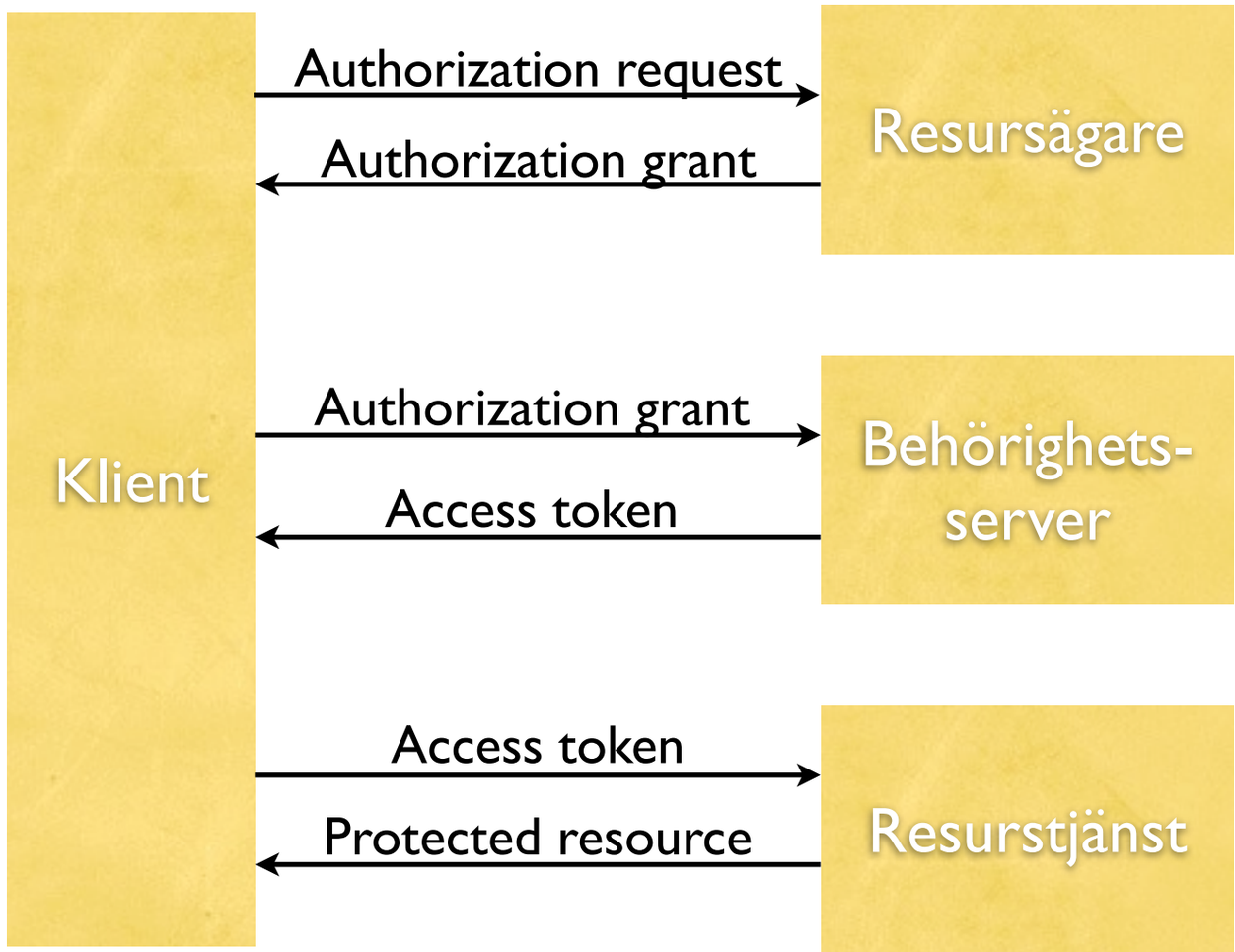
OAuth2.0

- Ett OAuth2 ramverk tillåter en tredje part begränsad tillgång till en HTTP tjänst antingen på uppdrag av en resursägare eller på eget uppdrag.

De fyra rollerna

- Resursägare
- Resurstjänst
- Klient
- Behörighetsserver (AS)

Abstrakt protokollflöde



Klient profiler

- web application
- user-agent-based
- native

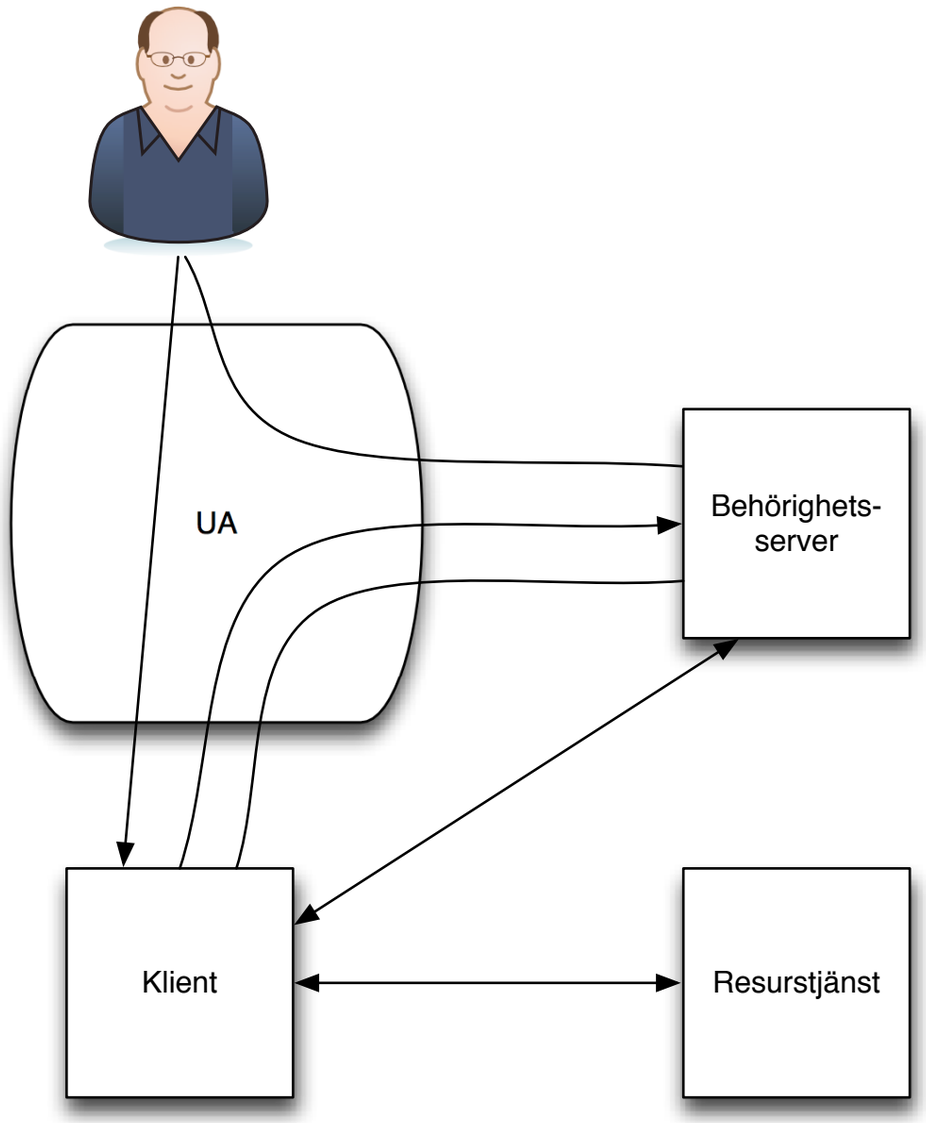
De fyra ‘authorization grant’ typerna

- Authorization code
- Implicit
- Resource owner password credentials
- Client credentials

Utelämnade saker

- Klient registrering
- Behörighets serverns egenskaper
- Hur man upptäcker ändpunkter

Authorization code grant


UA
Behörighets-
server
Klient
Resurstjänst

Authorization Request

GET /authorize?
response_type=code&
client_id=s6BhdRkqt3&
state=xyz&
redirect_uri=https://client/example/com/cb

Authorization response

HTTP/1.1 302 Found

Location: https://client.example.com/cb?
code=SplxlOBeZQQYbYS6WxSbIA&
state=xyz

Access Token Request

POST /token HTTP/1.1

Host: server.example.com

Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded;charset=UTF-8

grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA
&redirect_uri=https://client/example/com/cb

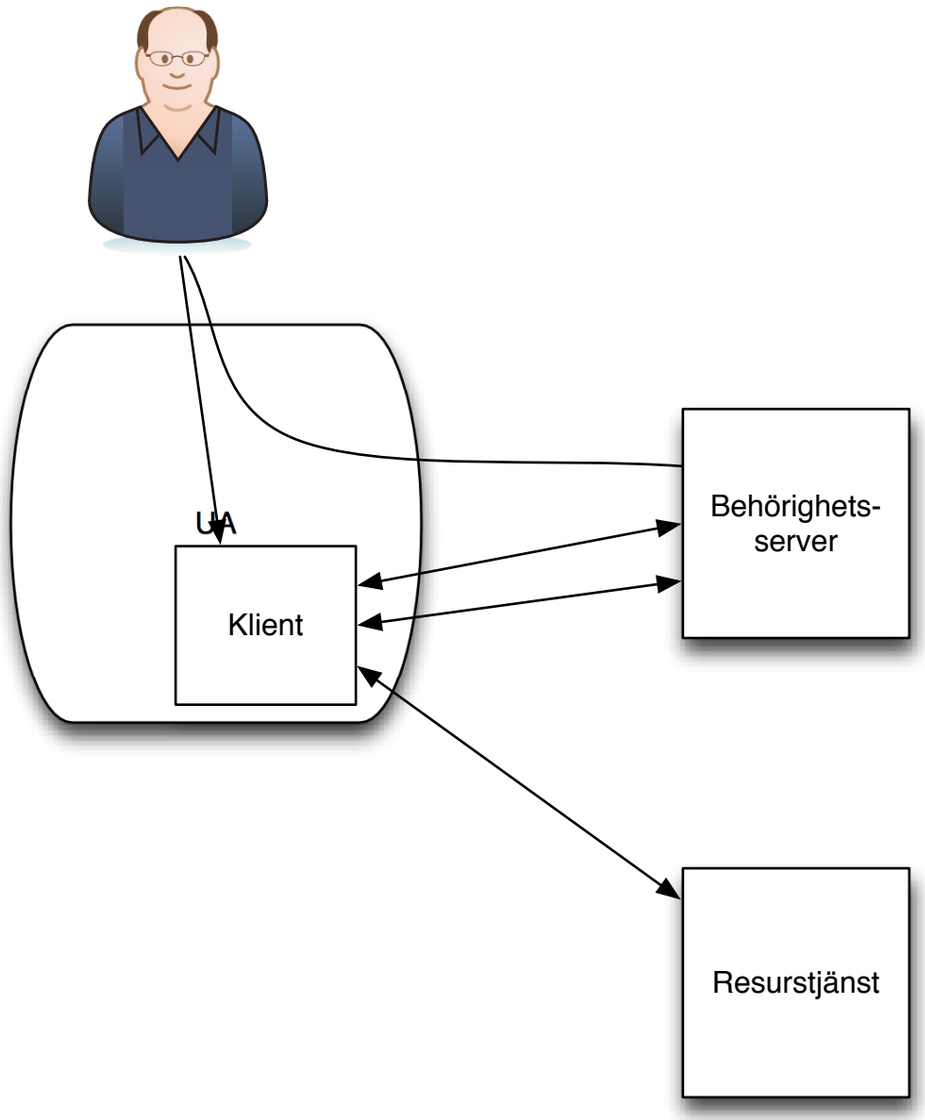
Access Token Response

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache


```
{
    "access_token":"2YotnFZFEjr1zCsicMWpAA",
    "token_type":"example",
    "expires_in":3600,
    "refresh_token":"tGzv3JOkF0XG5Qx2TlKWIA",
    "example_parameter":"example_value"
}
```

Implicit grant


UA
Klient
Behörighets-
server
Resurstjänst

Authorization Request

GET /authorize?
response_type=token&
client_id=s6BhdRkqt3&
state=xyz&
redirect_uri=https://client/example/com/cb

Access Token Response

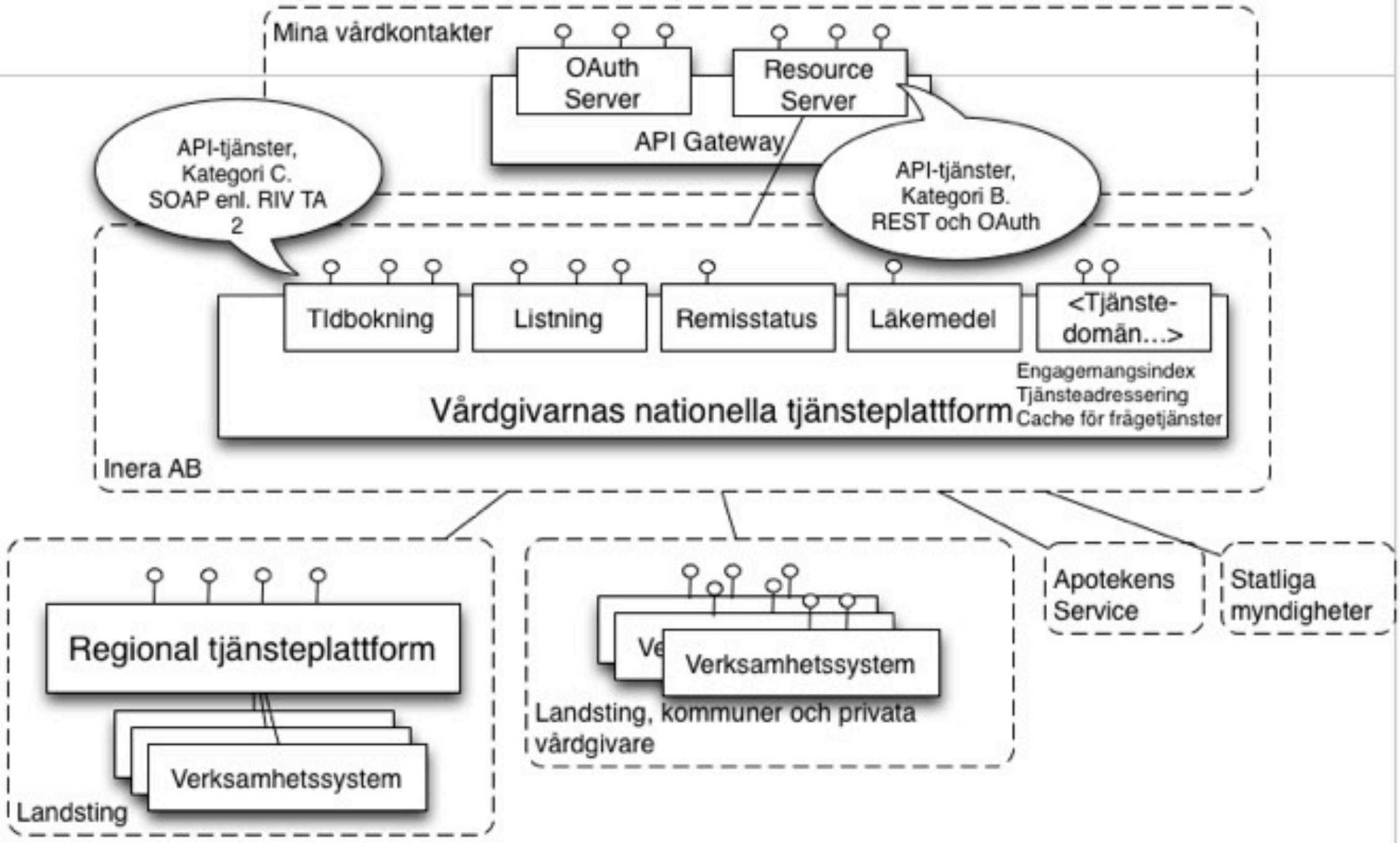
HTTP/1.1 302 Found
Location: http://example.com/cb#
access_token=2YotnFZFEjr1zCsicMWpAA&
state=xyz&
token_type=example&
expires_in=3600

Extension grant

grant_type=urn:ietf:params:oauth:grant-type:saml2-bearer&
assertion=PEFzc2VydGlvbiBJc3N1ZUluc3RhbnQ9IjIwMTEt
MDU....

Mina vårdkontakter

Publika API-tjänster (REST). Invånarstyrd tillit med OAuth + Servercertifikat.



Vårdgivarnas API-tjänster (Tjänstekontrakt). Organisationstillit med Server-certifikat.