# CONTEXT HANDLER

## OIDC og Roadmap

KOMB:T

Kommunernes it-fællesskab

# STATUS

KOMBIT
Kommunernes it-fællesskab

# Status

Hovedaktiviteter efter Context Handler 2 (CH2) og Security Token Service 2 (STS2) er i produktion

- Kommunale IdPers oprettelse af CH2 som relying party
  - Herunder test af integration i produktion med Claim apps
- Test af føderation med SEB
- Planlægning af systemers overgang til CH2 og STS2

KOMBIT
Kommunernes it-fællesskab

# OPEN ID CONNECT

KOMBIT
Kommunernes it-fællesskab

# Baggrund

Context Handler 2 udstiller en service til autentifikation og autorisation baseret på sub-profilering OIOSAML profilen.

Dette har sikret fælles log-in i det kommunale domæne men også interoperabilitet til NemLog-in og SEB brokeren.

Den kommunale verden har (i mange år) haft brug for en nemmere understøttelse af mindre applikationer og apps.

- stadig behov for samme niveau af  sikkerhed i autentifikation
- men knap så meget behov for en uddybet autorisations del

# SAML

## Fordele

- SAML understøtter services til autentifikation (hvem er du) og autorisation (hvad må du)
- Autorisationer kan i SAML være meget specifikke da de udtrykkes i en XML struktur. Dvs at man i højere detaljegrad kan forklare hvad en bruger må.
- Eksempelvis har et stort system så som SAPA, behov for at en bruger kun må tilgå helt specifikke dele af systemet

## Ulemper

- Netop fordi SAML indeholder en stor detaljegrad, kan det være svært at implementere

KOMBIT
Kommunernes it-fællesskab

# OpenID Connect - Forretning

**Fordele**

- Nemmere og hurtigere for tjenesteudbydere at anvende OpenID Connect frem for (OIO)SAML,  grundet ældre teknologi og med mindre udbredt understøttelse i moderne udviklings-rammeværk.

- OpenID Connect understøtter bedre nye og moderne typer af klientapplikationer som fx Native Apps og Single Page applikationer.

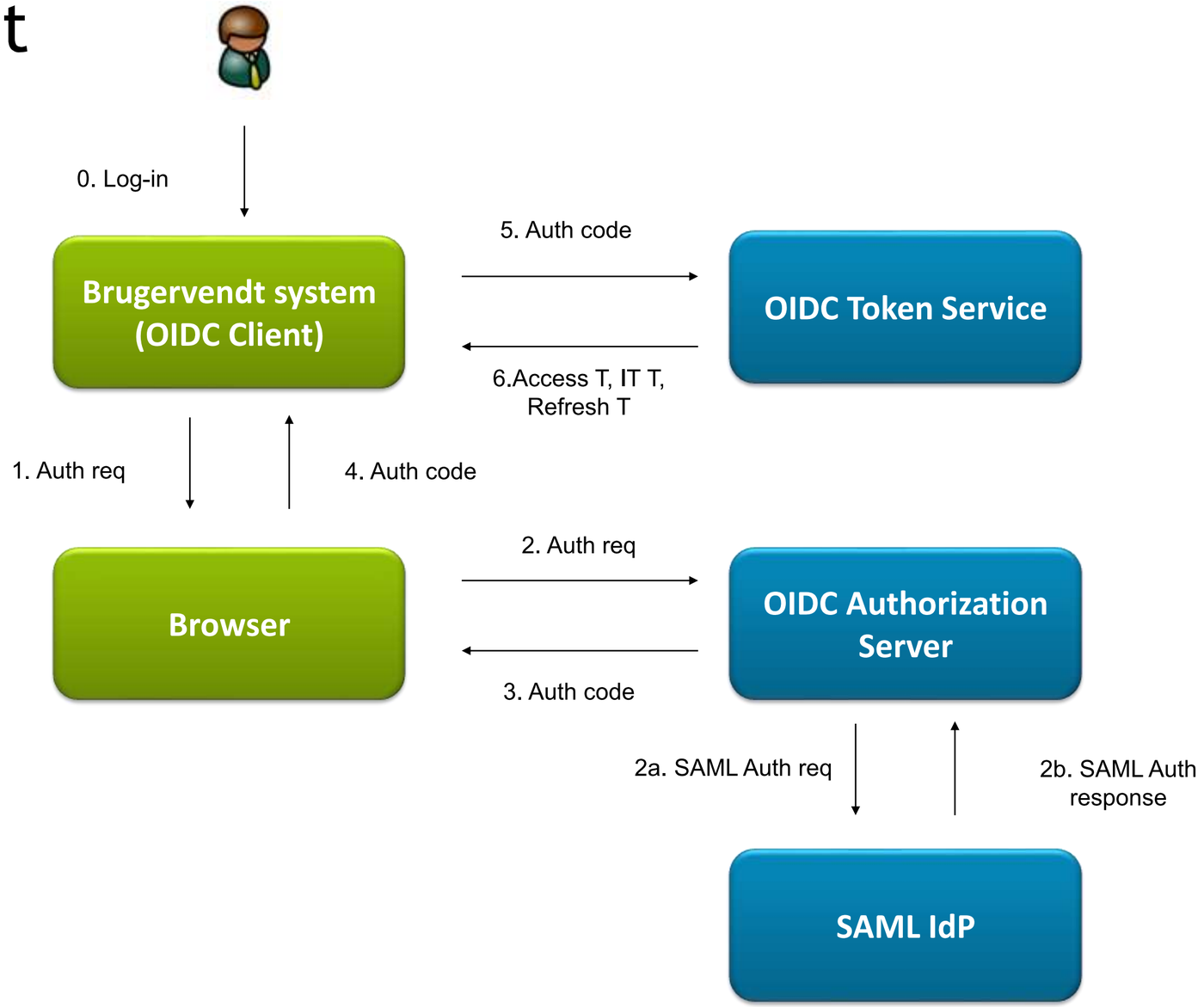
- Transition til OpenID Connect repræsenterer modernisering af teknologistakken

**Ulemper**

- OpenID Connect er som udgangspunkt designet simpelt og man skal derfor tilpasse det til offentlige behov for at de dækker en høj nok detaljegrad, og kan anvendes til komplekse systemer

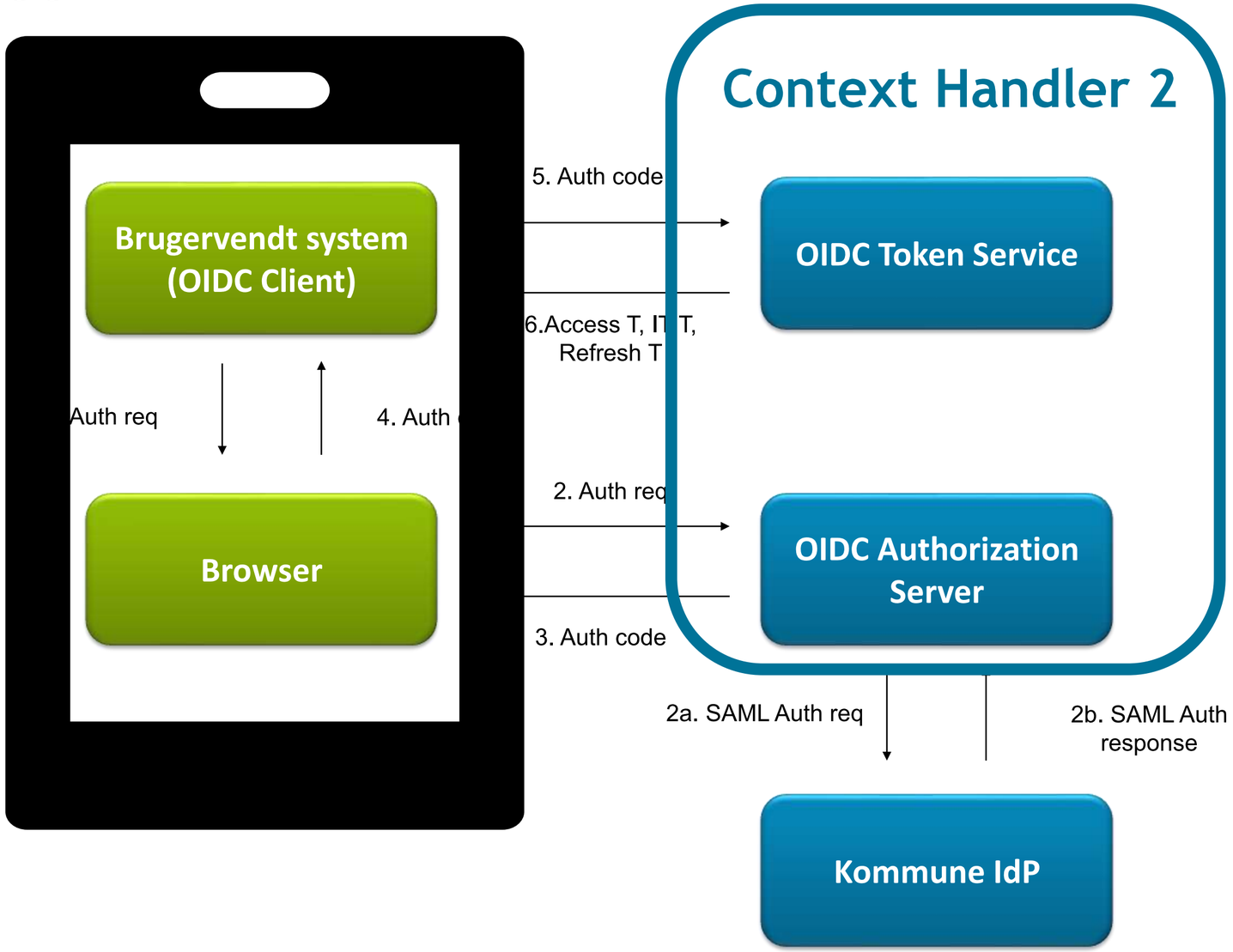
KOMBIT
Kommunernes it-fællesskab

# OpenID Connect – flow




KOMBIT
Kommunernes it-fællesskab

# OpenID Connect
– App




KOMBIT
Kommunernes it-fællesskab

# Fremadrettet

For at understøtte komplekse applikationer, Native Apps og Single Page applikationer. Vil Context Handler 2 udstille både SAML services og OpenID Connect

Begge dele baserer sig fortsat på kommunernes rettighedstildelinger via deres IdPer

Den anden del af OIDC der svarer til IdPer i SAML, vil der først blive lavet en PoC på for at sikre at det kan anvendes i den kommunale verden.

Men det er ikke fokus lige nu da kommunerne lige har fået oprettet deres NSIS IdPer

# ROADMAP

KOMBIT
Kommunernes it-fællesskab

# Roadmap

Udvikling:
- Open ID Connect - IdP delen
- NSIS i relay state
- Flere OIOSAML profiler, så kommunerne kan styre hvordan sikringsniveauer formidles til deres IdPer

Afklaring: NIS2
- Dækker lovkrav om NIS2 Context Handler og Security Token Service (1 og 2)

Afklaring: Rettighedsstyring for Robotter/IoT i en NSIS verden
- Hvordan det understøttes det fremadrettet når NSIS kræves i de brugervendte systemer?

Afklaring: Profiler i adgangsstyring for brugere
- Behov og løsning er afklaret, men det skal prioriteres

KOMBIT
Kommunernes it-fællesskab

# Boblere

Implementering: NIS2

Udvikling: Understøttelse af rettighedsstyring for Robotter / IoT i en NSIS verden

Afklaring: AI til loganalyse, eksempelvis:

- Ændringer i brugeres rettigheder
- Ens rettigheder på tværs af brugere
- Specielle kombinationer af rettigheder som ikke er lovlige for enkeltsystem
- Specielle kombinationer af rettigheder som ikke er lovlige på tværs af systemer
- Manipulerede profiler

Afklaring: Relationship-based access control (ReBAC) i kommunal adgangsstyring

- Er det noget som der er behov for og hvordan kunne det understøttes?

# TAK FOR OPMÆRKSOMHEDEN