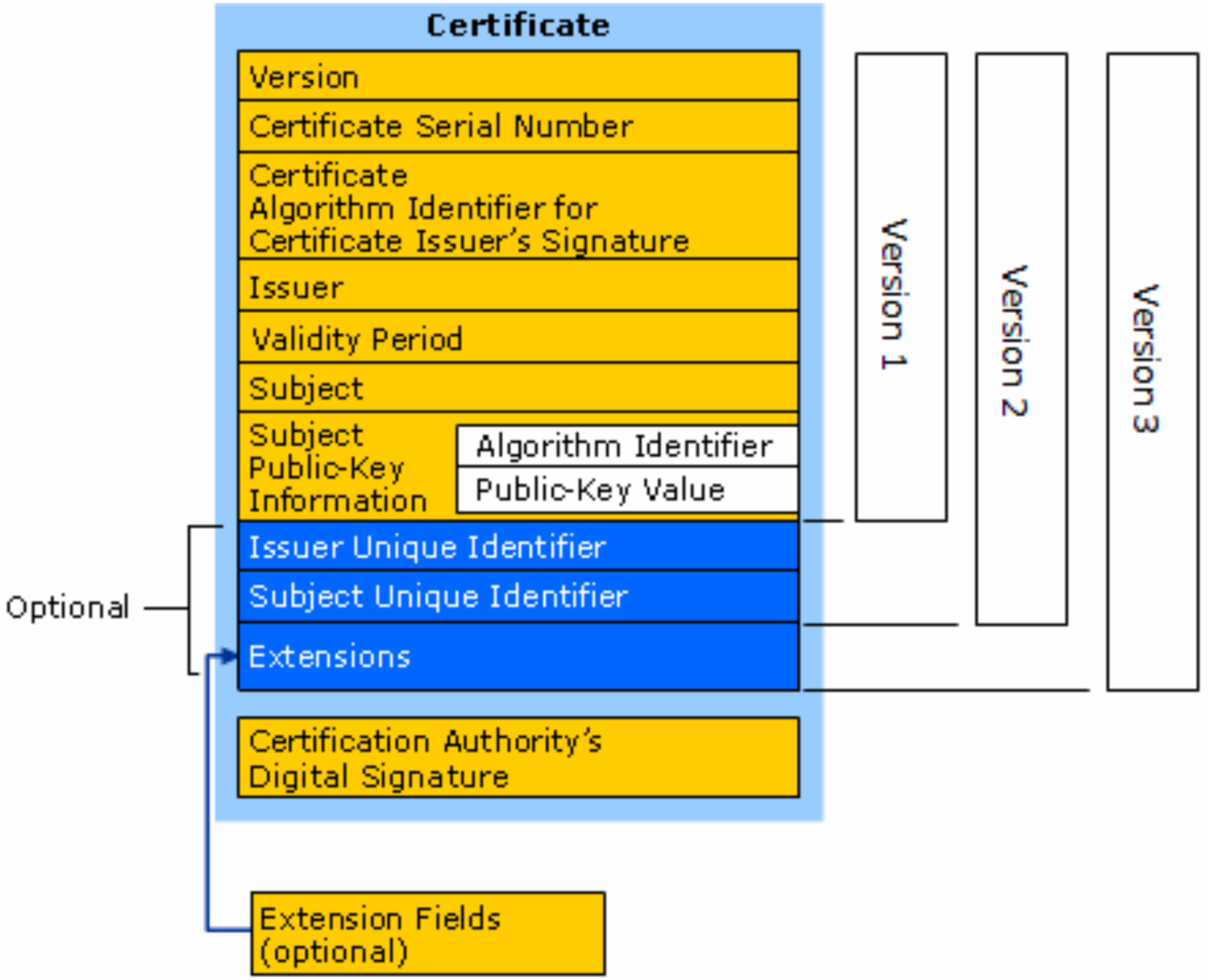
https://www.cloudflare.com/en-gb/learning/access-management/what-is-mutual-tls/

Zero Trust

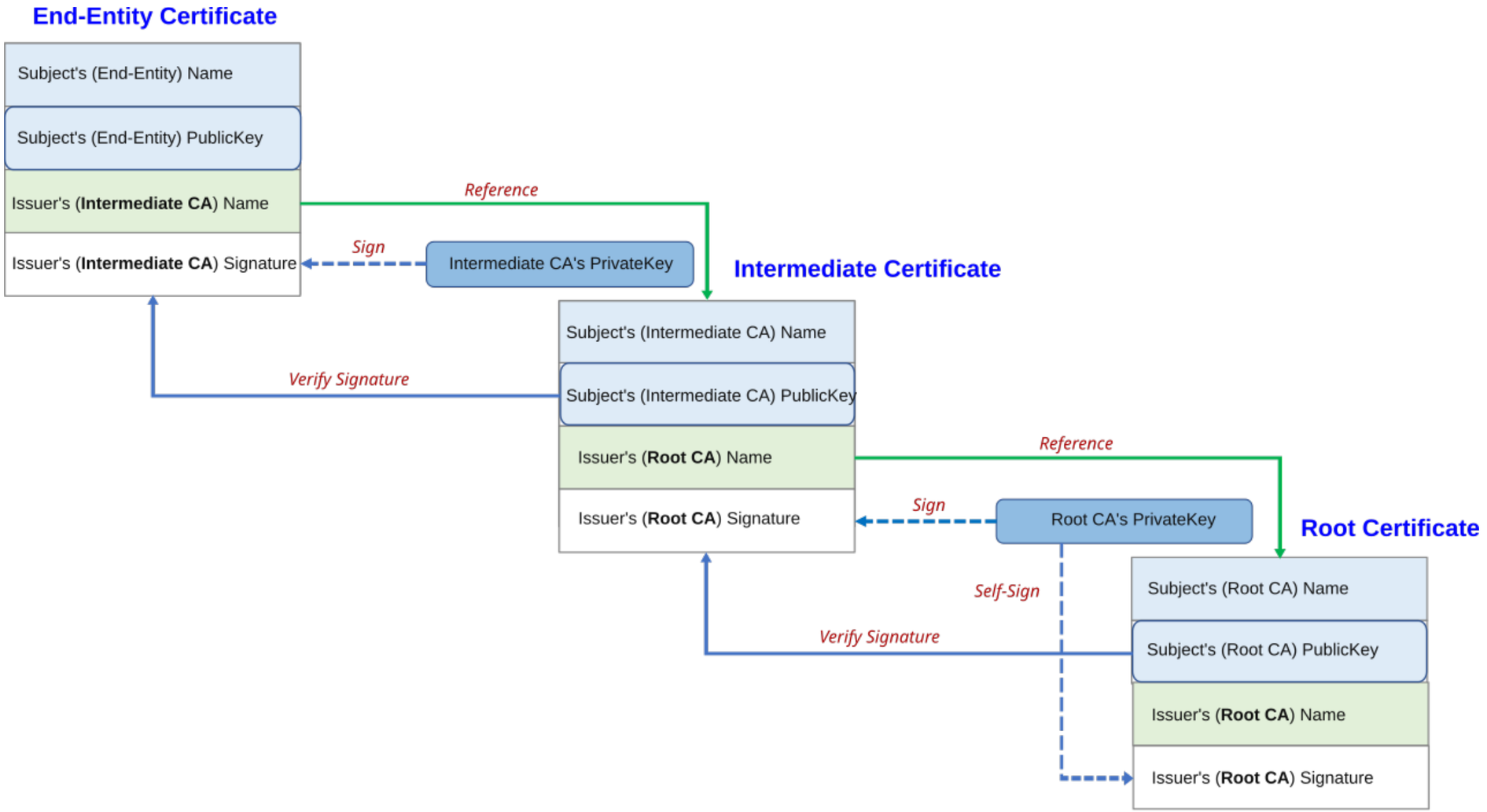
с использованием mTLS

Сертификаты, их атрибуты и проверка подлинности

- Основные атрибуты сертификатов
- Удостоверяющие центры и доверительные отношения
- Проверка сертификатов: цепочки доверия и атрибуты
- Проверка запросов на выпуск сертификатов: политики и атрибуты

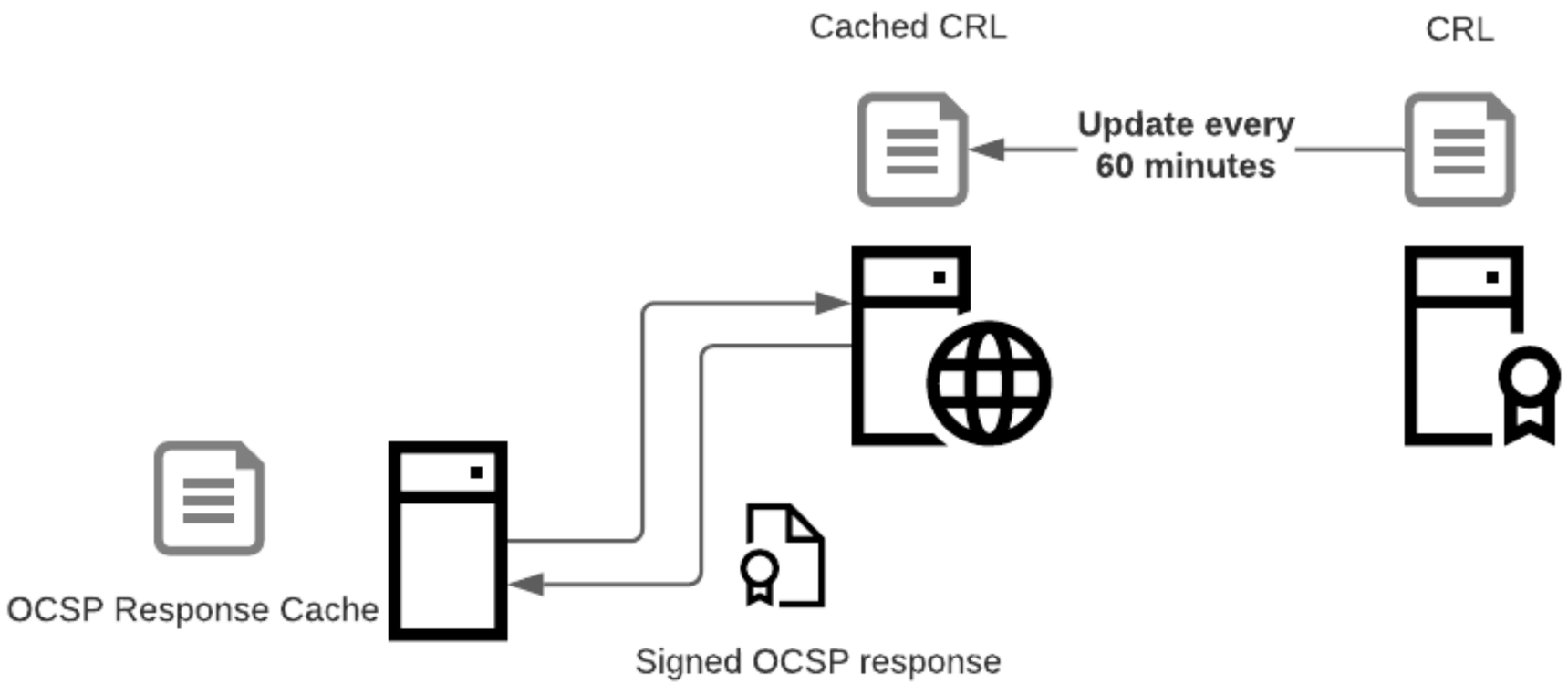


Цепочка доверия



https://en.wikipedia.org/wiki/Root_certificate#/media/File:Chain_of_trust_v2.svg

Проверка срока действия сертификата



Типы SSL сертификатов

1. Extended Validation certificates (EV SSL)
2. Organization Validated certificates (OV SSL)
3. Domain Validated certificates (DV SSL)
4. Wildcard SSL certificates
5. Multi-Domain SSL certificates (MDC)
6. Unified Communications Certificates (UCC)

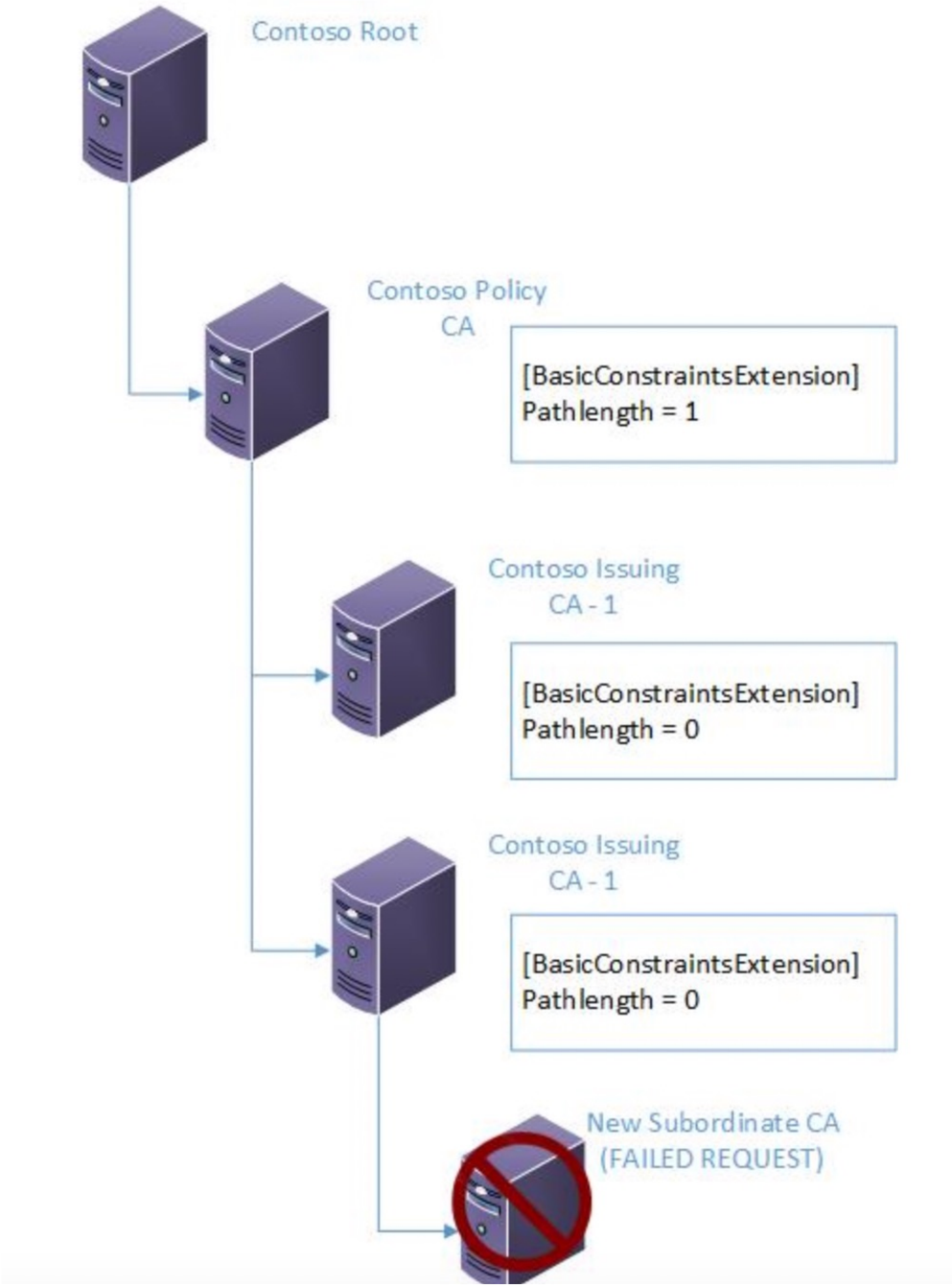
Частые ошибки при настройке сертификатов

- Игнорирование и некорректная проверка клиентских сертификатов
- Неправильная работа с ключами (ошибки при генерации и управлении ключами)
- Просроченные сертификаты и их влияние на систему
- Ошибки при проверке отзыва сертификатов и цепочек доверия
- Самоподписанные сертификаты

Корневой УЦ (Root CA)

Security

Иерархия УЦ и BasicConstrainsExtention



https://blogs.technet.microsoft.com/pki/2014/03/05/constraints-what-they-are-and-how-theyre-used/

AIA и CDP

Timeouts

CTL vs CRL

Timeouts

Закрытый ключ (Private key)

Security

Количество сертификатов

Performance

Чек лист

1. Иерархия УЦ
2. Атрибуты сертификата
3. Политики выпуска
4. Криптографические алгоритмы
5. Срок жизни сертификатов

CLEARWAY INTEGRATION

Спасибо за внимание!

Для связи с нами

Clearwayintegration.net