Лекция 25а

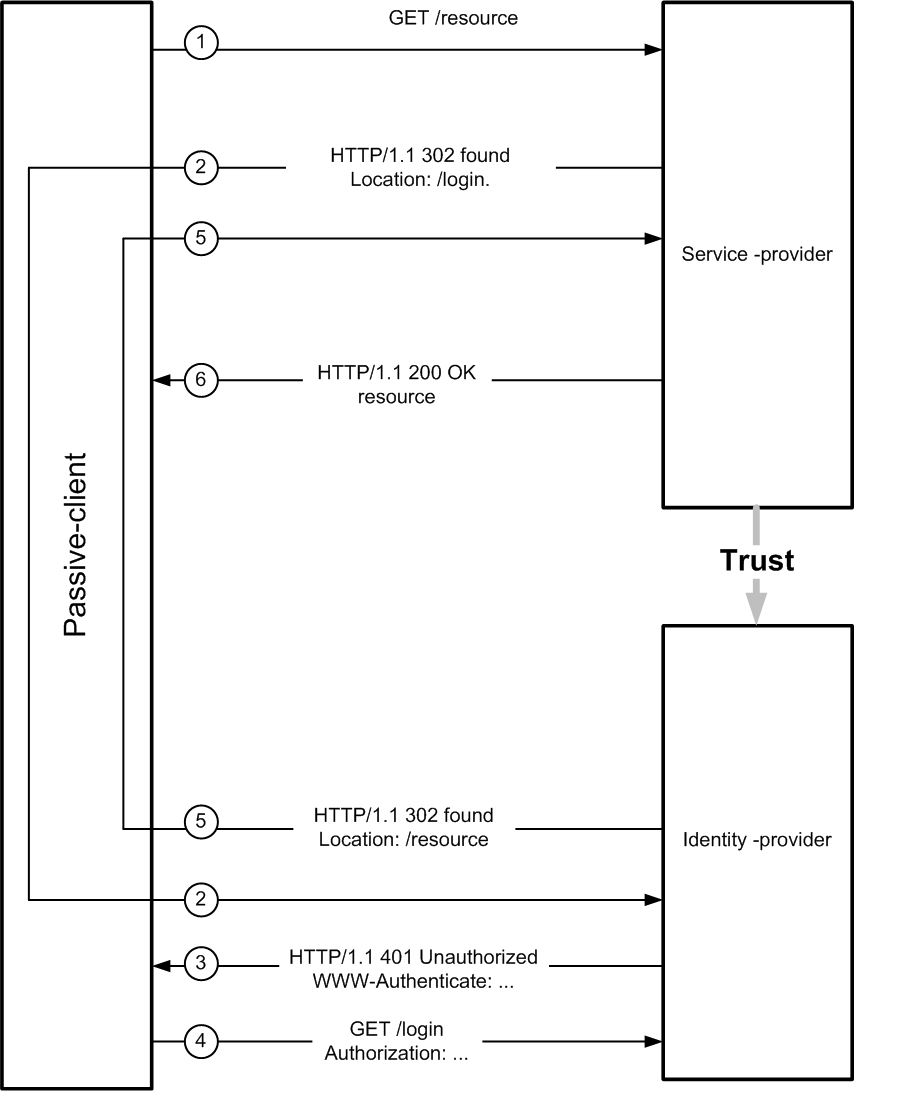
ПСКП, ПОИТ-3

**Token-аутентификация**

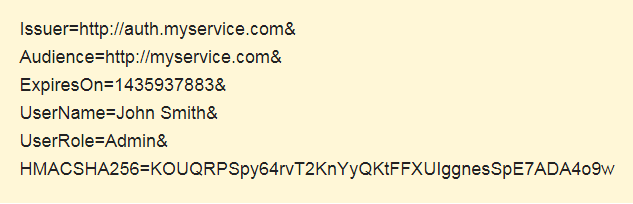
1. **Token:** битовая последовательность, построенная по определенному принципу.
2. **Token-аутентификация:** аутентификация, использующая token для идентификации пользователя или авторизации операции пользователя.
3. **Token-аутентификация:** применяется, как правило, для реализации Single Sign-On в распределенных системах.
4. **Token-аутентификация:** Identity-provider - сервер, генерирующий token.
5. **Token-аутентификация**: Service-provider – сервер, предоставляющий сервис клиенту.
6. **Token-аутентификация**: активный клиент – программный код, который может выполнять любые запросы и обрабатывать любые ответы. Обычно – это пользовательская программная реализация http-клиента. Пассивный клиент – браузер.
7. **Token-аутентификация**: схема работа с активным клиентом.



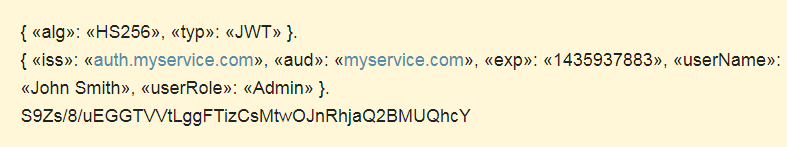
1. **Token-аутентификация**: схема работа с пассивным клиентом (браузером).

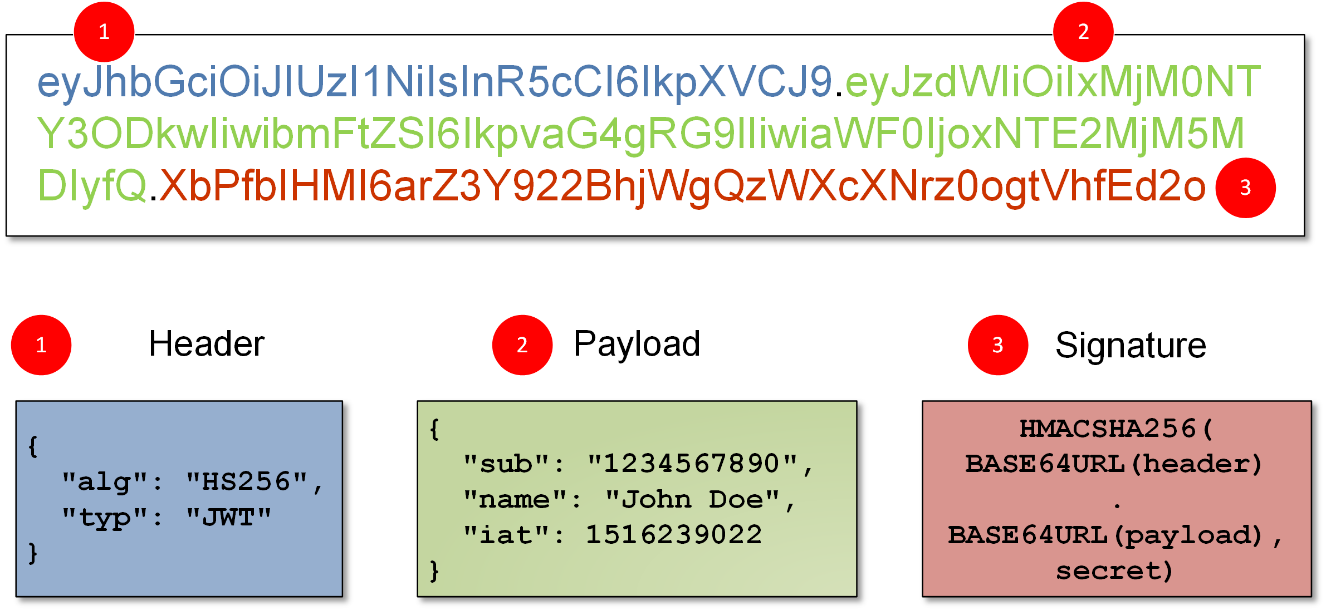
****

1. **Token-аутентификация**: Service-provider и Identity-provider должны иметь общий секретный ключ для шифрования/проверки token’а.
2. **Token-аутентификация**: token обычно строится на базе Issuer(эмитент), Audience (аудитория), Expires On (время жизни), Claim (сведение о пользователе) & Statements (дополнительные утверждения о пользователе), HMAC (хеш).
3. **Token-аутентификация**: Simple Web Token (SWT)

****

1. **Token-аутентификация**: JSON Web Token (JWT)

****



1. **Token-аутентификация**: JSON Web Token (JWT): access\_token, иногда refresh\_token.
2. **Token-аутентификация**: access\_token используются для получения доступа к защищенным ресурсам; короткоживущий, многоразовый.
3. **Token-аутентификация**: refresh\_token используется, когда access\_token истёк, для получения новой пары refresh\_token+access\_token; отправляется на специальный url; возвращается access\_token + refresh\_token; долгоживущий, одноразовый.
4. **Token-аутентификация**: при краже access\_token им можно пользоваться ограниченное время; при краже refresh\_token он становится бесполезным при ре-логине.
5. **Token-аутентификация**: Security Assertion Markup Language (SAML), разработчик OASIS, XML-формат, механизм подтверждения токенов, подпись ассиметричный ключ.

****