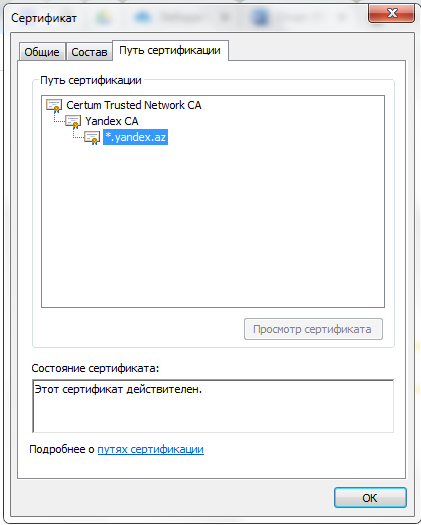
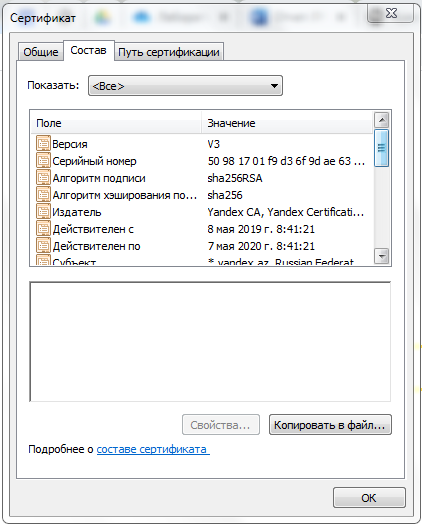
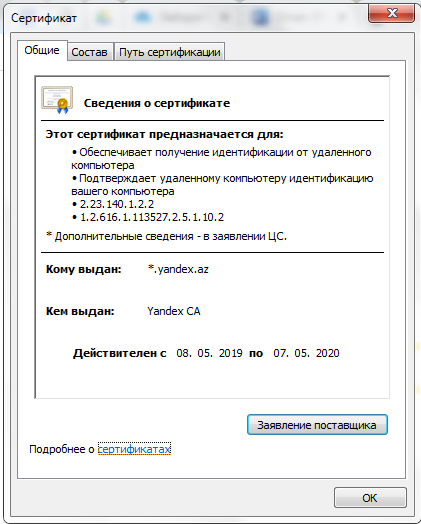
Сетевая безопасность

**Продемонстрировать и объяснить поля цифрового сертификата на SSL-соединении**

  
Вкладка «Общие»

Можно просмотреть сведения о полях, расширениях и свойствах, которые определяют выданный сертификат. Для этого дважды щелкните любой сертификат, отображенный в хранилище сертификатов.  
На вкладке Общие содержатся общие сведения о сертификате.

1. Поддерживаемые способы использования сертификата. Сводные сведения о приложениях, подписывании, шифровании и проверке подлинности, поддерживаемых сертификатом. В этой области также содержатся сведения об истечении срока действия и действительности сертификата.
2. Кому выдан сертификат. Имя получателя сертификата. Получателями сертификатов могут быть пользователи, компьютеры или такие субъекты, как центры сертификации.
3. Кем выдан сертификат. Название центра сертификации, выдавшего сертификат.
4. Срок действия сертификата. Период с начала действия сертификата до окончания срока его действия.
5. Заявление поставщика. При нажатии кнопки Заявление поставщика открывается новое окно с дополнительными сведениями о сертификате или URL-адресом страницы, содержащей дополнительную информацию.

На вкладке «Сведения» отображается следующая информация о сертификате.

1. Версия. Номер версии протокола X.509.
2. Серийный номер. Уникальный серийный номер, присвоенный сертификату центром сертификации. Серийный номер уникален для всех сертификатов, выданных определенным центром сертификации.
3. Алгоритм подписи. Алгоритм хеширования, используемый центром сертификации для цифровой подписи сертификата.
4. Издатель. Информация о центре сертификации, выдавшем сертификат.
5. Действителен с. Начальная дата периода действия сертификата.
6. Действителен по. Конечная дата периода действия сертификата.
7. Субъект. Имя лица, компьютера, устройства или центра сертификации, которому выдан сертификат. Если выдающий сертификаты центр сертификации находится на рядовом сервере домена предприятия, это будет различающееся имя внутри предприятия. Иначе это может быть полное имя и адрес электронной почты или другой персональный идентификатор.
8. Открытый ключ. Тип и длина открытого ключа, связанного с сертификатом.
9. Алгоритм отпечатка. Алгоритм хеширования, по которому формируется сводка данных (или отпечаток) для цифровых подписей.
10. Отпечаток. Сводка данных (или отпечаток) сертификата.
11. Понятное имя. (Необязательно.) Отображаемое имя, которое будет использоваться вместо имени, указанного в поле «Субъект».
12. Улучшенный ключ. (Необязательно.) Цели, в которых может использоваться сертификат.

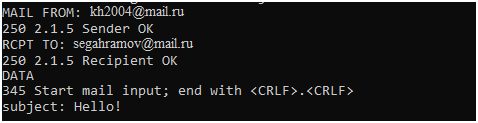
На вкладке «Путь» сертификации отображается путь от выбранного сертификата до центров сертификации, выдающих сертификат.

Прежде чем сертификат станет доверенным, системе Windows необходимо убедиться, что он получен из надежного источника. Эта процедура проверки называется подтверждением пути.

Подтверждение пути включает обработку сертификатов открытых ключей и сертификатов соответствующих издателей по иерархической структуре вплоть до завершения пути сертификации доверенным самозаверяющим сертификатом. Обычно цепочка завершается сертификатом корневого центра сертификации. Если при обработке одного из сертификатов в пути возникает проблема или не удается найти сертификат, путь сертификации считается ненадежным.

Обычно путь сертификации включает корневой сертификат, а также один или несколько промежуточных сертификатов. Нажав кнопку Просмотреть сертификат, можно получить дополнительные сведения о сертификатах каждого центра сертификации в пути.

**Продемонстрировать отправку сообщения по электронной почте через telnet**


**Настроить сетевую трансляцию адресов (SNAT) для общего доступа в интернет**

Эту настройку можно включить/отключить в админ-панели роутера

