MEDIEINSTITUTET

Systemintegration och integration med tredjepartssystem

Föreläsning 04 - Autentisering

Mikael Olsson
mikael.olsson@emmio.se
076-174 90 43

emmio

Vårt API

- PUT & DELETE

    - Hur går det?

Dagens ämnen

- Basic Authentication
- API key
- Oauth2

Autentisera

- Anledningar:
  - Skydda data
  - Skydda servern från överbelastning
  - Statistik

Basic authentication

- Metod för att låta en HTTP-användare skicka namn och lösenord i ett request.

- Klienten autentiserar sig genom en header
  - `Authorization: Basic <credentials>`

  - Credentials är en base64-kodad sträng bestående av användare:lösenord.

- En användare kan autentisera sig genom URL:en: https://Aladdin:OpenSesame@www.example.com/

Basic authentication - ex

- exercises/04-authentication/01-basic/

API-key

- Ganska simpelt och vanligt sätt att hantera åtkomst.

- Varje användare / konto får en nyckel som används i varje request.

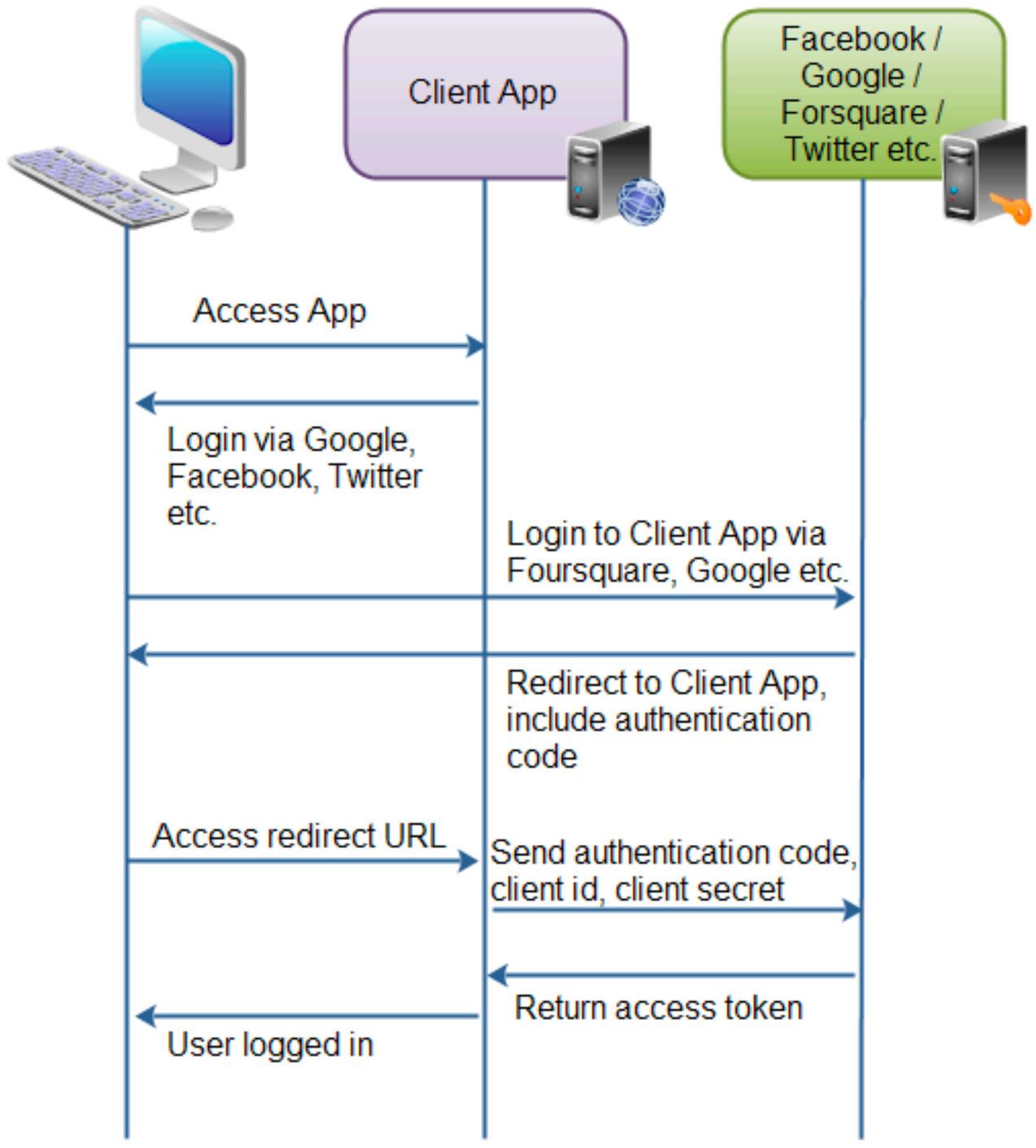
API-key - ex

- exercises/04-authentication/02-api-key

- Validate phonenumber with https://numvalidate.com/

Oauth2

- Ett protokoll för att låta applikationer komma åt varandras data.



Oauth2

1. Användaren går till klientapplikationen, som har en knapp typ ”logga in via Facebook/ Google/Twitter”.

2. Användaren klickar och hamnar på den autentiserande applikationen (dvs FB etc). Användaren loggar in på denna plattform och får frågan om hen vill acceptera att klienten får access till vissa av de data som finns på den autentiserande applikationen.

3. Den autentiserande applikationen skickar användaren vidare till en URI som klientapplikationen har specat. Att tillhandahålla denna görs normalt av klienten när den registrerar sig hos autentiseraren. Då får även klienten sitt *client id* och *client password*. Autentiseraren lägger till en auktoriseringskod till URI:en.

4. Användaren kommer till redirect-sidan specad av klienten. I bakgrunden kontaktar klienten autentiseraren och skickar client id, client password och auktoriseringskoden. Autentiseraren skickar tillbaka ett *access token*.

5. När klienten har fått detta access token kan detta användas för att anropa resurser hos FB/Google/Twitter etc.

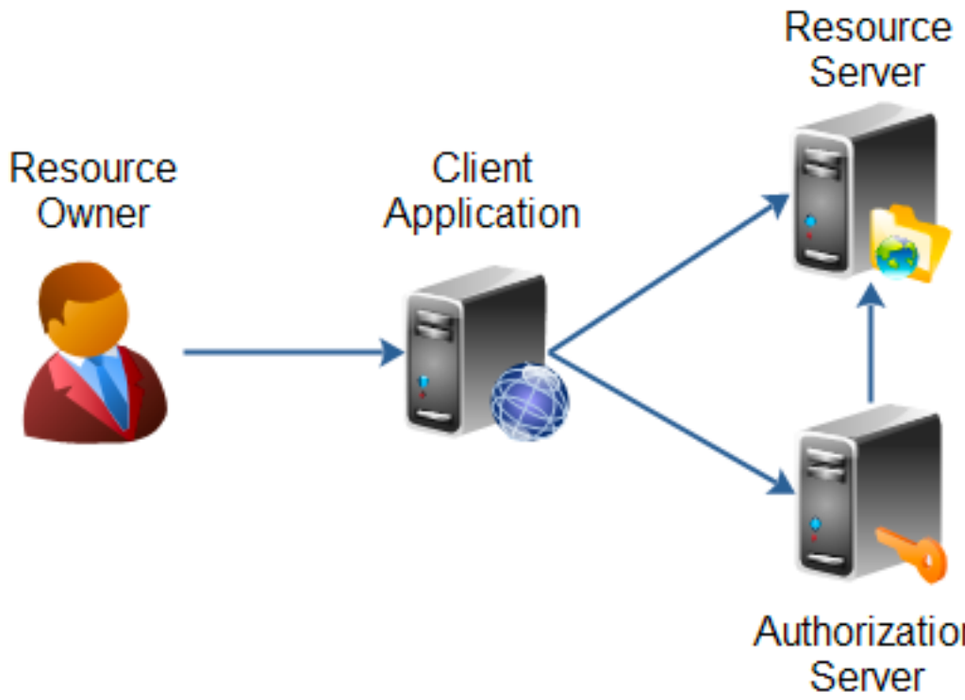
Oauth2

- Resursägaren är den person eller resurs som äger datat. En användare på FB kan t ex vara en resursägare. Resursen är oftast användarens data.

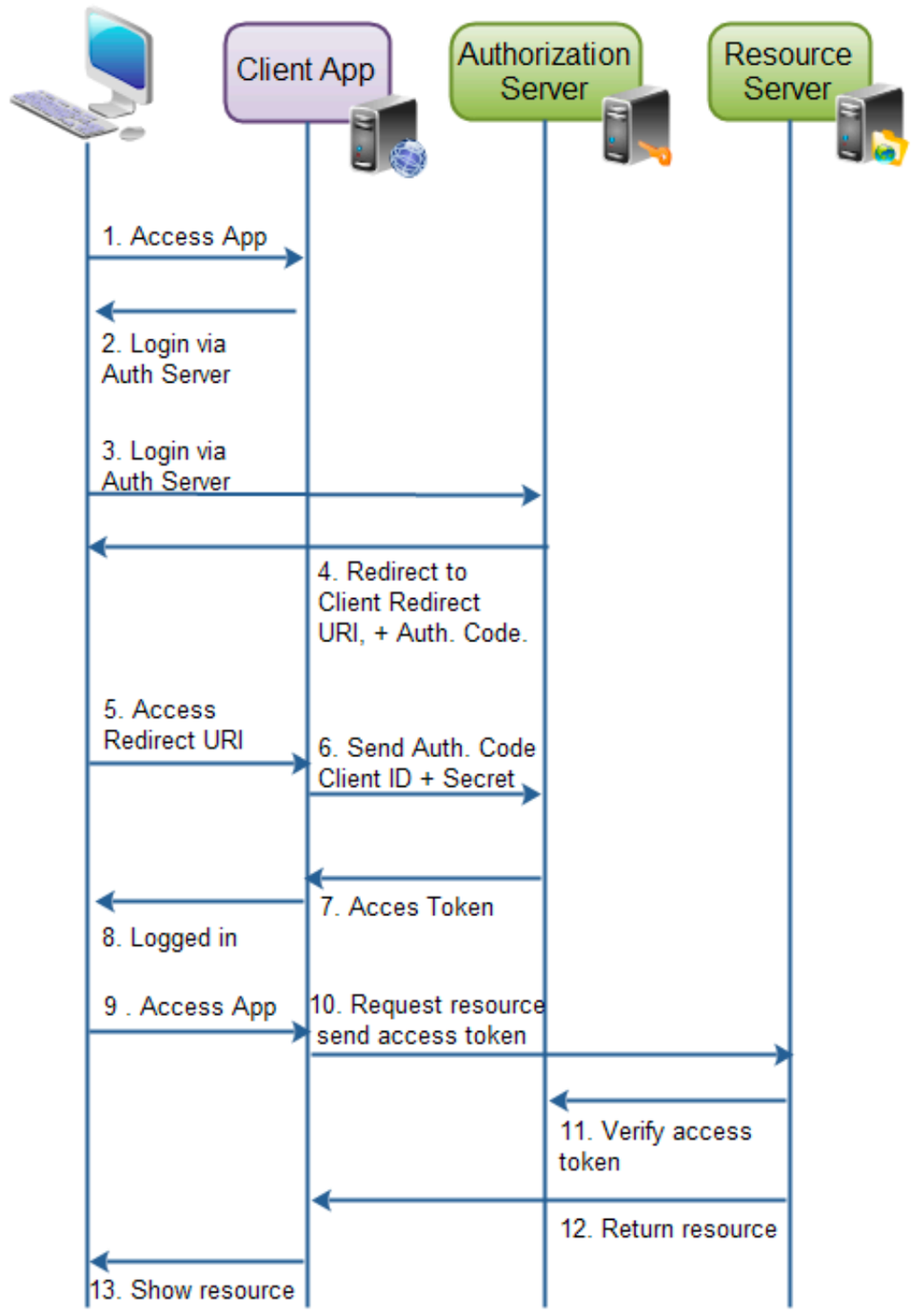
- Resursservern är servern som har datat, t ex FB.

- Klienten är applikationen som vill ha åtkomst till data på resursservern. Kan t ex vara ett spel som vill ha åtkomst till användarens FB-konto.

- Autentiseringsservern är servern som behandlar åtkomst. Kan vara samma som resursservern, men måste inte vara.

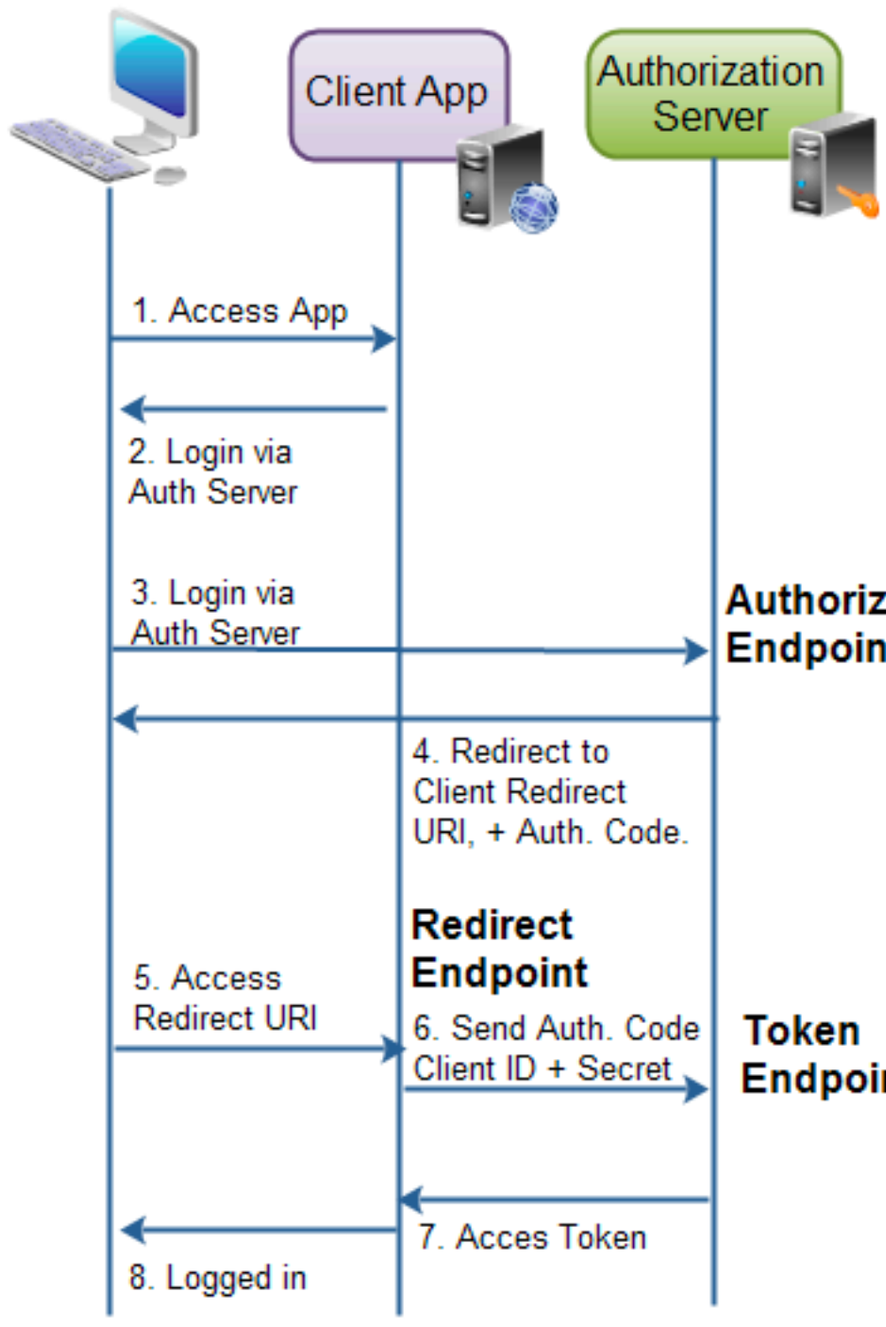


Oauth2 - Autentisering



Oauth2 - Endpoints

- Authorization Endpoint
    - Där på autentiseraren som resursägaren loggar in och godkänner (grants) autentisering till klienten.
- Token Endpoint
    - Där på autentiserare som klienten byter autentiseringskoden, client id och client password mot en access token.
- Redirect Endpoint
    - Där på klienten som resursägaren skickas vidare till efter att ha fått (granted) access.



Tills nästa tillfälle

- Skapa en FB-inloggning på din site.
  - https://www.codexworld.com/login-with-facebook-using-php/
- Läs på om Facebooks Graph API.
  - https://developers.facebook.com/docs/graph-api/overview/

Sammanfattning

- Basic Authentication
- API key
- Oauth2

Utvärdering

- Prata i grupper om 2-3 personer i två minuter.

- Vad har varit bra idag?

- Vad skulle kunna förbättras?

MEDIEINSTITUTET

Tack för idag!

Mikael Olsson
mikael.olsson@emmio.se
076-174 90 43

emmio