Лекция 24а

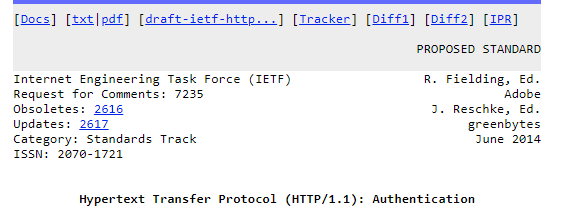
ПСКП, ПОИТ-3

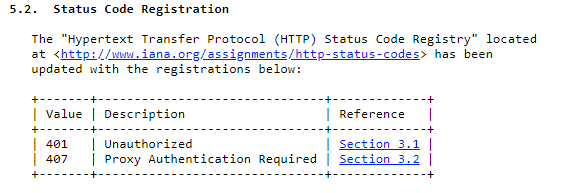
**HTTP-Аутентификация (Authenticate)**

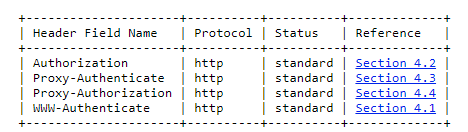
1. **Идентификация** – заявление пользователя о себе.
2. **Аутентификация** – процедура проверки подлинности идентификации пользователя.
3. **Авторизация** -процедура проверки прав аутентифицированного пользователя.



1. **HTTP Authentication**: заголовки, статус коды: 401, 403



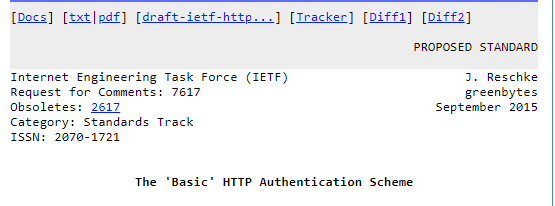




1. **HTTP Authentication**: общая схема

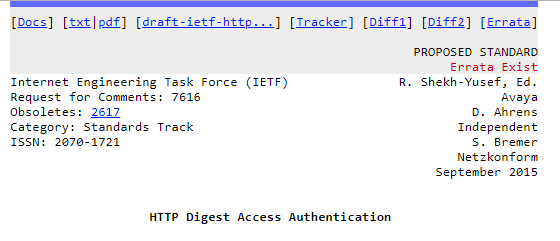


1. **HTTP Authentication**: **BASIC**

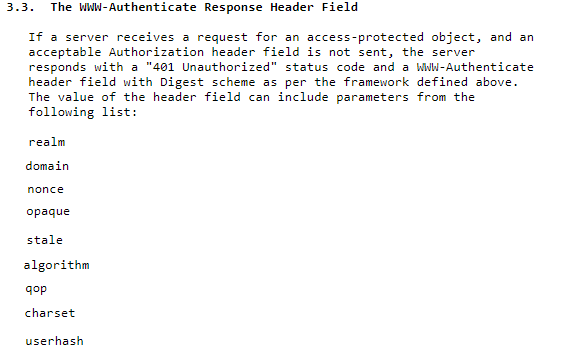


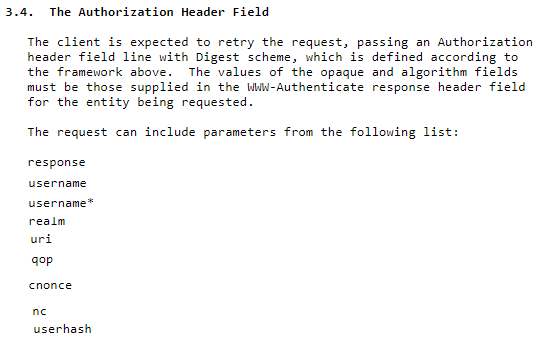


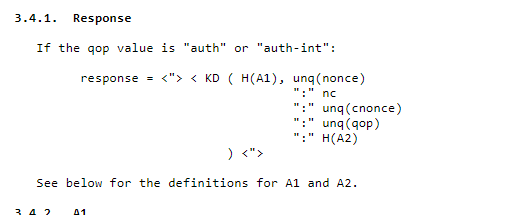
1. **HTTP Authentication**: **Digest**

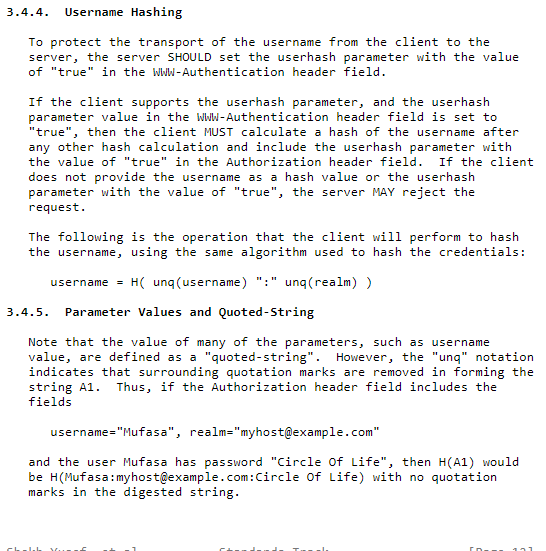








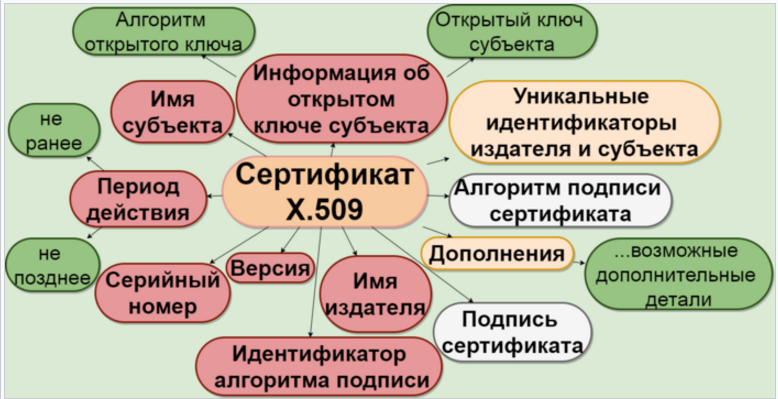




1. **Forms Authentication**: нет стандарта, но применяется



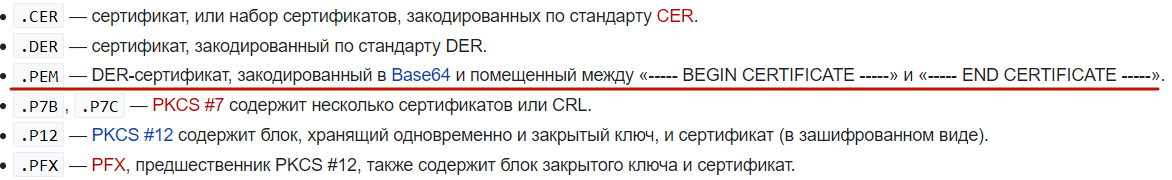
1. **Certificate Authentication**:cертификат X.509.
2. **Сертификат X.509:** стандартныйформат хранения и транспортировки атрибутов безопасности; главное – открытый ключ; сертификаты выдают центры сертификации (Certificate Authority, CA). <https://www.thawte.com/>, <https://www.verisign.com/>; если это intranet, то можно использовать **Certificate Server Active Directory**; сертификат содержит: имя субъекта, которому выдан сертификат, имя издателя, серийный номер, срок действия, открытый ключ субъекта, алгоритм подписи сертификата, подпись сертификата.

****

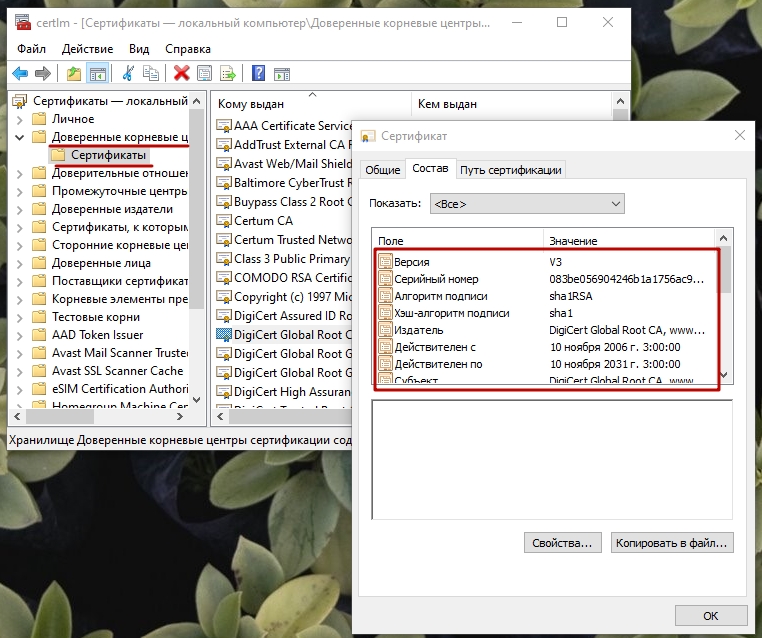
1. **Сертификат X.509:** во время аутентификации происходит проверка сертификата:
2. проверка подписи (д.б. подписан CA);
3. проверка срока действия (д.б. действительным);
4. проверка списком исключения (не д.б. CA).

После успешной аутентификации веб-приложение может выполнить авторизацию запроса на основании данных сертификата.

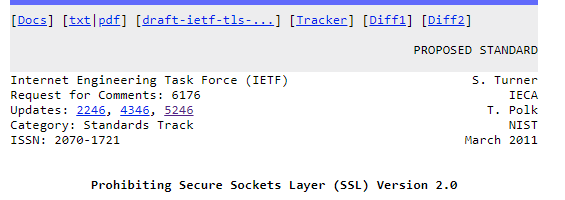
1. **Сертификат X.509:** форматы файлов сертификатов X.509

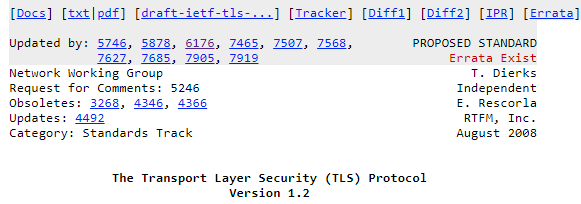


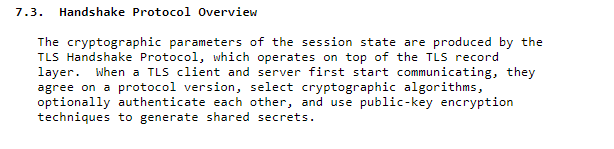
1. **Сертификат X.509:** хранилище сертификатов (Управление сертификатами компьютера –> Доверенные корневые центры серификации -> Сертификаты или Win+R -> *certmgr.msc*)

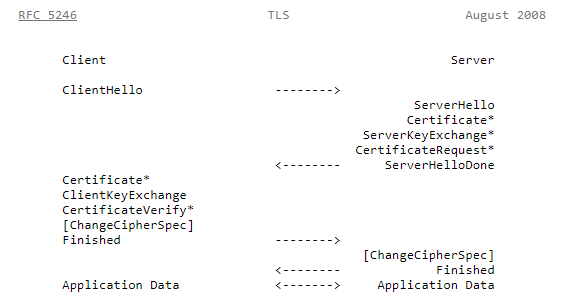


1. **TLS:** обеспечиваетконфиденциальность (сокрытие информации); обеспечивает целостность (обнаружение подмены); аутентификация узлов (проверка подлинности источника сообщений); последняя версия 1.3; поверх потокового надежного соединения (для ненадежной передачи есть DTSL);
2. **TLS. RFC 2246,** новое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









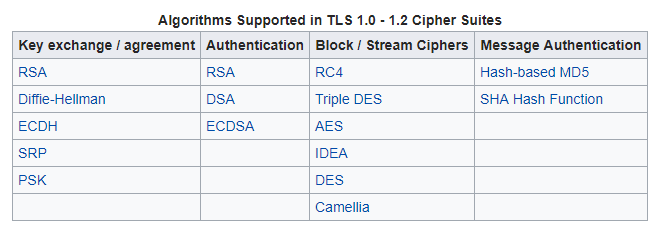
1. **TLS:** пересылает записи

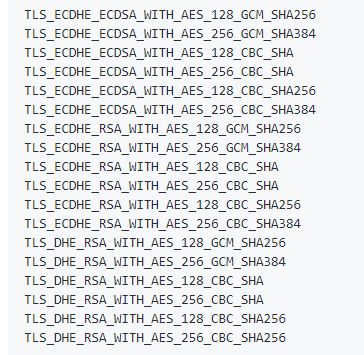


1. **TLS:** handshake



1. **TLS:** Cipher Suites – шифронаборы; в шифронабор входят: криптосистема для получения общего секрета; 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 генерации 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. **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.
2. **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. Для работы Kerberos клиенту необходимо запросить билет у KDC (центр распределения ключей, хранит базу данных с информацией об учётных записях всех клиентов сети).