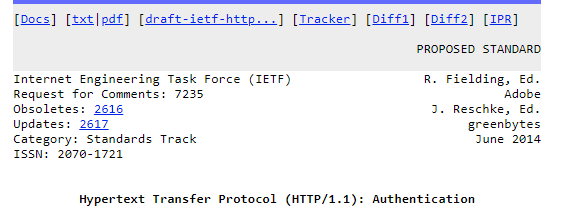
Программирование в интернет

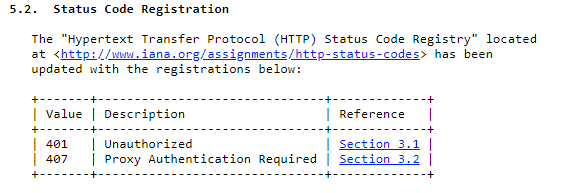
ИСиТ, ПОИБМС, 3к

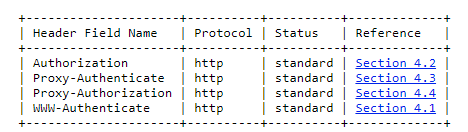
**HTTP Authentication**

1. **Идентификация** – заявление пользователя о себе.
2. **Аутентификация** – процедура проверки подлинности идентификации пользователя.
3. **Авторизация** -процедура проверки прав аутентифицированного пользователя.

1. **HTTP Authentication**:

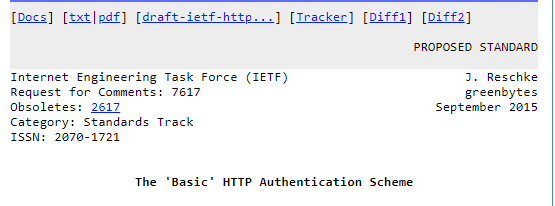






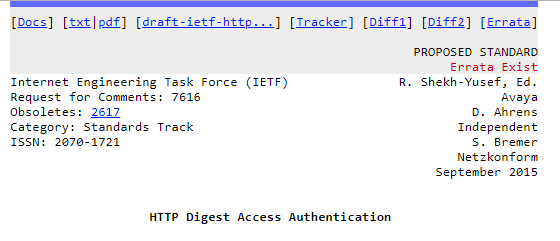


1. **HTTP Authentication**: **BASIC**

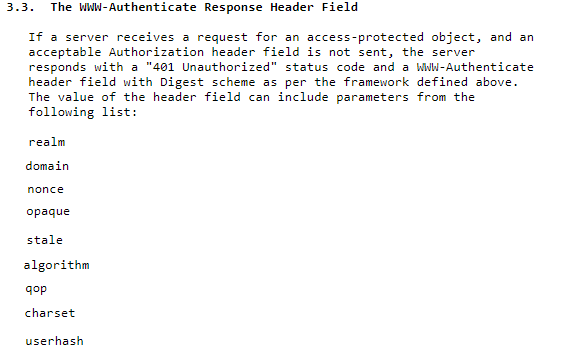


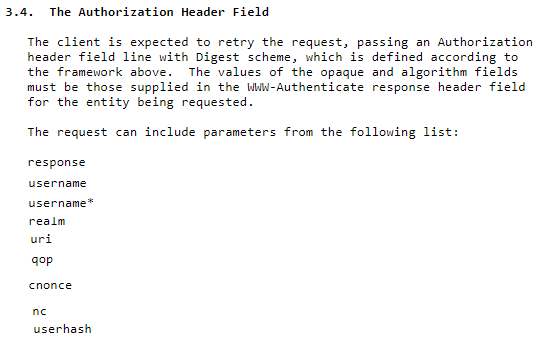


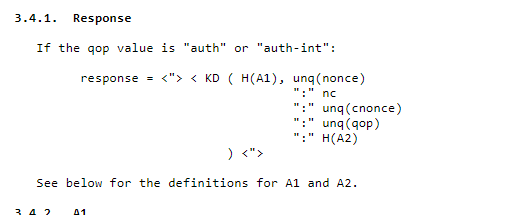
1. **HTTP Authentication**: **Digest**

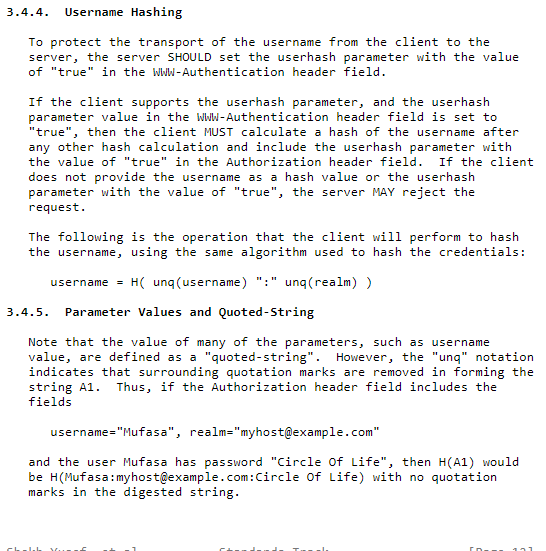








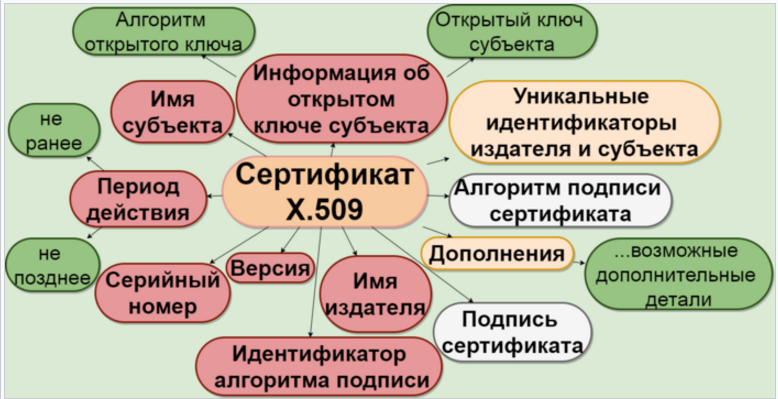




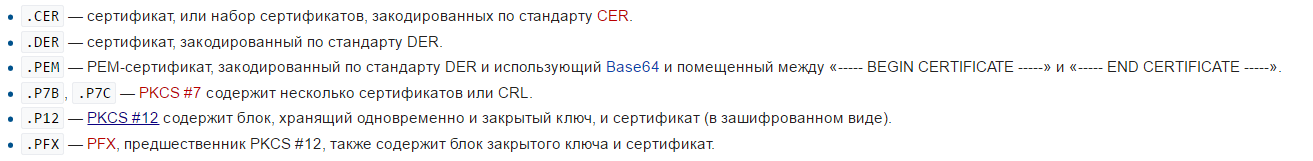
1. **HTTP Authentication**: Forms (нет стандарта, но применяется)



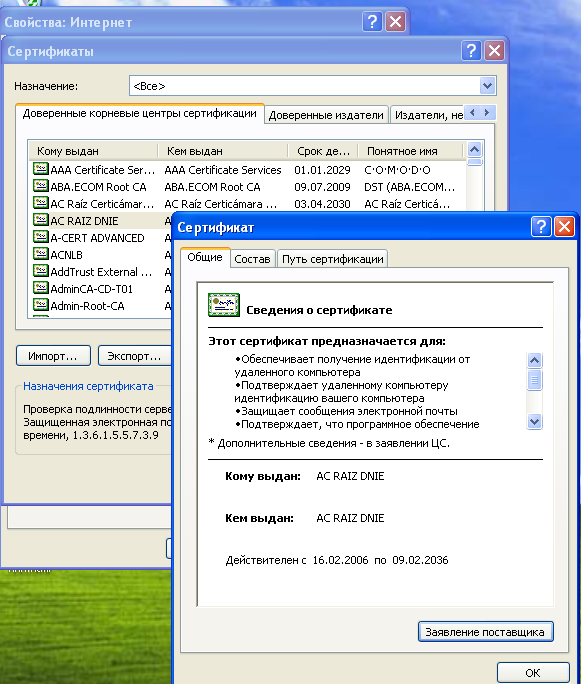
1. **HTTP Authentication**: TSL-аутентификация.
2. **Сертификат X.509:** стандартныйформат хранения и транспортировки атрибутов безопасности; главное – открытый ключ; сертификаты выдают центры сертификации (Certificate Authority, CA). <http://www.thwate.com>, <http://www.Verysign.com>; если это intranet, то можно использовать **Certificate Server Active Directory**; сертификат содержит: имя держателя, адрес, серийный номер сертификата, даты проверки, открытый ключ держателя.

****

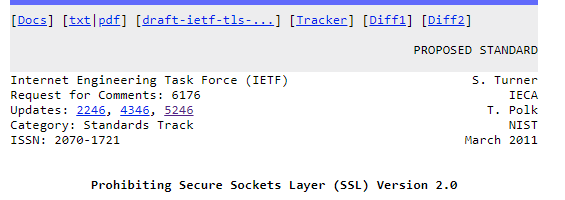
1. **Сертификат X.509:** Выдает центр сертификации (СА). <http://www.thwate.com>, <http://www.Verysign.com>. Если это intranet, то можно использовать **Certificate Server Active Directory**. Сертификат содержит: имя держателя, адрес, серийный номер сертификата, даты проверки, открытый ключ держателя.
2. **Сертификат X.509:** форматы файлов сертификатов X.509

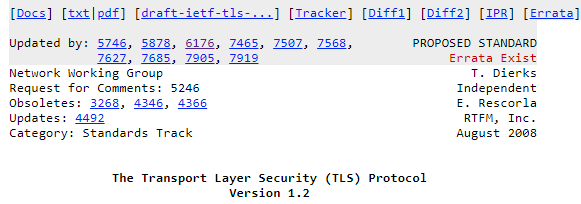


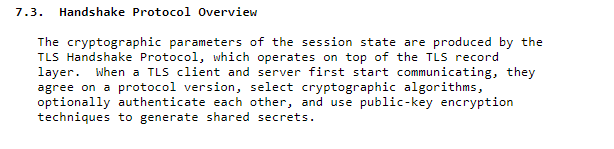
1. **Сертификат X.509:** хранилище сертификатов

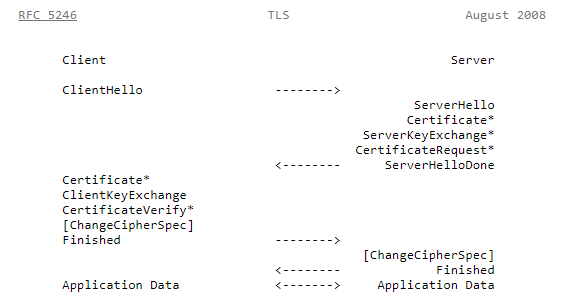


1. **TLS:** 1)обеспечиваетконфиденциальность; 2) обеспечивает целостность (обнаружение подмены); 3) аутентификация узлов (проверка подлинности источника сообщений); последняя версия 1.2, в разработке 1.3 (значительные изменения от 1.2); поверх потокового надежного соединения (для ненадежной передачи есть DTSL);
2. **TLS. RFC 2246,** новое название **Transport Layer Security (TLS).** Последние обновления RFC 5246, 6176**.**





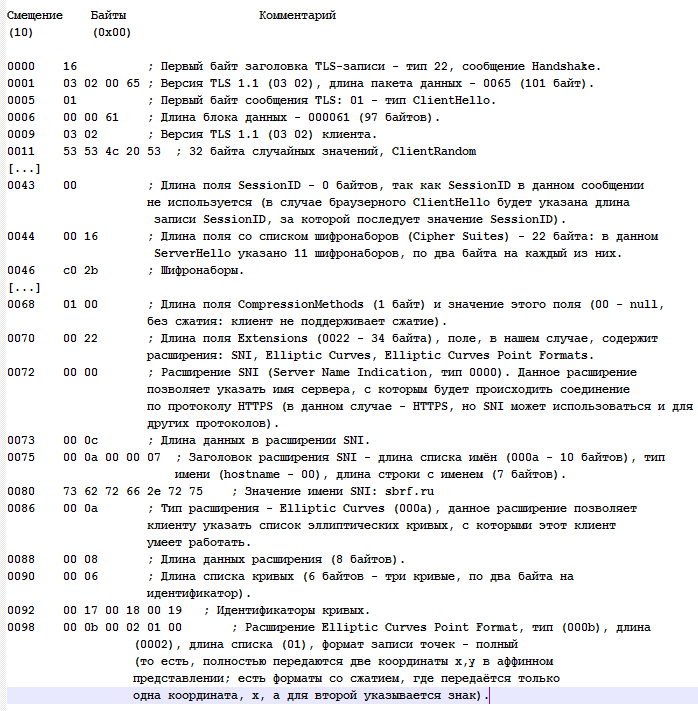




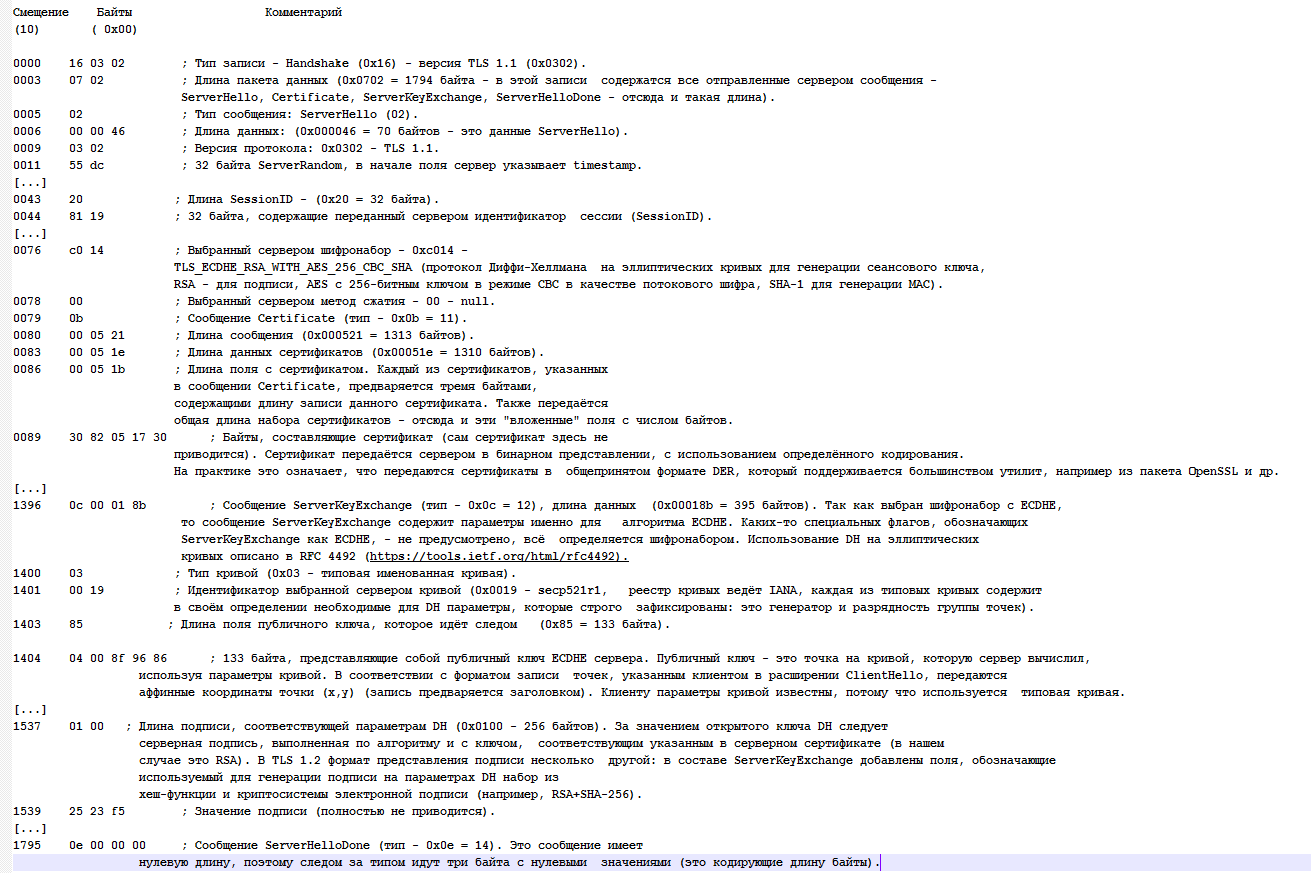
1. **TLS:**  пересылает записи



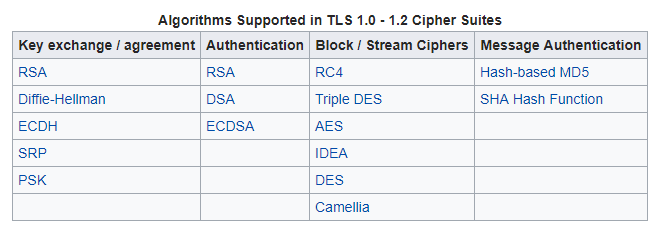
1. **TLS:** Client Hello, пример

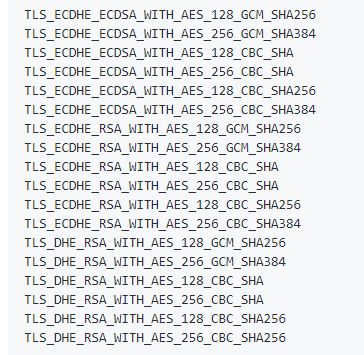


1. **TLS:** Server Hello, пример

****

1. **TLS:**  Cipher Suites – шифронаборы; в шифронабор входит: криптосистема для аутентификации сервера и сеансового секрета; шифр для защиты передаваемых данных; хеш-функция для кода аутентификации HMAC.

****

****

**TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256**

**ECDHE -** Диффи-Хеллман на эллиптических кривых для вычисления общего секрета;

**ECDSA -** аутентификацияданных на этапе установления соединения на основе цифровой подписи на эллиптических кривых;

**AES\_128** – шифрование полезной нагрузки с помощью алгоритма AES с 128-битным ключом в режиме GCM;

**SHA256** -для хеширования применяется алгоритм SHA с 256-битным ключом.

1. **TLS:** Схема работы
2. **Клиент** выдает запрос серверу (Client Hello).
3. **Сервер** подписывает свой сертификат и высылает клиенту (Server Hello).
4. **Клиент** проверяет сертификат в центре сертификации, которому доверяет.
5. **Клиент** сравнивает данные сертификата с информацией центра сертификации.
6. **Клиент** сообщает серверу, какие ключи шифрования он поддерживает.
7. **Сервер** выбирает подходящую длину ключа.
8. **Клиент** генерирует симметричный ключ, шифрует его открытым ключом.
9. **Сервер** получает симметричный ключ и расшифровывает его.



1. **NTLM** (Windows authentication): пароль не передается в чистом виде. Эта схема не является стандартом HTTP, но поддерживается большинством браузеров и веб-серверов. Преимущественно используется для аутентификации пользователей Windows Active Directory в веб-приложениях.

1. **Negotiate** (Windows authentication): клиенту выбрать можно выбрать между NTLM и Kerberos -аутентификацией. Kerberos – протокол, основанный на принципе Single Sign-On, клиент и сервер должны находятся в зоне intranet и являться частью домена Windows.
2. OpenID
3. OAuth 2.0
4. WS-\*
5. Bearer
6. HOBA
7. Mutual