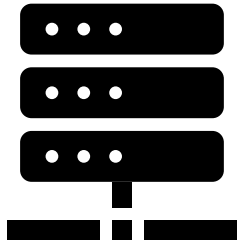
Установка соединения в TLS

Компьютерные сети

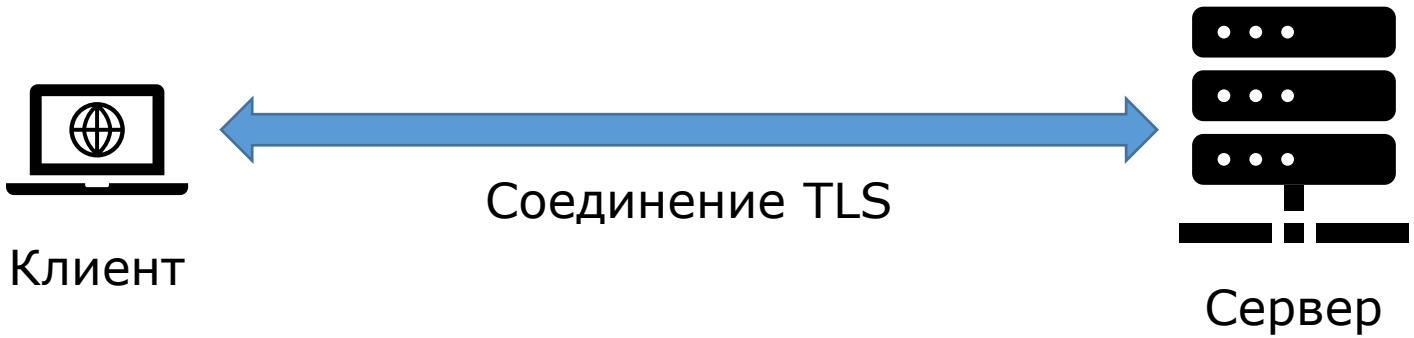
Установка соединения TLS

Клиент



Сервер

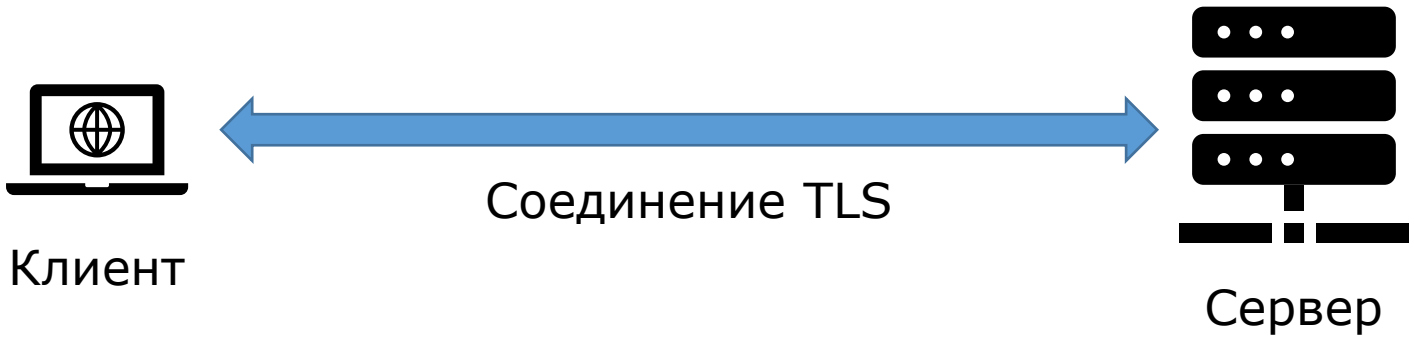
Установка соединения TLS



Установка соединения TLS

Набор шифров TLS:

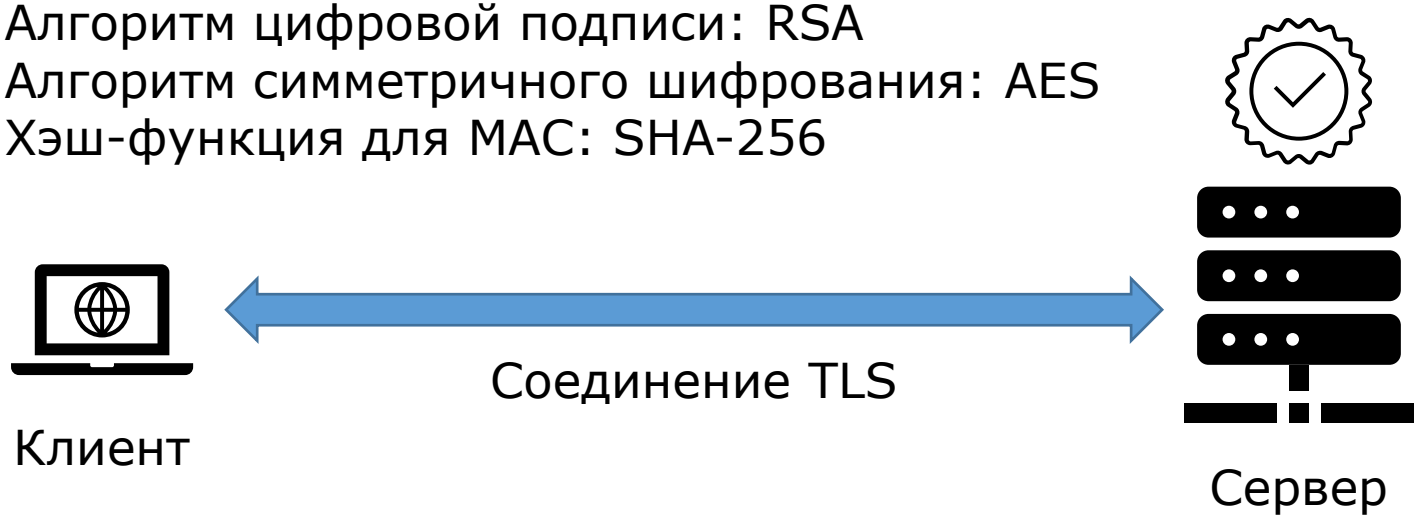
- Алгоритм обмена ключами: Диффи-Хеллман
- Алгоритм цифровой подписи: RSA
- Алгоритм симметричного шифрования: AES
- Хэш-функция для MAC: SHA-256



Установка соединения TLS

Набор шифров TLS:

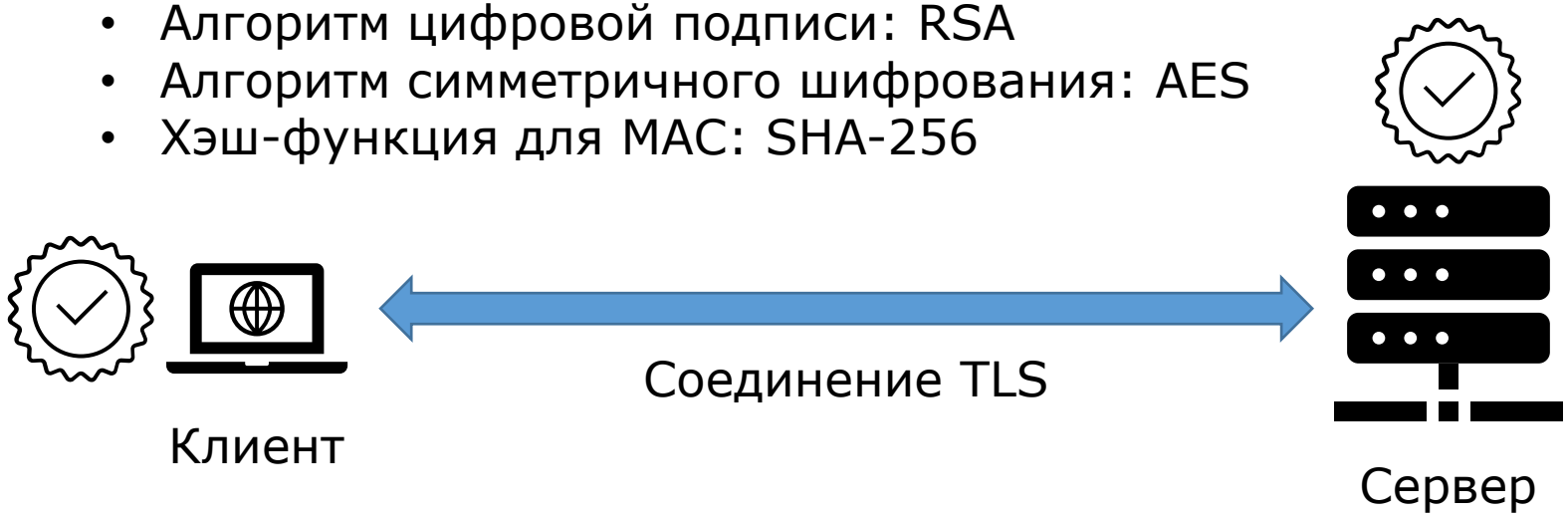
- Алгоритм обмена ключами: Диффи-Хеллман
- Алгоритм цифровой подписи: RSA
- Алгоритм симметричного шифрования: AES
- Хэш-функция для MAC: SHA-256



Установка соединения TLS

Набор шифров TLS:

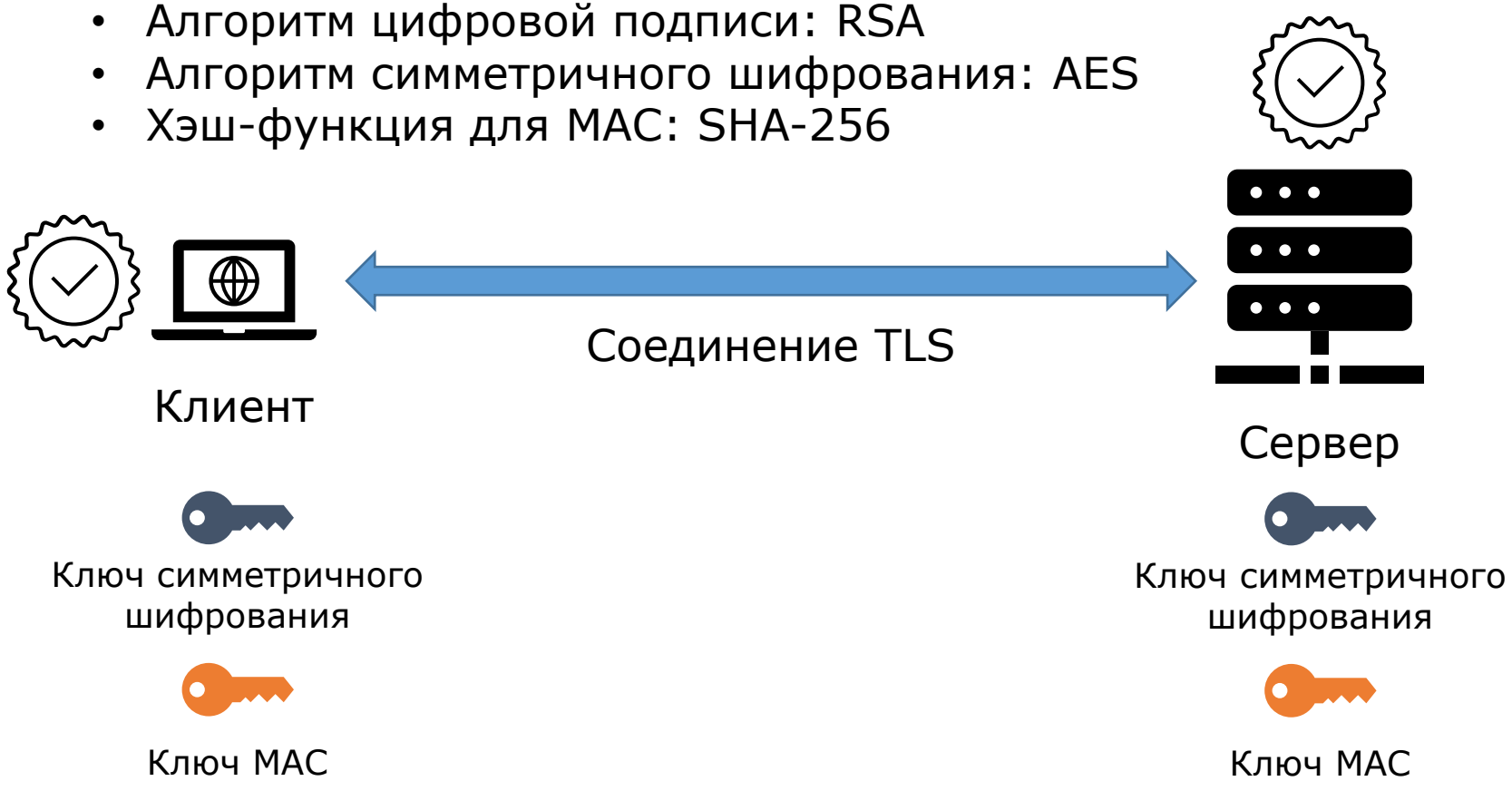
- Алгоритм обмена ключами: Диффи-Хеллман
- Алгоритм цифровой подписи: RSA
- Алгоритм симметричного шифрования: AES
- Хэш-функция для MAC: SHA-256



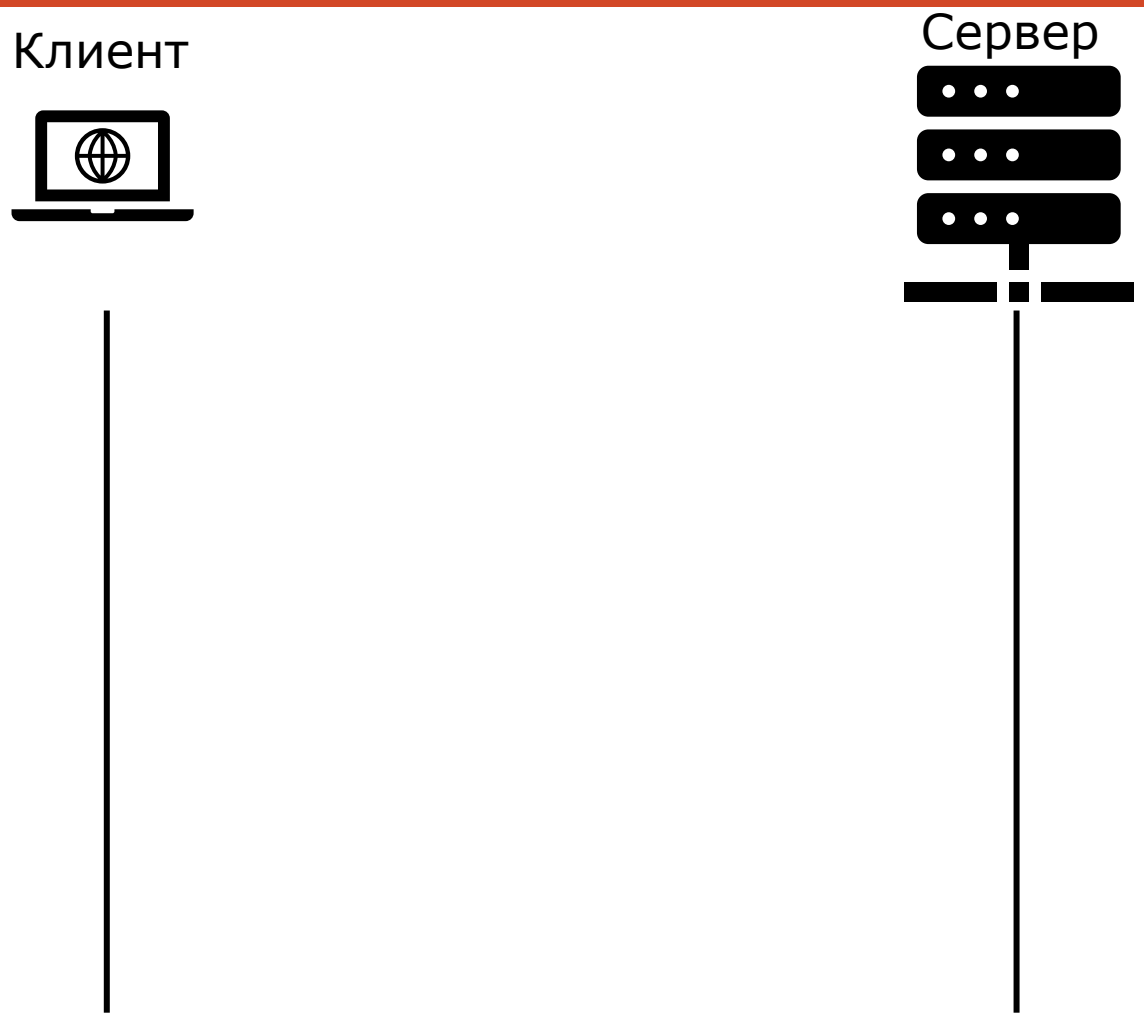
Установка соединения TLS

Набор шифров TLS:

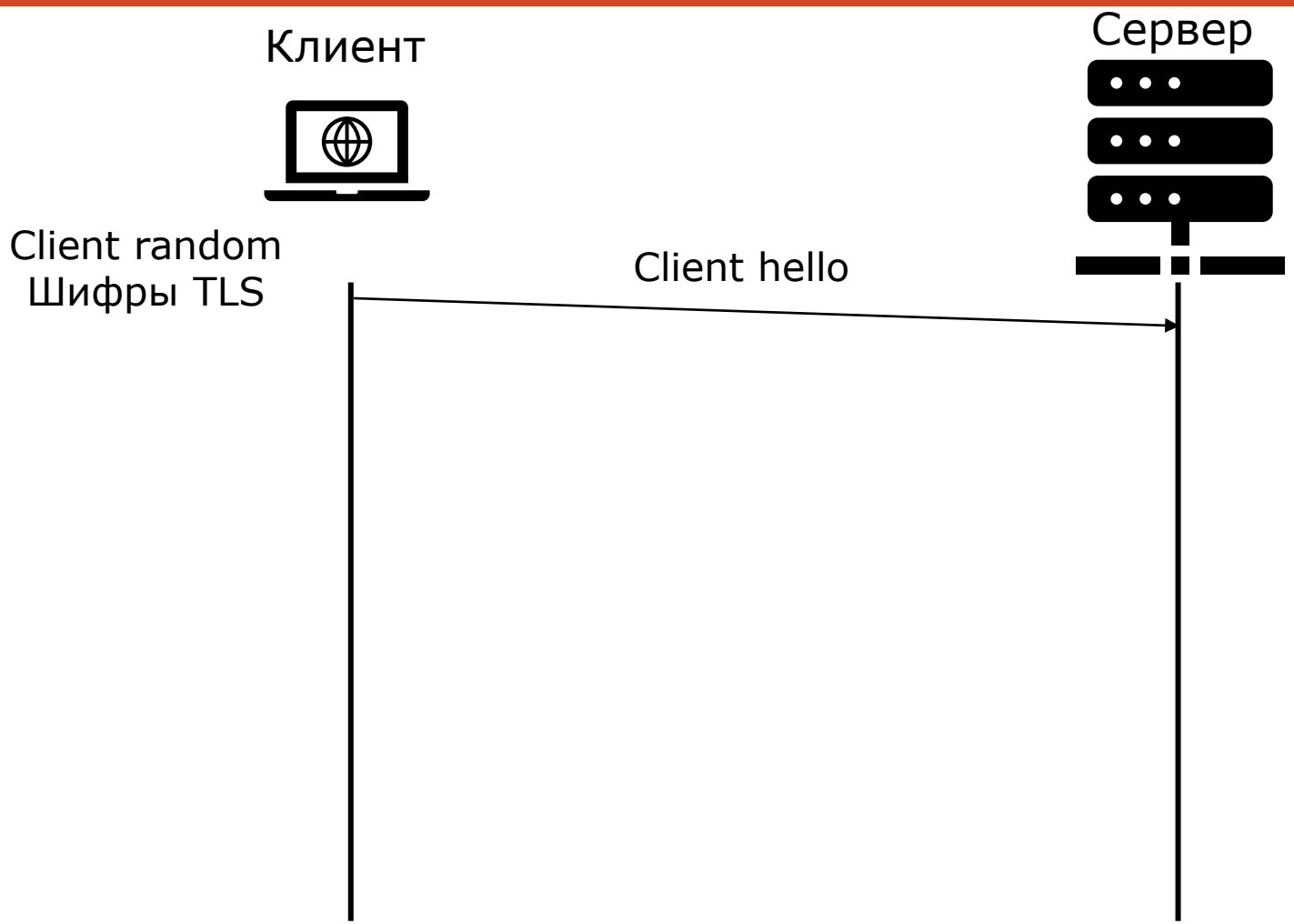
- Алгоритм обмена ключами: Диффи-Хеллман
- Алгоритм цифровой подписи: RSA
- Алгоритм симметричного шифрования: AES
- Хэш-функция для MAC: SHA-256



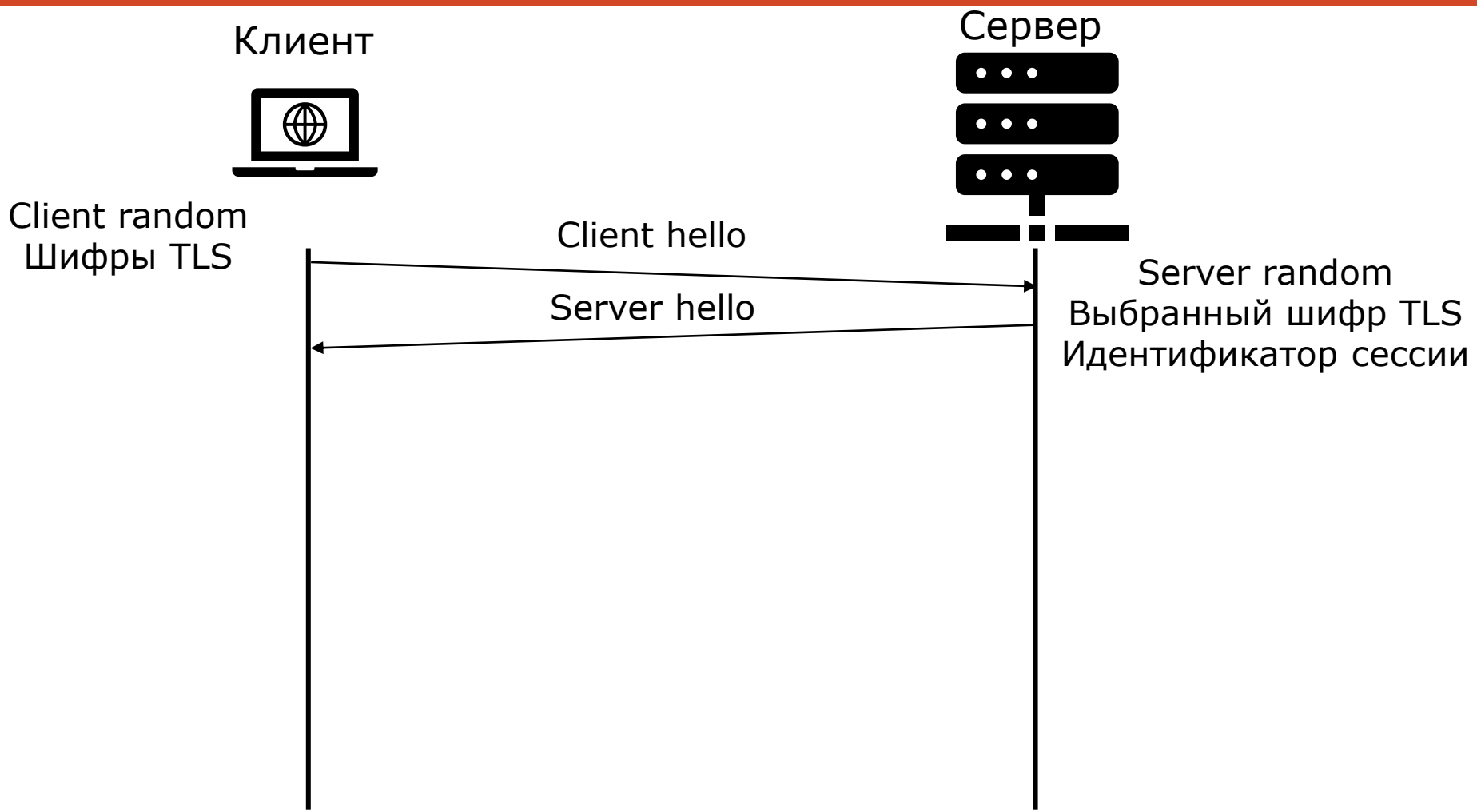
Установка соединения TLS



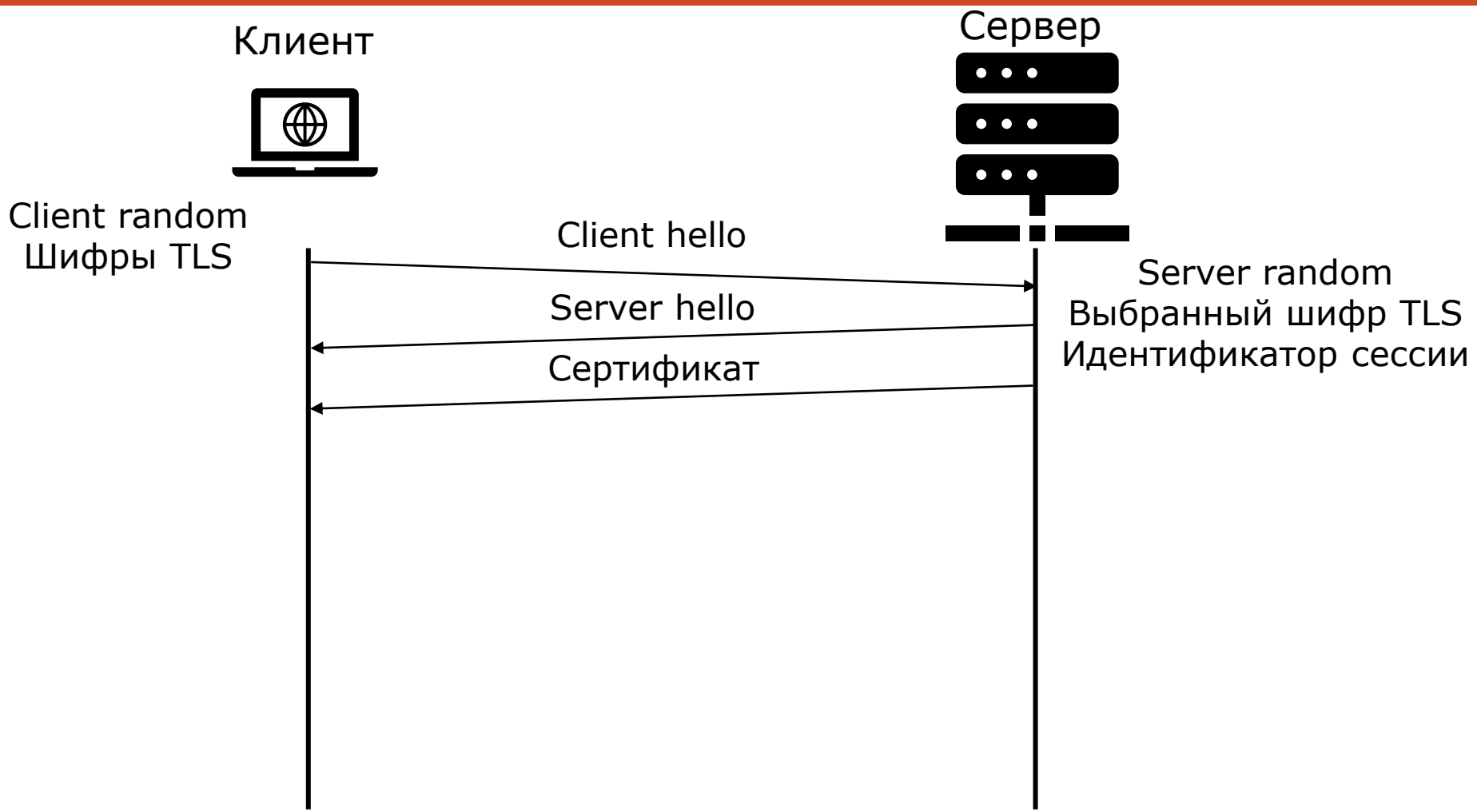
Установка соединения TLS



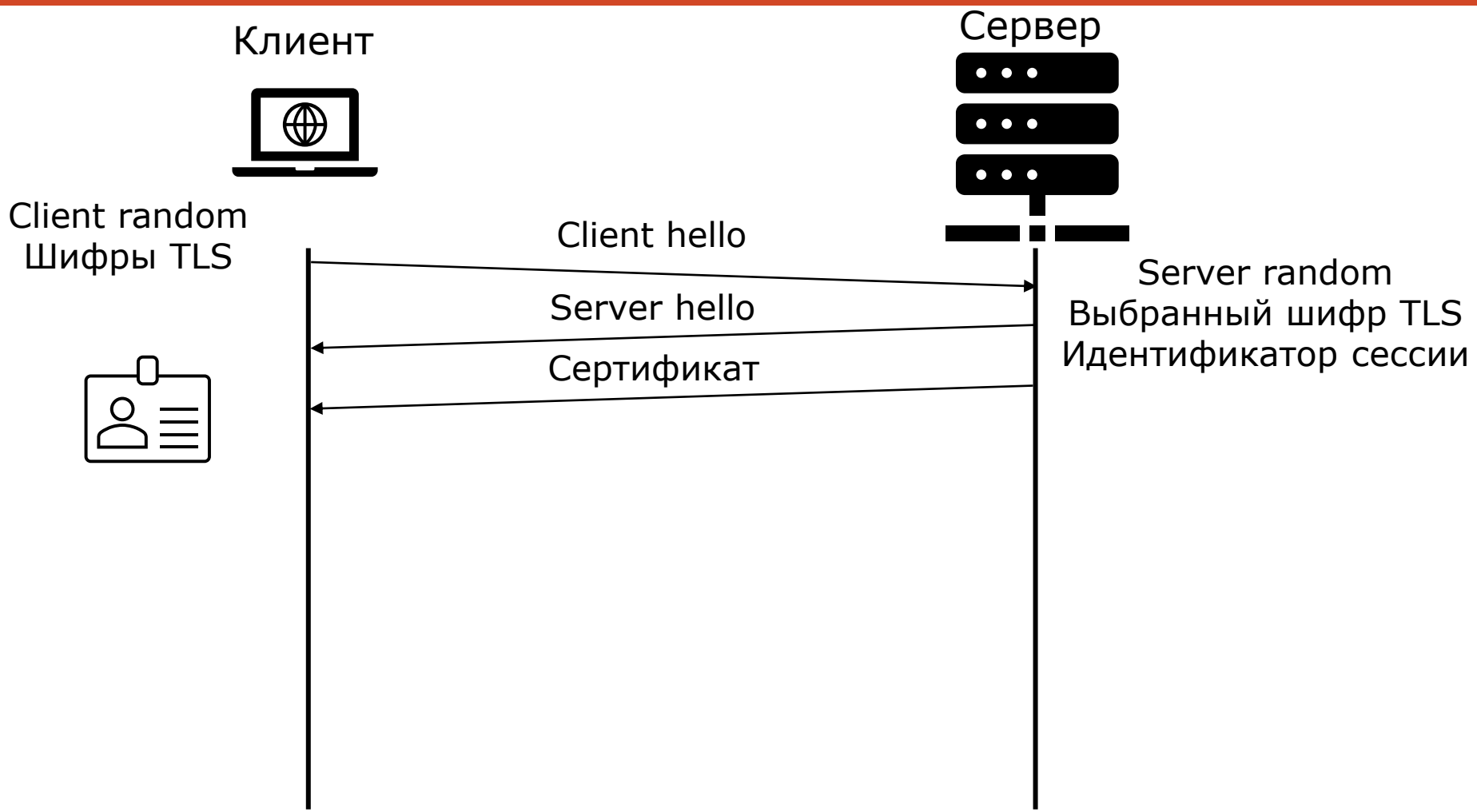
Установка соединения TLS



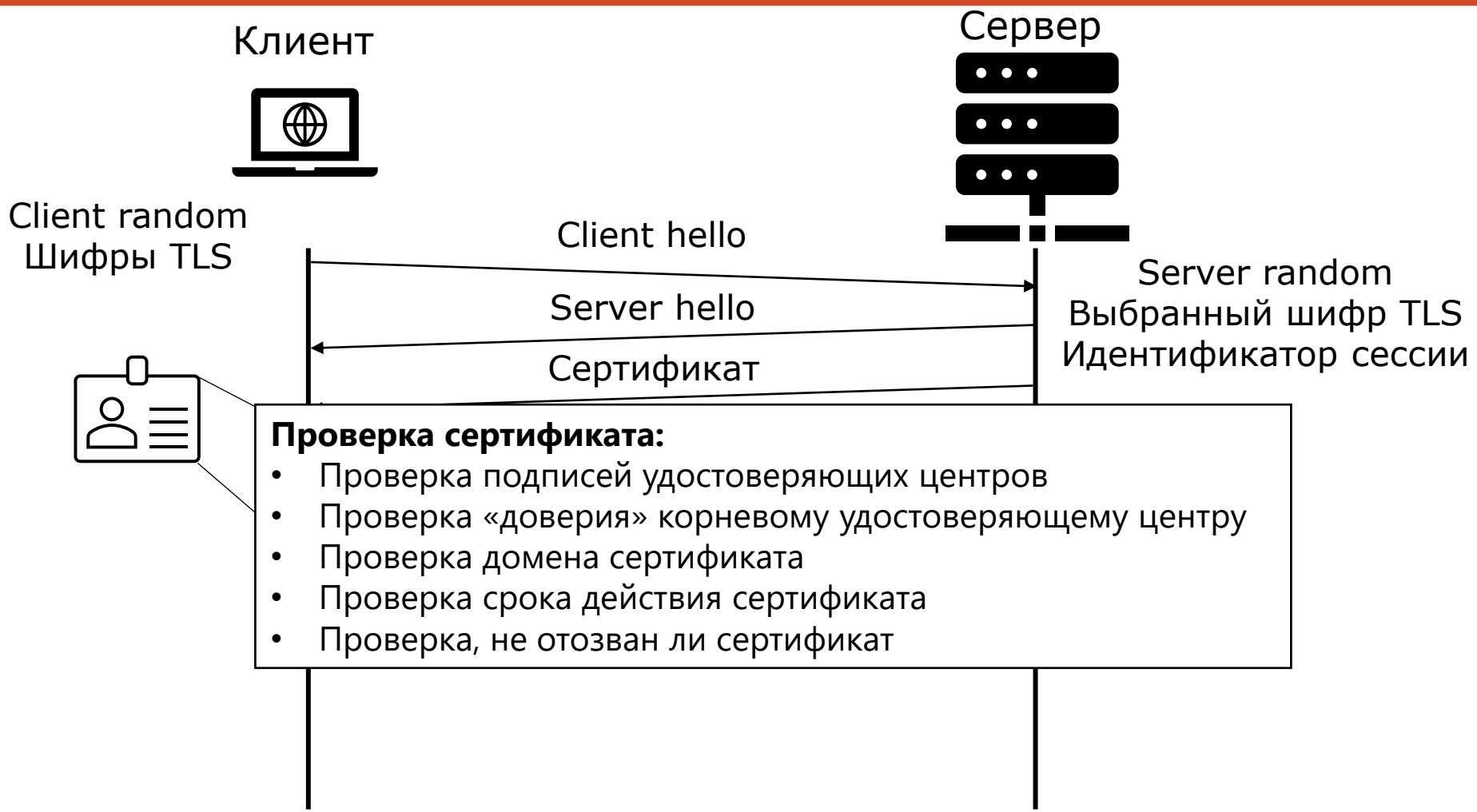
Установка соединения TLS



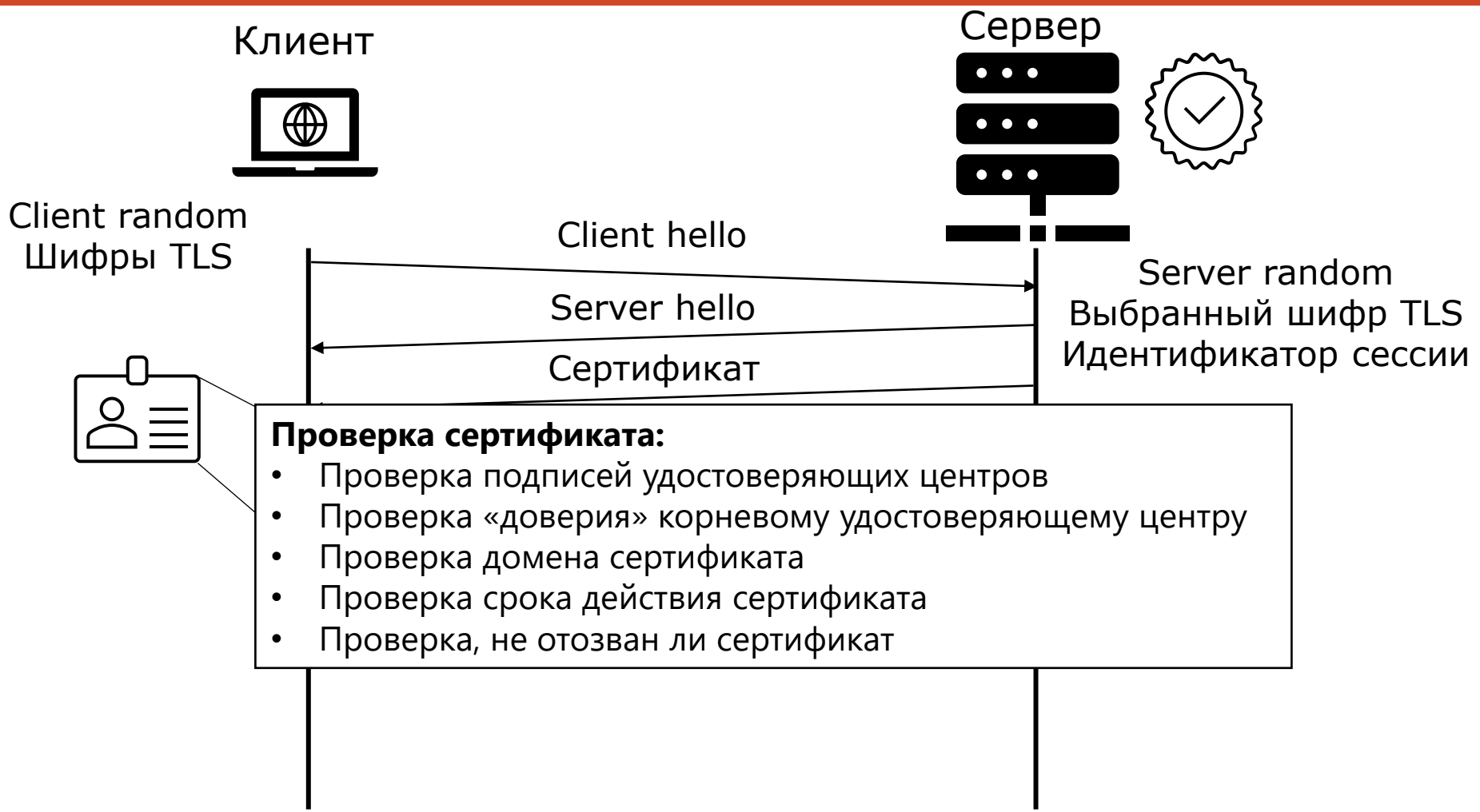
Установка соединения TLS



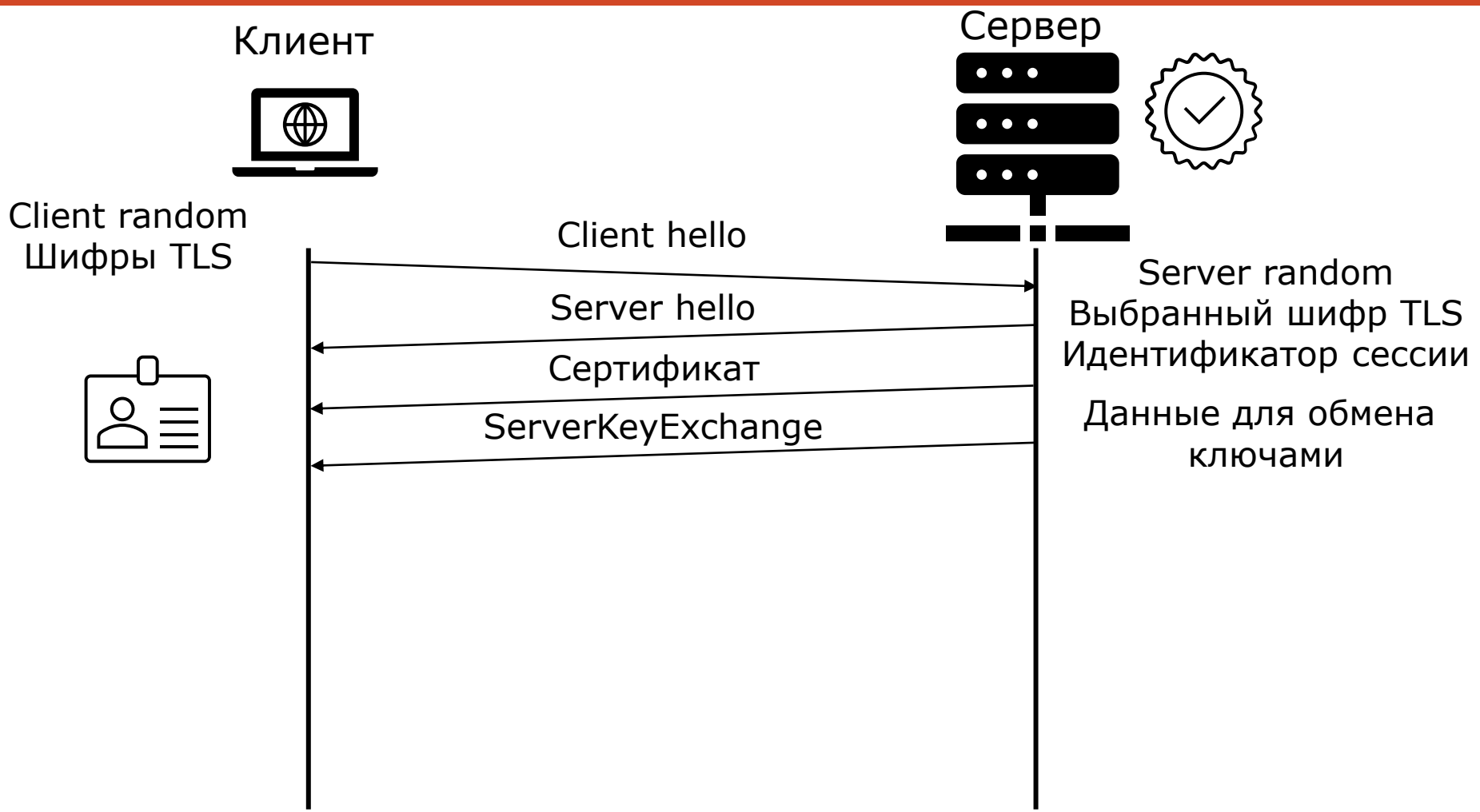
Проверка сертификата сервера



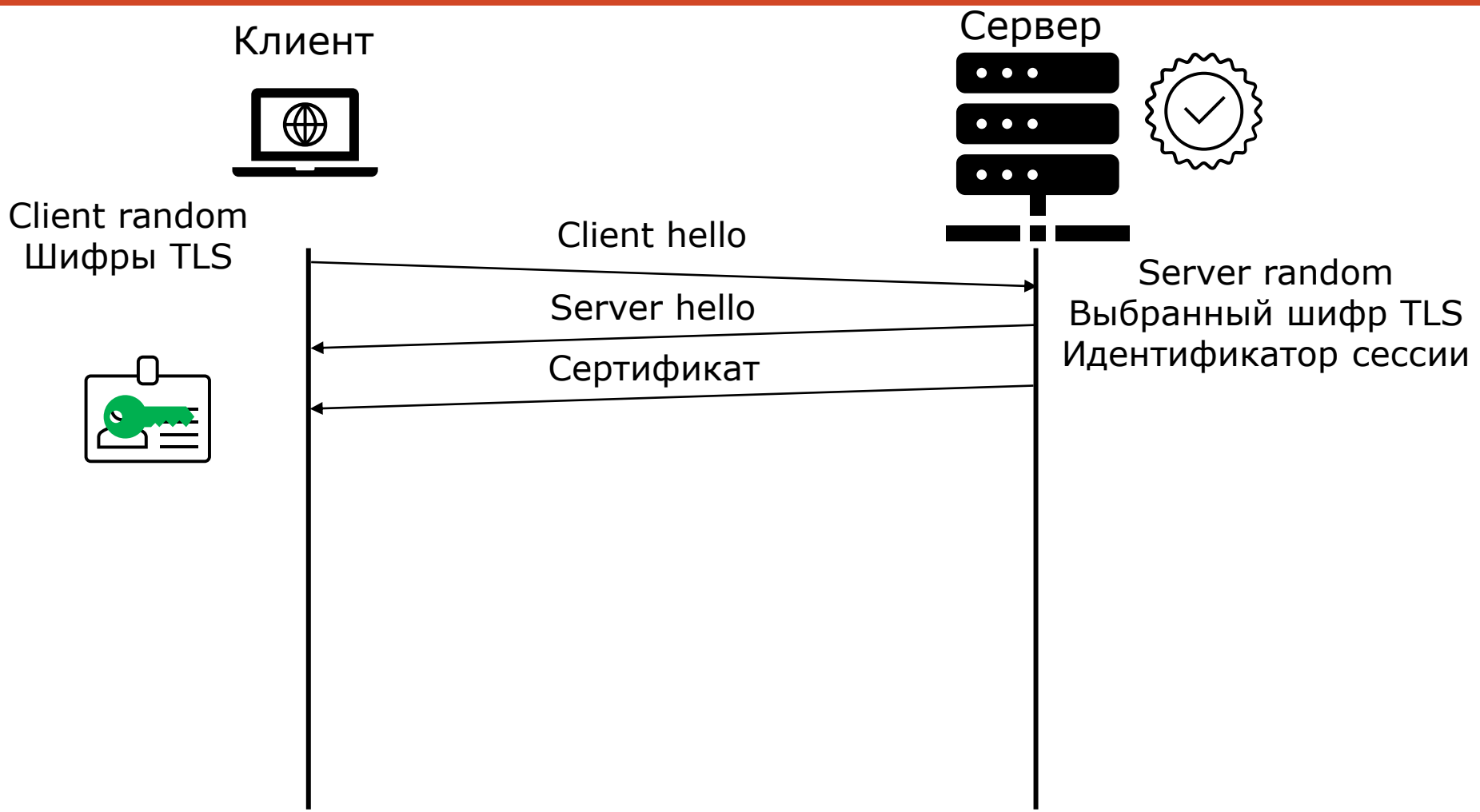
Проверка сертификата сервера



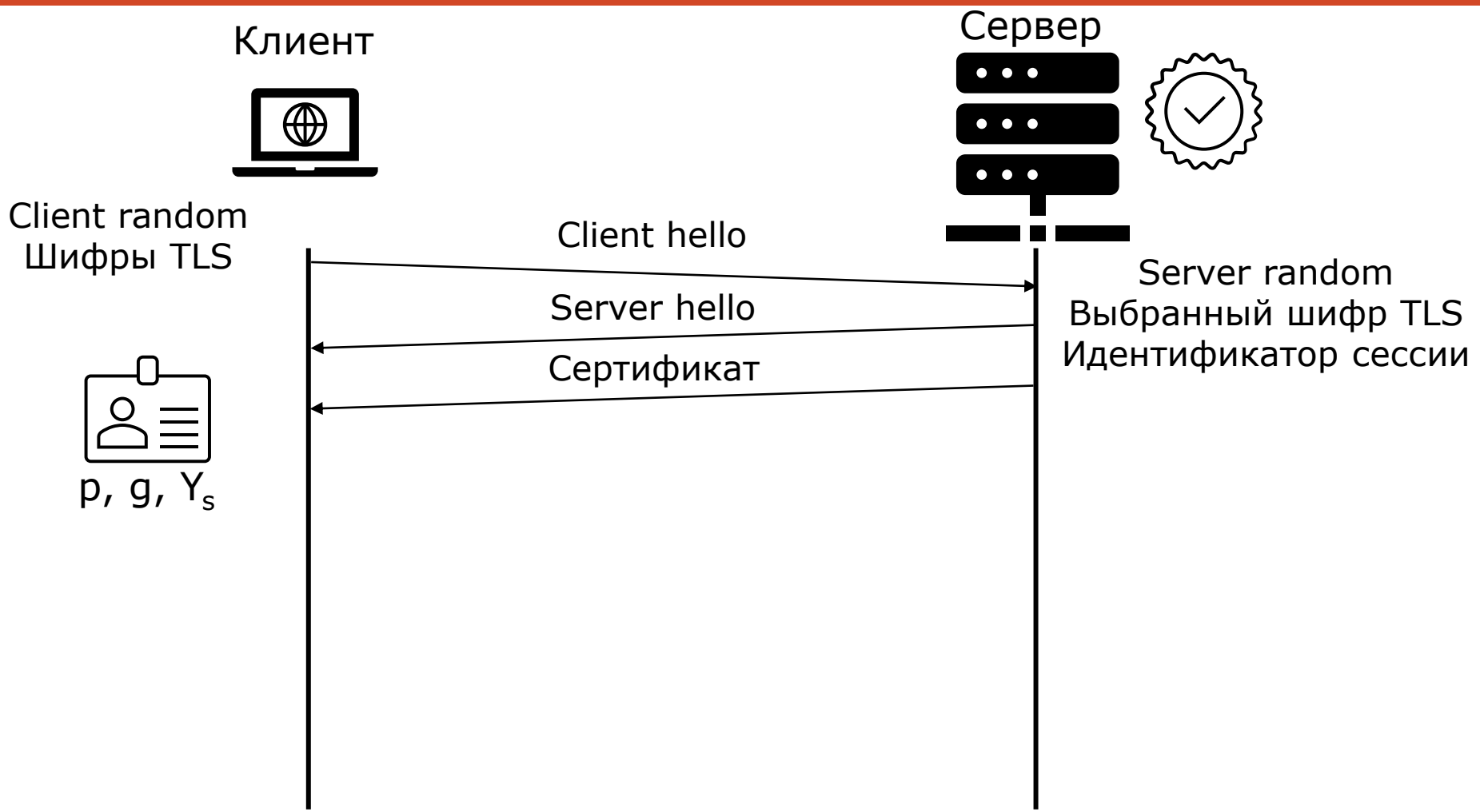
Установка соединения TLS



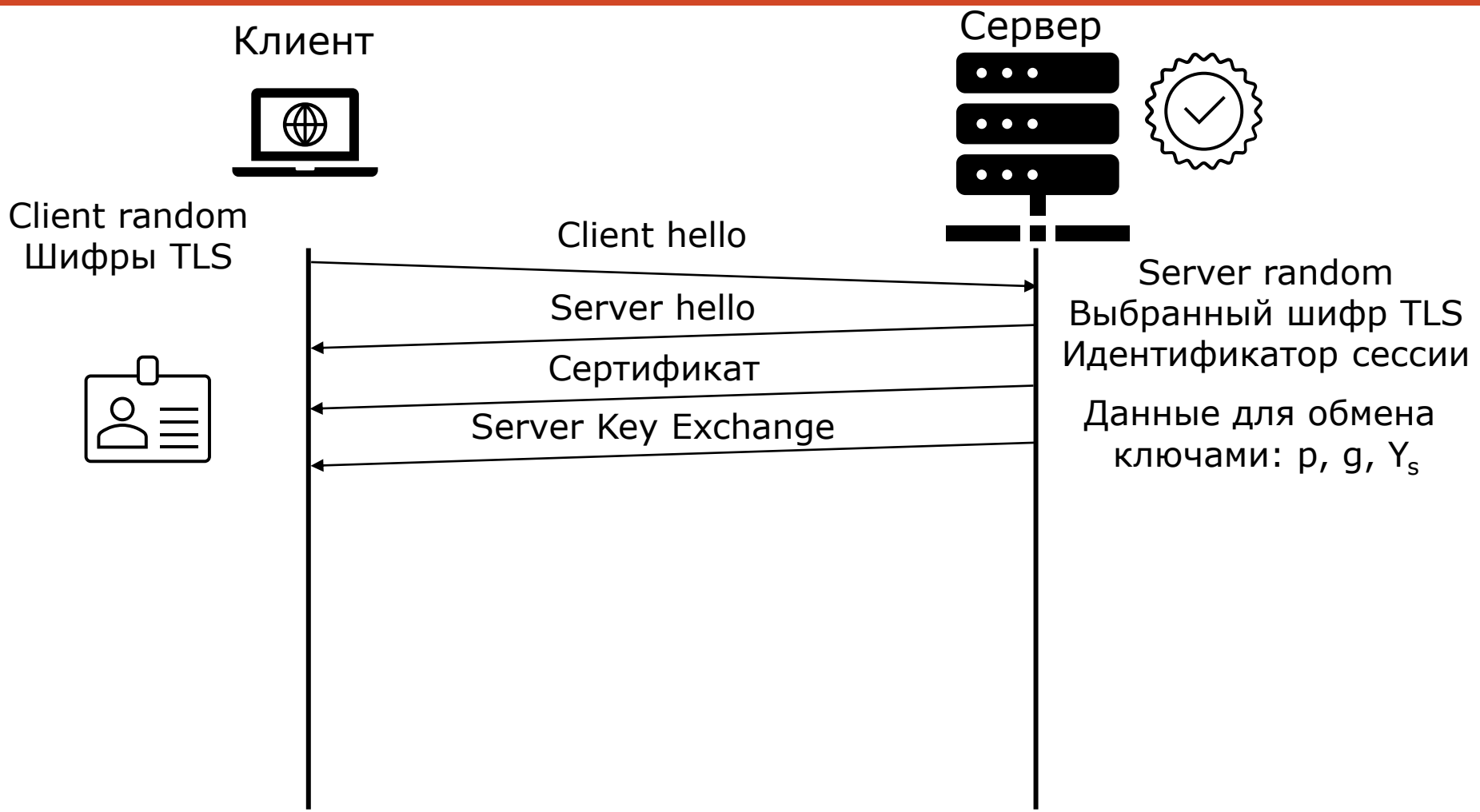
Обмен ключами: алгоритм RSA



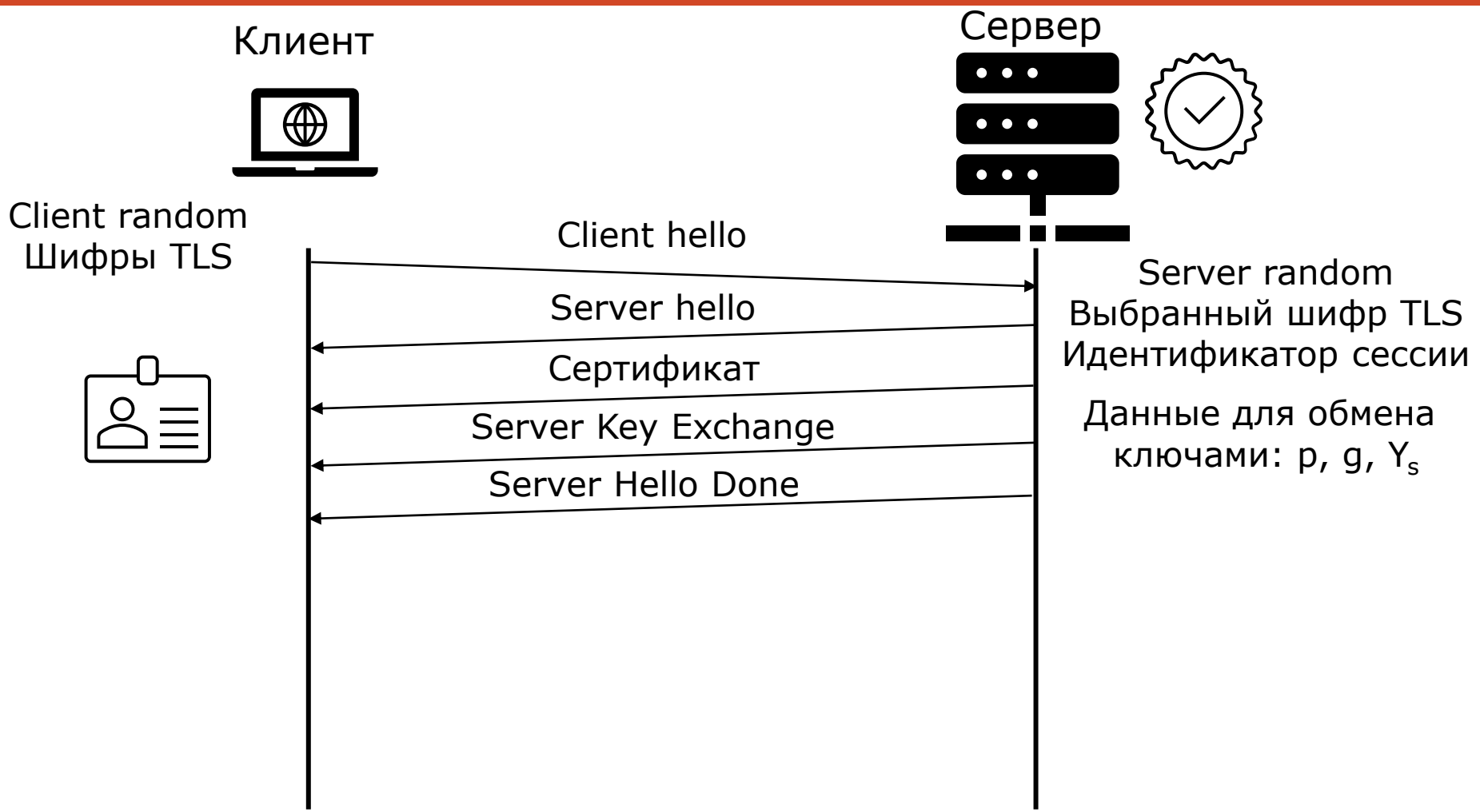
Обмен ключами: статический Диффи-Хеллман



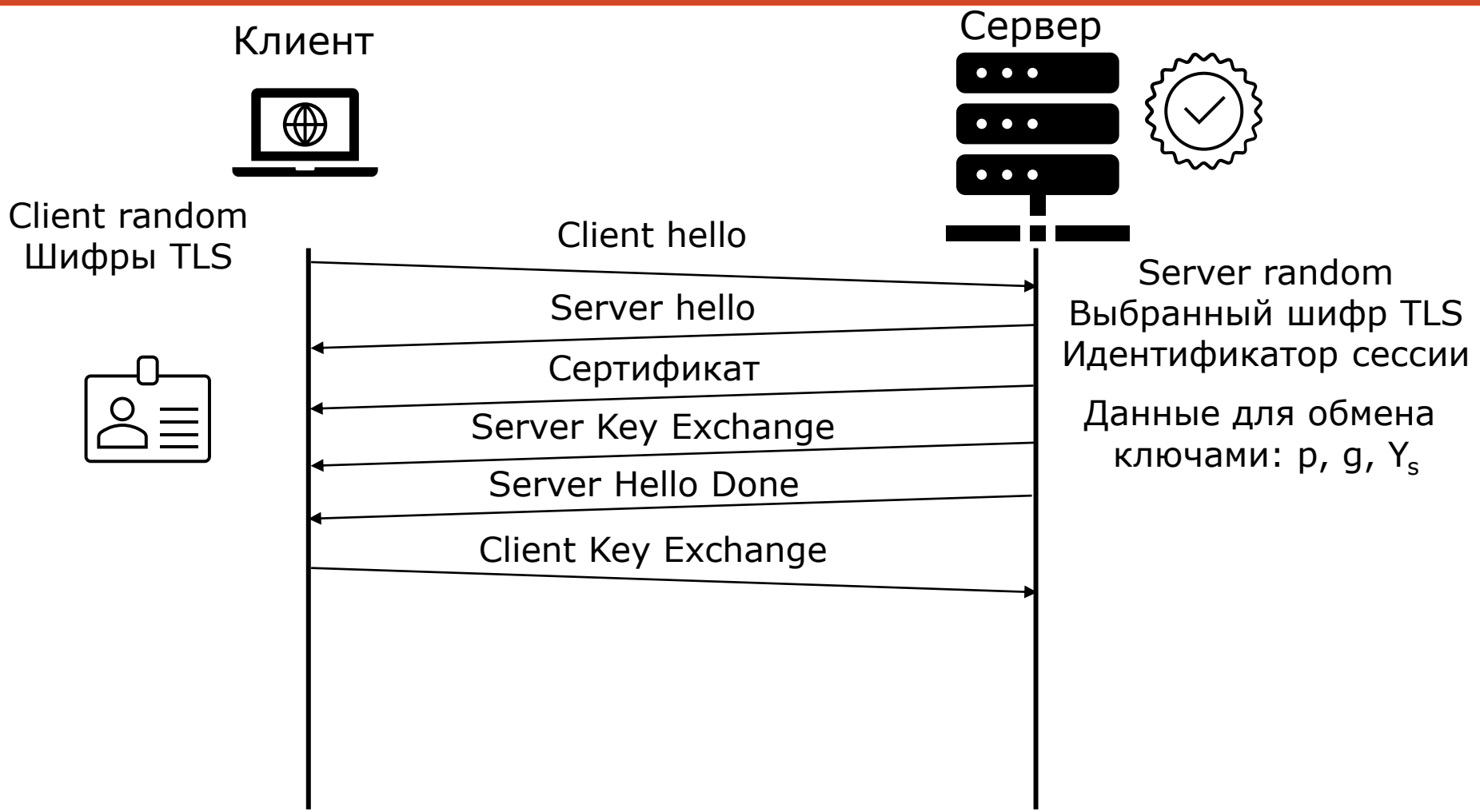
Обмен ключами: Диффи-Хеллман с одноразовыми параметрами



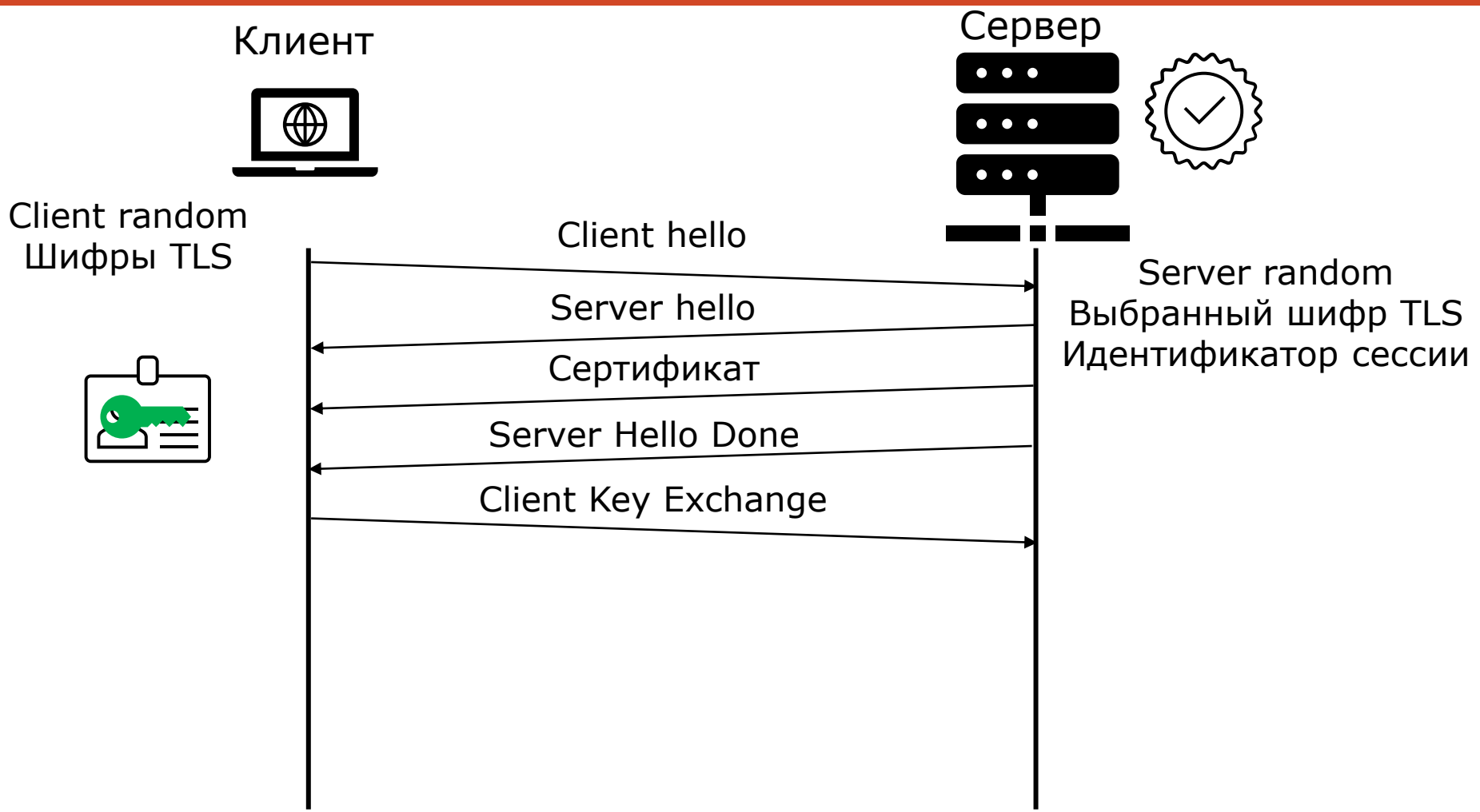
Установка соединения TLS



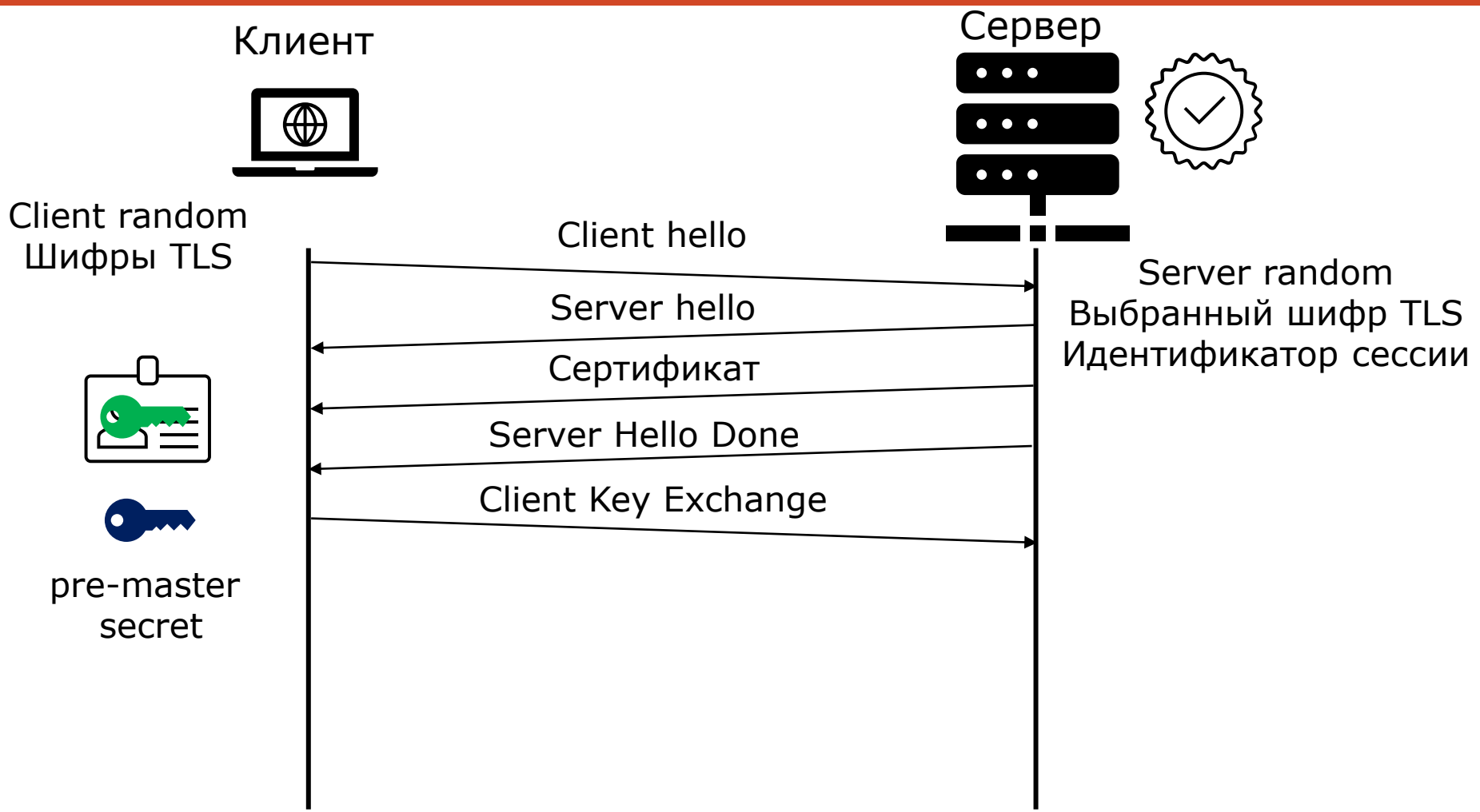
Установка соединения TLS



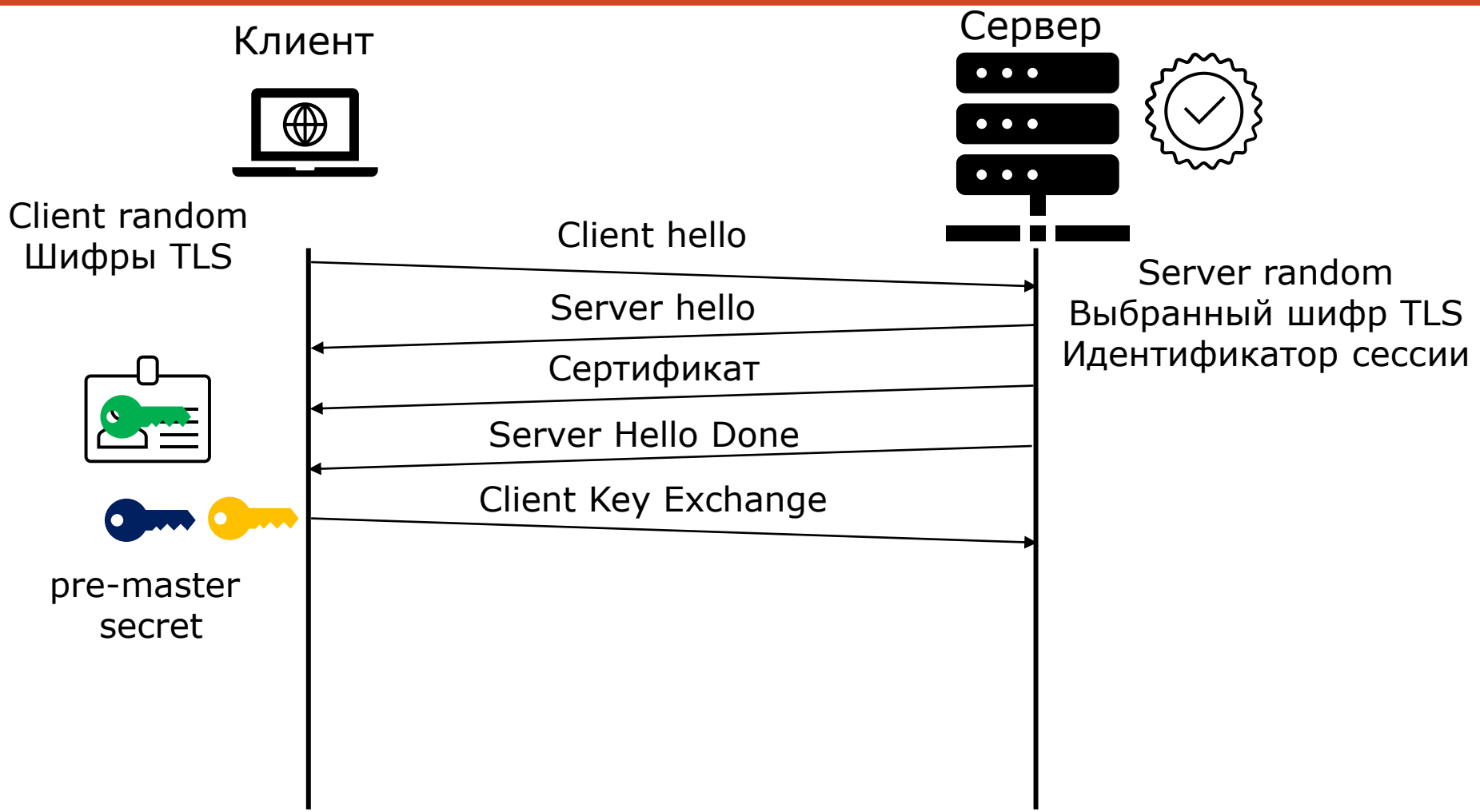
Обмен ключами: RSA



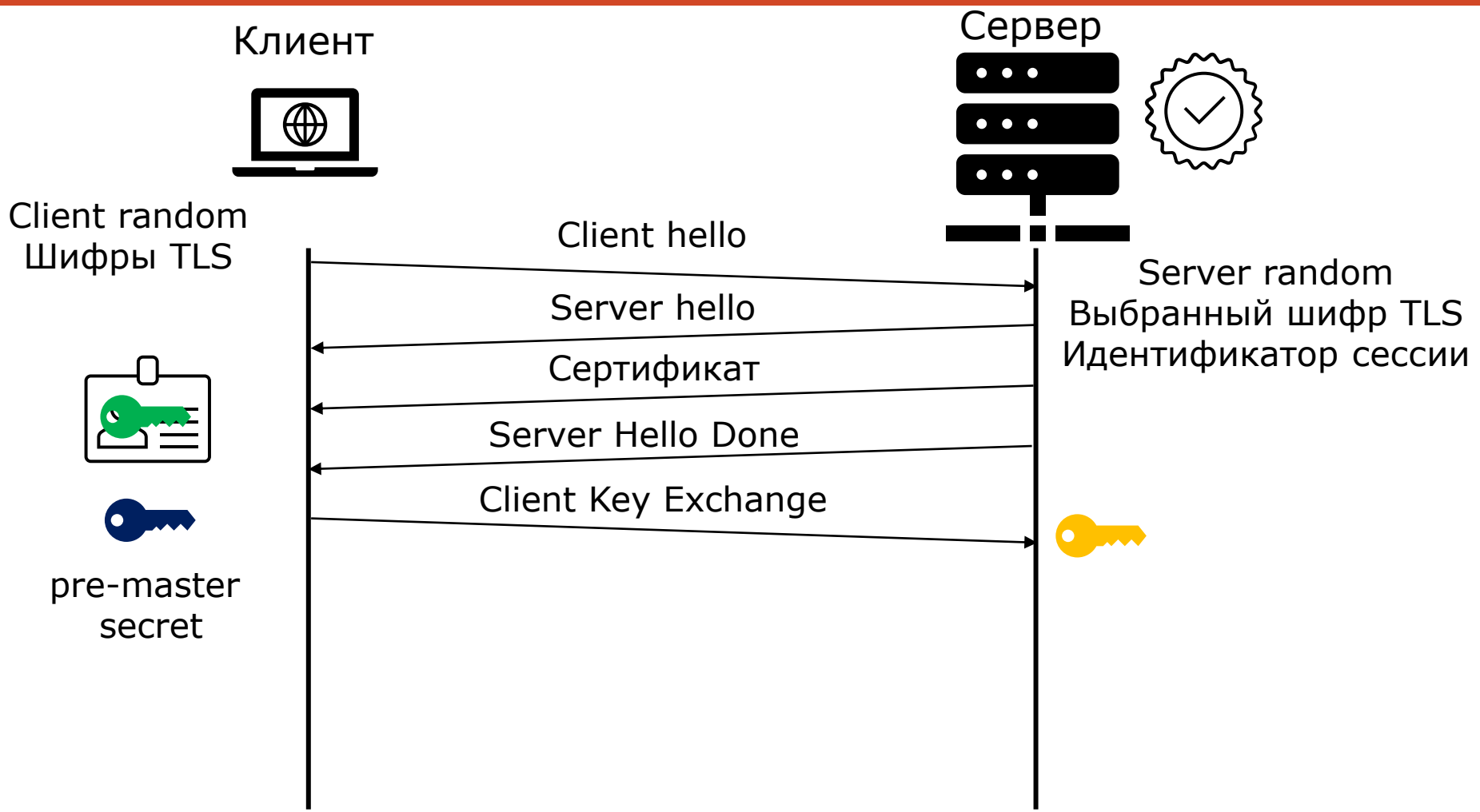
Обмен ключами: RSA



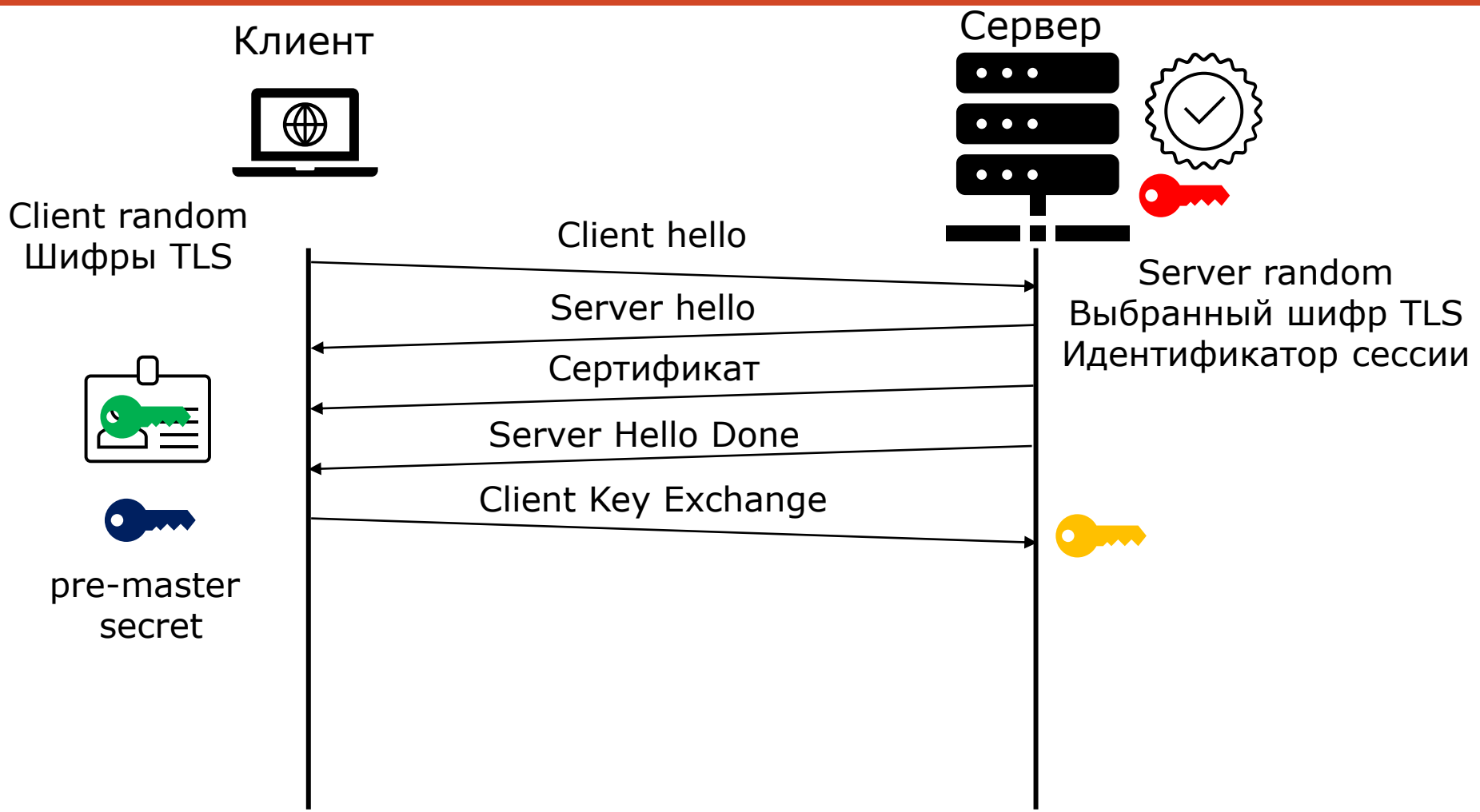
Обмен ключами: RSA



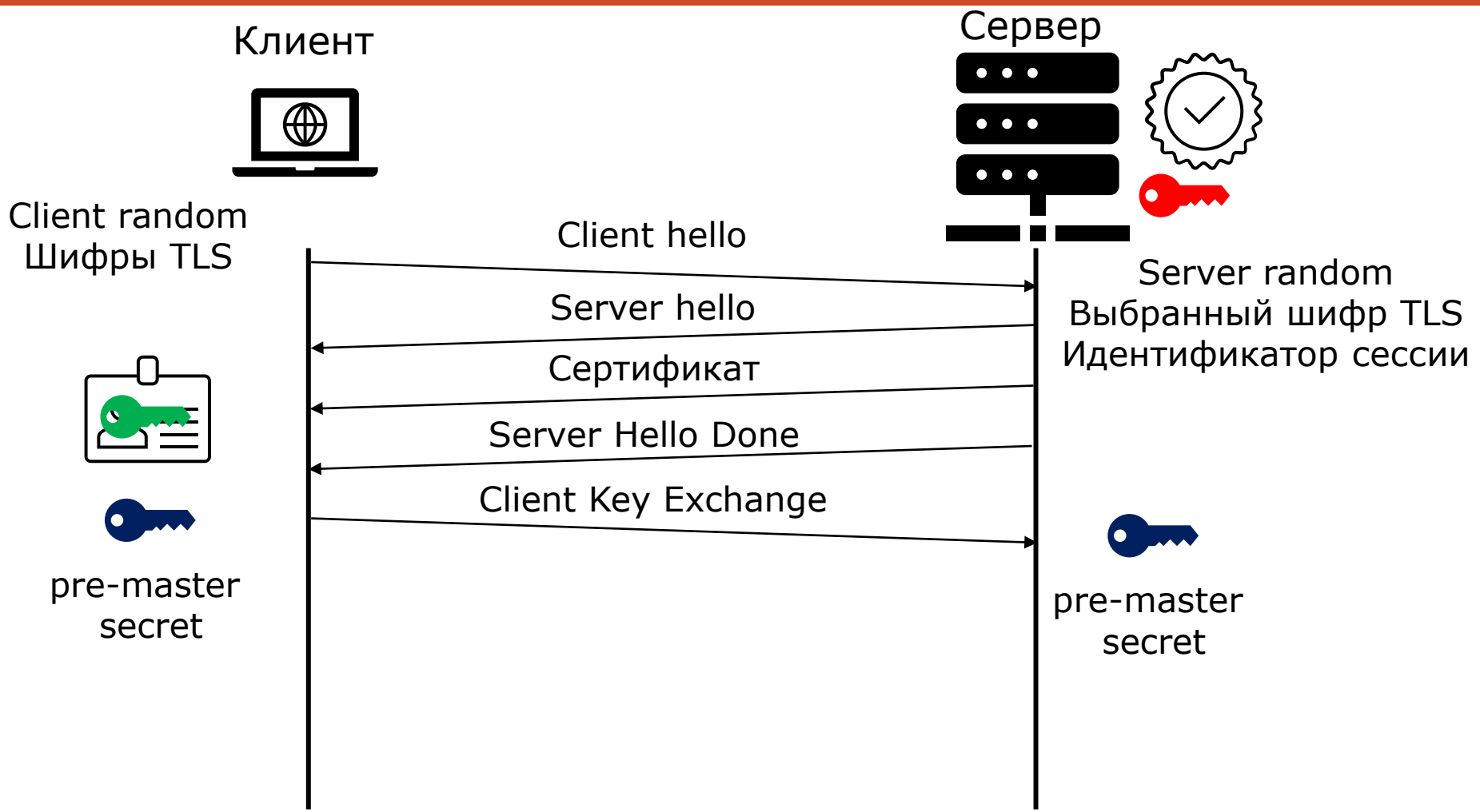
Обмен ключами: RSA



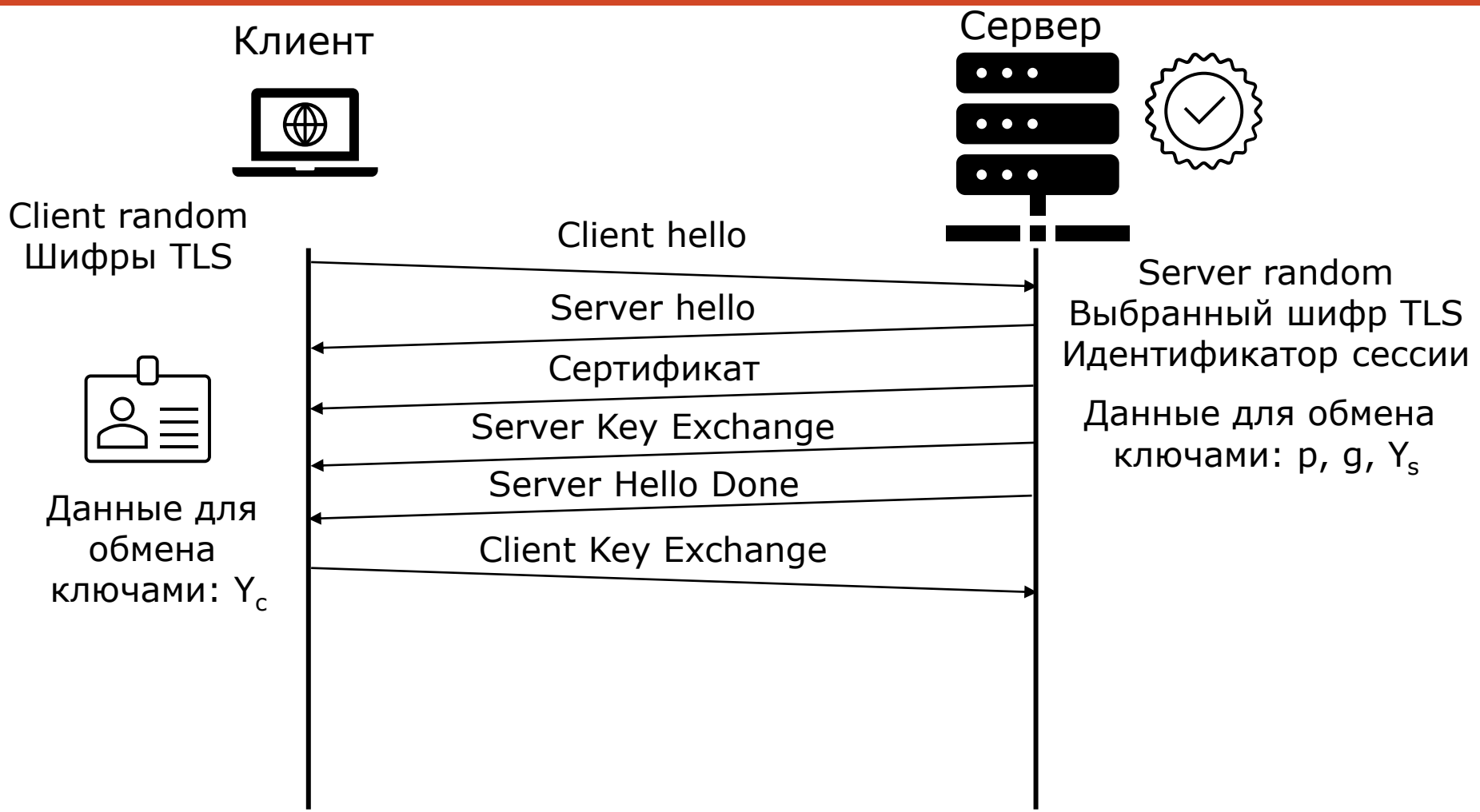
Обмен ключами: RSA



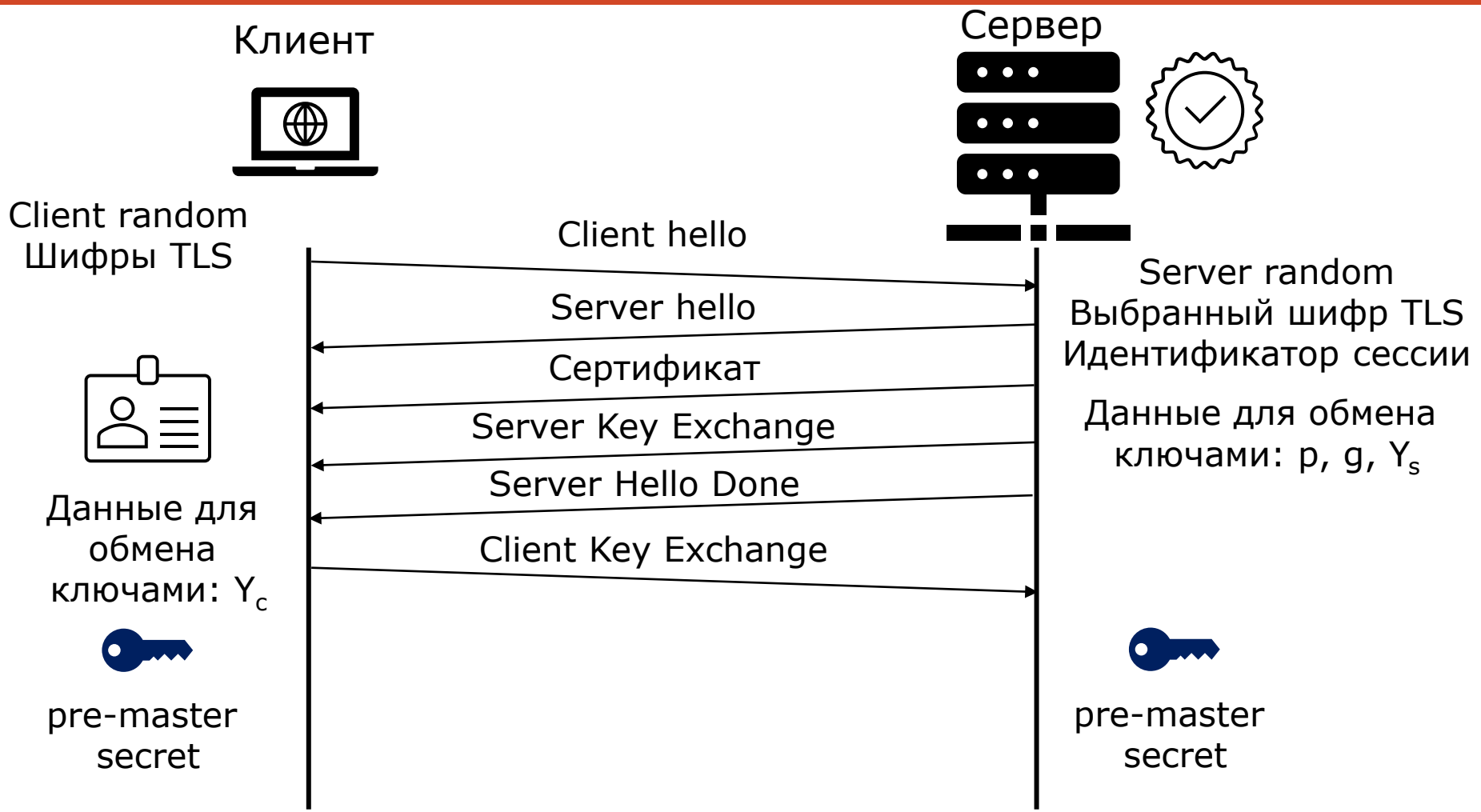
Обмен ключами: RSA



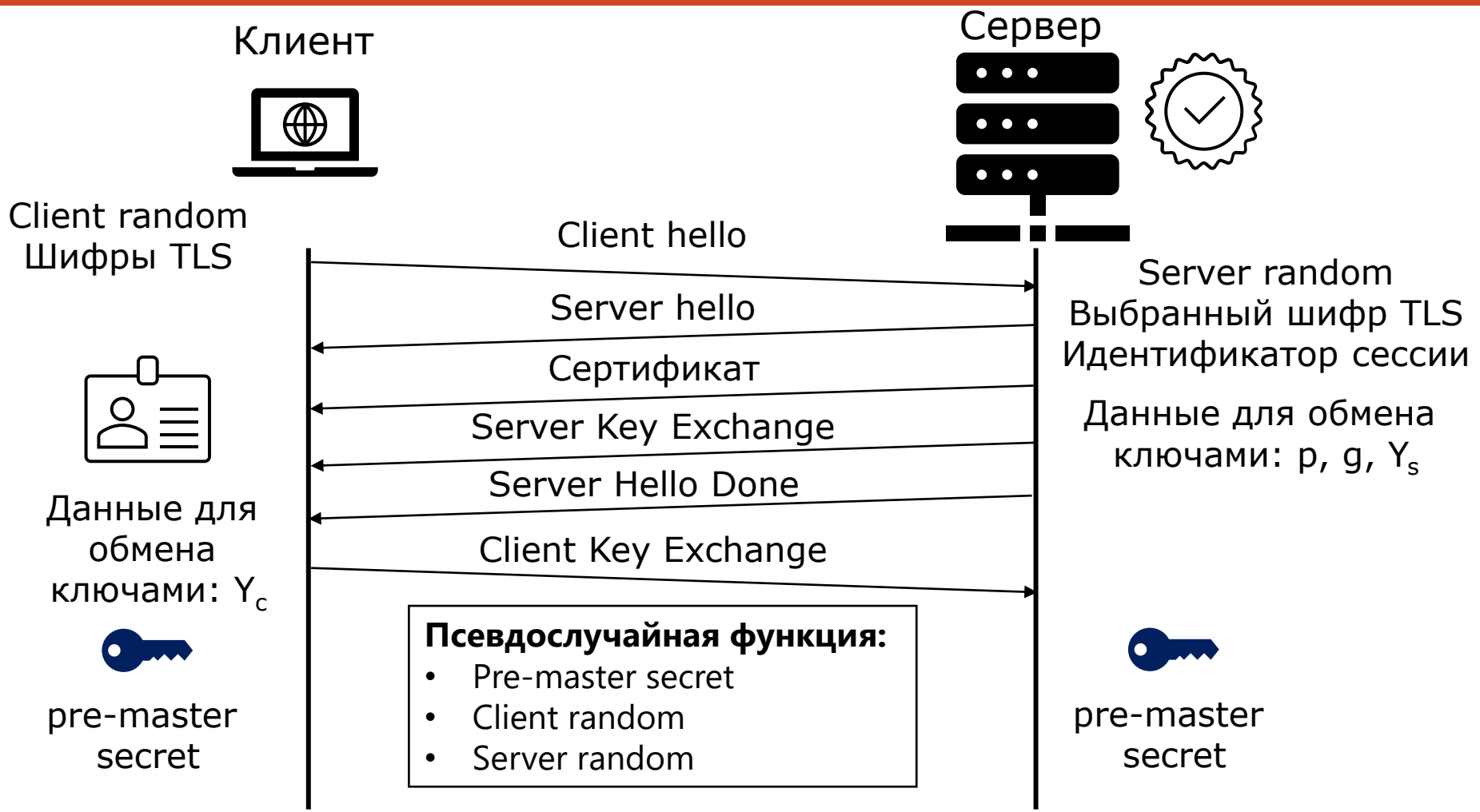
Обмен ключами: Диффи-Хеллман



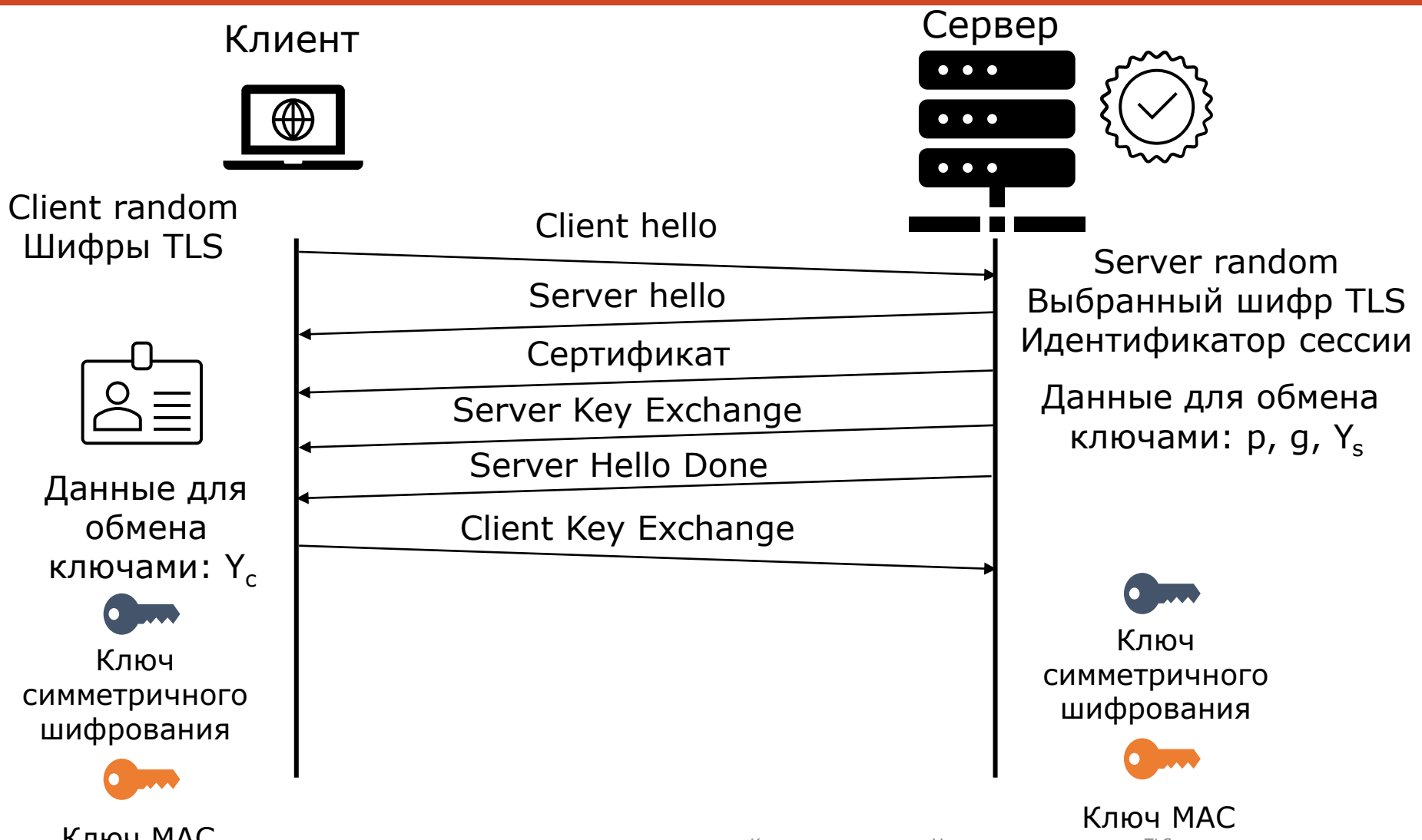
Обмен ключами: Диффи-Хеллман



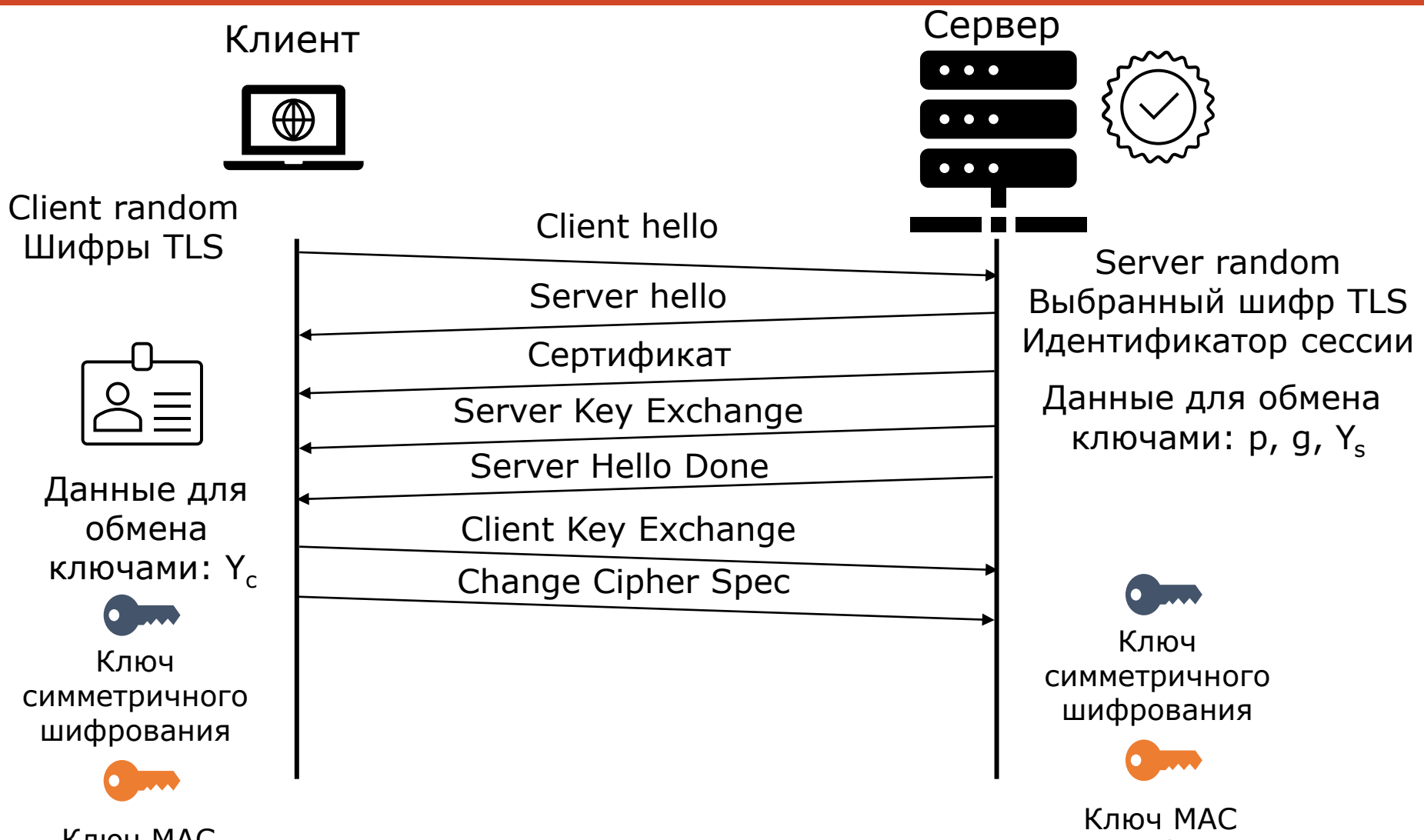
Расчет ключей симметричного шифрования



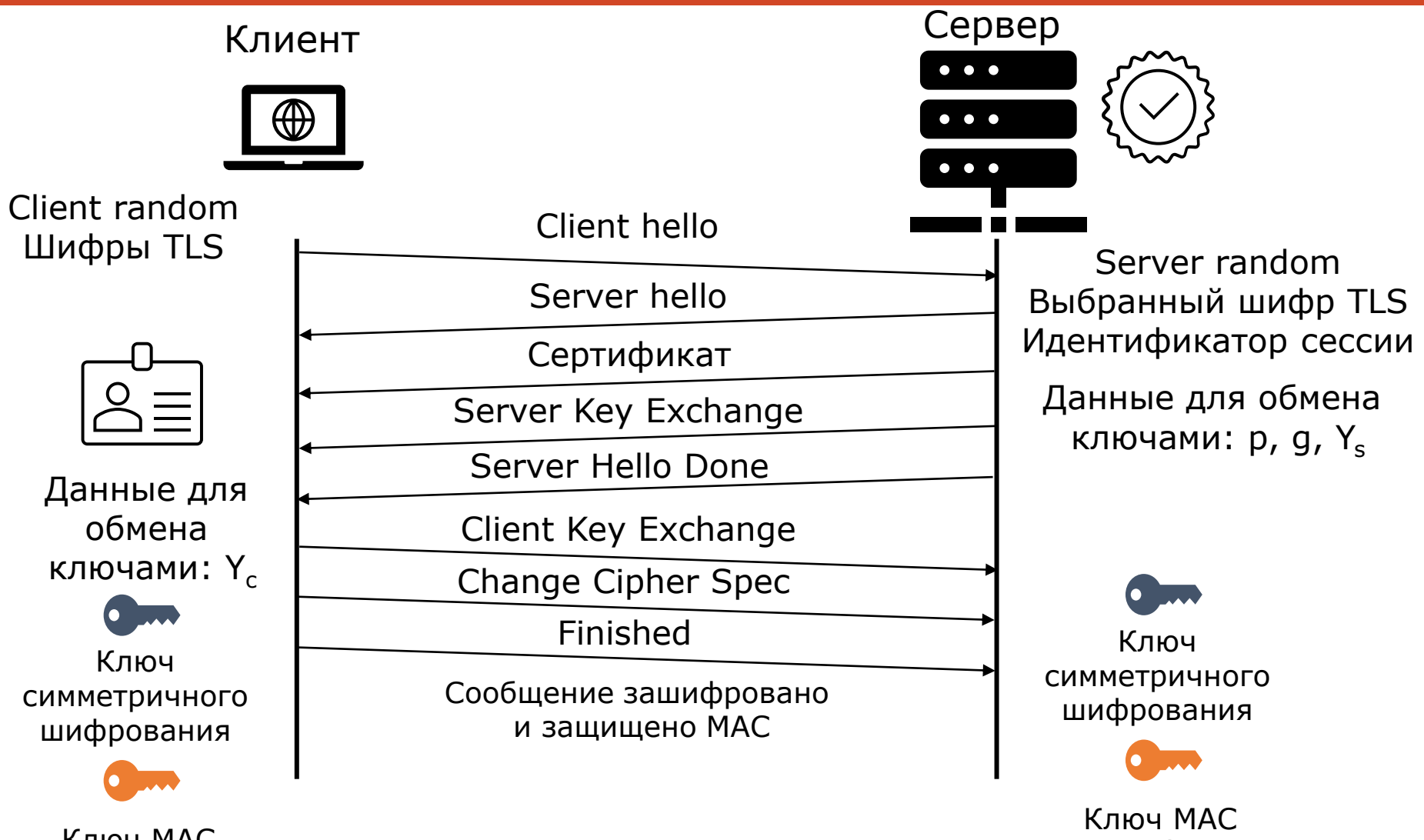
Расчет ключей симметричного шифрования



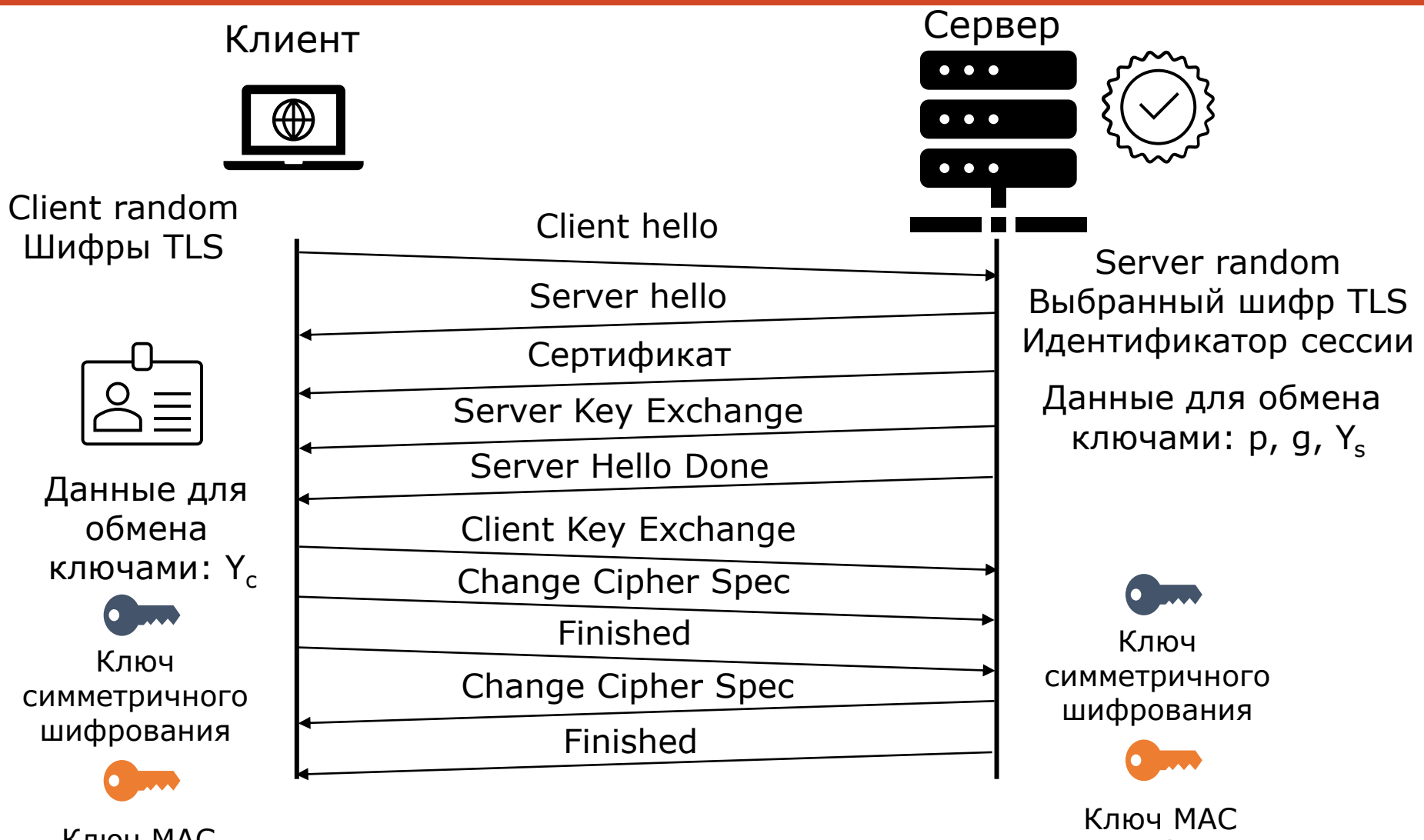
Установка соединения TLS



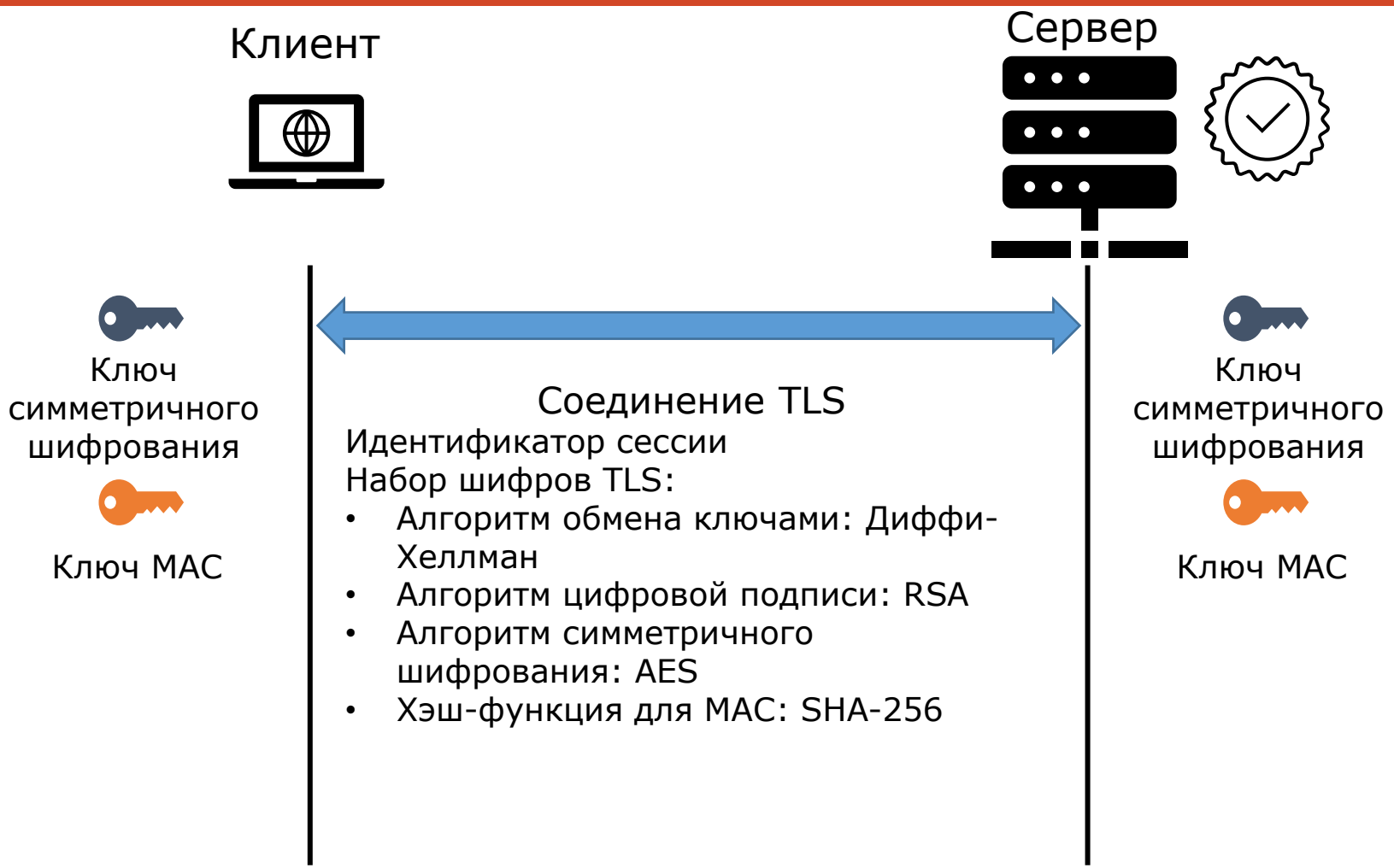
Установка соединения TLS



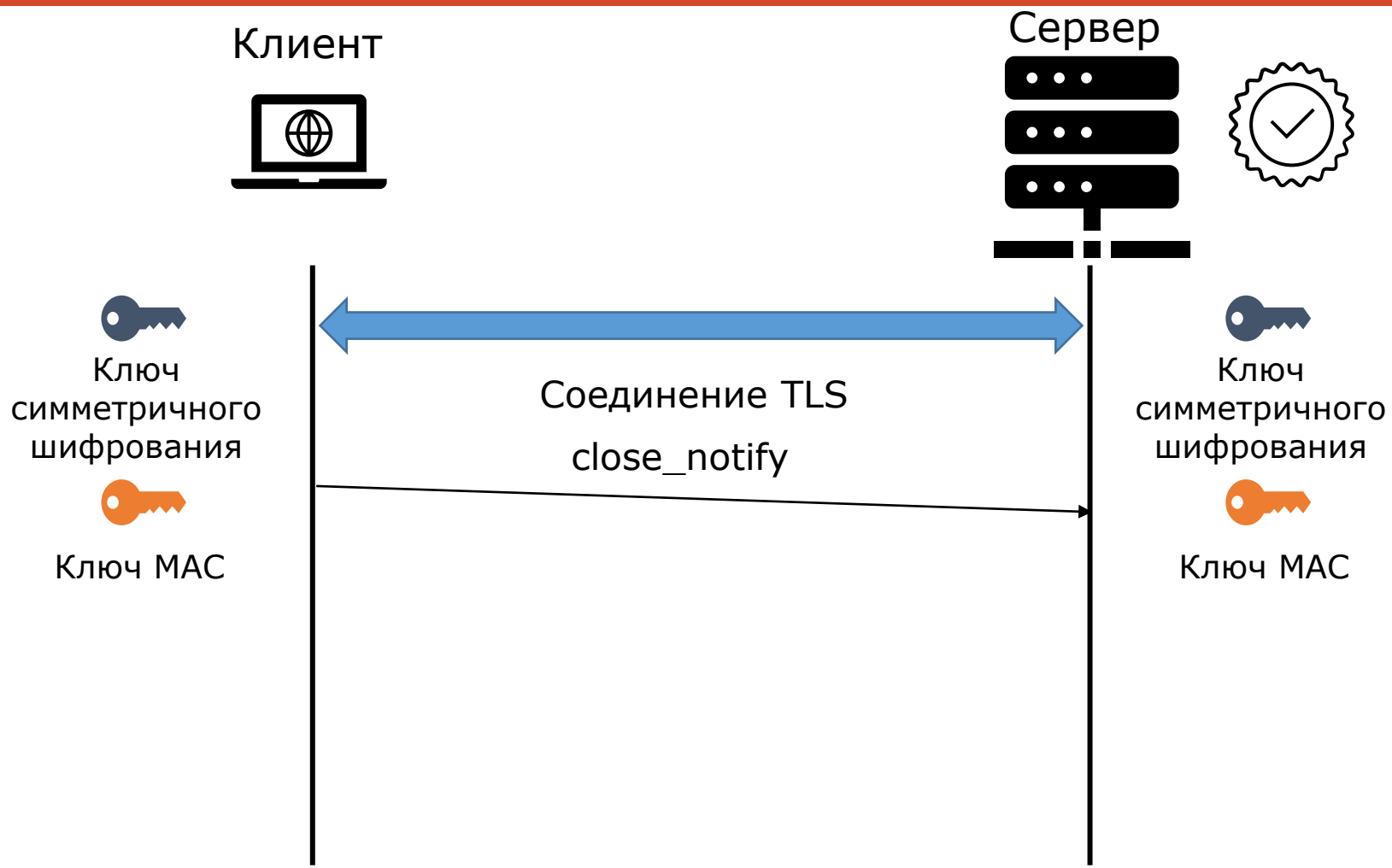
Установка соединения TLS



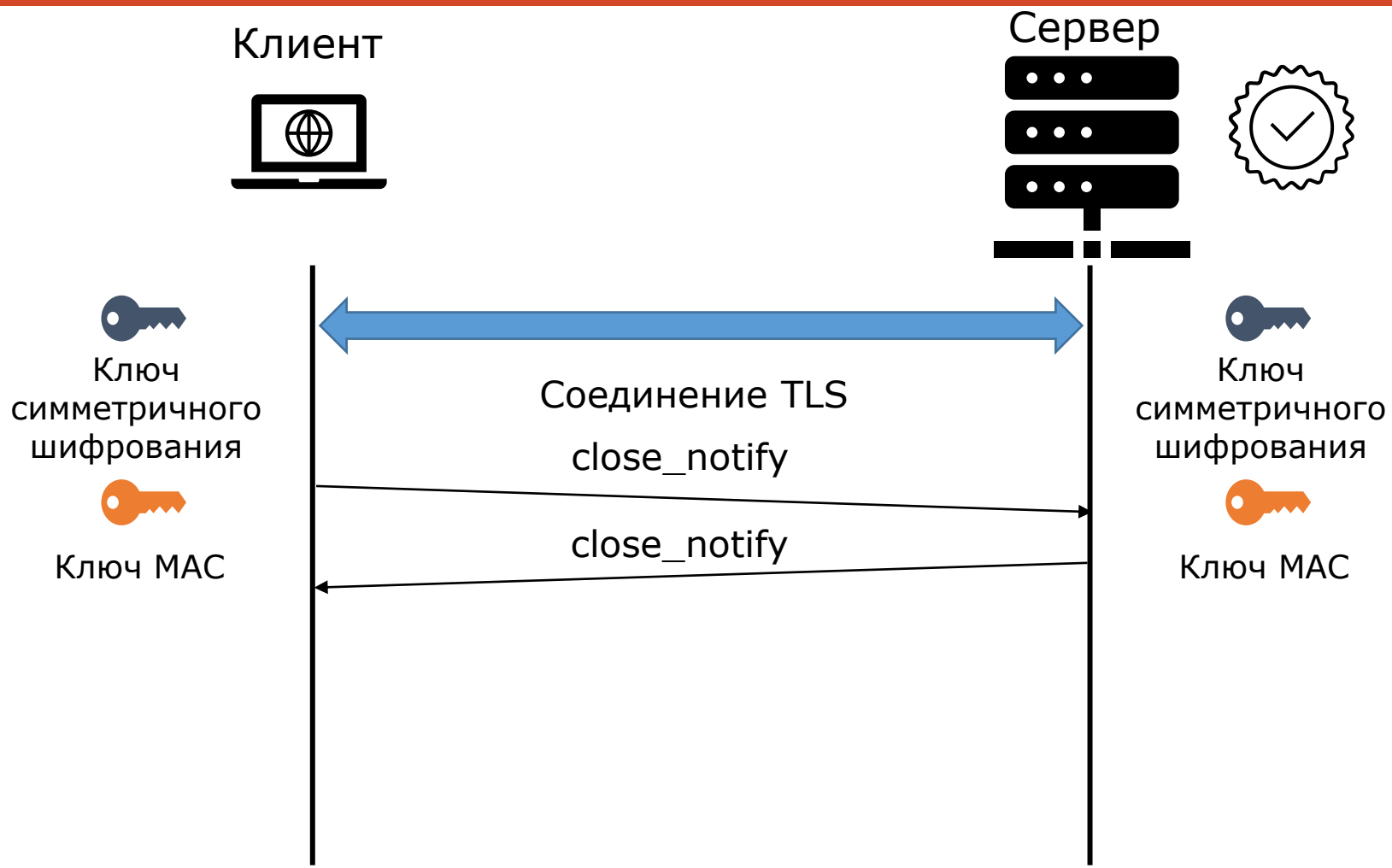
Соединение TLS



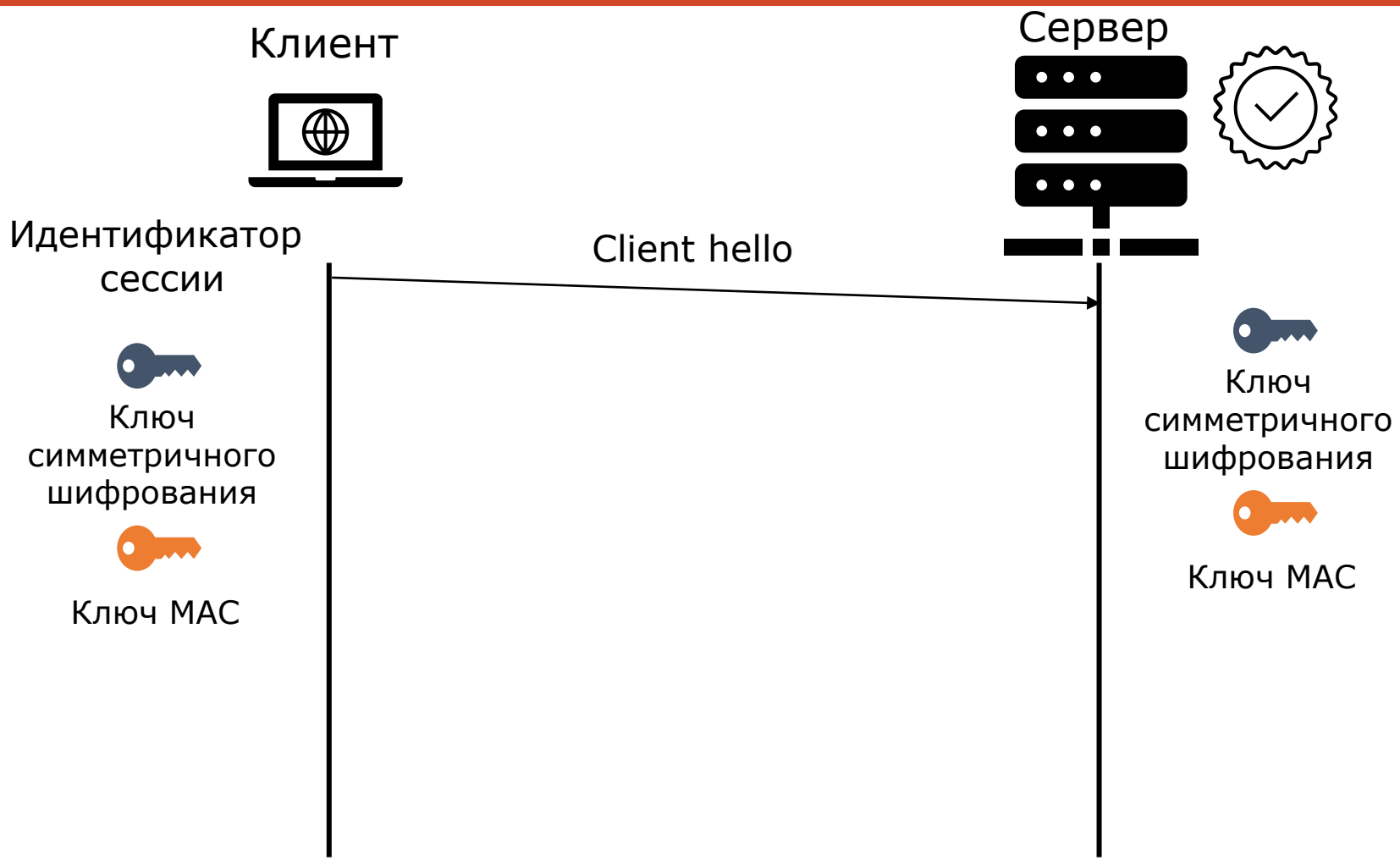
Разрыв соединения TLS



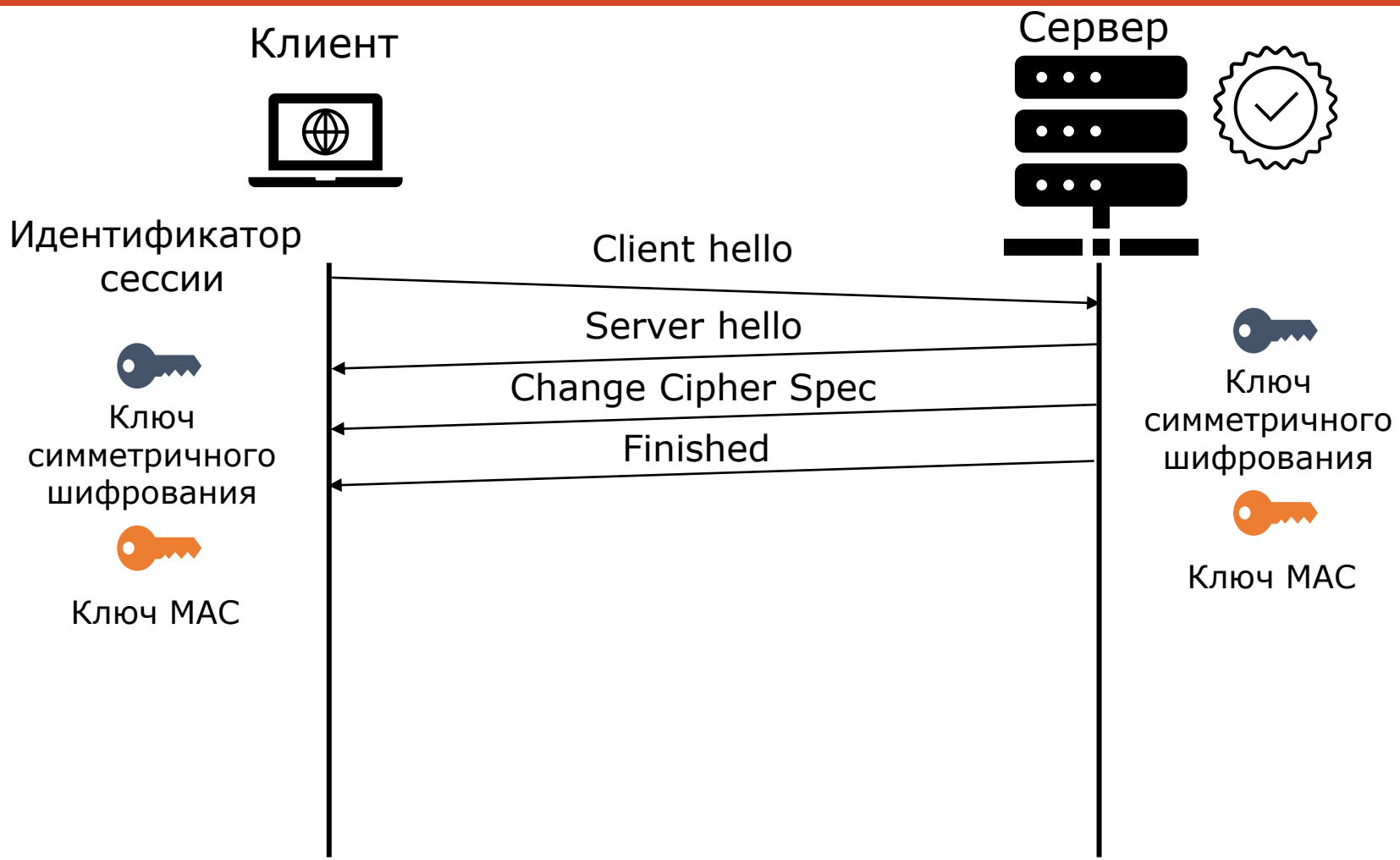
Разрыв соединения TLS



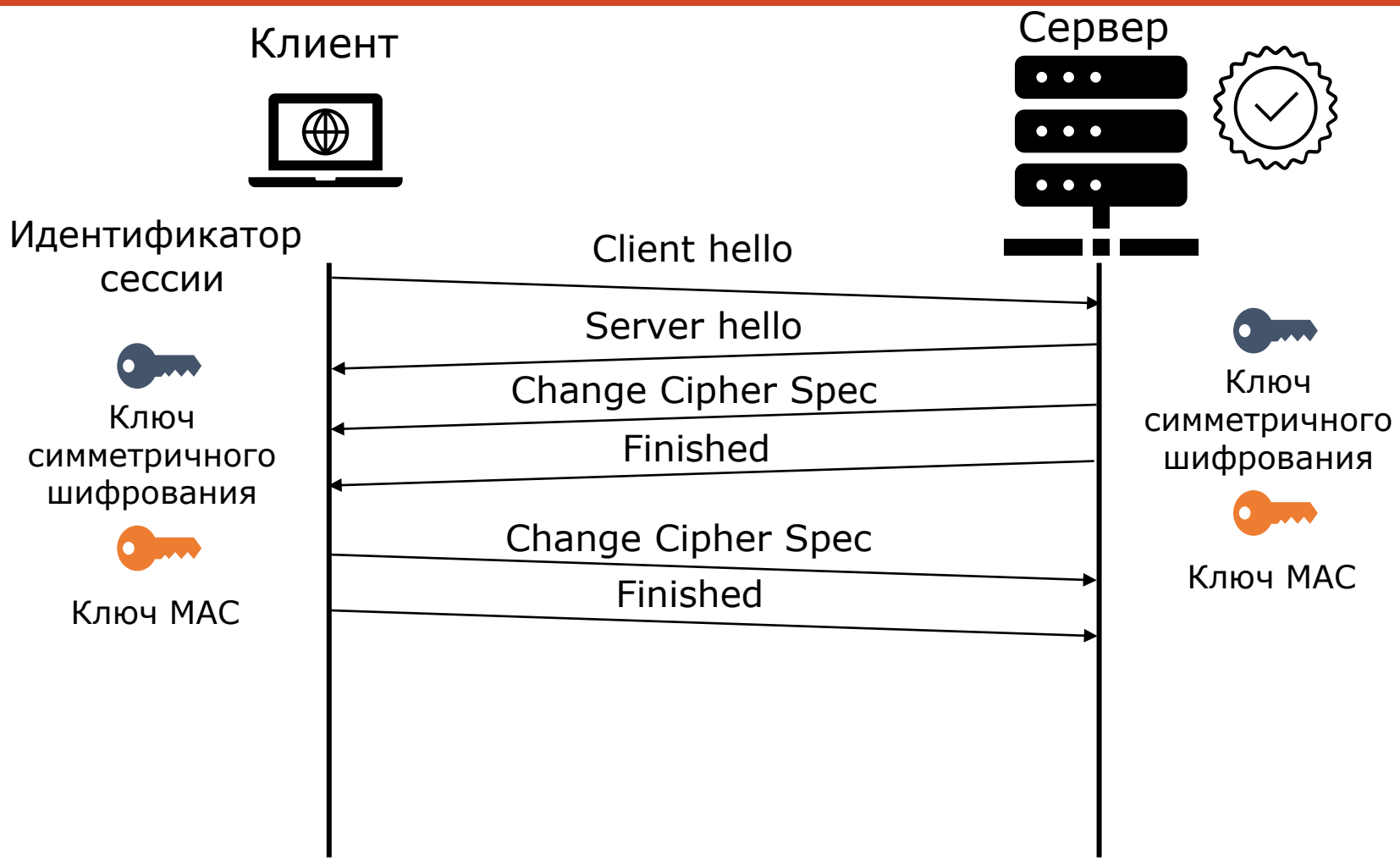
Восстановление сессии TLS



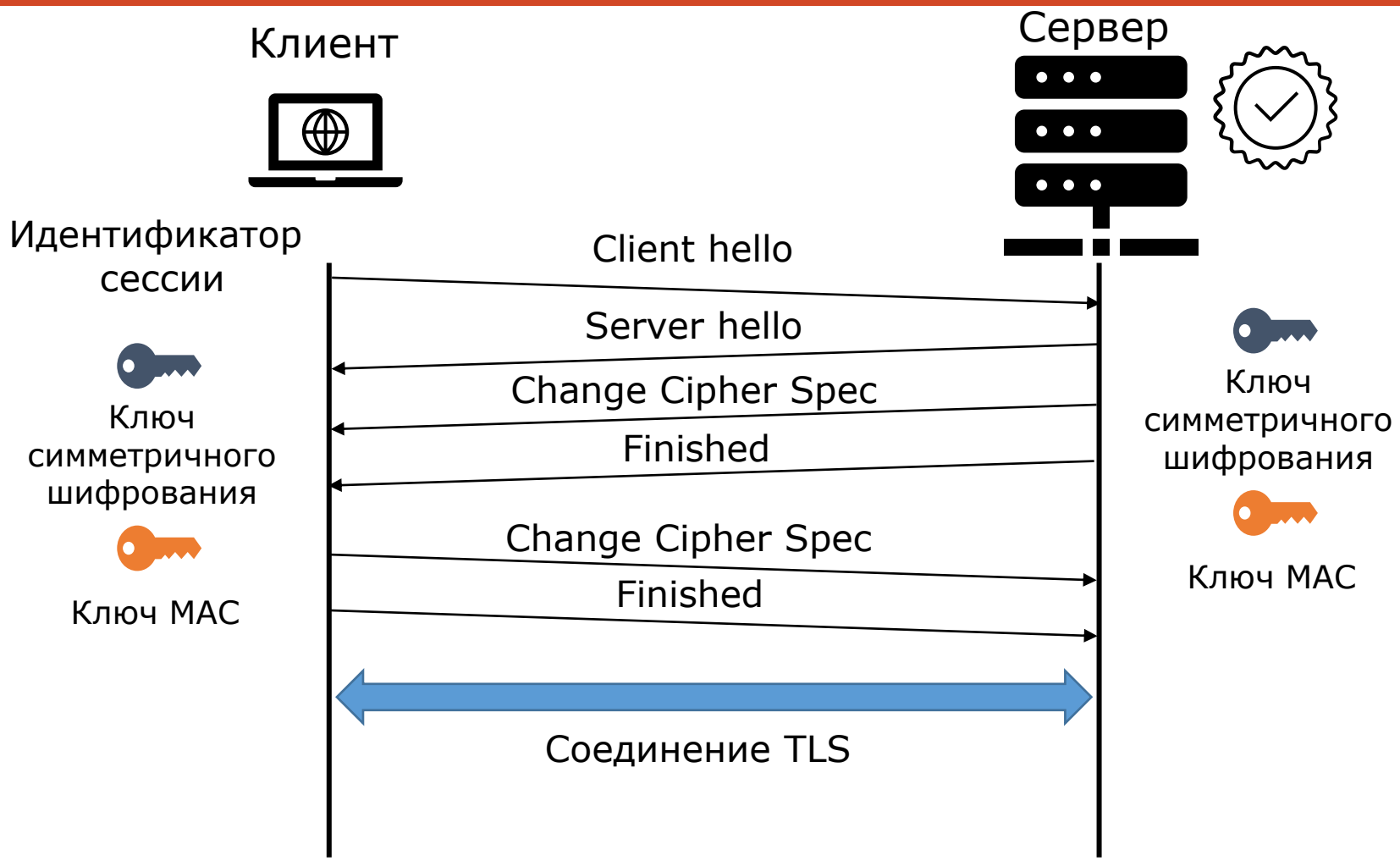
Восстановление сессии TLS



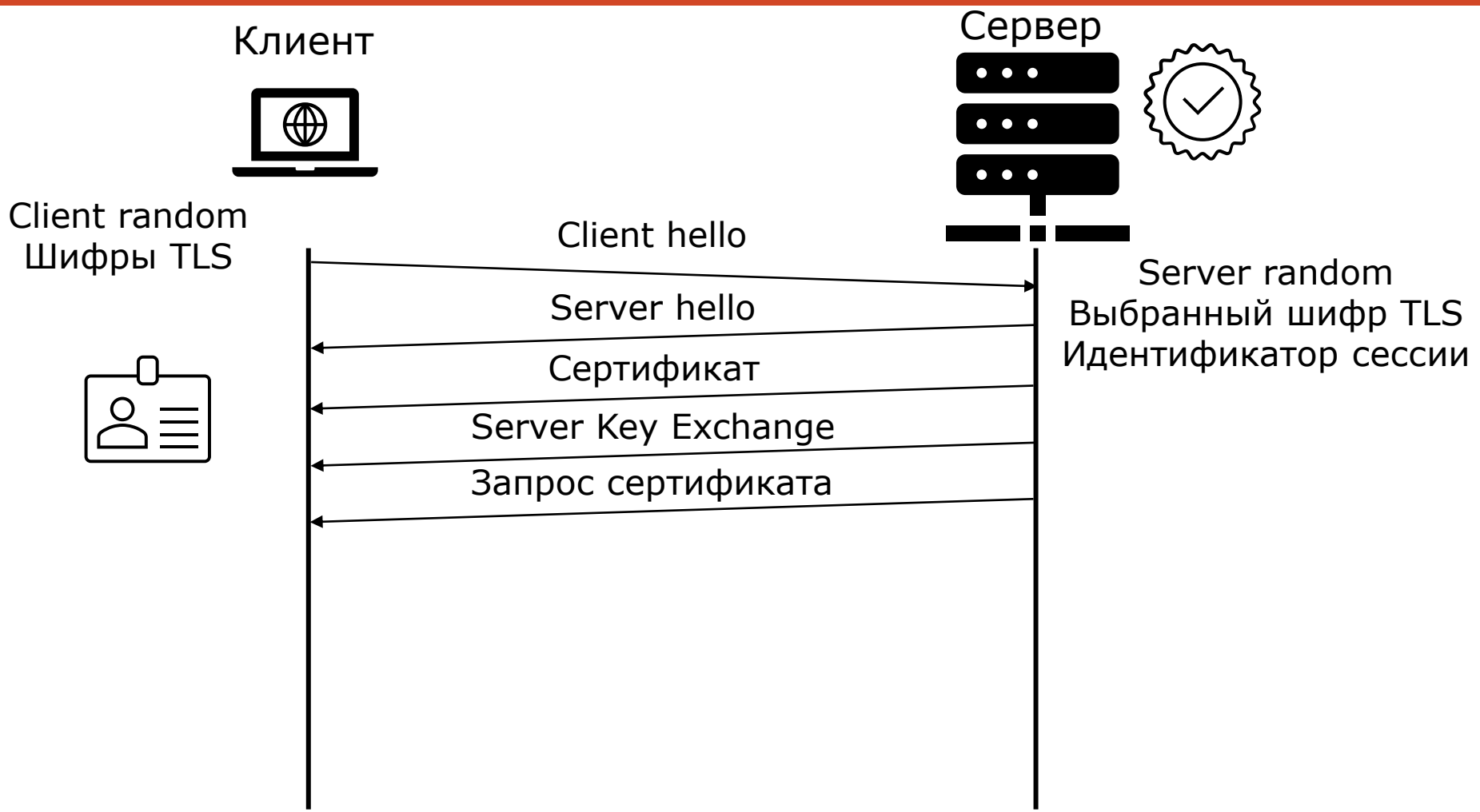
Восстановление сессии TLS



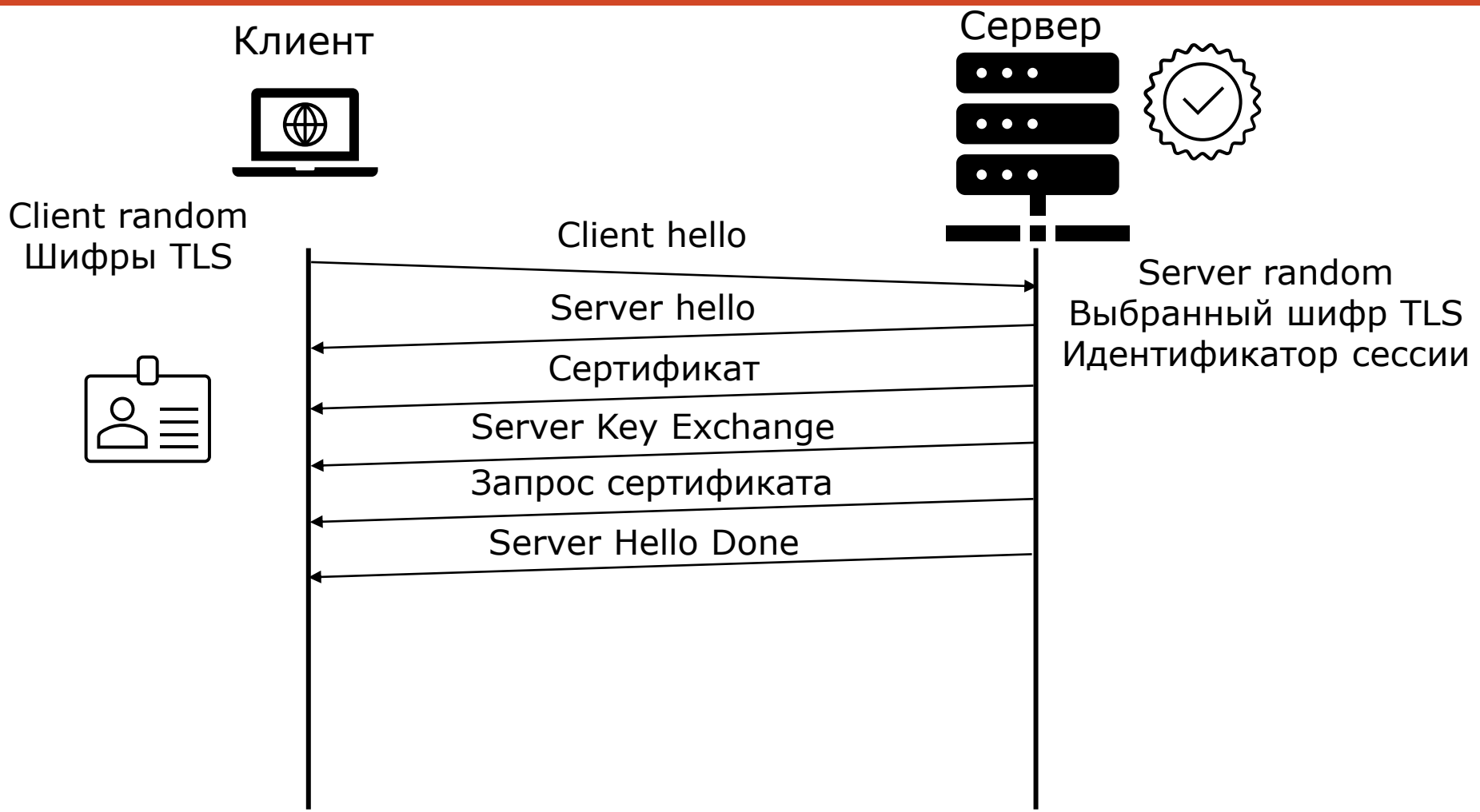
Восстановление сессии TLS



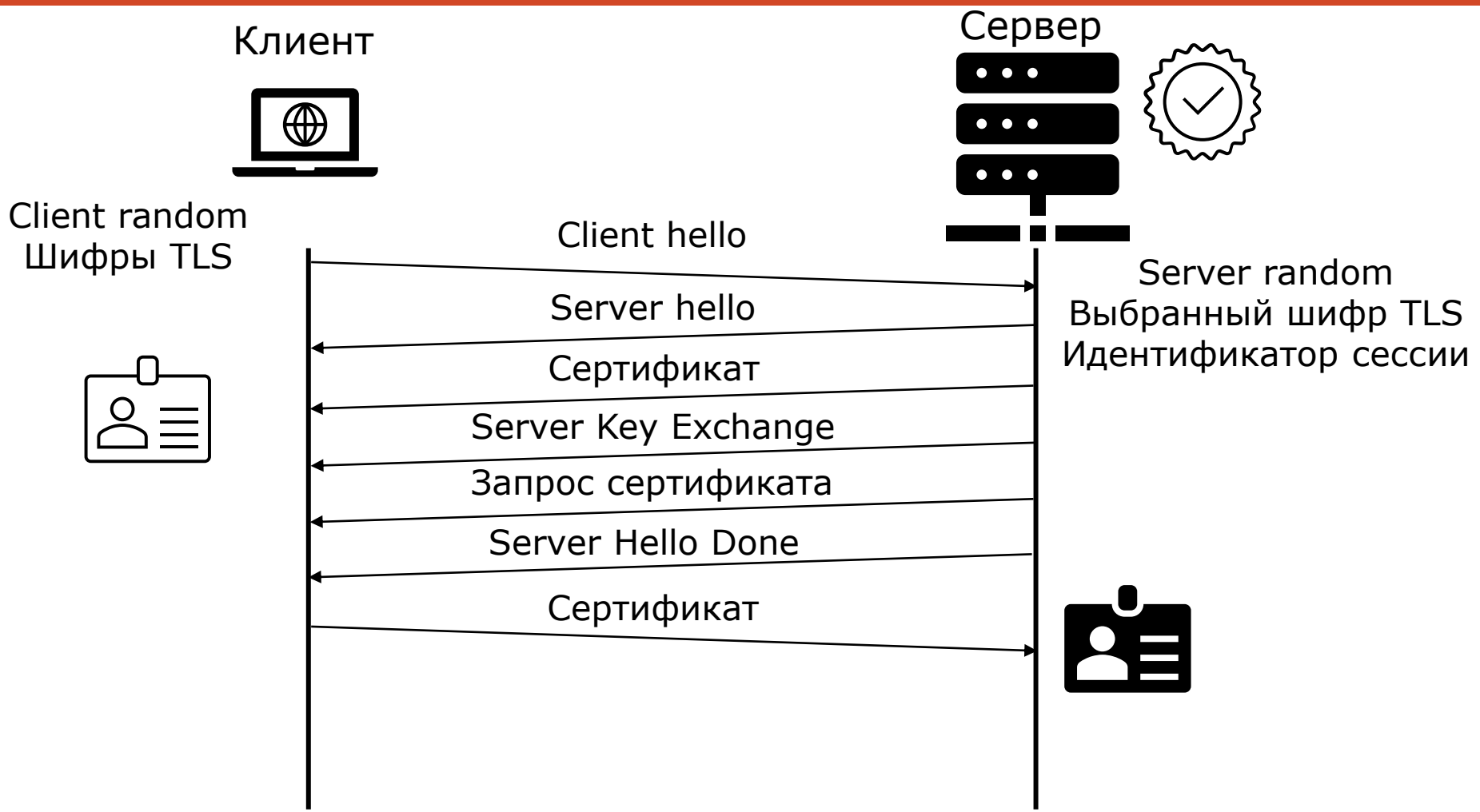
Проверка подлинности клиента



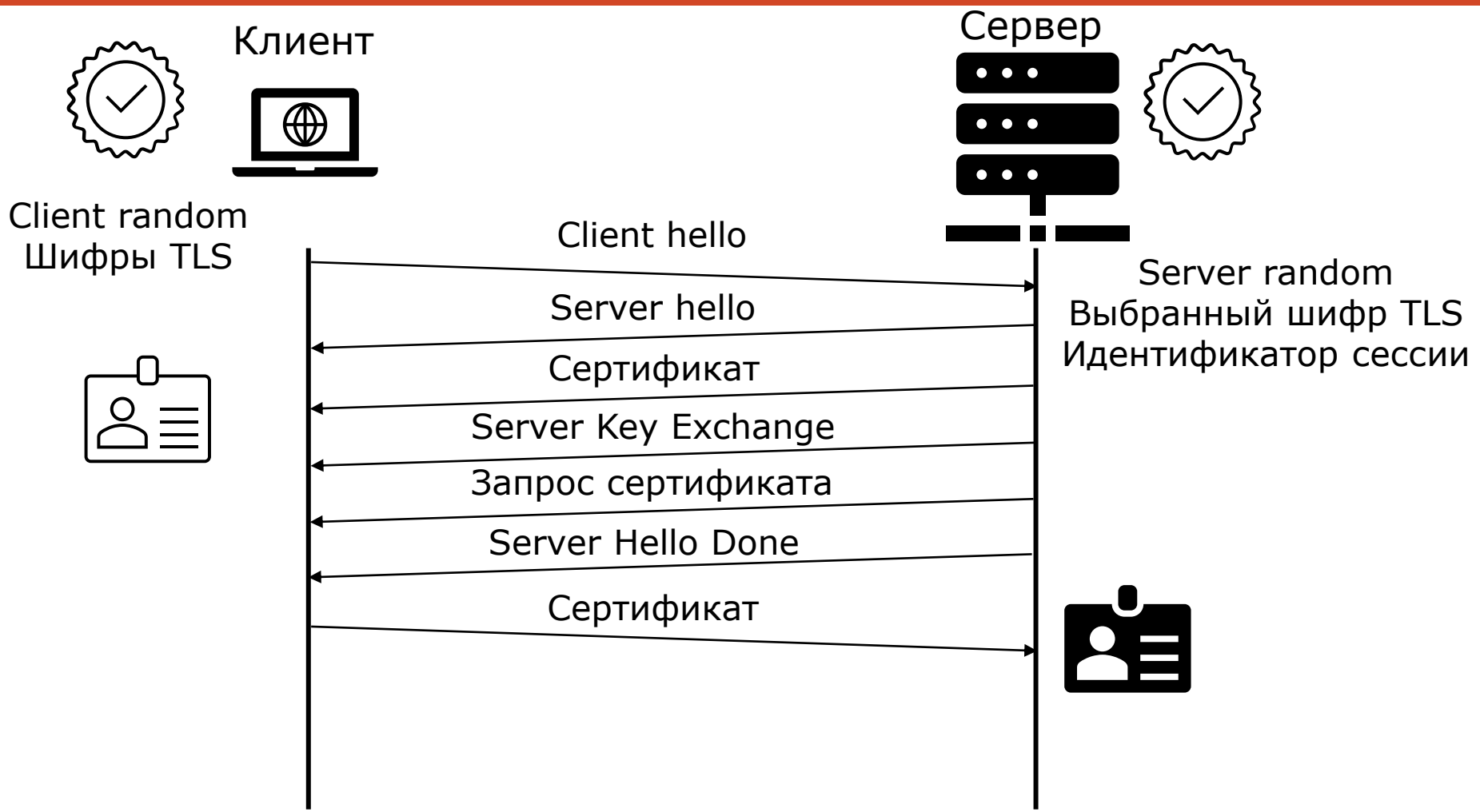
Проверка подлинности клиента



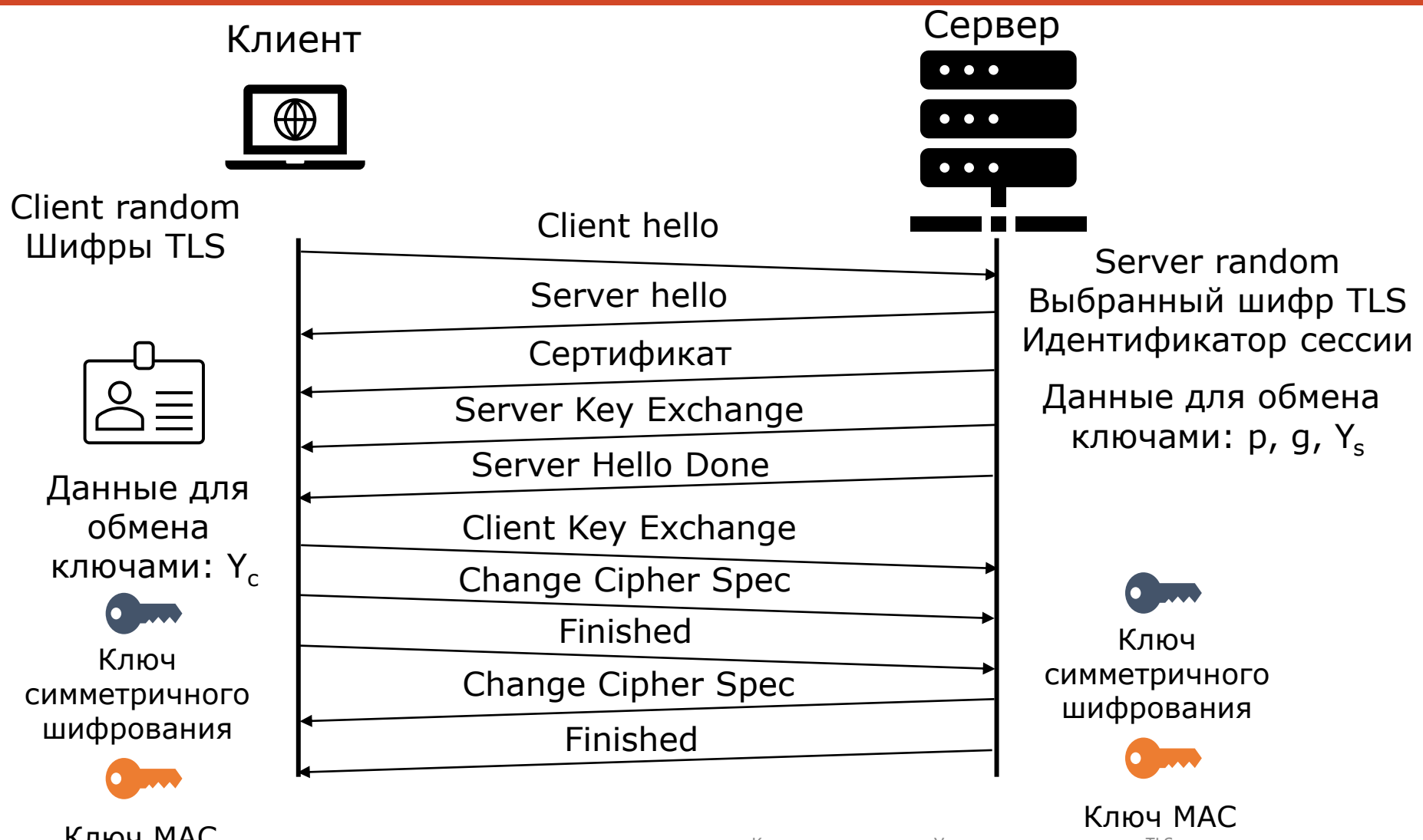
Проверка подлинности клиента



Проверка подлинности клиента



Пересылка сообщений в TLS



Установка соединения в TLS

Соединение в TLS:

- Набор шифров TLS
- Проверка подлинности сервера (и клиента)
- Обмен ключами симметричного шифрования

Установка соединения в TLS:

- Протокол установки соединения (handshake protocol)
- Протокол смены шифра (change cipher protocol)

Разрыв соединения в TLS:

- Сообщение close_notify протокола оповещений (alert protocol

Восстановление сессии в TLS:

- Повторное использование шифров и ключей