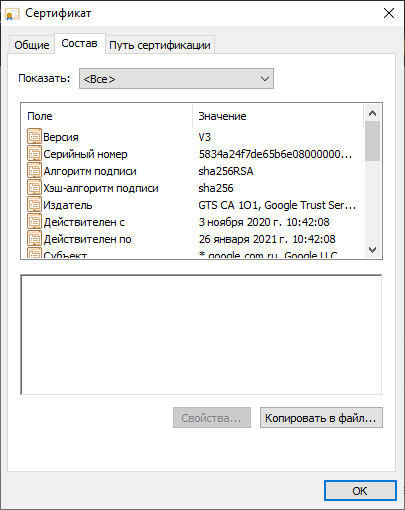
Лабораторная работа №8

Задачи:

1. Продемонстрировать и объяснить поля цифрового сертификата на SSL-соединении
2. Продемонстрировать отправку сообщения по электронной почте через telnet

Ход выполнения:

1. SSL (англ. Secure Sockets Layer — слой защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений

Состав SSL сертификата на сайте google.com

**Версия**Указывает номер версии закодированного сертификата. Текущие возможные значения этого поля: 0, 1 или 2.

**Серийный номер**  
Содержит положительное уникальное целое число, присвоенное сертификату центром сертификации (ЦС).

**Алгоритм подписи**

Содержит идентификатор объекта (ИО), указывающий алгоритм, применявшийся ЦС для подписания сертификата. Например, 1.2.840.113549.1.1.5 указывает на использование хэш-алгоритма SHA-1 вместе с алгоритмом шифрования RSA, разработанного RSA Laboratories.

**Поставщик**

Содержит различающееся имя (РИ) X.500 ЦС, создавшего и подписавшего сертификат.

**Срок действия**

Указывает промежуток времени, в течение которого действует сертификат. Для дат до конца 2049 года используется формат всемирного координированного времени (времени по Гринвичу) (ггммддччммссз). Для дат с 1 января 2050 года используется универсальный формат времени (ггггммддччммссз).

**Субъект**Содержит различающееся имя X.500 объекта, связанного с открытым ключом, содержащимся в сертификате.

**Открытый ключ**

Содержит открытый ключ и данные связанного алгоритма.

**Уникальный идентификатор поставщика**

Содержит уникальное значение, которое может быть использовано для того, чтобы имя ЦС по стандарту X.500 однозначно идентифицировало этот ЦС при последующем многократном использовании различными объектами.

**Уникальный идентификатор субъекта**

Содержит уникальное значение, которое может быть использовано для того, чтобы имя субъекта по стандарту X.500 однозначно идентифицировало этот субъект при последующем многократном использовании различными объектами.

**Идентификатор ключа центра сертификатов**

Идентифицирует открытый ключ центра сертификатов (ЦС), соответствующий закрытому ключу ЦС, который используется для подписания данного сертификата.

**Основные ограничения**

Определяет, может ли объект использоваться в качестве ЦС, и, если может, номера подчиненных ЦС, которые могут присутствовать в нисходящей цепочке сертификатов.

**Политики сертификата**

Определяет политики, регулирующие выдачу сертификата, и возможные цели его использования.

**Точки распространения списков отзыва сертификатов (CRL)**

Содержит URI основного списка отзыва сертификата (CRL).

**Использование улучшенного ключа**

Указывает механизм использования открытого ключа, содержащегося в данном сертификате.

**Дополнительное имя поставщика**

Определяет одну (или более одной) дополнительную форму имени для поставщика запроса сертификата.

**Использование ключа**

Определяет ограничения для операций, которые могут выполняться с использованием открытого ключа, содержащегося в данном сертификате.

**Ограничения имени**

Определяет пространство имен, в котором должны быть размещены все имена субъектов в иерархии сертификата. Это расширение используется только в сертификате ЦС.

**Ограничения политики**

Ограничивает проверку пути при помощи запрещения сопоставлений политики или требования, чтобы каждый сертификат в данной иерархии содержал допустимый идентификатор политики. Это расширение используется только в сертификате ЦС.

**Сопоставления политики**

Указывает, какие политики в подчиненном ЦС соответствуют политикам в выдающем ЦС.

**Период использования закрытого ключа**

Указывает срок действия закрытого ключа, отличающийся от срока действия сертификата, с которым связан этот закрытый ключ.

**Дополнительное имя субъекта**

Определяет одну (или более одной) дополнительную форму имени для субъекта запроса сертификата. Примеры дополнительных форм могут включать адреса электронной почты, DNS-имена, IP-адреса и URI.

**Атрибуты каталога субъекта**

Сообщает атрибуты идентификации, например национальную принадлежность субъекта сертификата. Значением расширения является последовательность пар значений кодов объекта (OID)

**Идентификатор ключа субъекта**

Служит для разделения нескольких открытых ключей, держателем которых является субъект сертификата. Значением расширения обычно является хэш SHA-1 ключа.

1. Отправка сообщения при помощи telnet

