Popular Protocols

- OpenID
  - A lightweight authentication protocol which uses REST based message flows using JSON web tokens (JWT)
- Security Assertion Markup Language (SAML)
  - XML-based standard for exchanging authentication and authorization data between IdPs and SPs
- OAuth 2.0
- And other vender-oriented protocols

SAML

- Open standard for exchanging authentication and authorization information between parties(actors), particularly an identity provider and a service provider in a federated identity domain.
- XML-based protocol
- Began in 2001 at OASIS to define "an XML framework for exchanging authentication and authorization information.
- In 2005, SAML 2.0 was announced as an OASIS standard, converging SAML 1.1Liberty ID-FF(Liberty Alliance) 1.2 and Shibboleth 1.3.
- SAML became common in enterprise-oriented services.

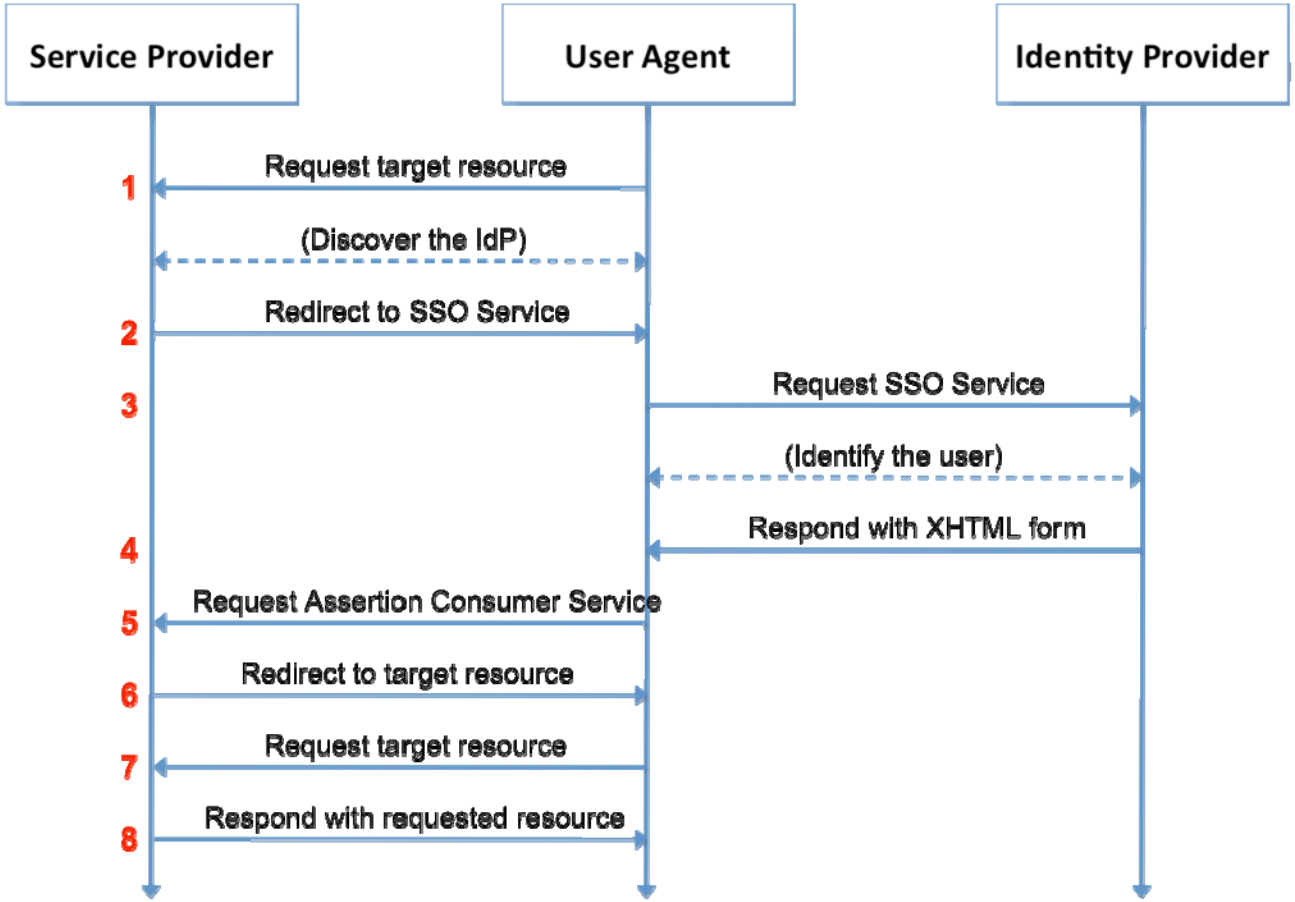
Parties (actors)

- Principal (user, subject)
- Identity provider (IdP)
- Service provider (SP)
- Use case (scenario)
  - A user requests a service from a service provider(SP). The SP requests and obtains an authentication and authorization token containing assertions from an IdP. Based on this token, the SP makes an access control decision to allow the user to access its resource.

What SAML specifies

- SAML specifies
  - How the token is transferred
  - Messages and what information are contained in their payloads
  - SAML assertion contains a security information, interpreted as: "Assertion A is issued at time t by issuer R regarding subject S, and is valid until C"

Common scenario: SAML Web Browser SSO



(source: Wikipedia)

Token transfer

- Passive profile
  - Getting token is well defined
- Active profile
  - API call instead of passive web browser
  - Sending token to SP is not well defined, no universal agreement

SAML security

- Make sure that a token is coming from a legitimate IdP and the toke is not tampered during transmission.
- An IdP has a certificate(public key) and a private key.
- The certificate is also shared with the SP.
  - The certificate is transferred to the SP out of band in one way or anther (depending on implementation).

OAuth 2.0

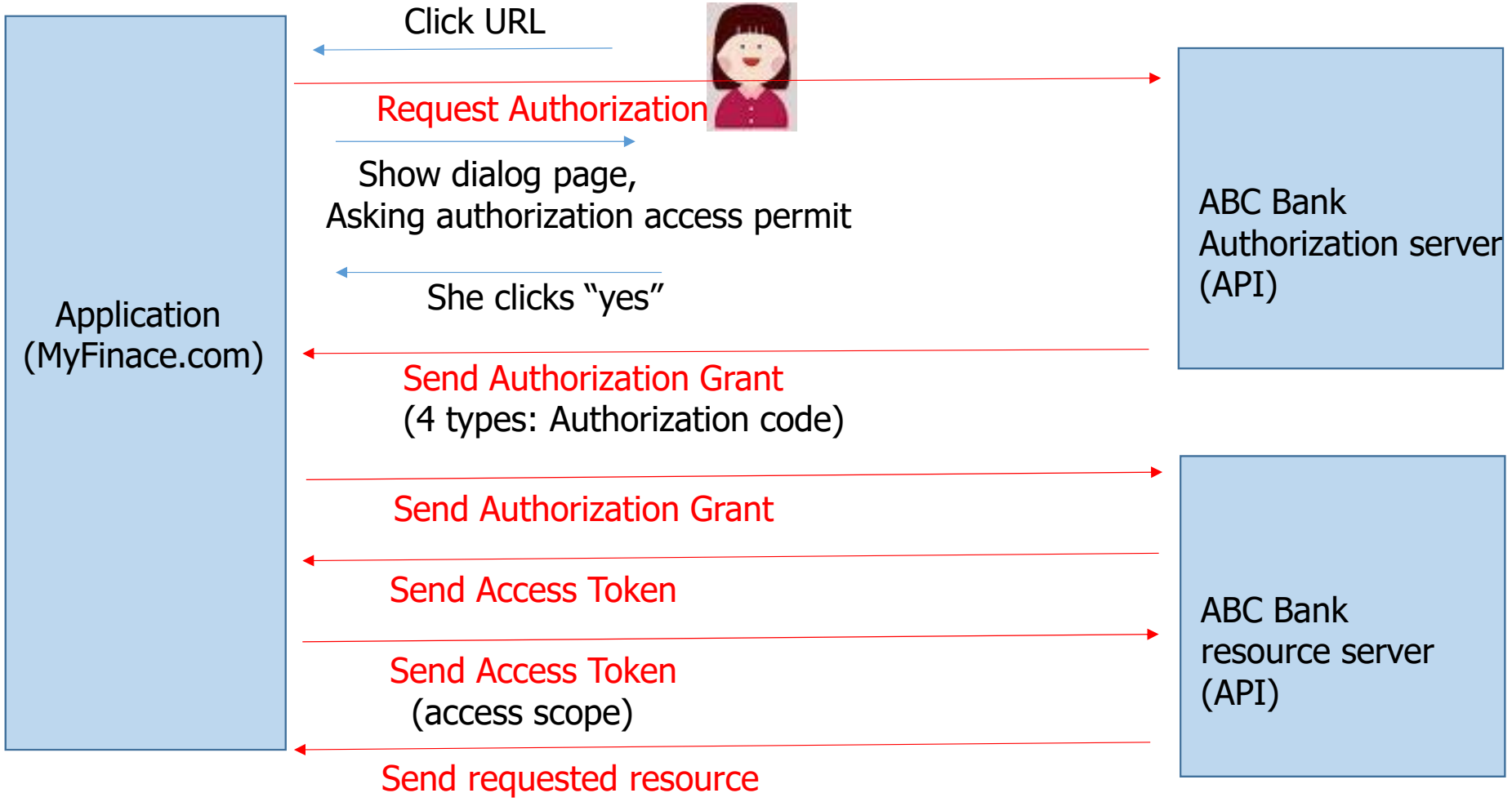
- OAuth began in 2006 due to the need for a way for web users to give web applications the permission to use their(user) information without giving them(application) their secret information.
- Provide a framework for authorization
  - Provide access token to web application (site)
- Published in Oct. 2012.
  - RFC 6749, 6750

Actors

- Resource owner (user)
  - Authorize an application to access its account. The application's access to the user's account is limited to the scope of the authorization grant.
- Client (Application)
  - Want to access the user's account.
- Resource server (API)
  - Hosts the protected user resources
- Authorization server (API)
  - Verifies the user identity and then issues access token to the application.

Example case

- MyFinance.com
  - Application that manages users' personal financial information
- Alice is a user to MyFinance.com and she want to access her current account and transaction data of the ABC bank.
- Now, she access the FinanceManager.com.


Application
(MyFinace.com)
Click URL
Request Authorization
Show dialog page,
Asking authorization access permit
She clicks "yes"
Send Authorization Grant
(4 types: Authorization code)
Send Authorization Grant
Send Access Token
Send Access Token
(access scope)
Send requested resource
ABC Bank
Authorization server
(API)
ABC Bank
resource server
(API)

Registration

- The application registers itself to the ABC bank API service with the application name, (callback) URL, etc.
- The bank API provides the application's credentials such as client ID and client secret.

OpenID and OpenID Connect (OIDC)

- OpenID
  - Open decentralized authentication protocol standard
  - Newest version in Nov. 2014
- OpenID Connect
  - Authentication layer on top of OAuth 2.0
  - follow the OAuth 2.0 authorization flow
  - Two tokens
    - ID Token – authentication token
    - Access Token – authorization token
  - Specifies a REST HTTP API, using JSON as a data format

OpenID actors

- End-user
- Relying party (RP) (service provider)
  - A web site or application that wants to verify the end-user's identity
- Identity provider or OpenID provider (OP)
  - Provide the OpenID authentication

ID token and Access token

- ID token
  - Similar to an identity card
  - In a standard JWT(JSON Web Token) format
  - Signed by on OpenID provider (OP)
- Access token
  - OAuth 2.0 doesn’t specify a standard token format.
  - It can be an opaque string or a JWT