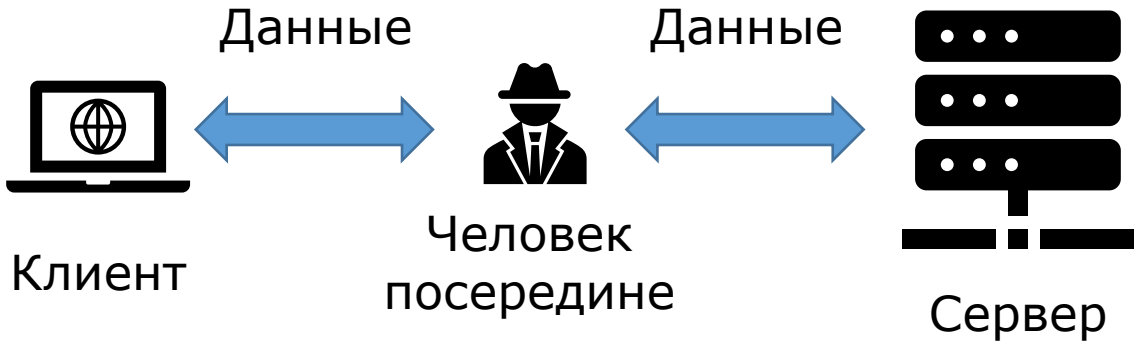
# Инфраструктура открытых ключей в TLS/SSL

Компьютерные сети

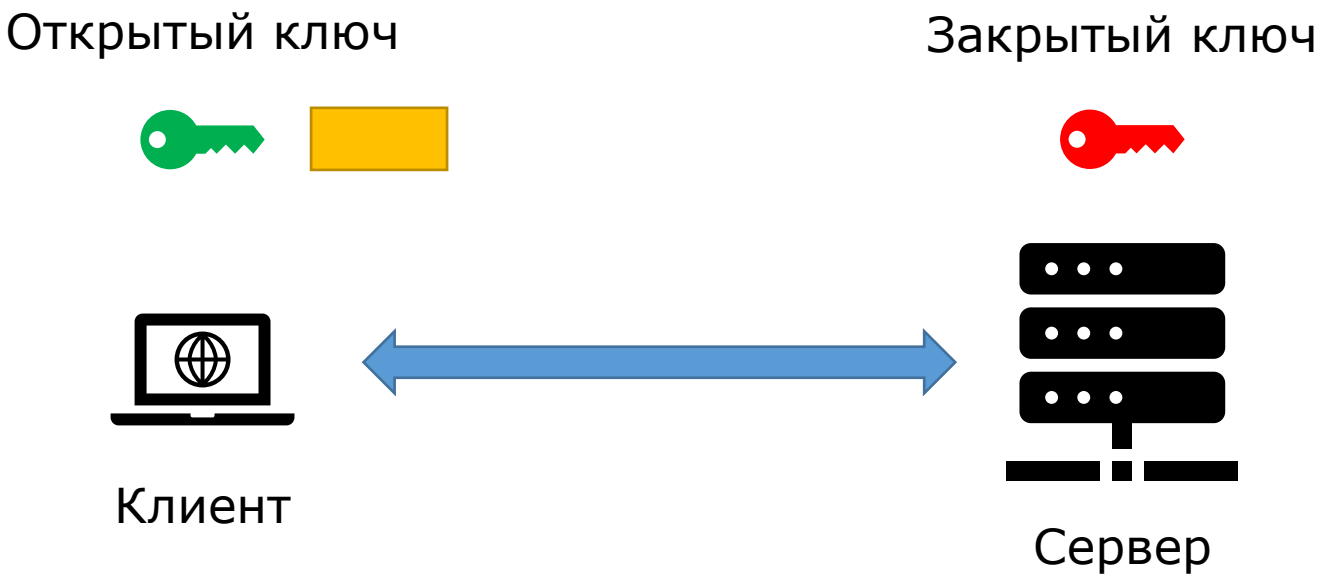
# Аутентификация в TLS/SSL

TLS/SSL – протоколы безопасной передачи данных по небезопасной сети:

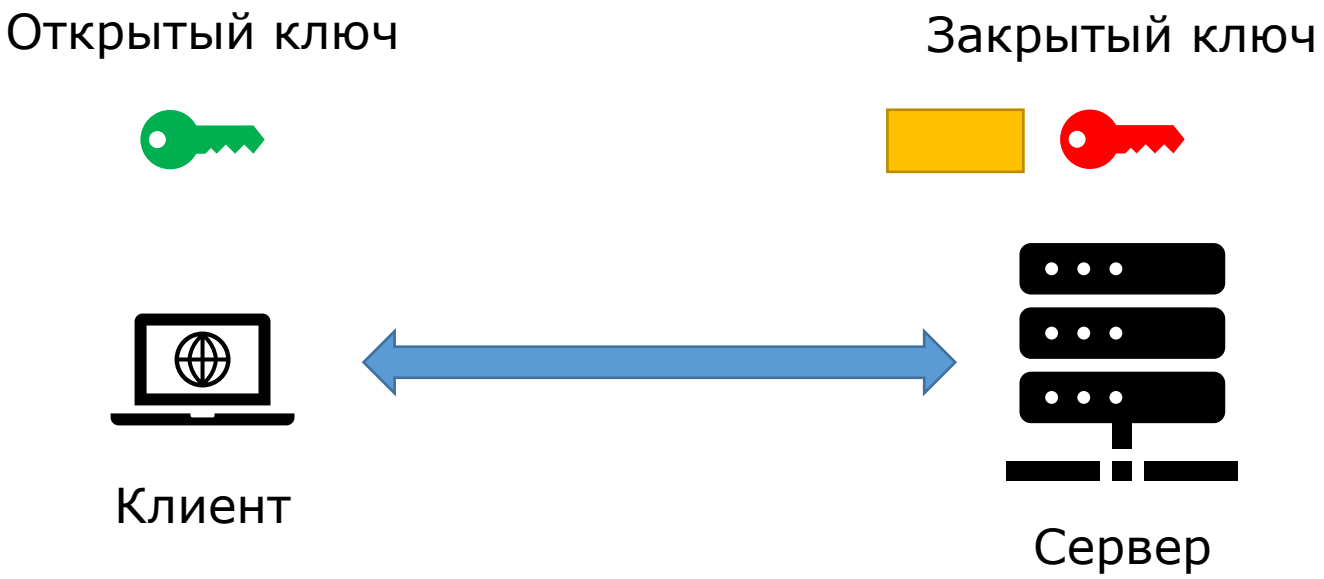
- Приватность
- Целостность
- Аутентификация



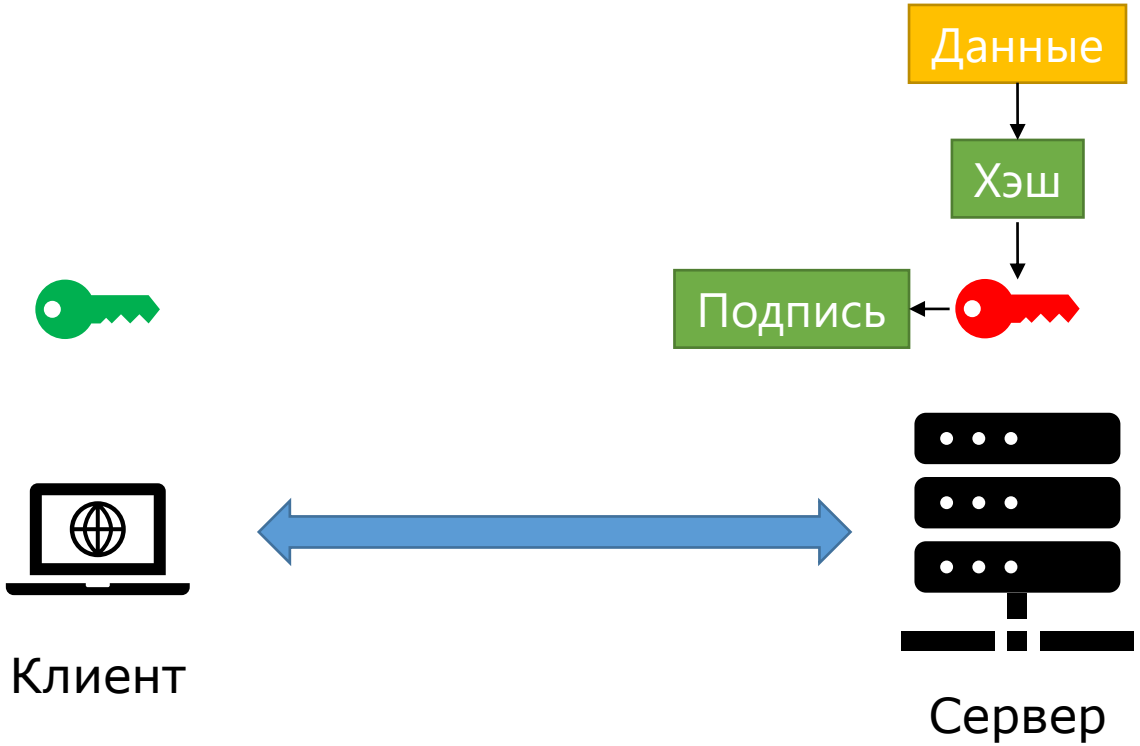
# Асимметричное шифрование



# Электронная подпись



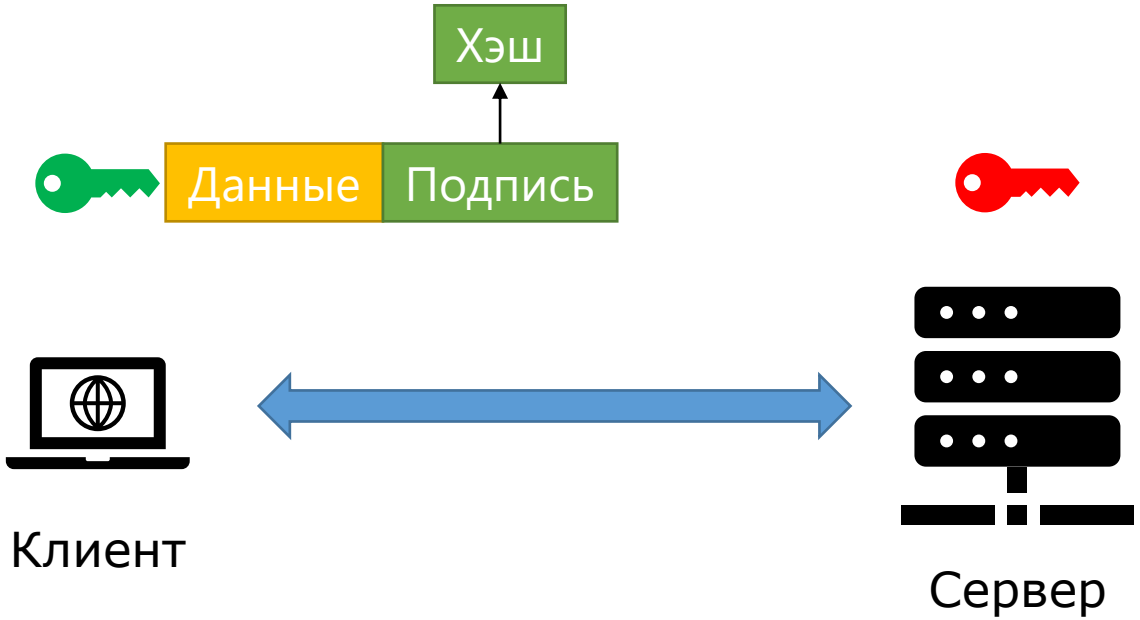
# Электронная подпись



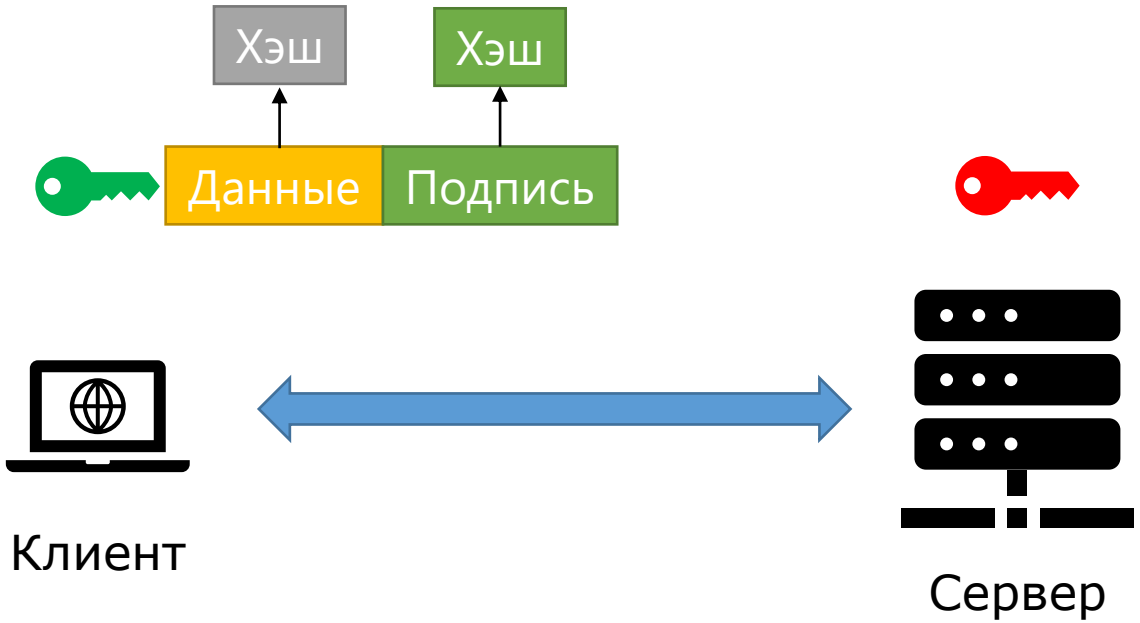
# Электронная подпись

# Электронная подпись

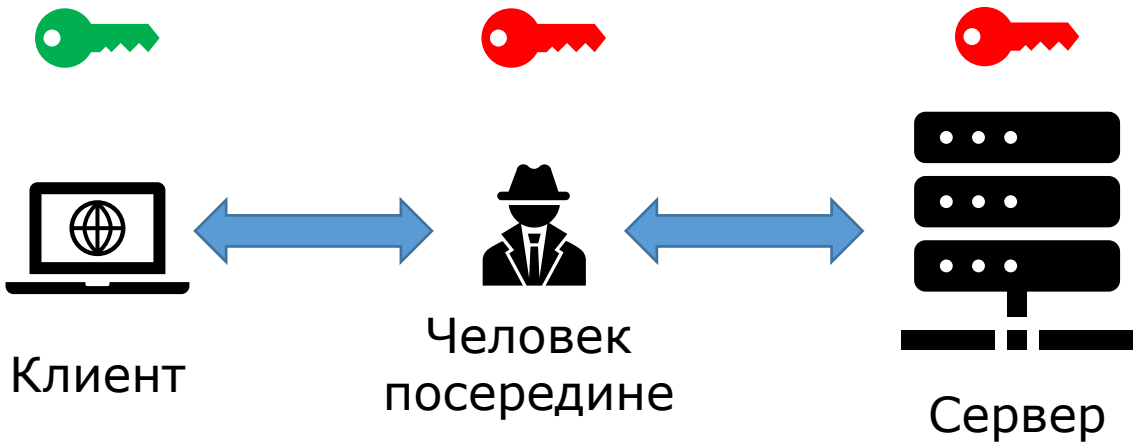
# Электронная подпись



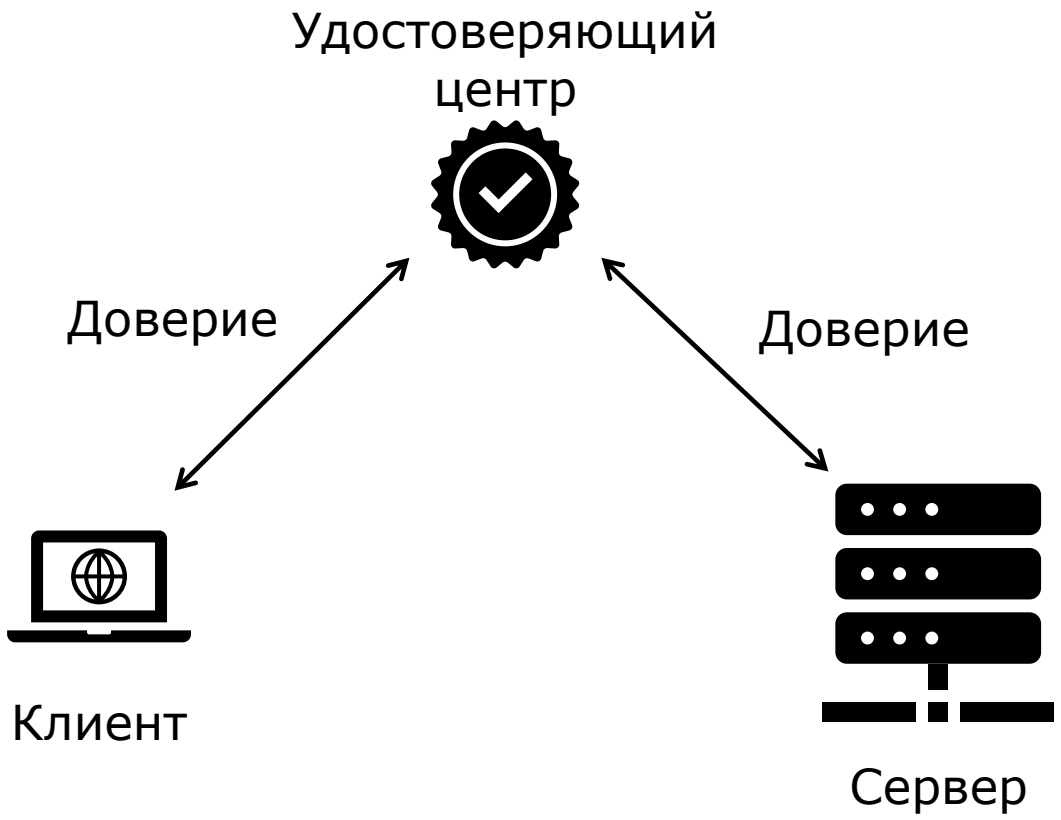
# Электронная подпись



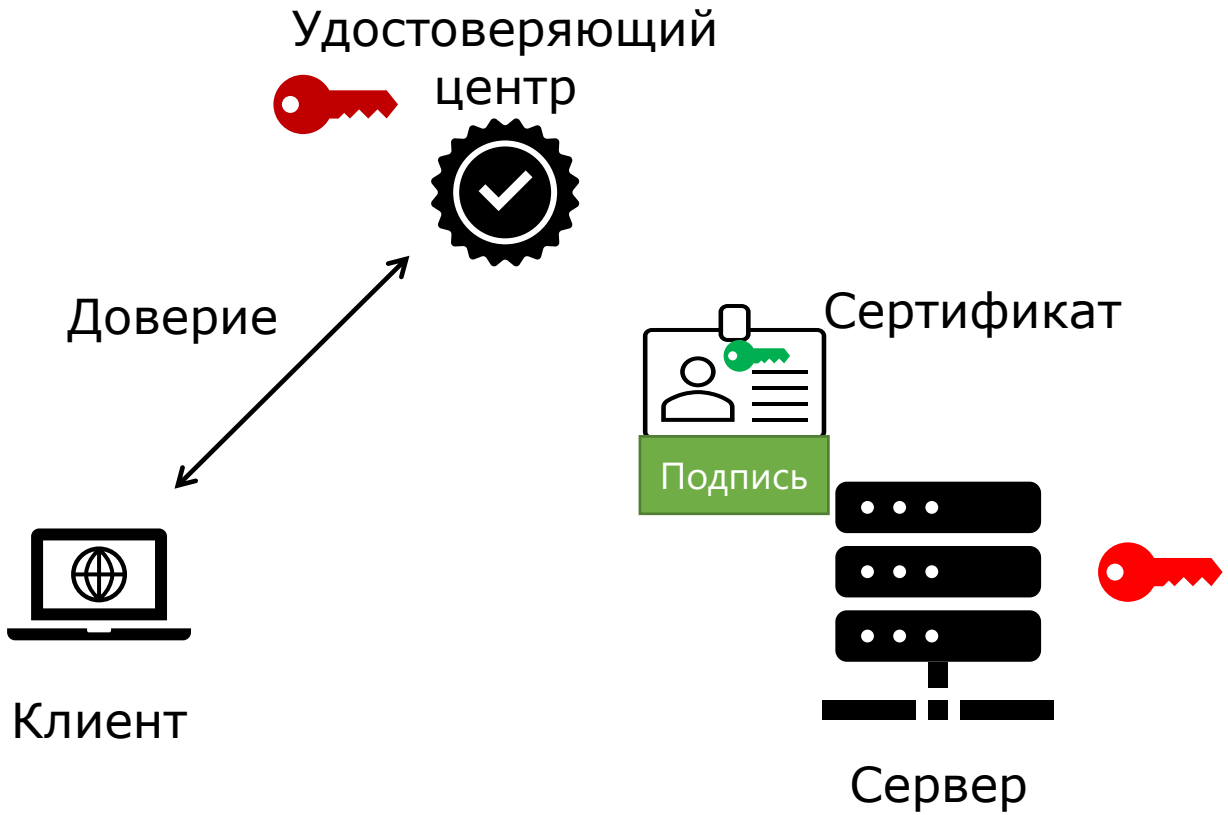
# Кому принадлежит открытый ключ?



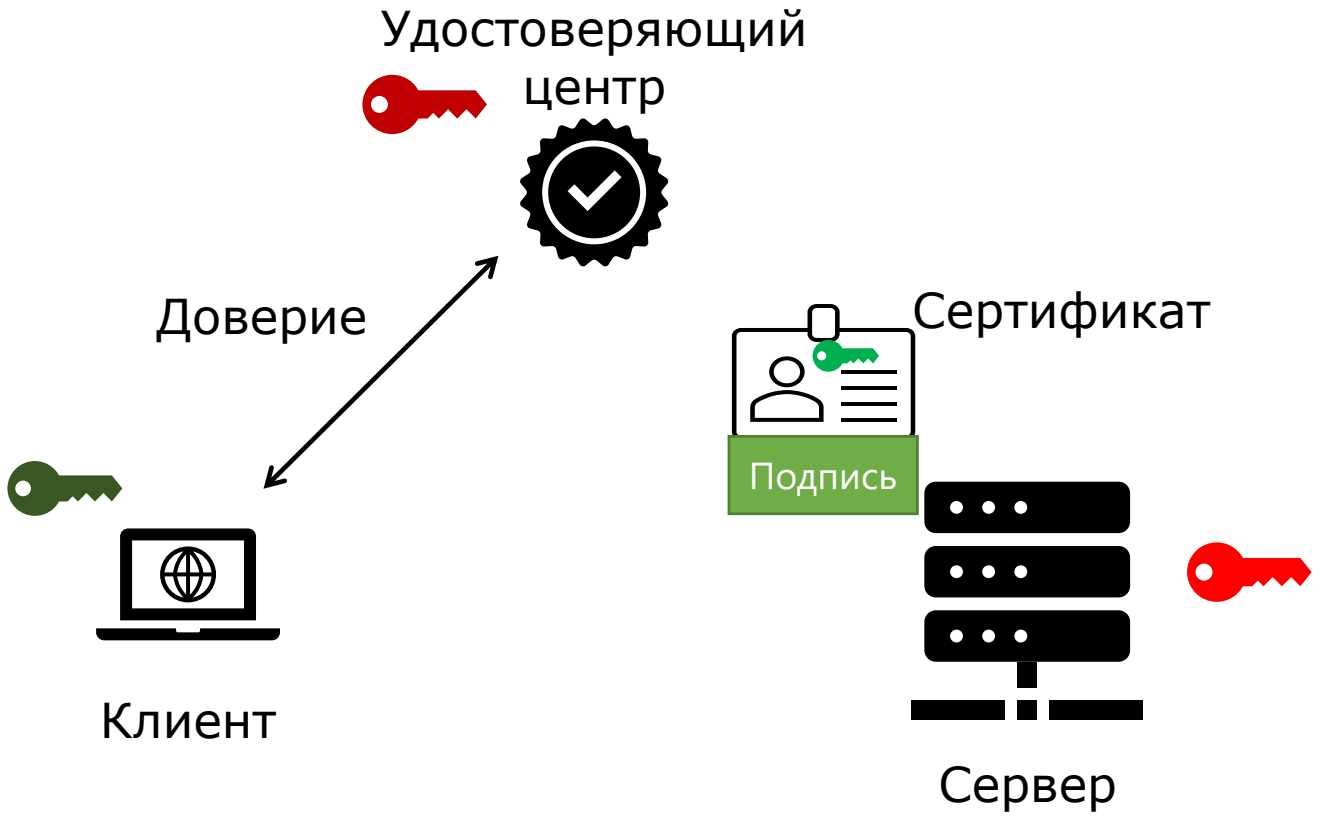
# Инфраструктура открытых ключей



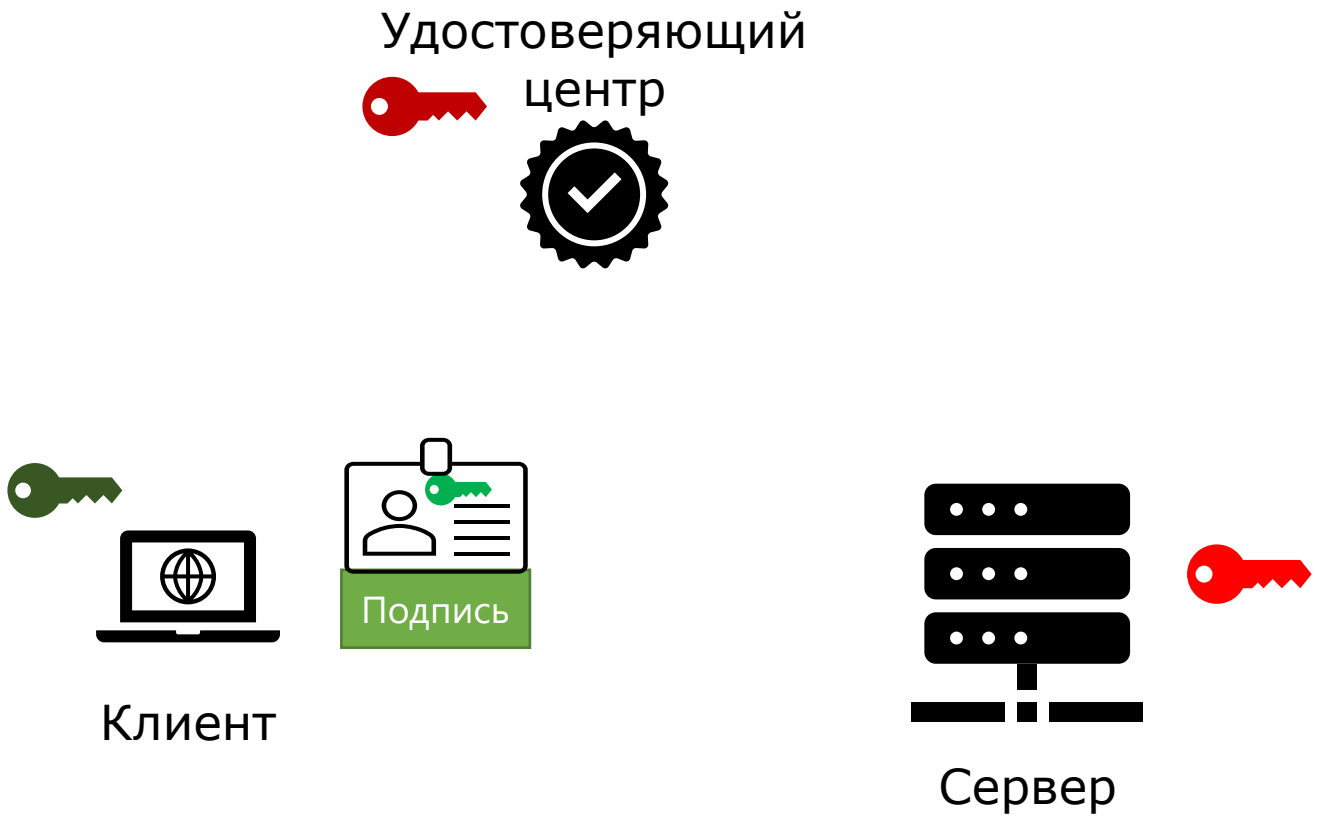
# Сертификаты



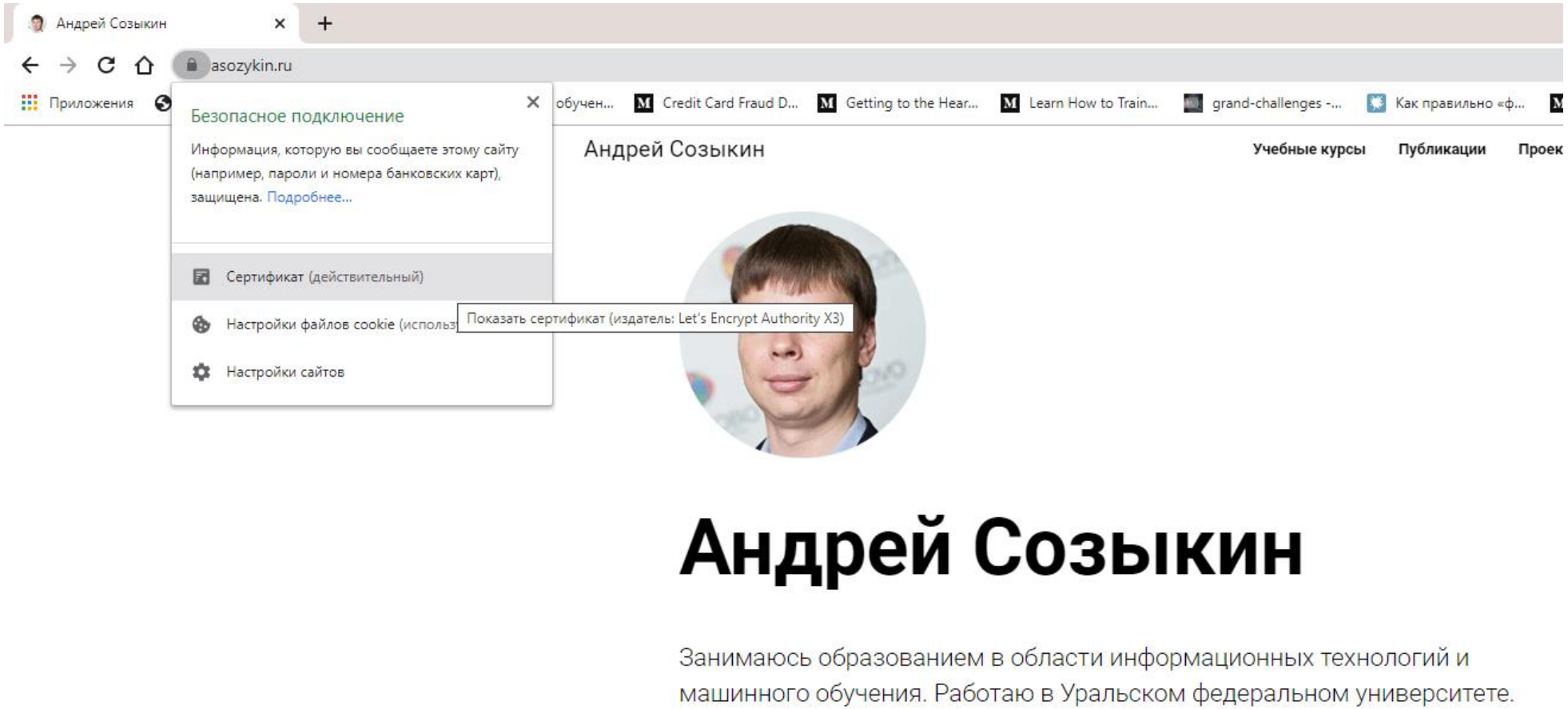
# Сертификаты



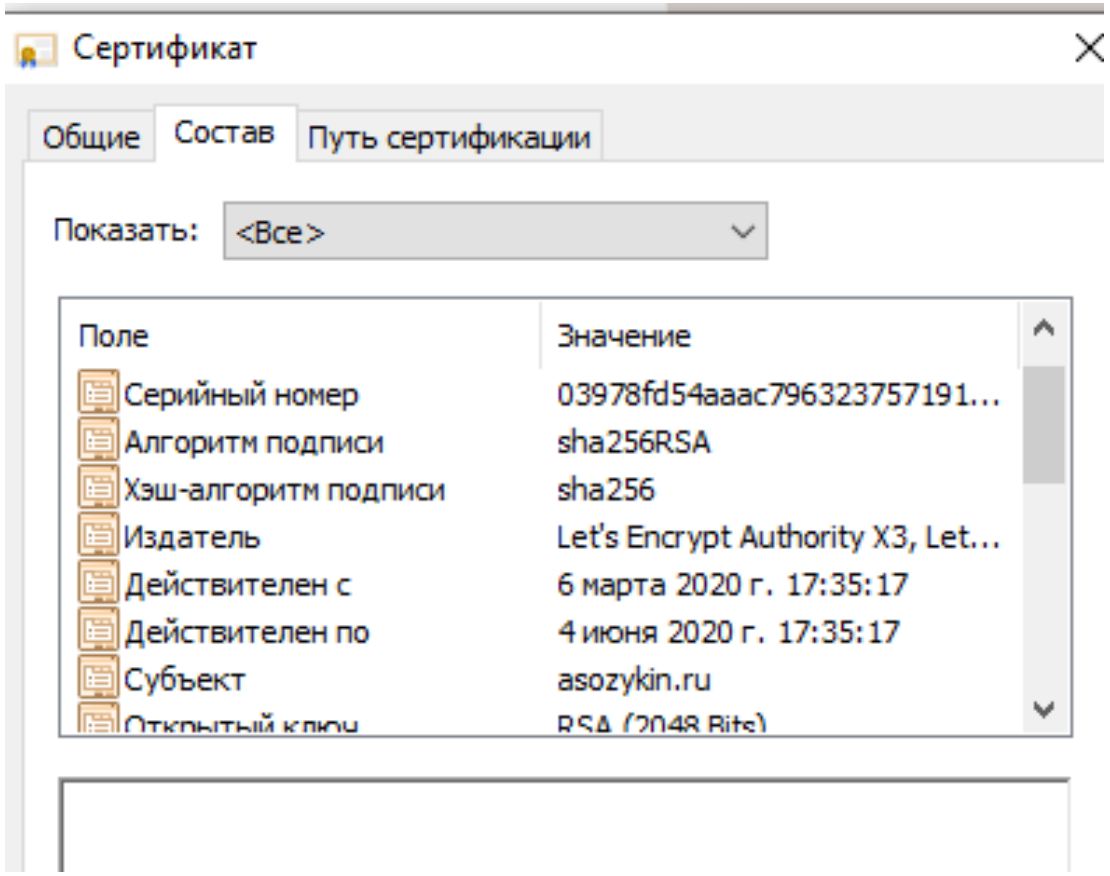
# Сертификаты



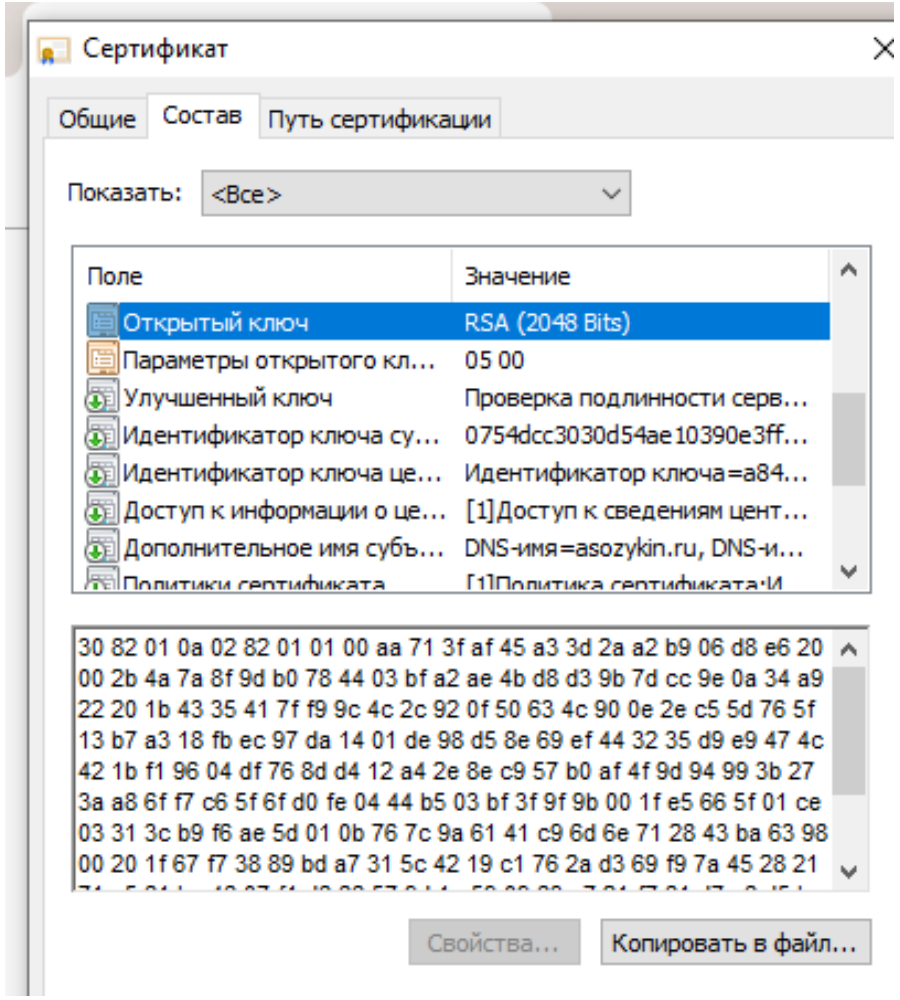
# Сертификаты



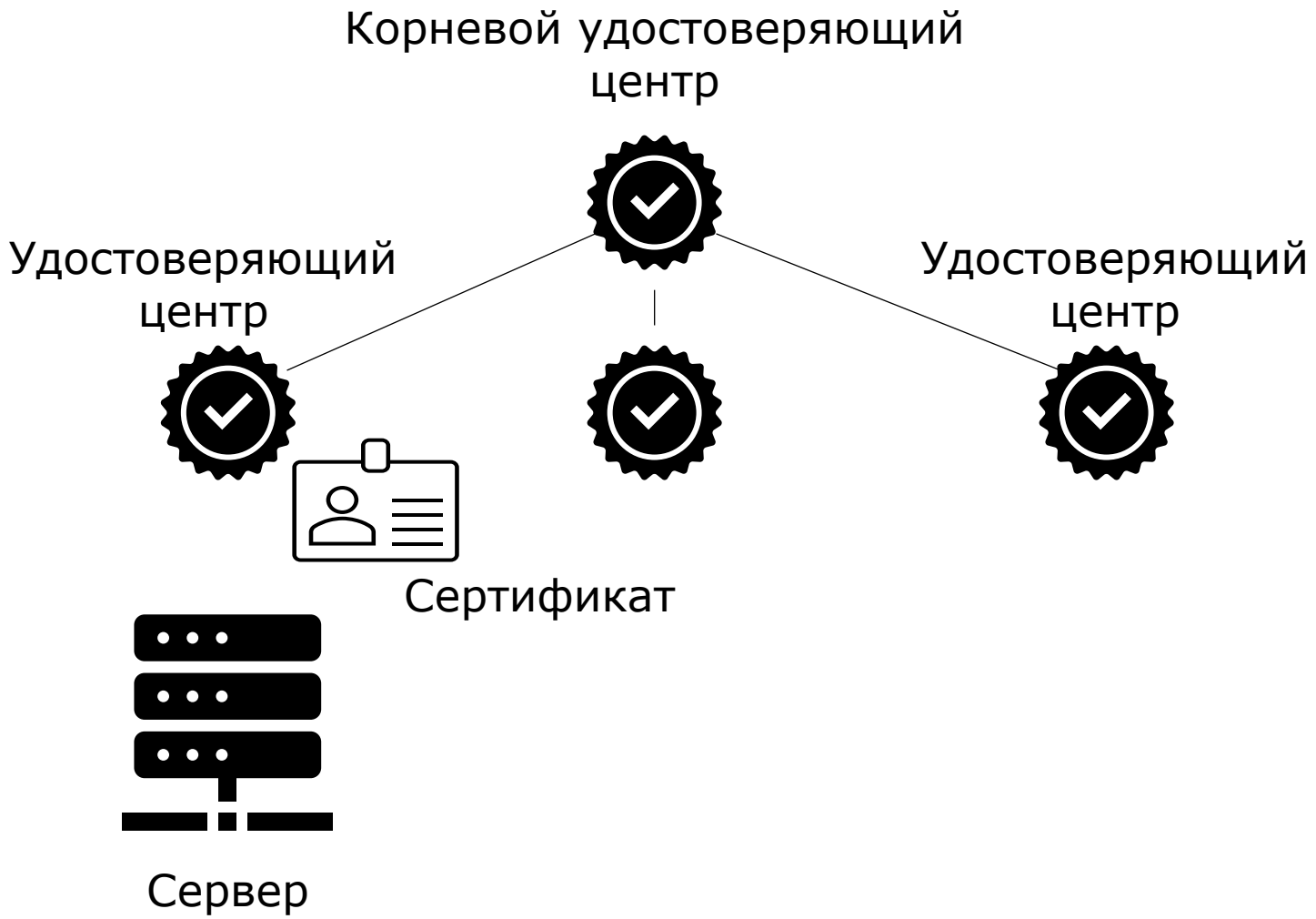
# Сертификаты



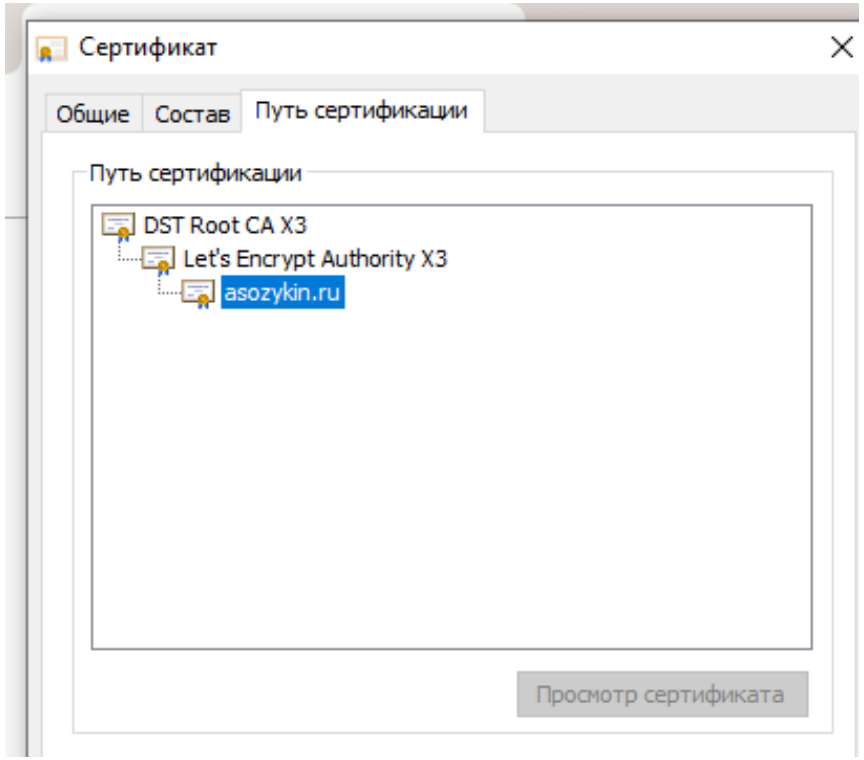
# Сертификаты



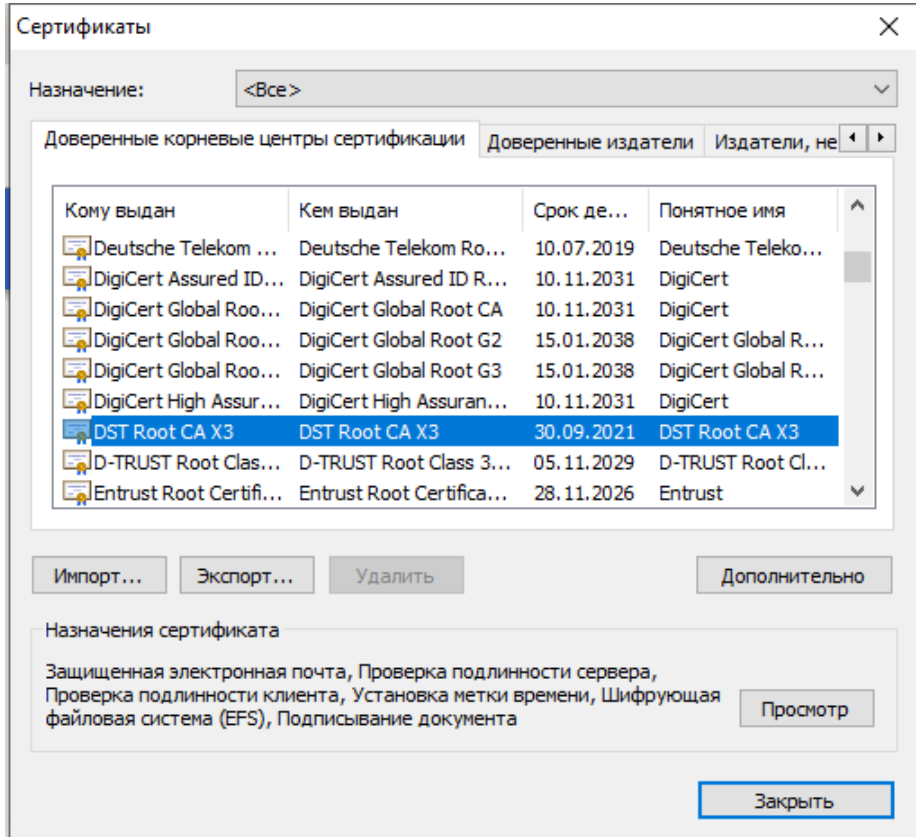
# Инфраструктура открытых ключей



# Путь сертификации

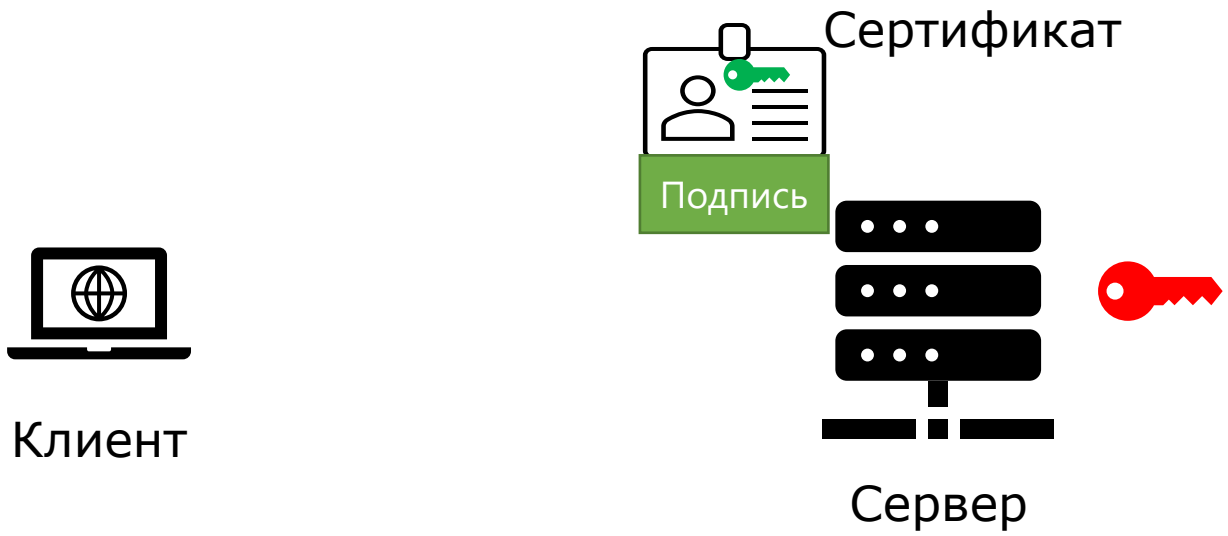


# Хранилище сертификатов

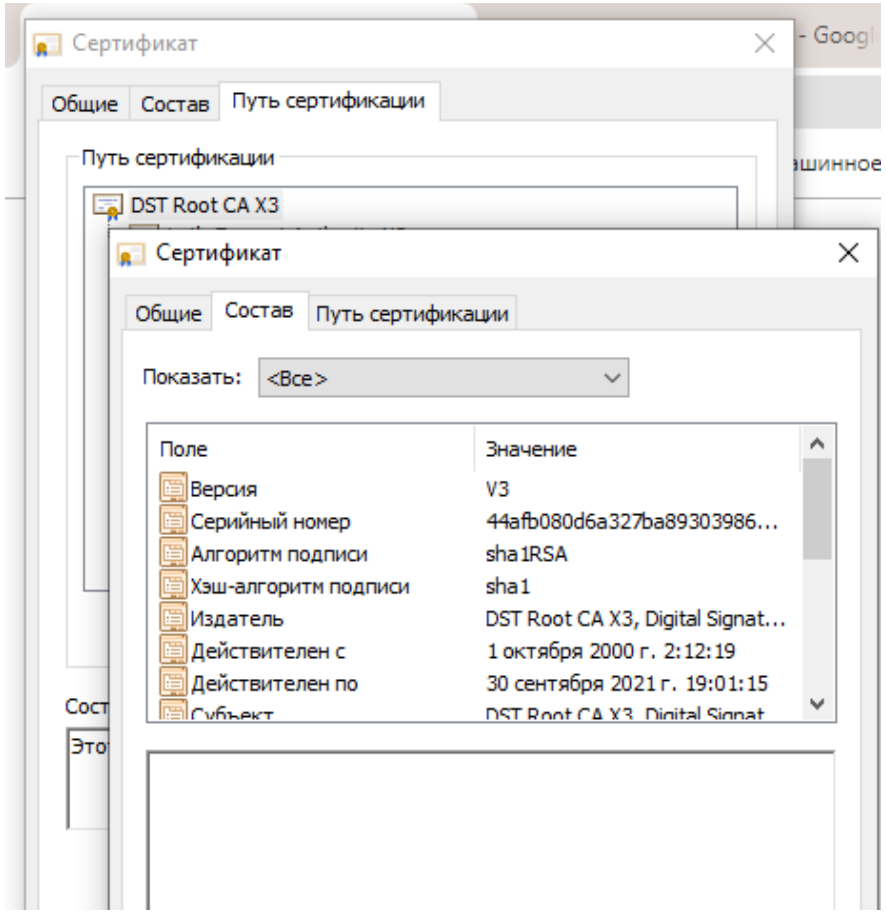


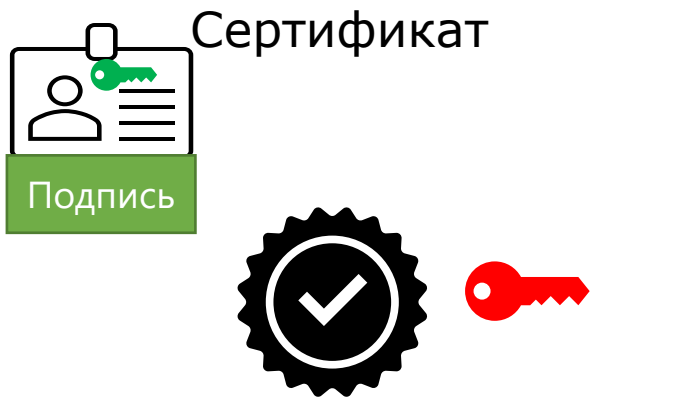

Chrome -> Настройки –> Конфиденциальность и безопасность -> Ещё –> Настроить сертификаты

# Самоподписанный сертификат



# Самоподписанный сертификат




Корневой удостоверяющий центр

# Набор шифров TLS/SSL

Алгоритм цифровой подписи в сертификате:

- RSA
- DSA (Digital Signature Algorithm)

Алгоритм обмена ключами:

- RSA
- Диффи-Хеллмана

Алгоритм симметричного шифрования:

- AES
- 3DES

Хэш-функция для вычисления MAC:

- MD5 (Message Digest 5)
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

# Итоги

Аутентификация в TLS/SSL:

- Подтверждение подлинности сервера/клиента

Электронная подпись:

- Шифрование с помощью закрытого ключа

Инфраструктура открытого ключа (public key infrastructure):

- Система распространения открытых ключей с помощью удостоверяющих центров (certification authority)

Сертификат:

- Файл с открытым ключом и информацией о сервере, подписанный удостоверяющим центром
- Формат сертификата – X.509