Протокол TLS

Компьютерные сети

Протокол TLS

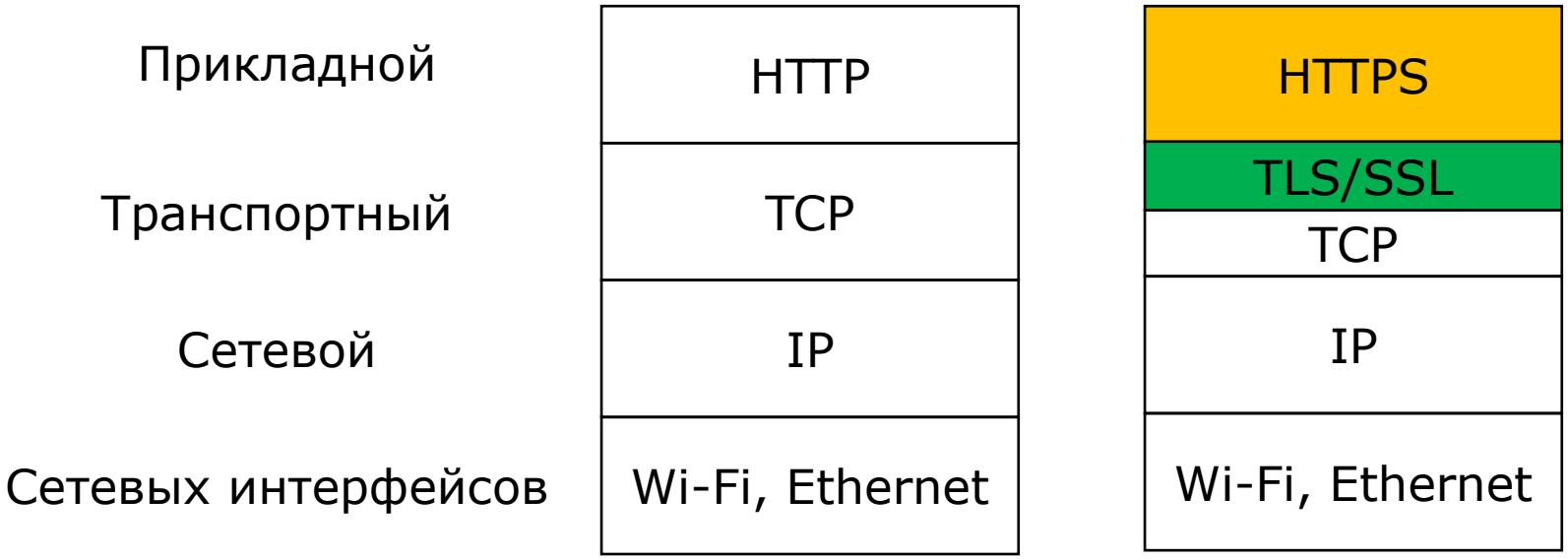
TLS/SSL – протоколы безопасной передачи данных по небезопасной сети:

- Приватность, целостность, аутентификация
- Как совместно использовать шифрование, цифровую подпись, сертификаты, MAC

Версии TLS/SSL:

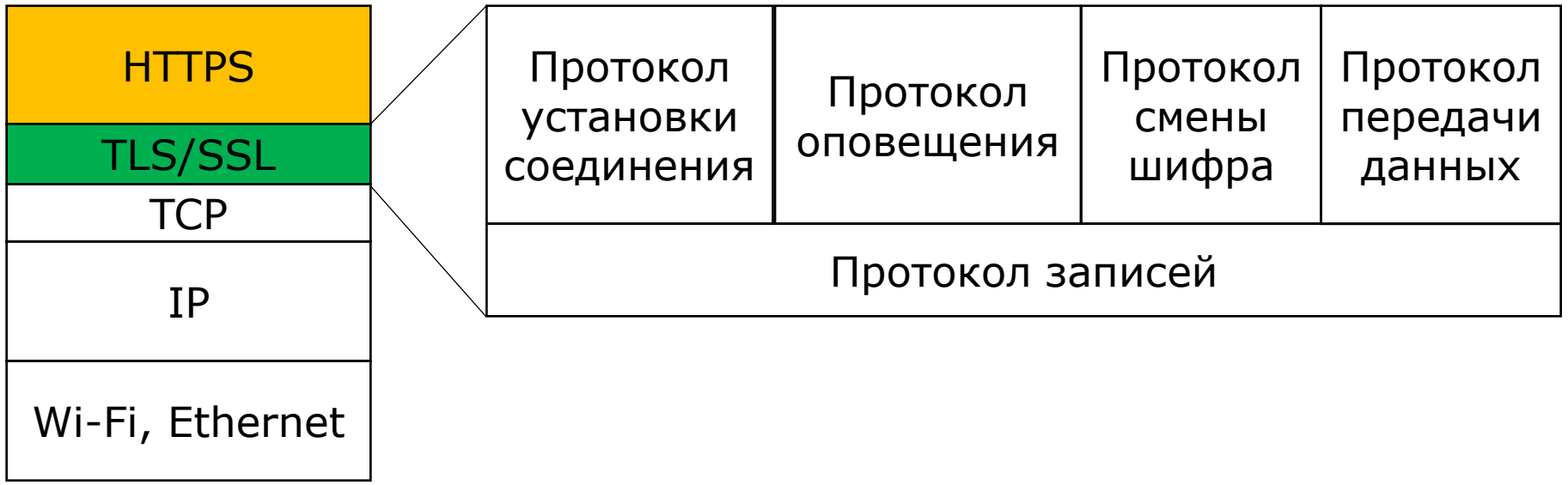
- TLS 1.2 – текущая версия
- TLS 1.3 – новая версия, вводится в эксплуатацию
- TLS 1.1, 1.0, SSLv3, SSLv2 – устарели, имеют проблемы с безопасностью, не рекомендованы к использованию (deprecated)

Место TLS в модели TCP/IP

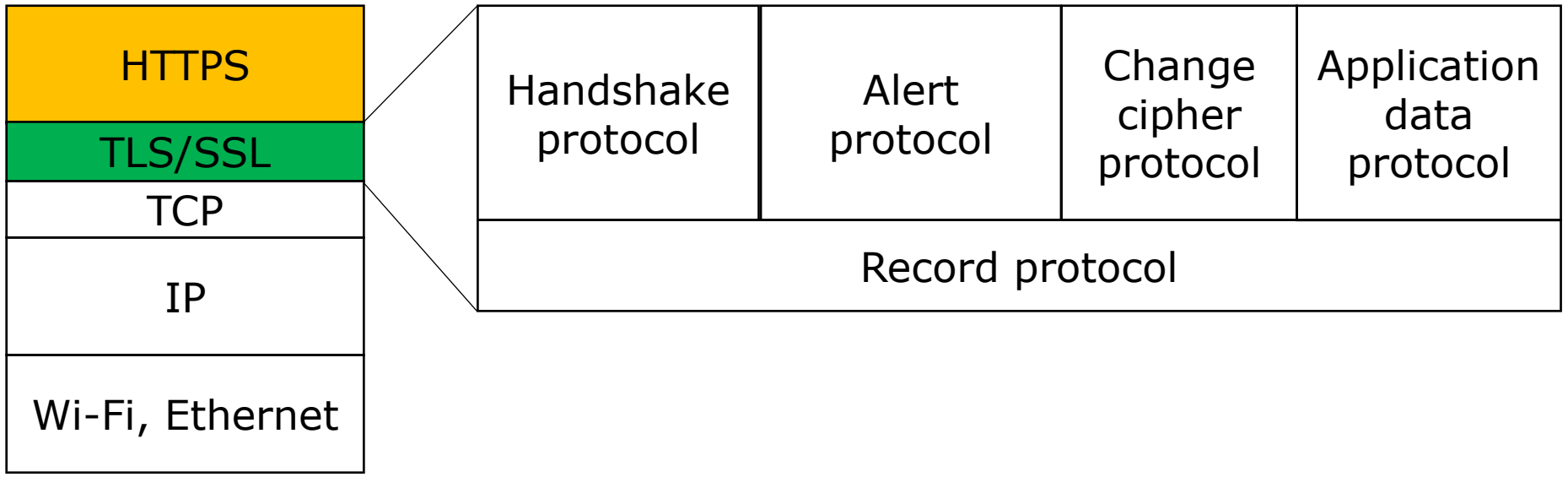


Уровни модели TCP/IP

Уровни TLS


HTTPS
TLS/SSL
TCP
IP
Wi-Fi, Ethernet
Протокол установки соединения
Протокол оповещения
Протокол смены шифра
Протокол передачи данных
Протокол записей

Уровни TLS


HTTPS
TLS/SSL
TCP
IP
Wi-Fi, Ethernet
Handshake protocol
Alert protocol
Change cipher protocol
Application data protocol
Record protocol

Протокол записей

Протокол записей (record protocol) – основа TLS

- В записи record protocol вкладываются сообщения вышестоящих протоколов TLS
- Алгоритмы шифрования и целостности работают на уровне записей
- Сообщения протокола записей вкладываются в сегменты TCP

Формат сообщения протокола записи:

Сессия TLS

Набор шифров TLS:

- Алгоритмы симметричного шифрования и MAC

Разделяемые ключи:

- Ключи для симметричного шифрования
- Ключи для MAC

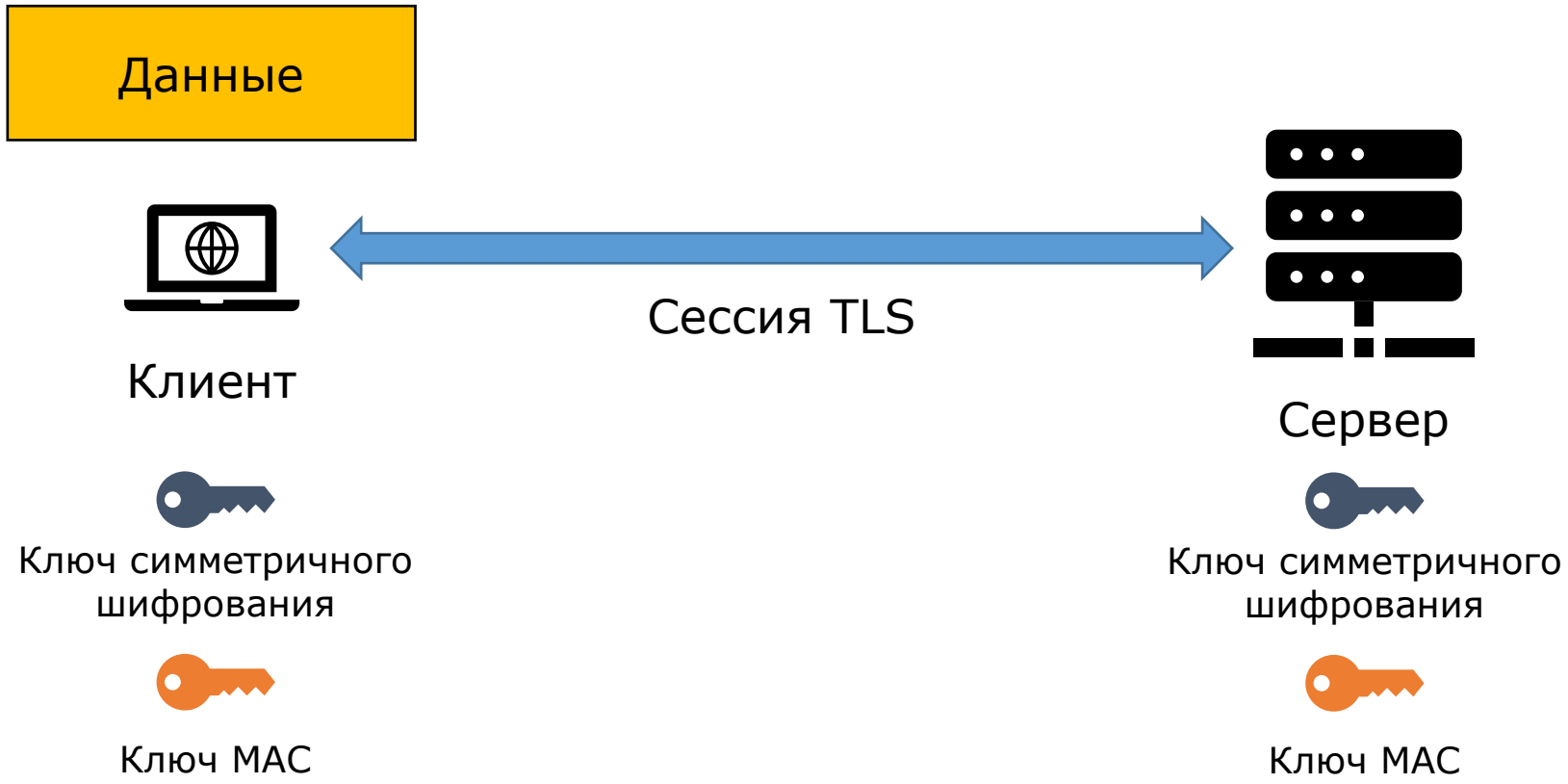
Описание сессии:

- Идентификатор сессии
- Узел, с которым установлено соединение

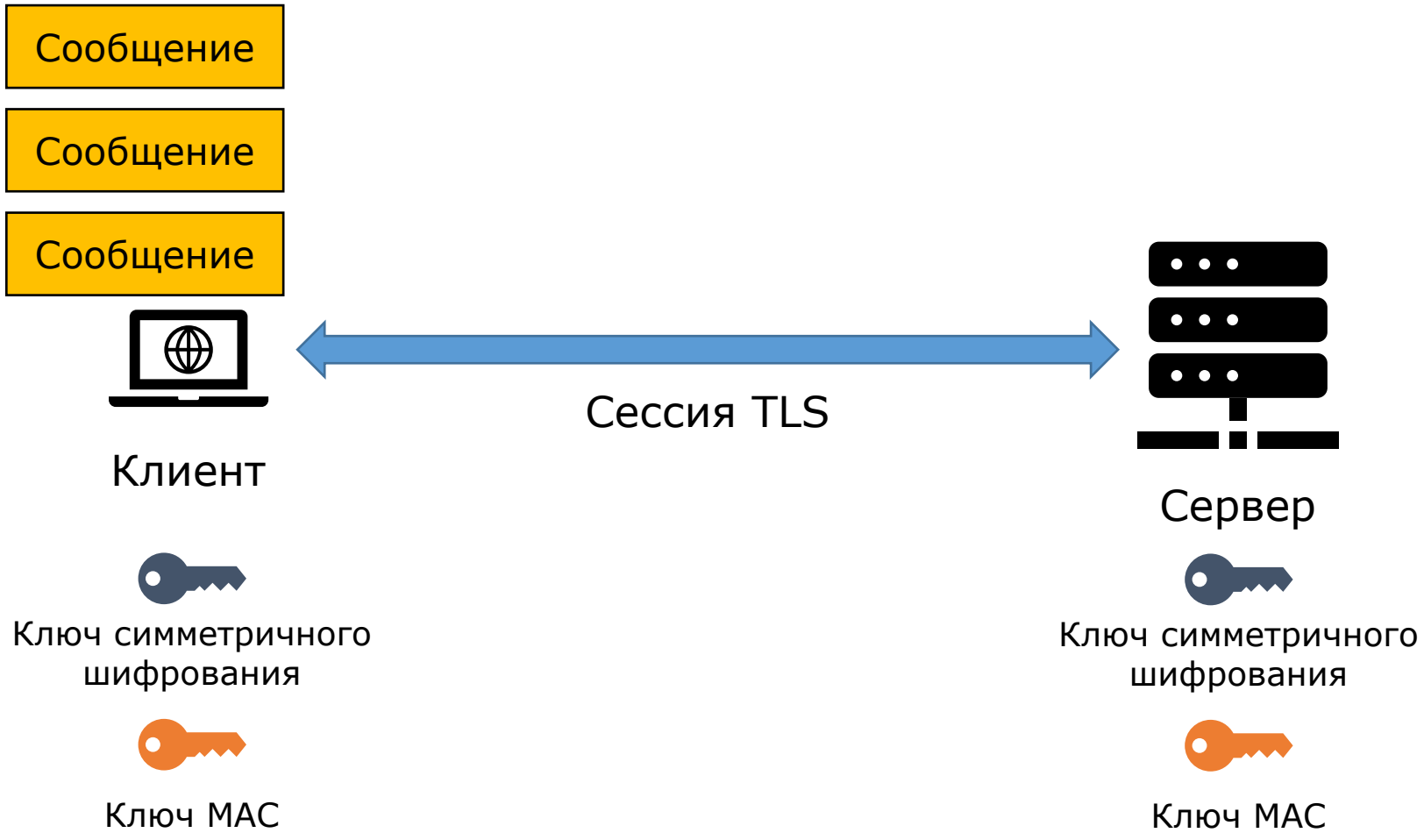
Создание сессии:

- Установка соединения с помощью Handshake protocol
- Возобновление соединения, которое было установлено ранее

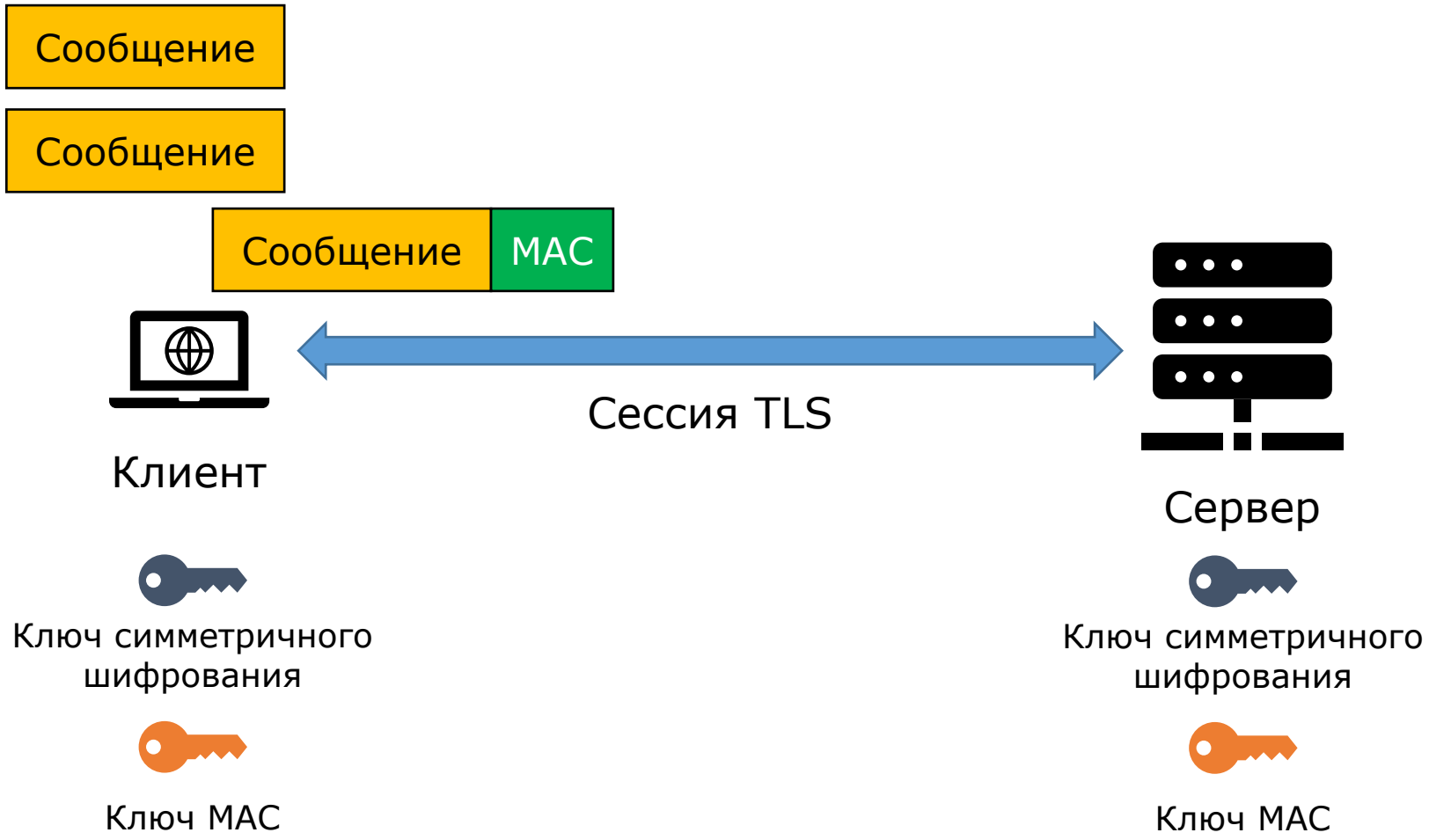
Протокол передачи данных в TLS



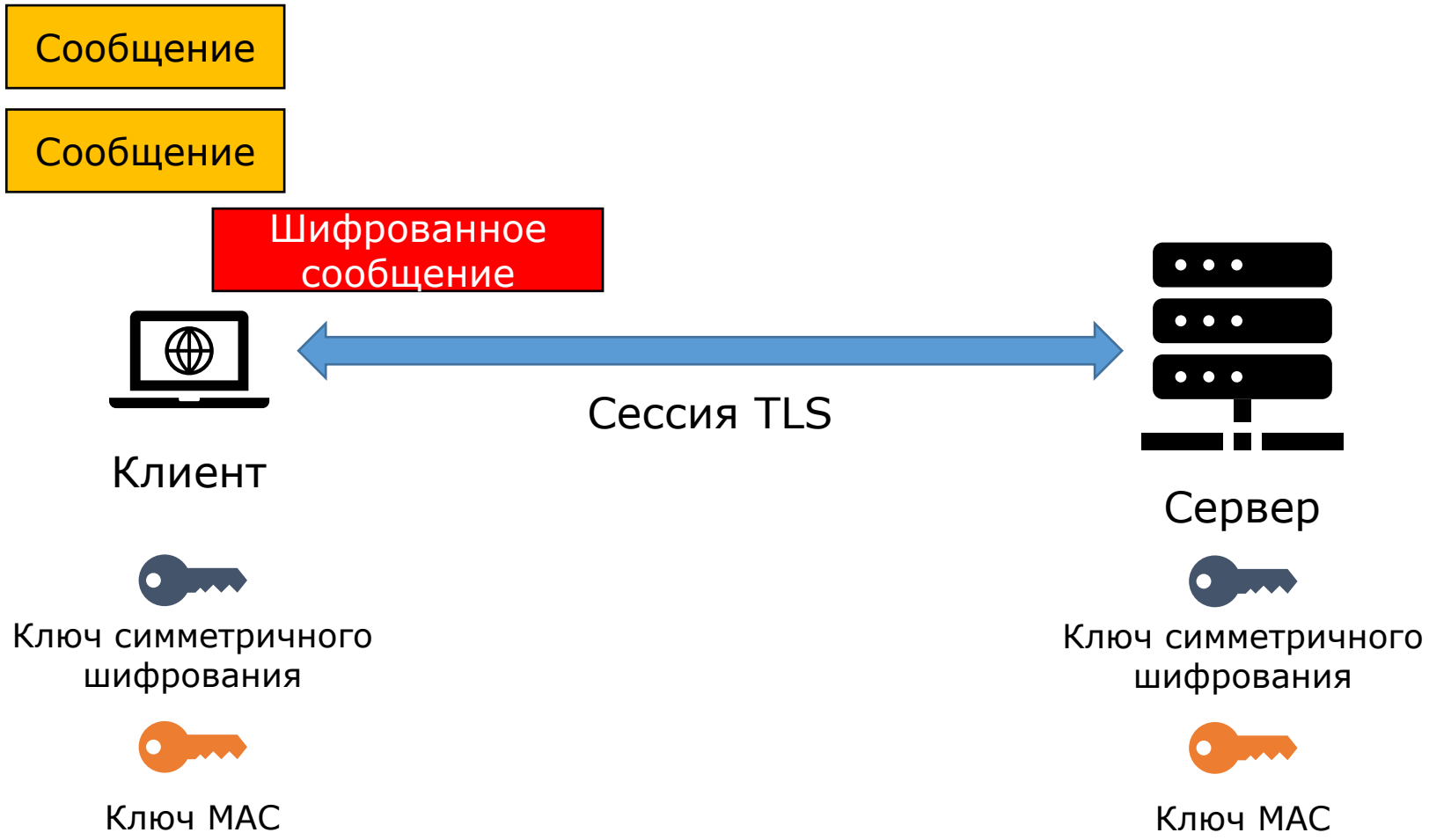
Протокол передачи данных в TLS



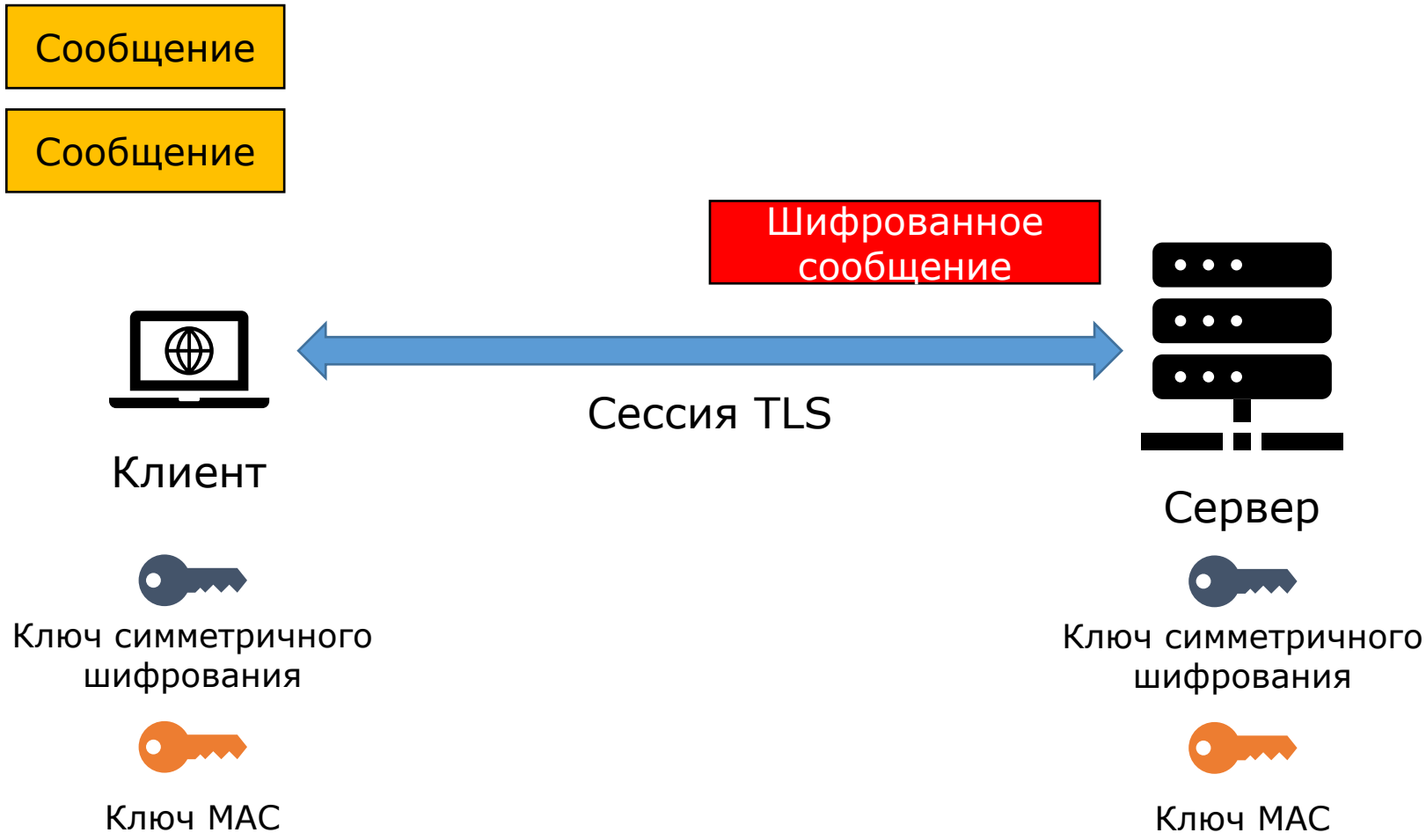
Протокол передачи данных в TLS



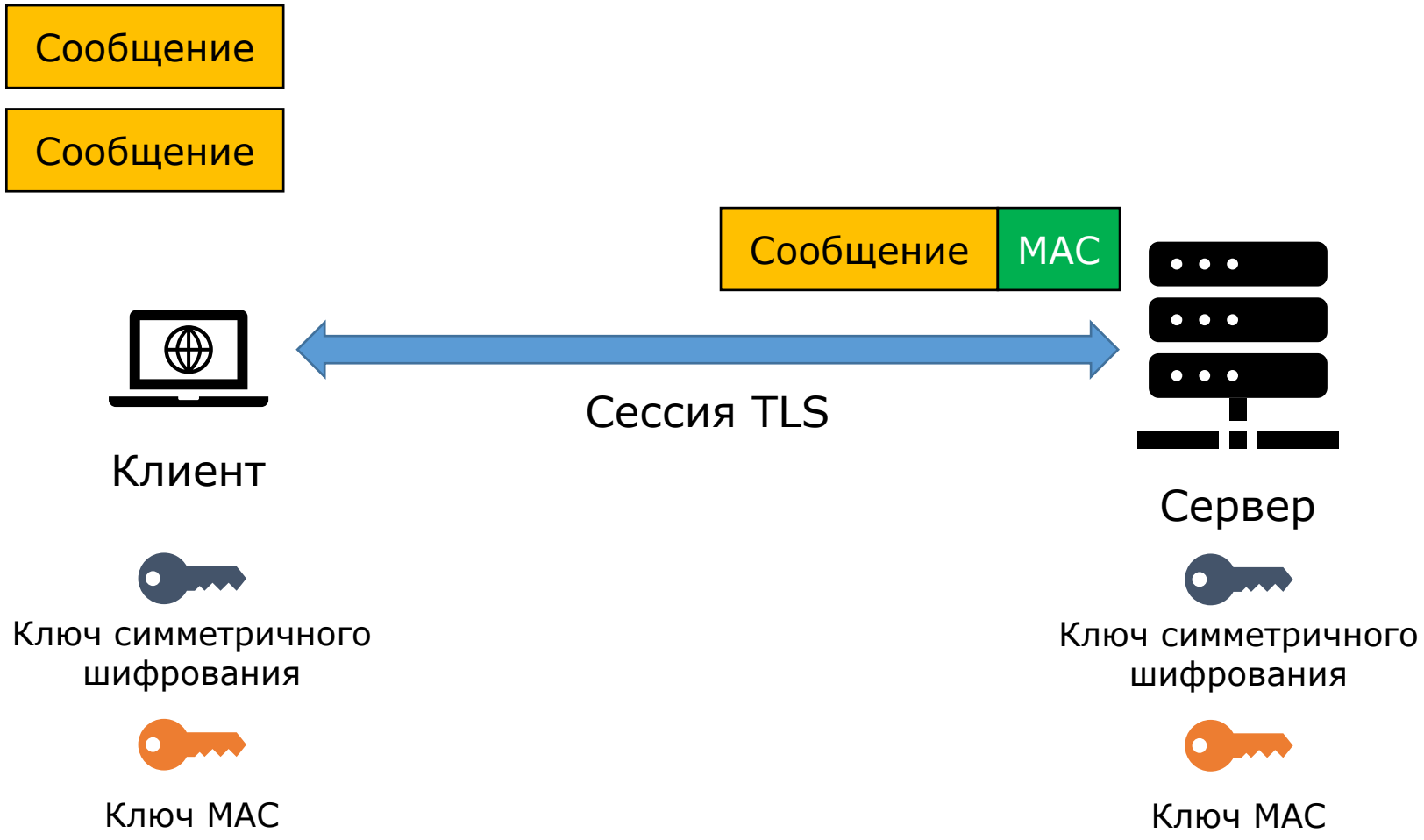
Протокол передачи данных в TLS



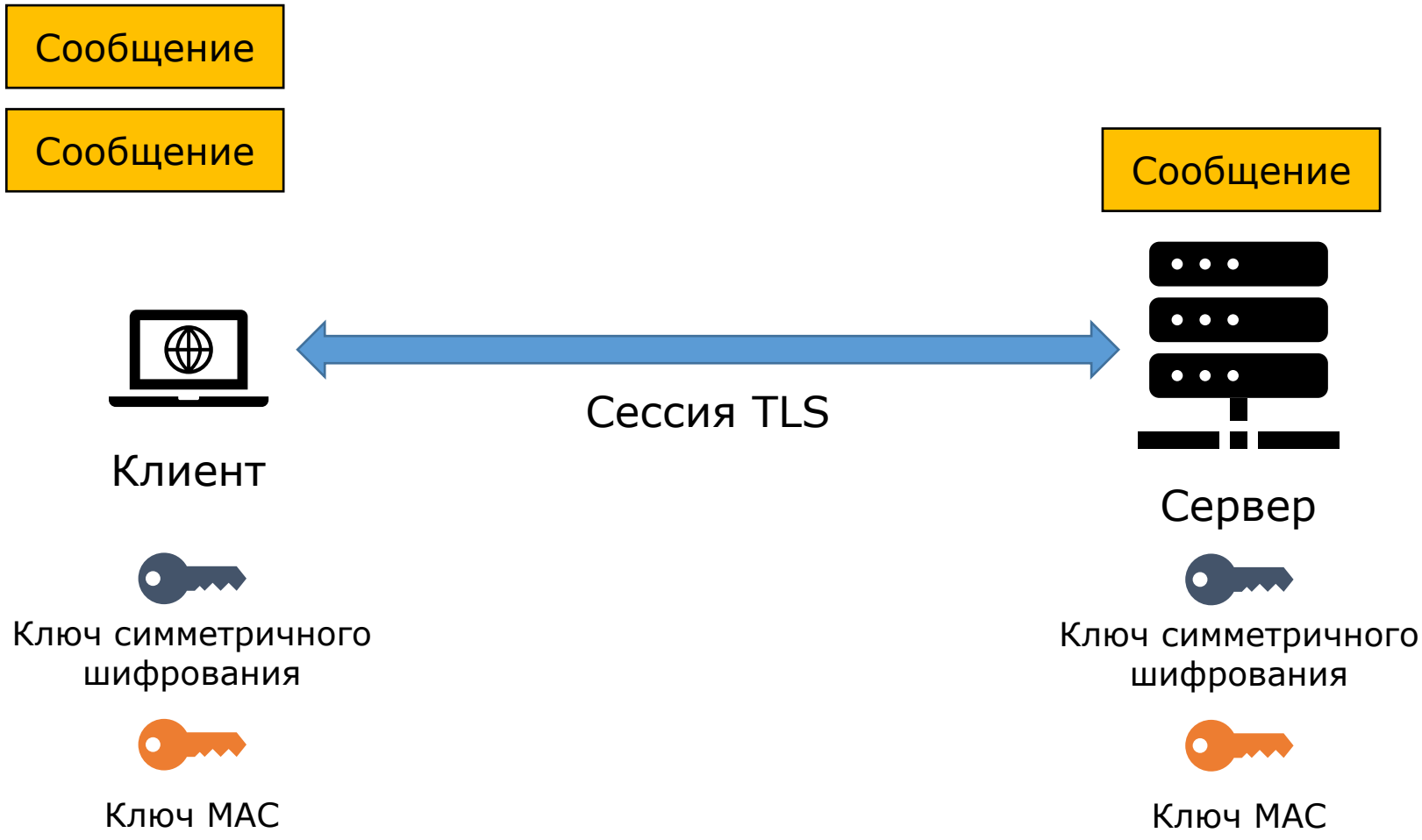
Протокол передачи данных в TLS



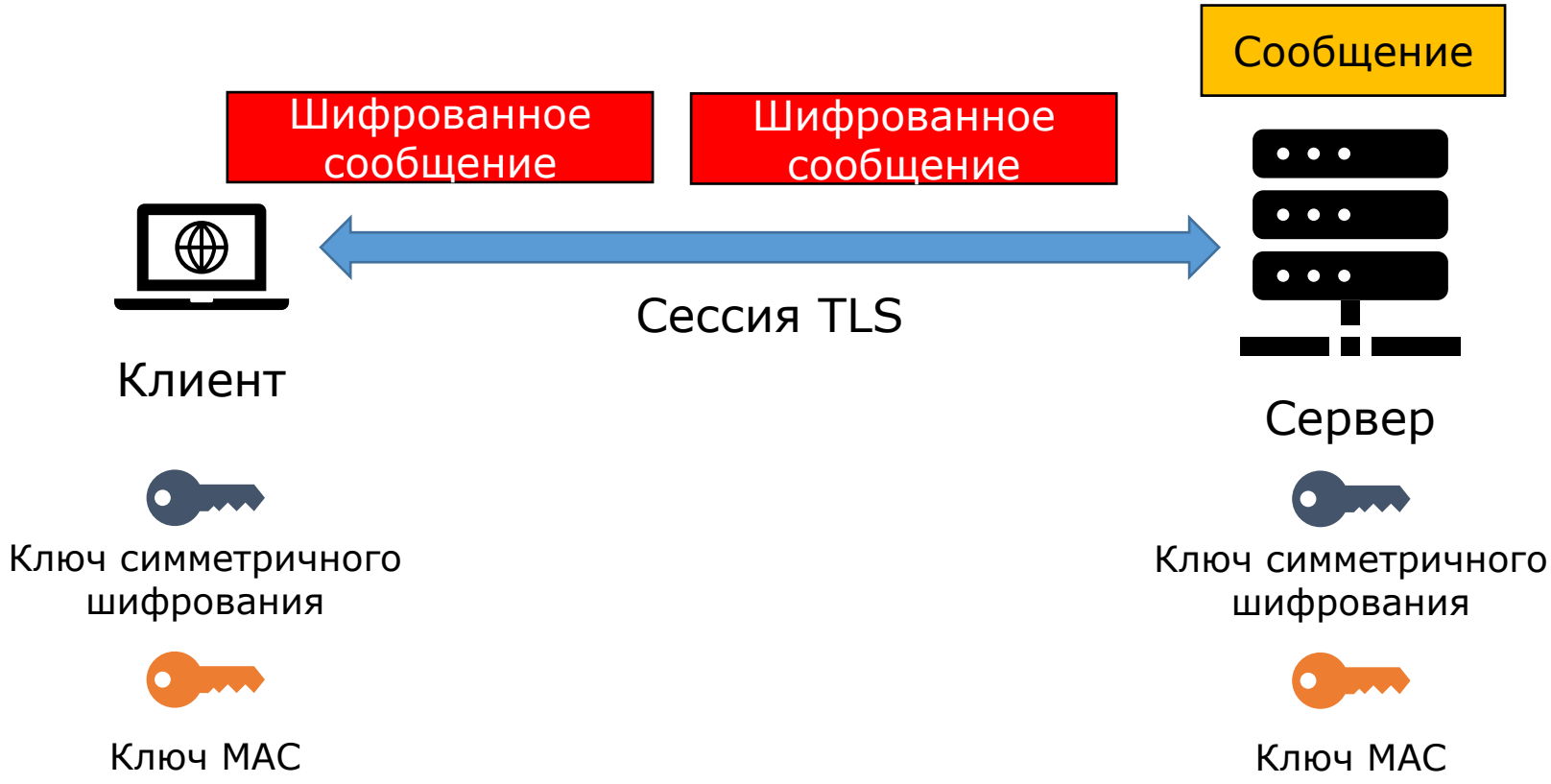
Протокол передачи данных в TLS



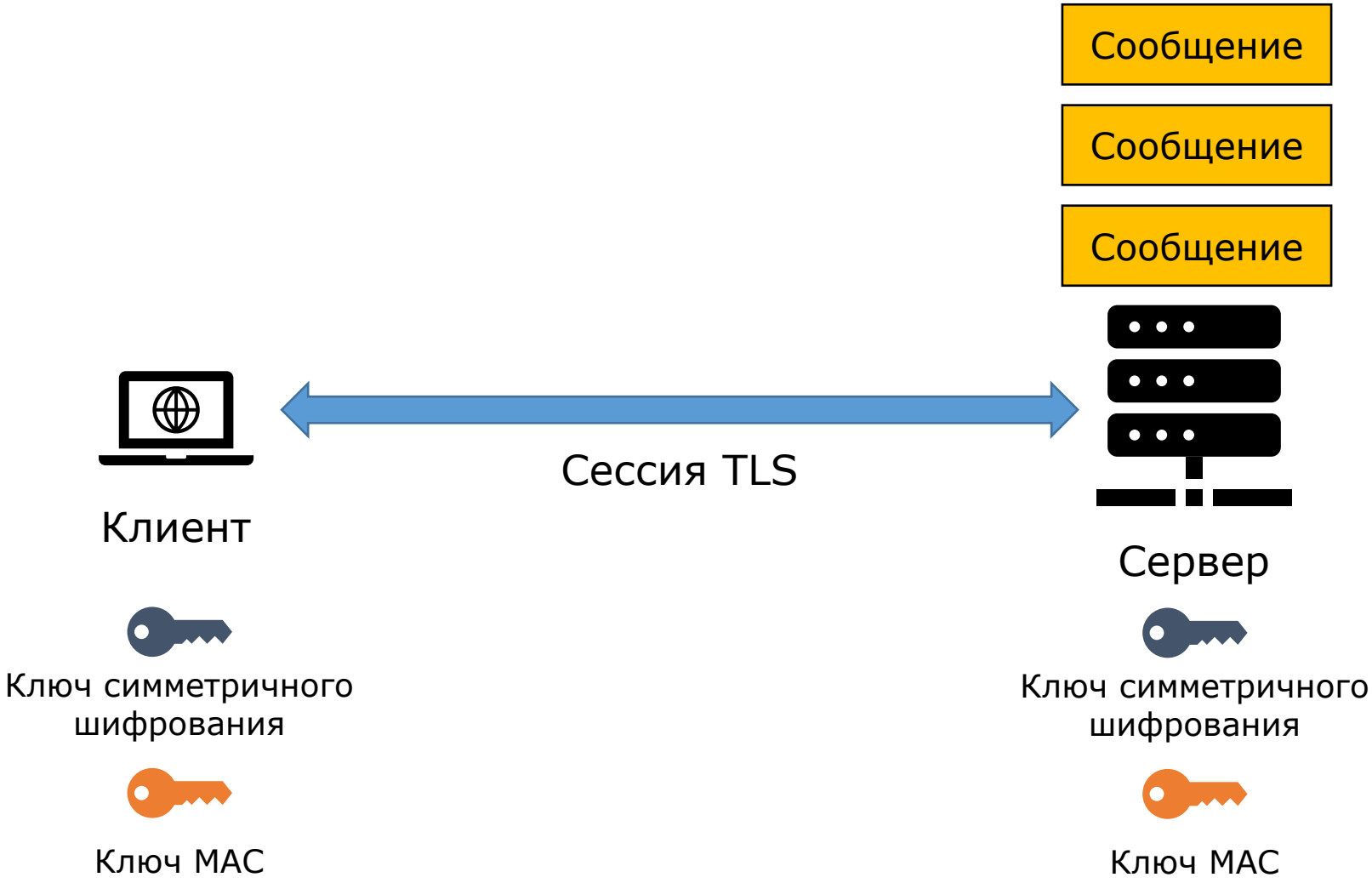
Протокол передачи данных в TLS



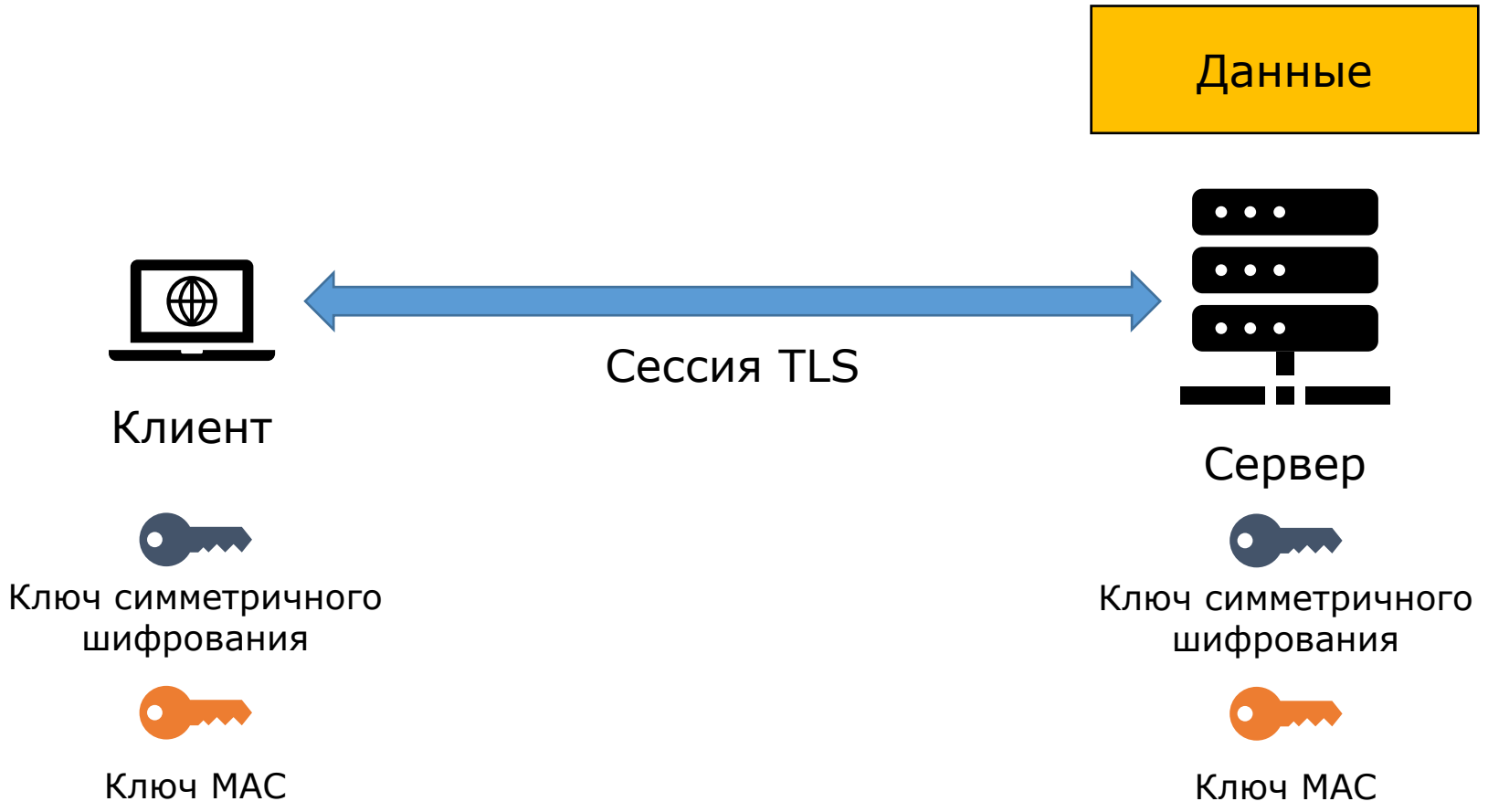
Протокол передачи данных в TLS



Протокол передачи данных в TLS



Протокол передачи данных в TLS



Протокол оповещений

Протокол оповещение (alert protocol):

- Сообщения об ошибках в работе TLS

Фатальные ошибки:

- Сессия TLS должна быть разорвана немедленно
- Ошибка MAC (bad_record_mac)
- Неизвестный удостоверяющий центр (unknown_ca)
- Ошибка расшифровки (decrypt_error)

Предупреждения:

- Сессия может продолжать работать
- Срок действия сертификата завершен (certificate_expired)
- Сертификат отозван (certificate_revoked)
- Неизвестный формат сертификата (unsupported_certificate)

Итоги

Протокол TLS:

- Описывает, как использовать шифрование, MAC и сертификаты для обеспечение безопасной передачи данных

Уровни TLS:

- Протокол записей
- Протоколы установки соединения, оповещения, смены шифра, передачи данных

Сессия в TLS:

- Типы алгоритмов шифрования и ключи шифрования

Протокол передачи данных в TLS:

- Вычисление MAC с последующим шифрованием