Сети, часть 3. Домашнее задание

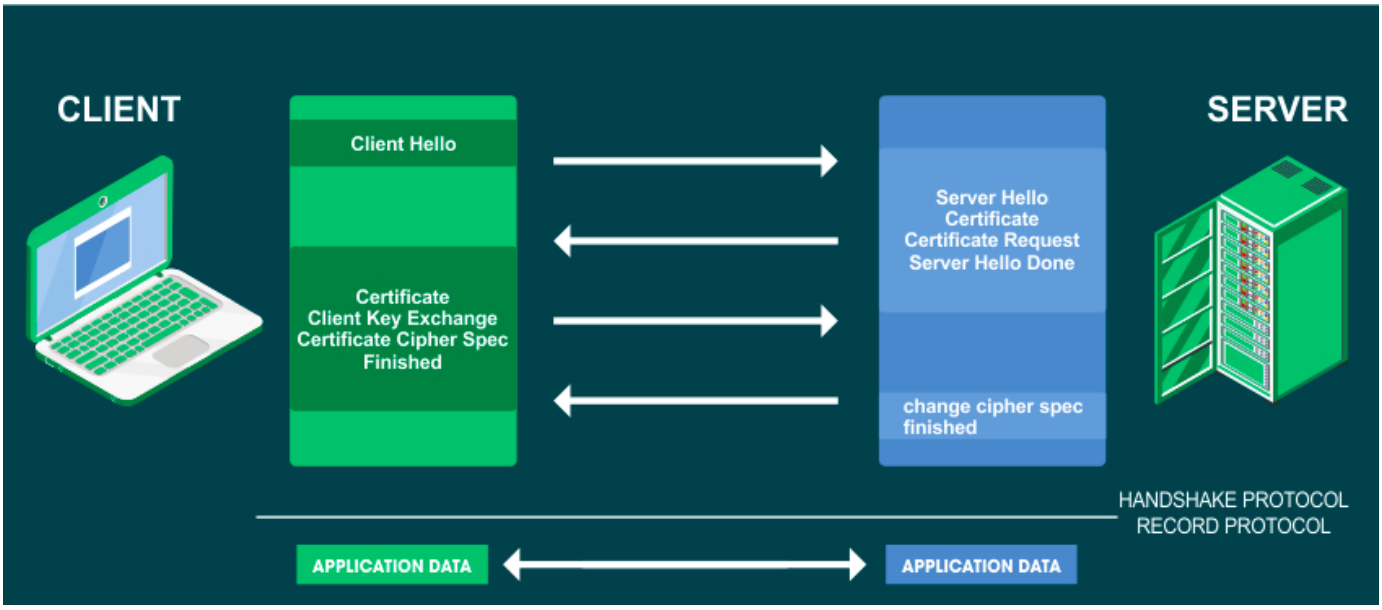
1. Перечислите пять компаний, которые являются корневыми международными центрами сертификации

Ответ:

1. IdenTrust;
2. DigiCert;
3. Sectigo (Comodo Cybersecurity);
4. Let’s Encrypt;
5. GoDaddy

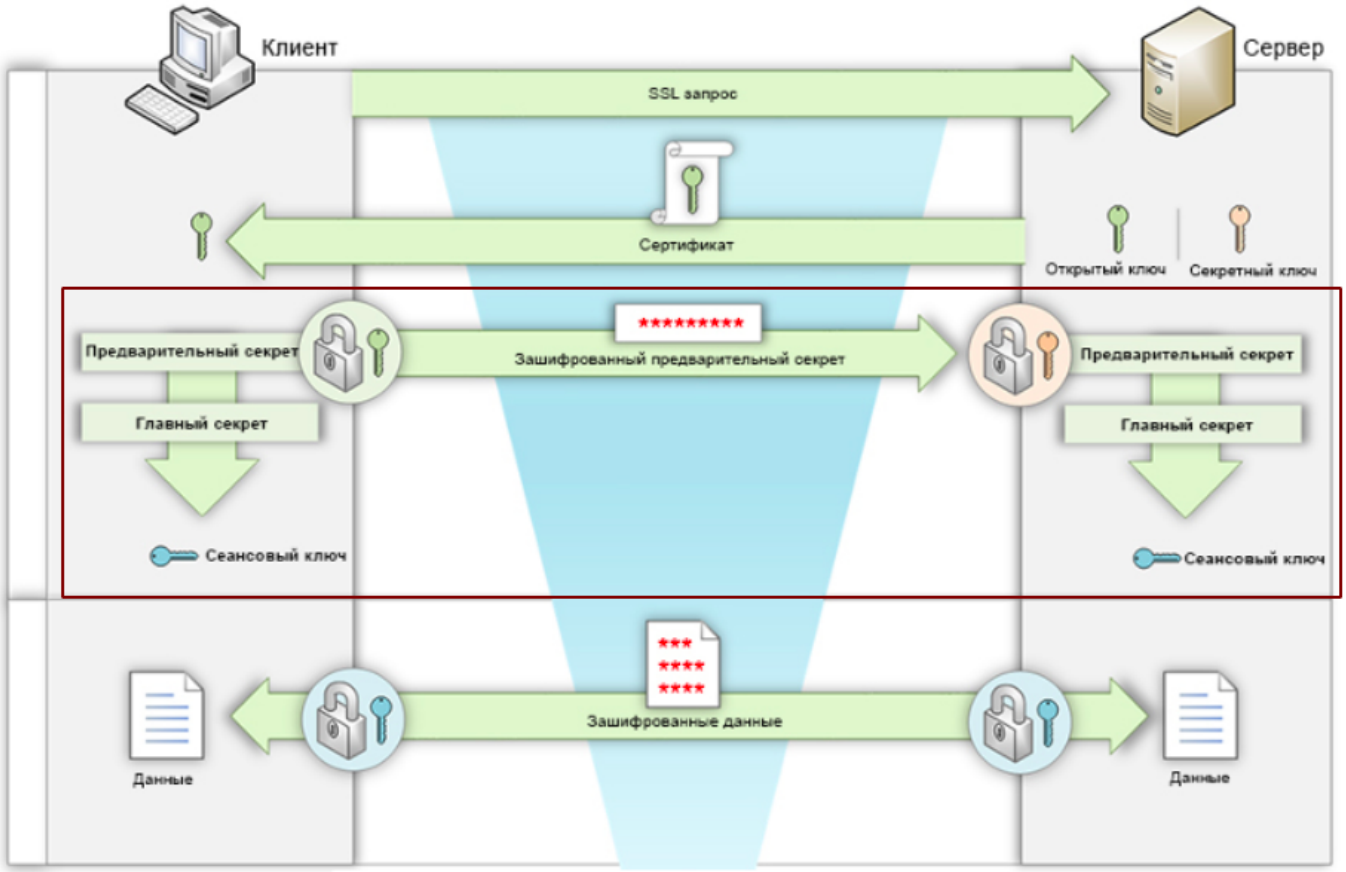
Опишите процесс аутентификации с помощью клиентского и серверного сертификата посредством протокола SSL/TLS

Ответ:



1. Первым делом клиент отправляет сообщение Client Hello, запрос на создание безопасного соединения. Это сообщение также содержит версию TLS (TLS 1.0, 1.2, 1.3 и т. д.), поддерживаемую клиентом, список поддерживаемых наборов шифров (алгоритм обмена ключами, алгоритм массового шифрования, алгоритм MAC, псевдослучайная функция, записанная по порядку), список методов сжатия (необязательно) и расширений, а также случайную строку, которая будет использоваться для генерации криптографических сеансовых ключей.

2. Сервер отвечает сообщением Server Hello. Это сообщение содержит версию TLS, поддерживаемую сервером, номер идентификатора сеанса, шифр, выбранный из предпочтительного списка клиентов, алгоритм сжатия, согласованный обеими сторонами (необязательно), и случайную строку байтов, созданную сервером, которая позже используется для генерации криптографические ключи.
3. Сервер также отправляет цепочку сертификатов, которая является доказательством личности сервера, которое должно быть аутентифицировано и проверено клиентом из клиентского хранилища сертификатов доверия. Цифровая подпись ЦС вместе с открытым ключом сервера прикрепляется к цепочке сертификатов, и клиент проверяет все подписи в сертификате, пока не будет получен корневой сертификат ЦС.
4. Серверу необходимо аутентифицировать сертификат клиента. Следовательно, сервер отправляет запрос на получение клиентского сертификата с указанием типа сертификата, алгоритмов подписи сертификата и ЦС, поддерживаемых сервером (из хранилища доверенных сертификатов сервера).
5. В конце сервер отправляет Server Hello Done и ждет ответа.
6. Когда сервер запрашивает аутентификацию клиента, клиент подтверждает это с помощью сертификата клиента. Перед отправкой сертификата клиент сверяет DN эмитента со списком доверенных ЦС сервера. Если DN эмитента отсутствует, клиент воздержится от отправки сертификата клиента на сервер.
7. Обмен предварительными секретами. Клиент на своей стороне вырабатывает предварительный секрет (большое случайное число), шифрует его на публичном ключе сервера, и этот зашифрованный секрет отправляет по сети серверу.Сервер, используя свой приватный ключ, расшифровывает предварительный секрет, и обе стороны независимо друг от друга вырабатывают Главный секрет, используя криптографическую магию. После того, как на обеих сторонах имеется одинаковый главный секрет, вырабатываются сеансовые ключи. На их основе уже и происходит шифрование траффика через симметричный алгоритм шифрования.



8. Клиент проверяет сертификат сервера.
9. Клиент уведомляет сервер, что процесс рукопожатия пройден успешно, в конце обе стороны обмениваются зашифрованными данными.