# HelselD for FHIR-hoder



# Tema i dag

- 1. HelseID for n00bs
- 2. Tokens
  - Hvor er vi
  - Hvor kan vi havne

### Hva er HelselD?

- 1. Tilbyr pålogging for helsepersonell

## Hva er HelselD?

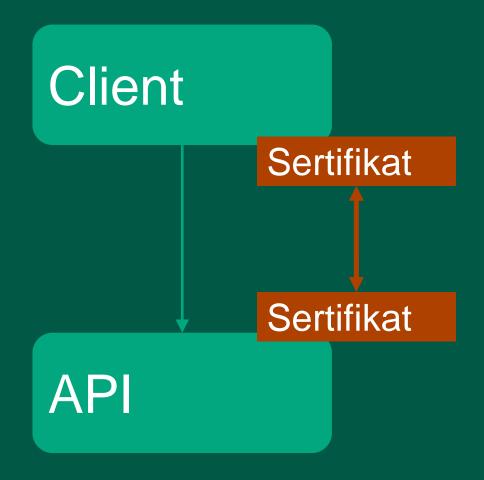
Implementert vha 2 protokoller

- OpenID Connect
- •OAuth 2

## Grunnleggende begreper

- Client (aka "Applikasjon")
- •Resource (f.eks et "REST API")
- Secret (f.eks "Private Key" eller "Passord")
- Token (aka "Sikkerhetsbillett")
- •Identitetstilbyder, IDP (f.eks "BankID")
- Authorization Server (f.eks «HelseID»)

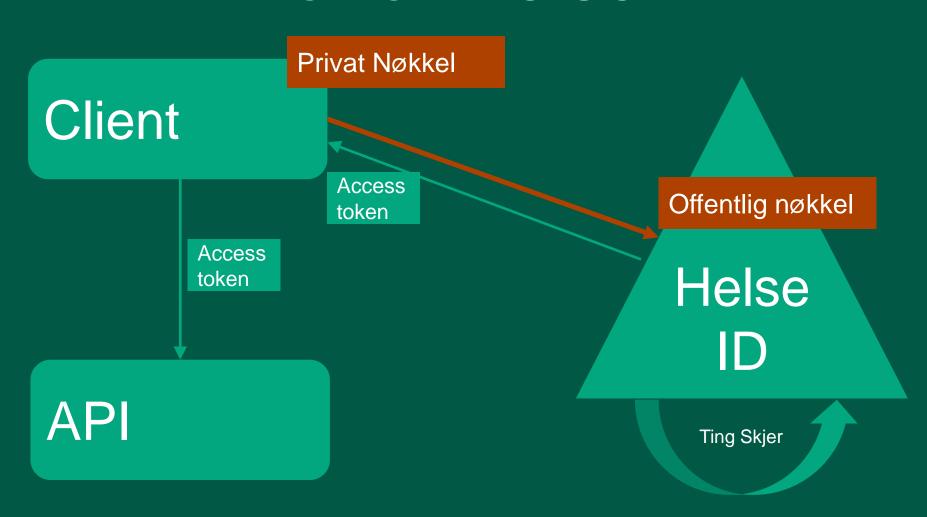
## Hvorfor HelselD?



### Problemer:

- Skalering
- Sluttbrukeridentitet

## Hvorfor HelselD?



## Tokens (aka «Sikkerhetsbillett»)

To typer

- OpenID Connect Identity Tokens
- •OAuth 2 Access Tokens

### Tokens

- Format er «JSON Web Token» JWT
- Signert med en privat nøkkel som HelselD besitter
- Valideres av de som skal tilgjengeliggjøre data
  - Altså API-er

## Tokens - Struktur

- Hode- «Hvilket type token er dette, og hvordan er det signert»
- Kropp «Her er informasjonen du er på utkikk etter»
- Signatur «Her er beviset på at det er HelseID som har utstedt tokenet»

## Tokens - Struktur



Crafted by auth0 @

### Encoded PASTE A TOKEN HERE

### ZFNDEiLCJ4NXOiOiJ0TXJrVXNpMnFKTzJxRUNza klUN0J3cENia0UiLCJ0eXAiOiJKV1QifQ.eyJpc 3MiOiJodHRwczovL2hlbHNlaWQtc3RzLnV0dmlr bGluZy5uaG4ubm8iLCJuYmYiOjE2NjE5MjkxODM sImlhdCI6MTY2MTkyOTE4MywiZXhwIjoxNjYxOT MyNzgzLCJhdWQi0iJlLWhlbHNlOnNmbS5hcGkiL CJzY29wZSI6WyJvcGVuaWQiLCJwcm9maWxlIiwi aGVsc2VpZDovL3Nib3Blcv9pZGVudGl0eS9waWO iLCJoZWxzZWlk0i8vc2NvcGVzL2lkZW50aXR5L3 BpZF9wc2V1ZG9ueW0iLCJoZWxzZWlk0i8vc2Nvc GVzL2lkZW50aXR5L2Fzc3VyYW5jZV9sZXZlbCIs ImhlbHNlaWQ6Ly9zY29wZXMvaWRlbnRpdHkvc2V jdXJpdHlfbGV2ZWwiLCJoZWxzZWlk0i8vc2NvcG VzL21kZW50aXR5L251dHdvcmsiLCJoZWxzZW1k0 i8vc2NvcGVzL2hwci9ocHJfbnVtYmVyIiwiZS1o ZWxzZTpzZm0uYXBpL3NmbS5hcGkiXSwiYW1yIjp bInB3ZCJdLCJjbGllbnRfaWQiOiJyby1kZW1vIi wiY2xpZW50X2FtciI6InByaXZhdGVfa2V5X2p3d CIsImF1dGhfdGltZSI6MTY2MTkyOTE4MywiaWRw IjoidGVzdGlkcC1vaWRjIiwiaGVsc2VpZDovL2N sYWltcy9pZGVudGl0eS9waWQi0iIxNTAzNzEwND IyOSIsImhlbHNlaWQ6Ly9jbGFpbXMvaWRlbnRpd Hkvc2VjdXJpdHlfbGV2ZWwi0iI0IiwiaGVsc2Vp ZDovL2NsYWltcy9pZGVudGl0eS9hc3N1cmFuY2V fbGV2ZWwi0iJoaWdoIiwiaGVsc2VpZDovL2NsYW ltcy9ocHIvaHByX251bWJlciI6IjQ5MDk0MDIiL CJoZWxzZWlk0i8vY2xhaW1zL2NsaWVudC9hbXIi OiJyc2FfcHJpdmF0ZV9rZXkiLCJoZWxzZWlkOi8 vY2xhaW1zL2NsaWVudC9jbGFpbXMvb3JnbnJfcG FyZW50IjoiOTk50Tc3Nzc0IiwiaGVsc2VpZDovL 2NsYWltcy9jbGllbnQvY2xhaW1zL29yZ25yX2No aWxkIjoiOTk5OTc3Nzc1IiwiZS1oZWxzZTpzZm0 uYXBpL2NsaWVudC9jbGFpbXMvc2ZtLWlkIjoiND U2MTIzIiwic3ViIjoiQlpNY3FTYWprRzJxazdzc 1BGZHAyTmozWXhBK3I0NmpjODRuMUVjT3NsUT0i LCJzaWQiOiJGNzY5N0I2MzhBMDA2MTgwMUQ2N0I 2QzYy0EYwQ0ExNiIsImp0aSI6IjZBRDk00TA3NU E0QTc0MDlGMDhDMTg2NUIy0TMxMDBCIn0.gV7St q49VFdGkfchqE8ef51h2PtWFEroVV0l5dTvqShM D16rKrbVKF02T7svRijddv2KngiQMoNzhcsSc\_y ZerJIf0qBL1LzUj7v6QPC4-YXwb00Qo5mVU0PLCPzlEvhKnF0ybX9BgRIdln1vJYb338Ryp\_Z-5vLwPJJYPbW83He3Uy\_en6Vzx-

m58RmkPLr0cbJ4z4X5qkIqL6Z3MtperfAKXZLHa AW6PyGqdbwHEhf907cIFytd0cqkYzBzfk3\_BFvY awIQN\_0tTZm80DGLhdEvqpNgIm7epICyZVbNMyH 516YQvs-J-KNOyjYKBvZhmkumVGG3A

QD4a8hYTWm-

```
Decoded EDITTHE PAYLOAD AND SECRET
 HEADER: ALGORITHM & TOKEN TYPE
     "kid": "B4CAE452C8B6A893B6A840AC8C84FB070A426E41".
     "x5t": "tMrkUsi2qJ02qECsjIT7BwpCbkE",
     "typ": "JWT"
 PAYLOAD: DATA
     "iss": "https://helseid-sts.utvikling.nhn.no".
     "nbf": 1661929183.
     "iat": 1661929183
     "exp": 1661932783
     "aud": "e-helse:sfm.api"
      "scope": [
       "openid"
       "profile"
       "helseid://scopes/identity/pid",
        "helseid://scopes/identity/pid_pseudonym",
        "helseid://scopes/identity/assurance_level"
       "helseid://scopes/identity/security_level".
       "helseid://scopes/identity/network"
       "helseid://scopes/hpr/hpr_number",
       "e-helse:sfm.api/sfm.api"
       "pwd"
      "client_id": "ro-demo"
      "client_amr": "private_key_jwt"
      "auth_time": 1661929183,
      "ido": "testido-oido"
      "helseid://claims/identity/pid": "15037104229"
      "helseid://claims/identity/security level": "4"
      "helseid://claims/identity/assurance_level": "high"
      "helseid://claims/hpr/hpr_number": "4909402",
      "helseid://claims/client/amr": "rsa_private_key"
      "helseid://claims/client/claims/orgnr_parent"
    "999977774",
     "helseid://claims/client/claims/orgnr_child":
    "999977775",
     "e-helse:sfm.api/client/claims/sfm-id": "456123",
     "sub":
    "BZMcqSajkG2qk7ssPFdp2Nj3YxA+r46jc84n1Ec0s1Q=",
     "sid": "F7697B638A0061801D67B6C628F0CA16"
      "jti": "6AD949075A4A7409F08C1865B293100B"
 VERIFY SIGNATURE
    base64UrlEncode(header) + "." +
       "e": "AQAB"
       "kty": "RSA",
       "n": "puikxvVtwBiWAPJSFKW 🔻
    Private Key in PKCS #8, PKCS #
     1, or JWK string format. The k
    ey never leaves your browser
```

## Tokens - innhold

Standarisert innhold

- Hvem utstedte tokenet
- Når ble tokenet utstedt
- Hvor lenge er det gyldig
- Hvem er mottager
- Hvilke rettigheter gir tokenet

```
"iss": "https://helseid-sts.utvikling.nhn.no",
"nbf": 1661929183.
      1661929183.
"exp": 1661932783,
"auth time": 1661929183
"sub": "BZMcqSajkG2qk7ssPFdp2Nj3YxA+r46jc84n1EcOslQ=",
"sid": "F7697B638A0061801D67B6C628F0CA16",
"jti": "6AD949075A4A7409F08C1865B293100B"
"aud": "e-helse:sfm.api",
"scope":
 "e-helse:sfm.api/sfm.api"
"e-helse:sfm.api/client/claims/sfm-id": "456123",
"amr":
  'pwd'
"client id": "ro-demo",
"client amr": "private key jwt",
"idp": "testidp-oidc",
"helseid://claims/identity/pid": "15037104229",
"helseid://claims/identity/security level": "4",
"helseid://claims/identity/assurance level": "high",
"helseid://claims/hpr/hpr number": "4909402",
"helseid://claims/client/claims/orgnr parent": "999977774"
"helseid://claims/client/claims/orgnr child": "999977775",
```

## Tokens - Innhold

- Identitet til helsepersonell
  - Fødselsnummer
  - HPR-nummer
  - Navn
  - Hvordan ble brukeren autentisert
  - Var brukeren på Helsenettet eller Internett

```
"iss": "https://helseid-sts.utvikling.nhn.no",
"nbf": 1661929183.
"iat": 1661929183,
"exp": 1661932783.
"auth time": 1661929183,
      "BZMcqSajkG2qk7ssPFdp2Nj3YxA+r46jc84n1EcOslQ=",
"sid": "F7697B638A0061801D67B6C628F0CA16",
"jti": "6AD949075A4A7409F08C1865B293100B"
"aud": "e-helse:sfm.api",
"scope":
  "e-helse:sfm.api/sfm.api"
"e-helse:sfm.api/client/claims/sfm-id": "456123",
"amr":
"client id": "ro-demo",
"client amr": "private key jwt",
"idp": "testidp-oidc",
"helseid://claims/identity/pid": "15037104229"
"helseid://claims/identity/security level": "4"
"helseid://claims/identity/assurance level": "high
"helseid://claims/hpr/hpr number": "4909402"
"helseid://claims/client/claims/orgnr_parent": "999977774"
"helseid://claims/client/claims/orgnr child": "999977775"
```

## Tokens - Innhold

- Identitet til virksomhet
  - Organisasjonsnummer til virksomhet
  - Organisasjonsnummer til «underenhet»

```
"iss": "https://helseid-sts.utvikling.nhn.no",
"nbf": 1661929183,
"iat": 1661929183,
"exp": 1661932783,
"auth time": 1661929183,
"sub": "BZMcqSajkG2qk7ssPFdp2Nj3YxA+r46jc84n1EcOslQ=",
"sid": "F7697B638A0061801D67B6C628F0CA16",
"jti": "6AD949075A4A7409F08C1865B293100B"
"aud": "e-helse:sfm.api",
"scope":
  "e-helse:sfm.api/sfm.api"
"e-helse:sfm.api/client/claims/sfm-id": "456123",
  "pwd"
"client id": "ro-demo",
"client amr": "private key jwt",
"idp": "testidp-oidc",
"helseid://claims/identity/pid": "15037104229",
"helseid://claims/identity/security level": "4",
"helseid://claims/identity/assurance level": "high",
"helseid://claims/hpr/hpr number": "4909402",
"helseid://claims/client/claims/orgnr parent"
"helseid://claims/client/claims/orgnr child":
```

## Tokens - Innhold

- Annet
  - Hvordan autentiserte
     klienten seg ovenfor HelselD
  - Hvilken klient var dette?

```
"iss": "https://helseid-sts.utvikling.nhn.no",
"nbf": 1661929183,
"iat": 1661929183.
"exp": 1661932783,
"auth time": 1661929183,
"sub": "BZMcqSajkG2qk7ssPFdp2Nj3YxA+r46jc84n1EcOslQ=",
"sid": "F7697B638A0061801D67B6C628F0CA16",
"jti": "6AD949075A4A7409F08C1865B293100B"
"aud": "e-helse:sfm.api",
"scope": [
  "e-helse:sfm.api/sfm.api"
"e-helse:sfm.api/client/claims/sfm-id": "456123",
"amr": [
  "pwd"
'client id": "ro-demo",
"client_amr": "private key_jwt",
"idp": "testidp-oidc",
"helseid://claims/identity/pid": "15037104229",
"helseid://claims/identity/security level": "4",
"helseid://claims/identity/assurance_level": "high",
"helseid://claims/hpr/hpr number": "4909402",
"helseid://claims/client/claims/orgnr parent": "999977774"
"helseid://claims/client/claims/orgnr child": "999977775",
```

# Hva \_kan\_ ett token fra HelselD inneholde i fremtiden?

- Informasjon som fagsystem sitter på
  - Mer informasjon om helsepersonell
  - Mer informasjon om behandlingssted
  - Mer informasjon om pasient

# Hva \_kan\_ ett token fra HelselD inneholde i fremtiden?

- Informasjon som kommer fra identititetstilbyder
  - Detaljert kontaktinformasjon
  - Lokale rettigheter / grupper

# Hva \_kan\_ ett token fra HelselD inneholde i fremtiden?

- Mer metainformasjon per informasjonselement
  - Kilde
  - "Tillitsnivå"
  - Type (f.eks type identifikator ReshID vs Orgnummer)



Norsk helsenett