Digdir

digdir.no

Prosjekt ny systemarkitektur for fellesløysingane

07.12.2022

Kva er systemarkitektur-prosjektet?

- Ny driftsplattform basert på skyteknologi
- Modernisering av fellesløysingane
  - Kontaktregisteret, Maskinporten og MinID
- Heilt ny ID-porten

Betre robustheit, høgare skalering, raskare innovasjon
og ikkje minst høgare sikkerheit i fellesløysingane

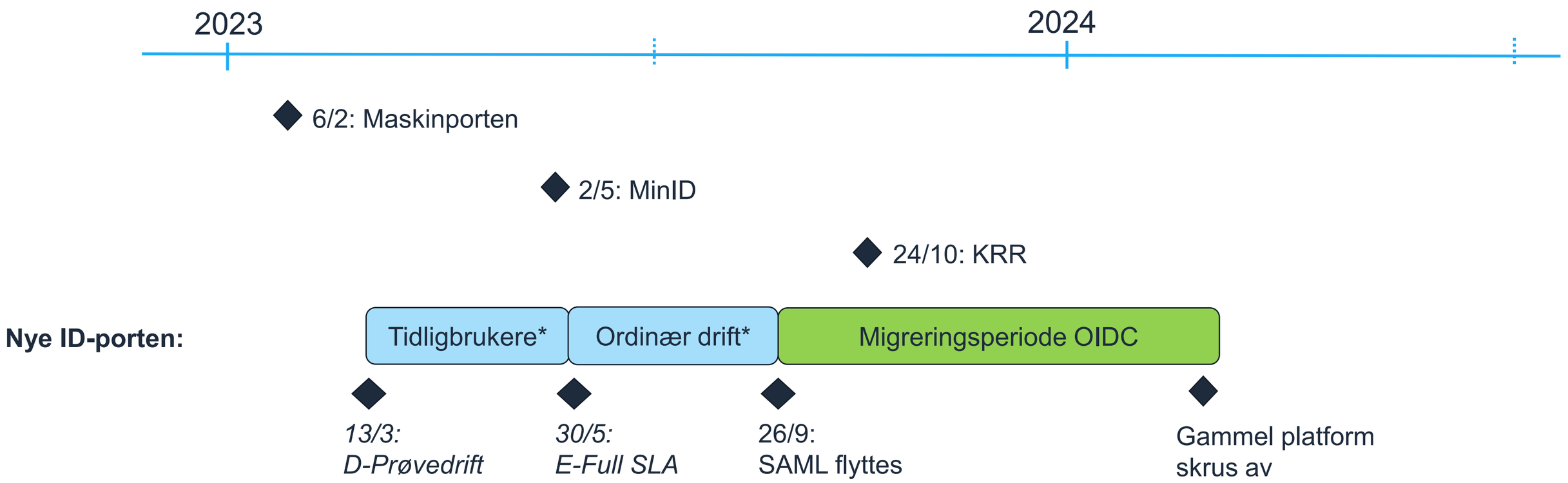
Korleis føregår overgangen?

- Maskinporten, Kontaktregisteret, MinID og sjølvbeteningsløysinga vert migrert **saumlaust** frå gamal til ny plattform
- ID-porten vil ha ein 6 månaders **migrasjonsperiode**, der kunde må flytte – og evt. tilpasse – eksisterande integrasjonar frå gamal til ny «port»

Mål: minst mogeleg påverknad for kundane

Per 26.10.2022

Milepælplan sys.ark.-prosjektet



*: *Ikkje SSO mellom ny og gamal løysing i denne perioden*

Me treng pilot-kundar på ny løysing – vil du hjelpe oss ?

Kva må eg som kunde gjere ?

- Sett deg inn i omfanget og følg løpande status på Samarbeidsportalen: https://samarbeid.digdir.no/736

- Lag ein migreringsplan for din bruk av ID-porten
  - Test at dine eksisterande integrasjonar virkar mot Nye ID-porten
  - Velg eit tidspunkt for flytting som passar deg

- Vurdér behovet for eigen beredskap ved migrasjonsdatoane for Maskinporten, MinID og KRR

Abonnér på varslingar frå statuspage!

status.digdir.no

Testmiljo.status.digdir.no

Digdir

digdir.no

Generelt om ny platform

Generelt om overgangen

- Alle tenester vil få nye IP-adresser
- Ein del tenester får nye endepunkt
  - farvel til difi.no...
- Testmiljøa (VER1, VER2, YT2) vert slått saman til eitt (TEST)
  - Kundar må konsolidere test-integrasjonar
  - Test får same ytelse som i prod
  - Som hovudregel ver2-data som vert migrert
  - Digdir kan ”spinne opp” dedikerte miljø dersom det trengs

Om driftsplattforma

- Privat sky hjå Tietoevry i Noreg
- Kontainerdrift basert på Managed Kubernetes (OpenShift)
- Infrastruktur og konfigurasjon som kode
- Automatisert pipeline med testar

Digdir

digdir.no

Omfang per fellesløying

Maskinporten PROD

Endringar

Ingen funksjonelle endringar

Ny IP-adresse – kundar med brannmur må opne

Flytting skjer via DNS-bytte – skal gå saumlaust

Gjennomføringsplan

(29.nov 22: Bytte av signeringssertifikat)

6. feb 23: Flytting til ny platform

Maskinporten TEST

Endringar

Ingen funksjonelle endringar

Ny IP-adresse – kundar med brannmur må opne

Konsolidering til 1 test-miljø (test.maskinporten.no)

- VER2-integrasjoner virkar mot TEST
- VER1 og YT2-integrasjonar må re-etableres mot TEST
- VER2 vil bli DNS-flytta til ny plattform, parallell-drift i ein periode, før den vert fasa ut.

Gjennomføringsplan

9. okt 22: Stopp for nye integrasjonar i VER1

8. des 22: TEST blir lansert

5. jan 23: VER2 blir flytta til ny plattform

Q3 23: VER2, VER1 og YT2 blir deaktivert (avhengigheit til KRR)

Kontaktregisteret PROD

Endringar

Nytt domene **kontaktregisteret.no** vert etablert allereie no, i gamal platform

- Alle kundar må sjølve oppdatere endepunkt før flytting

Ny IP-adresse ifbm med flytting

Gjennomføringsplan

Nov 22: nytt domene blir etablert. Migreringsperiode for kunder starter.

Q1: Kontaktinfo for innlogga brukere i nye ID-porten.

Okt 23: KRR blir flytta til ny platform. Gamle domener blir fasa ut

Kontaktregisteret TEST

Endringar

Nytt domene **test.kontaktregisteret.no,** elles same som for prod

Postkasse ende-til-ende-funksjonalitet vert flytta frå VER1 til VER2

- VER2 + postkasse-brukere frå VER1 vert migrert til nytt testmiljø.

Gjennomføringsplan

No: kundar kan oppdatere til nye endepunkt

Des 23: Flytting av postkasse-funksjonalitet til ver2

Aug-sep 23: Testmiljø migreres til ny platform

MinID PROD

Endringar

PIN-kodar vert fasa ut for å styrke sikkerheita i MinID. Brukarar må gå over til SMS eller app

Bytter databaseteknologi

Strengare passord-krav

Gjennomføringsplan

Q1 23: Eksisterande PIN-koder slutter å virke

16. feb 23: Database-migrering

2. mai 23: Applikasjonar flyttes til ny platform

MinID TEST

Endringar

Generelt: Kundar blir oppmoda om å bruke TestID i staden for MinID

Konsolidering til 1 testmiljø

Syntetiske fødselsnummer får statisk sms-kode

Gjennomføringsplan

Des 22: Konsolidering + database-migrering

Sjølvbetjening

Endringar

Nytt domene for API-basert sjølvbetjening (api.idporten.no ?)

Gjennomføringsplan

Okt 22: Stengd for sjølvbetjening VER1

Q4 23: Sjølvbetjening flyttar til ny plattform. Gamalt domene blir fasa ut.

Digdir

digdir.no

Omfang for ID-porten

ID-porten

Endringar

Heile ID-porten vert laga på nytt

Det aller meste vil fungere som idag, men reviderte krav til sikkerheit fører til at ID-porten vert litt “strengare”

Høve til SSO-fri innlogging

Konsekvensane for kunde er avhengig av bruksområde:

- Innlogging over OIDC-protokoll
- Innlogging over SAML-protokoll
- Brukarstyrt datadeling som konsument/sluttbrukarsystem
- Brukarstyrt datadeling som API-tilbydar

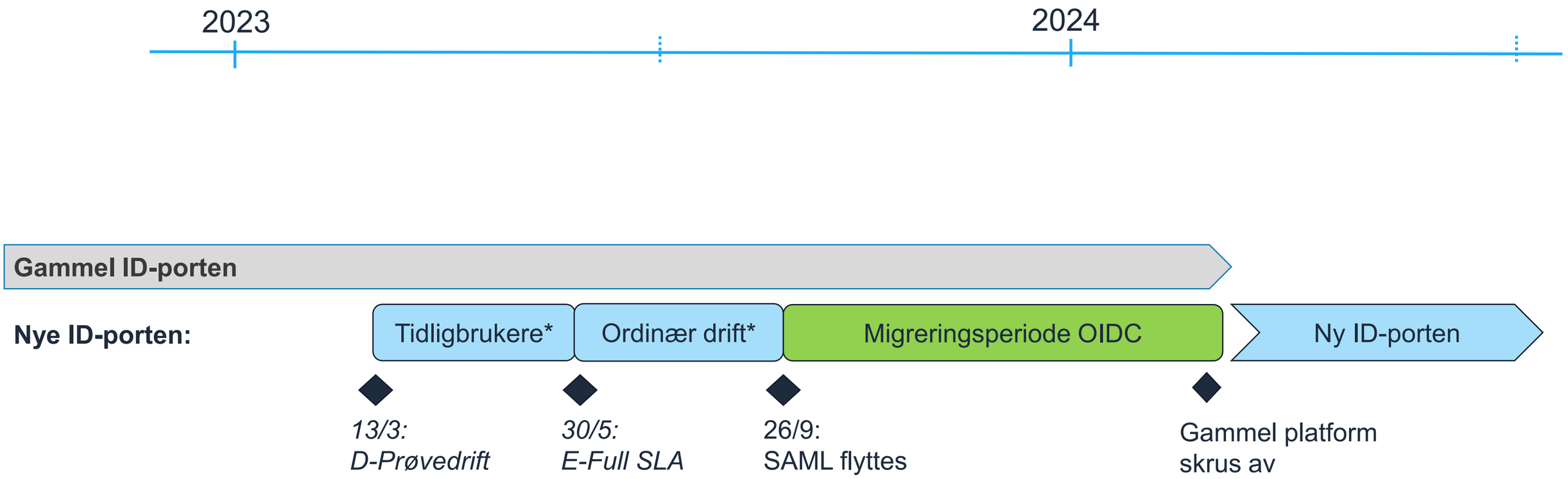
Gjennomføringsplan

Lang migreringsperiode der kunde sjølv kan flytte frå gamal til ny løysing når det passar

Sjå eigne slider

Per 26.10.2022

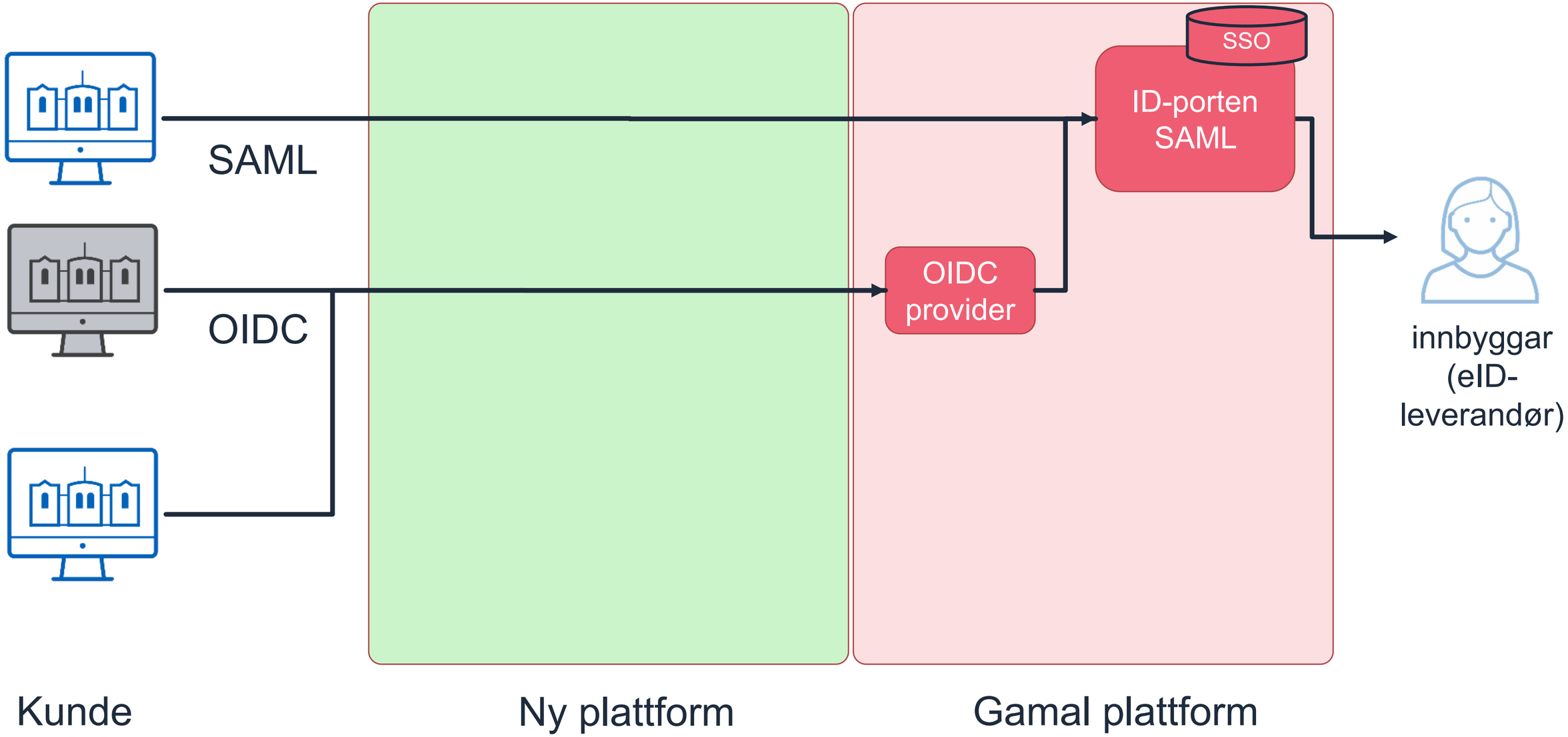
Milepælplan ID-porten



*: *Ikkje SSO mellom ny og gamal løysing i denne perioden*

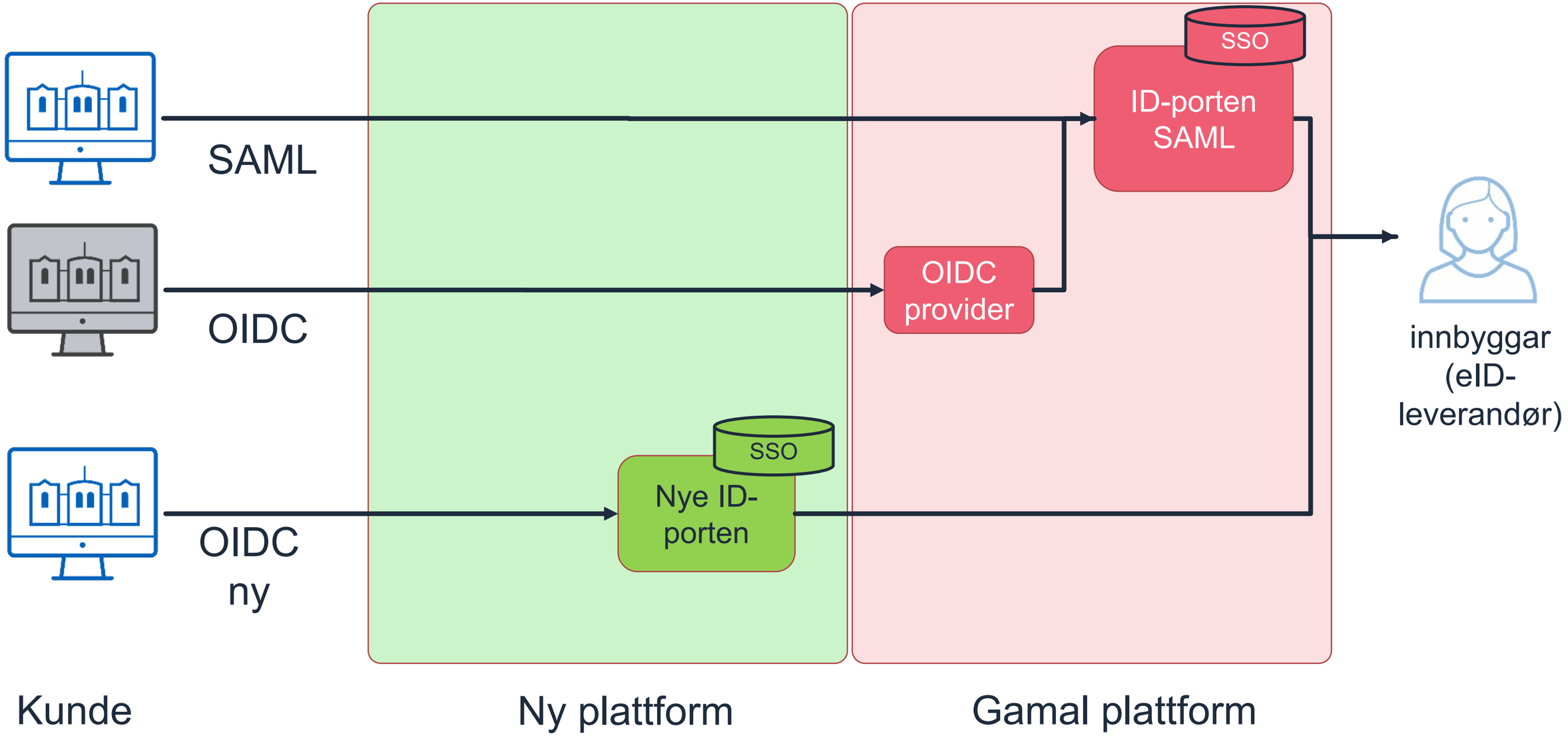
Store integrasjonar får **utdelt ei tidsluke** for migrasjon !

Dagens situasjon



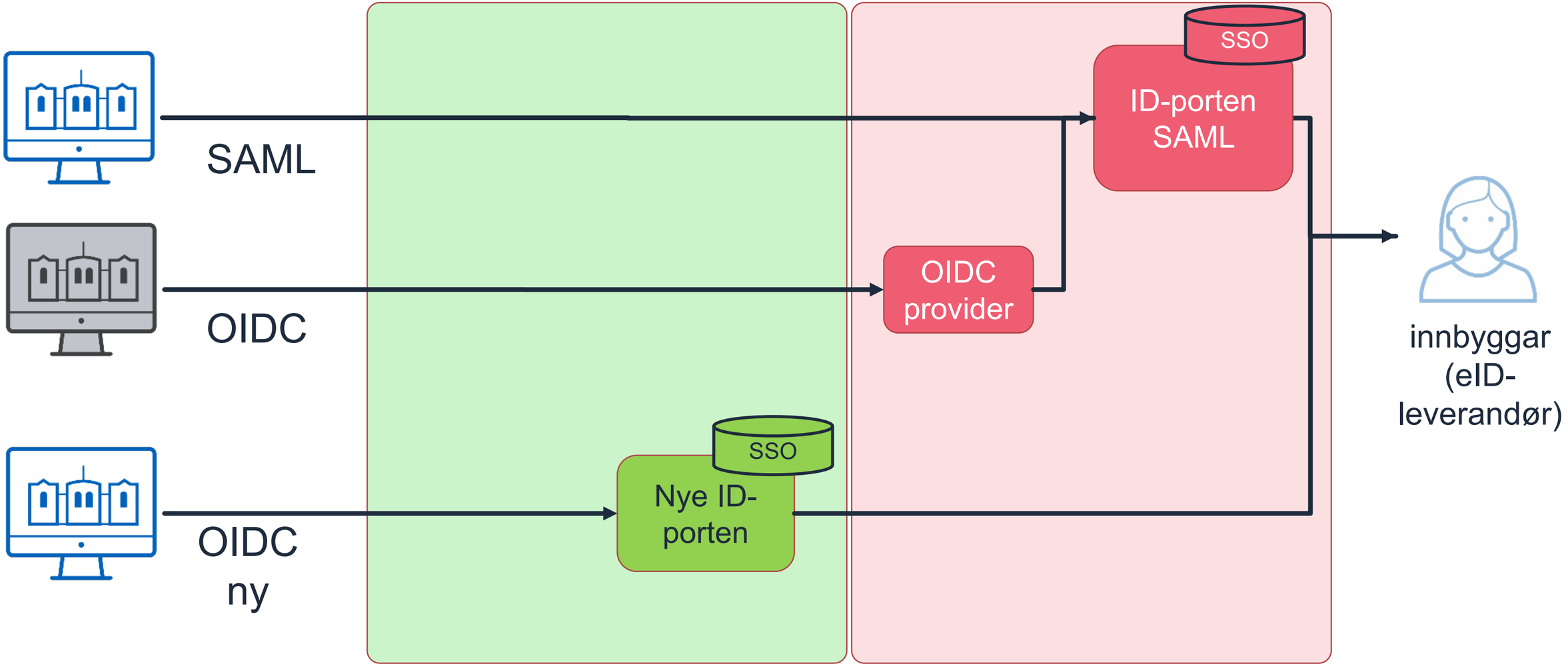
Mars 2023: **Nye ID-porten blir lansert**

- Prøvedrift; frivillig for tidleg-brukarar, og pålagt for nye integrasjonar
- Ikkje SSO mellom ny og gamal platform



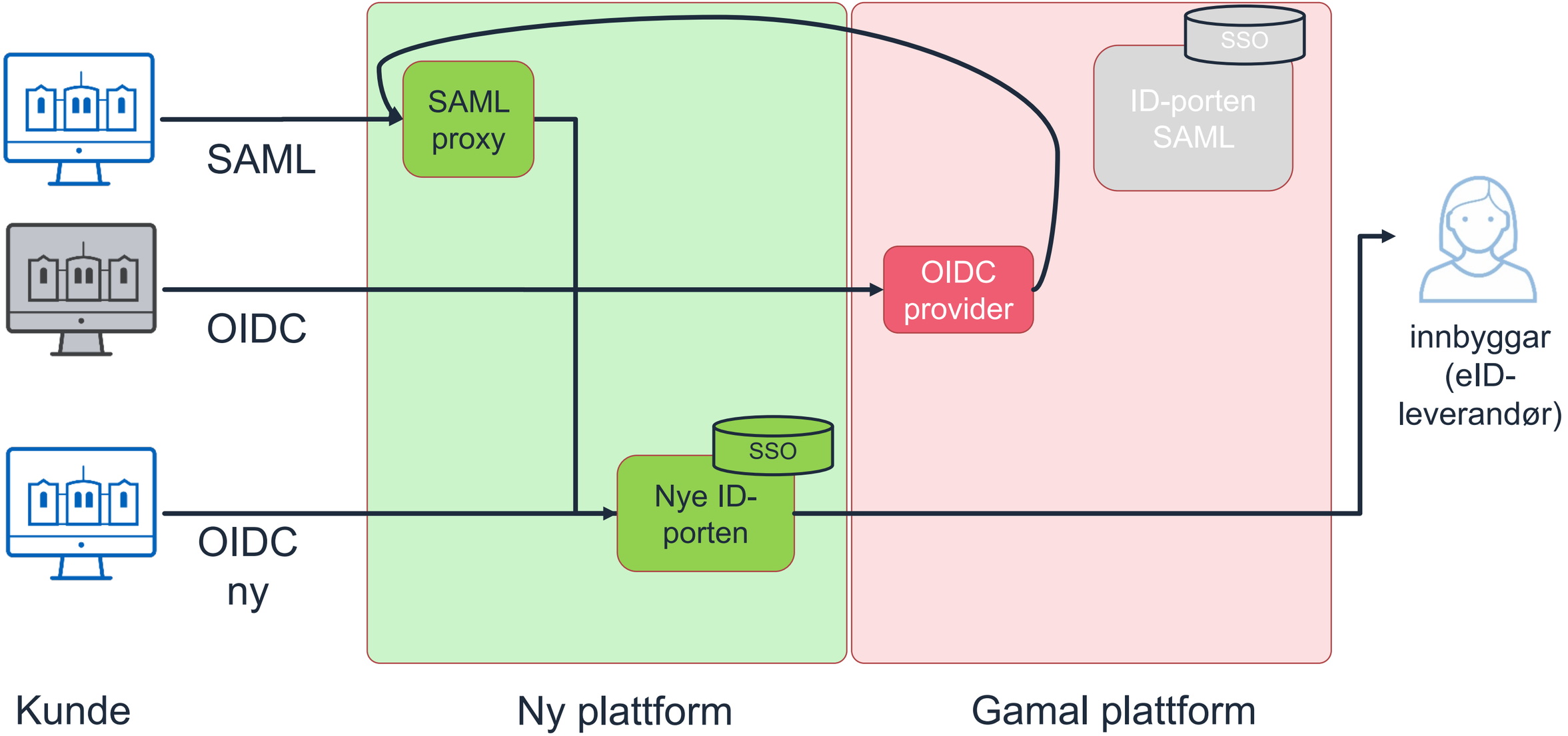
Mai 2023: **Ordinær drift**

- Alle tenester som ikkje krev SSO må starte migrering no



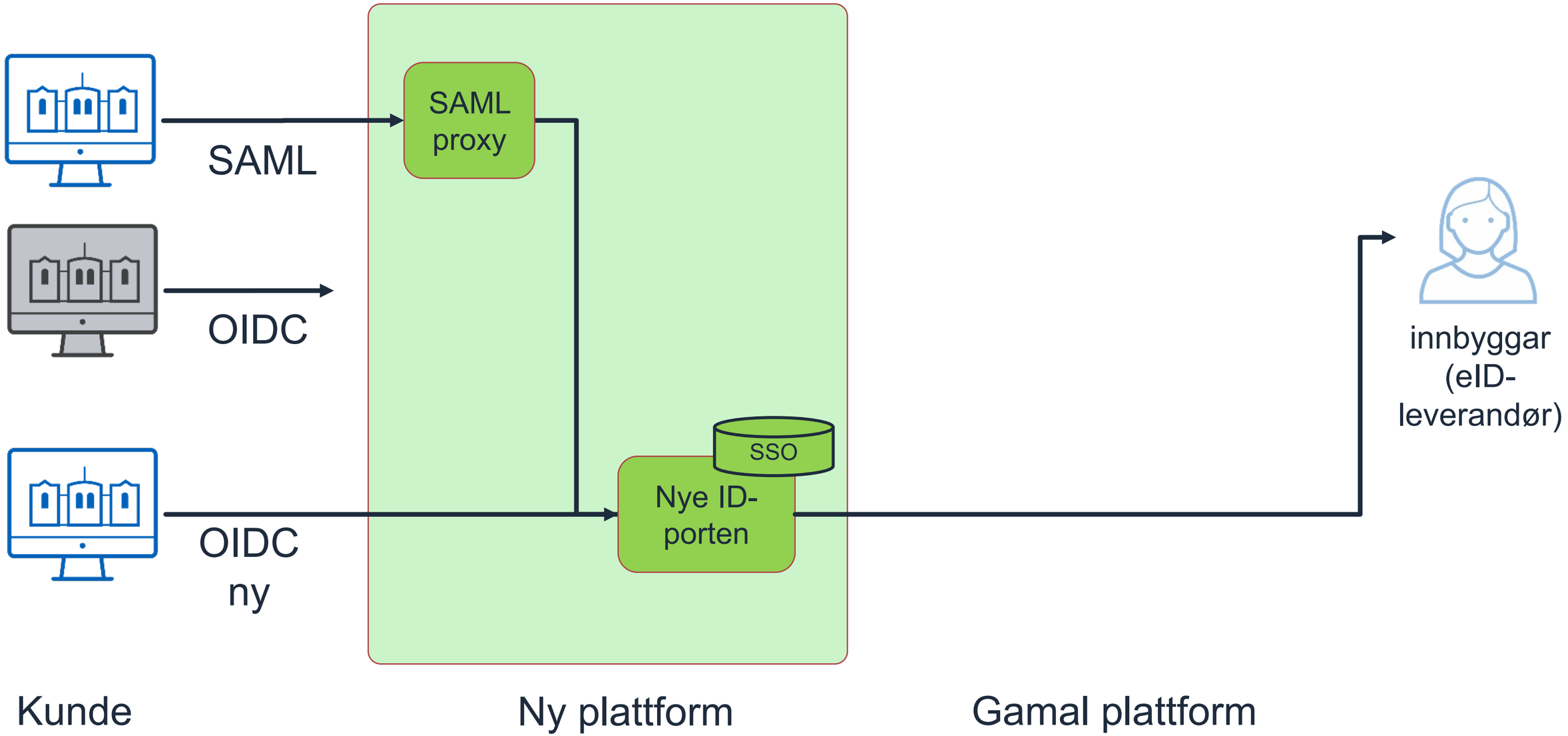
September 2023: **SAML vert flytta**

- I praksis vert mesteparten av trafikk flytta til ny løysing denne dagen
- Alle OIDC-kundar må starte migrering no



Q1 2024: **Gamal plattform skrus av**

- Ikkje-migrerte tjenester sluttar å virka



Overgang i 5 steg:

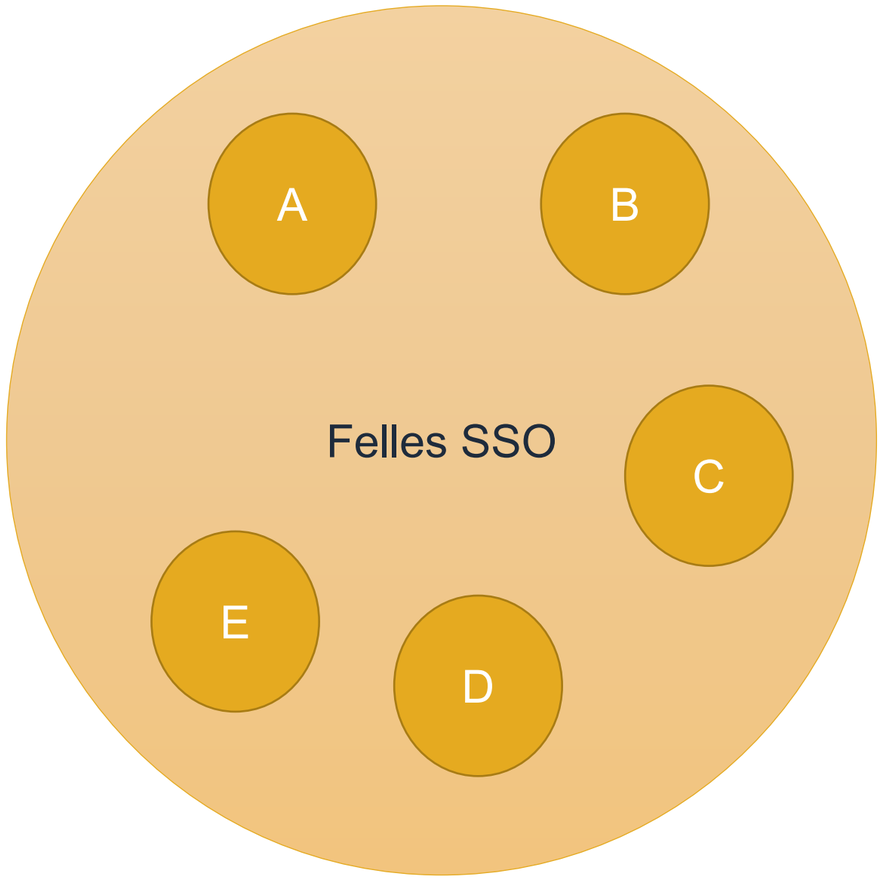
Steg	Dato	Beskrivelse
1: Prøvedrift	Mars 2023	Den nye OIDC-issueren er gjennomtestet og settes i produksjon, klar for reelle tjenester. Driftsplatformen vil være godkjent for 24/7-drift, og informasjonssikkerhet vil være ivaretatt på lik linje med dagens løsning. I denne fasen kan det oppstå mindre “innkjøringsproblemer” mens vi bygger hands-on-erfaring med den nye løsningen. For at prøvedriften skal bli vellykket, er vi derfor helt avhengige av at et tilstrekkelig antall kundetjenester tar løsningen i bruk tidlig. Nye integrasjoner vil derfor blir pålagt å bruke ny løsning, men vi ønsker også at mange eksisterende integrasjoner flyttes nå, i samarbeid med oss.
2: Ordinær drift	Mai 2023	Den nye OIDC løsningen skal nå ha full funksjonalitet og ytelse. Migreringsperioden starter. Alle OIDC-integrasjoner som ikke behøver SSO til andre skal starte flytting nå.
3: SAML flyttes	September 2023	Digdir flytter alle SAML-integrasjoner sømløst fra gamle Openam til ny proxy-løsning. Nye ID-porten styrer nå SSO-sesjonen og tilbyr SSO mellom ny og gammel platform. Siden dagens OIDC-provider også benytter SAML internt, medfører dette i praksis at all gjenstående trafikk flyttes til å gå gjennom ny løsning denne dagen.
4: Migrering SSO		Kunder som er avhengige av SSO til andre skal migrere sine OIDC-integrasjoner nå
5: Sanering	Jan 2024	Gammel OIDC-provider skrus av. OIDC-integrasjoner som ennå ikke har migrert til ny issuer, vil slutte å fungere.

ID-porten omfang OIDC

- Ny OIDC-løysing basert på nytt IAM-produkt (Connect2ID)
  - Nytt domene, issuer og signeringssertifikat
  - God erfaring med produktet frå Ansattporten og idporten-utland
  - Ynskjer følge oauth2.1-protokollen (code-flow m/PKCE,state,nonce)
- Blir “kjernen” i nye ID-porten, og styrer SSO-sesjonen
- Gamal funksjonalitet med “Maskinporten-i-IDporten” er ikkje inkludert

https://docs.digdir.no/docs/idporten/oidc/oidc_protocol_nye_idporten

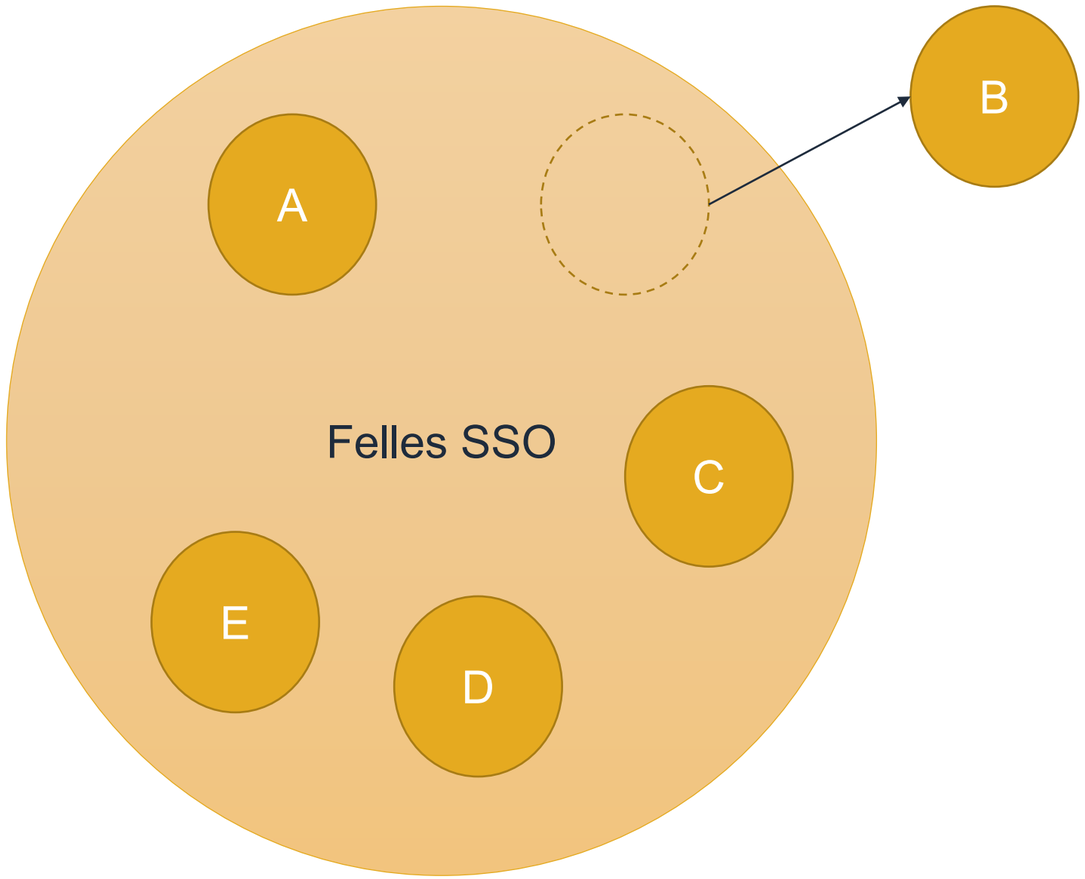
ID-porten: Ny sesjonshandtering



I dag:

- Alle tenester deltek i felles SSO-sesjon
- Enkelt-tenester kan tvinge re-autentisering, men det vert likevel oppretta SSO
  => brukar er sårbar for “utilsikta, etterfølgjande SSO”

ID-porten: Ny sesjonshandtering



"SSO-fri" tjeneste

- Eigen sesjon uavhengig av felles-SSO, identifisert med eigen cookie
- Inn- og utlogging påverker ikkje tilstanden til felles-SSO, og vice-versa
- Må registrerast på klienten (default er false)

Som i dag er datadelings-token (access og refresh) **uavhengige** av SSO-sesjonen, så **utlogging vil ikkje invalidere desse** (og vice-versa). Unntak er "openid profile"-tokens, desse tolkar me som "innloggings-token"

Andre endringar:

- Den proprietære onbehalfof-mekanismen vert vidareført for både OIDC og SAML
- PKCE er påtvungen for alle tjenester
  - er mogeleg å deaktivere via klient-registrering, dersom du bruker eit bibliotek/rammeverk med dårleg sikkerheit.
- implicit flow vert fjerna
- pseudonymisering via `no_pid` vert fjerna
- utanlandske brukarar/eIDAS – vil skje endringar her, men p.t. ikkje klarlagd

Endringar i token-format

- Annan `sub`-verdi for samme brukar til samme client_id i ny løysing kontra gamle
- Endra ACR-verdier:
  - frå “Level3” til “no:idporten:substantial”
  - frå “Level4” til “no:idporten:high”

ID-porten omfang SAML

- SAML vert ei nedskalert teneste
  - Går frå fullverdig IAM-produkt til “dum” proxy foran OIDC-løysinga
  - Støttar berre ArtifactResolution (ikkje form_post)
  - Kontaktinfo vert ikkje lenger utlevert i Assertion

- **Me oppfordrar alle kundar til å utnytte migreringsperioden til å gå over fra SAML til OIDC**

Konsekvensar: OIDC for innlogging

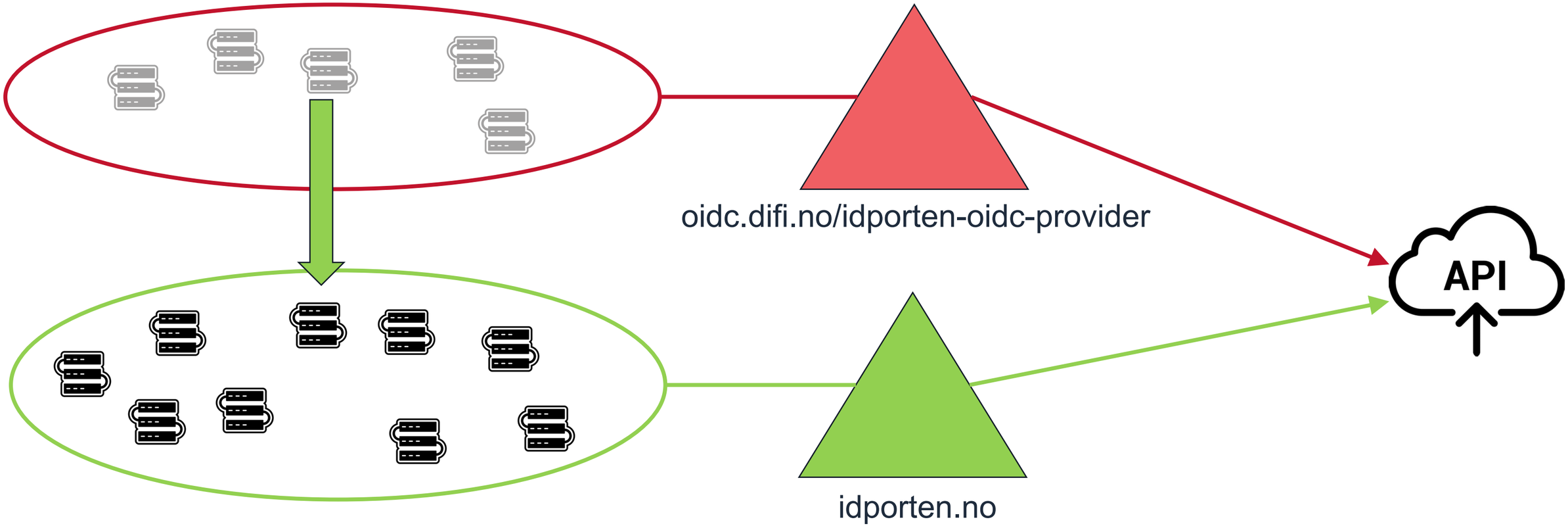
- Teste at integrasjonen din handterer strengare protokoll-validering
  - Mange må legge til støtte for PKCE
  - Dei få som ikkje brukar code-flow, må skrive om
  - Ikkje alle “sære” redirect-URIer vil virke lenger
  - Merk at mobil-appar og SPAer som nyttar eigne scopes til innlogging, må koordinere bytte av trust i eigen mobil backend
  - Mobil-app’er (og evt. SPAer) bør vurdere overgang til SSO-fri innlogging.
  - Full teknisk dokumentasjon: https://docs.digdir.no/docs/idporten/oidc/oidc_protocol_nye_idporten
  - Alle sjølvbetente integrasjonar som tilfredstiller minimumskrav(!) vert synka til ny løysing kvart 10. minutt
- Tidspunkt for eigen migrasjon er primært eit spørsmål om kva tenester ein ynskjer SSO mellom. Dersom du treng SSO til Altinn eller andre SAML-tenester, må du vente til SAML-flytting

Konsekvensar: SAML for innlogging

- Optimalt sett ingen konsekvensar; Digdir flytter SAML-integrasjonar saumlaust, men...
  - STERK oppmoding til å skrive integrasjonen om til OIDC
  - ENNO STERKARE oppmoding til å teste proxyen dersom du held fram med SAML

- Avvikande/“sær” SAML-bruk som tilfeldigvis virkar idag i openam, vil ikkje fungere lenger
  - Proxy støttar berre ei mimimums-variant av SAML2 Web Browser SSO med Artifact Resolution med 1 assertionconumerurl
  - SAML form post ikkje støtta
  - Avgrensa utval signerings- og krypteringsalgoritmer og sterkt avgrensa utanpåliggande SOAP-støtte
  - Gamal protokoll-støtte er dokumentert her: https://docs.digdir.no/docs/idporten/saml/saml_stottede_profiler

Brukarstyrt datadeling krev koordinering av 3 partar



Konsumentar

ID-porten

API-tilbydar

Konsekvensar: datadeling konsument

- Test det same som står under “OIDC for innlogging”.
- Du kan ikkje migrere før API-tilbydar har lagt til støtte for Nye ID-porten.
  - Ta kontakt med API-tilbydar for å få vite når APIet er klart. Digdir har ikkje oversikt over dette.

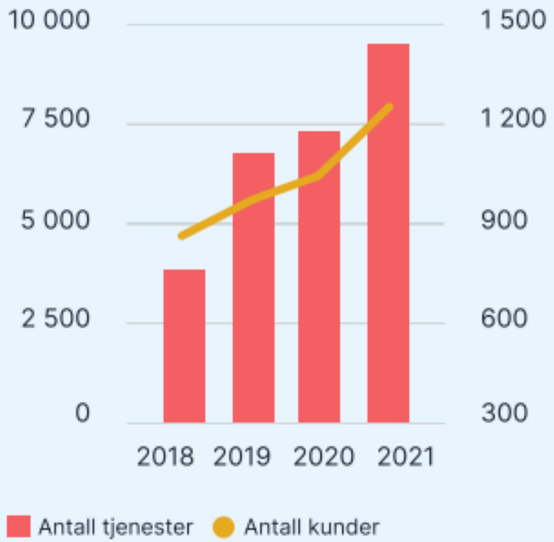
Konsekvensar: Datadeling API-tilbydar

- APIet bør stole på fleire issuere i parallell
  - Alternativt må alle konsumentar migrere koordinert
  - Merk at ny og gamal issuer har ulike signeringssertifikat

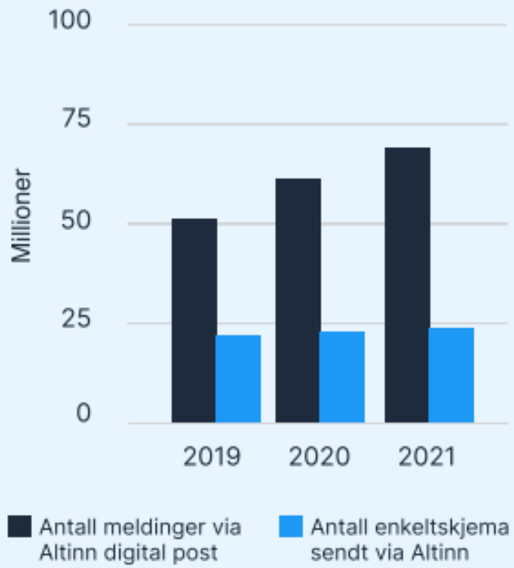
Bakgrunn

Vekst i bruk, kundar og funksjonalitet

Bruk av fellesløsningene



Altinn



317,6 mill ↑

Pålogginger i ID-porten.
Økning på 29 %.

9 257 ↑

Offentlige tjenester som bruker fellesløsningene.
Økning på 25 %.

94 mill ↑

Antall meldinger og skjema sendt i Altinn.
Økning på 10 %.

2,9 mill ↑

Antall forsendelser i eFormidling.
Økning på 154,5 %.

2,3 mrd ↑

Oppslag i Kontakt- og reservasjonsregisteret.
Økning på 67 %.

23,1 mill ↑

Antall brev sendt i digital postkasse.
Økning på 42,6 %

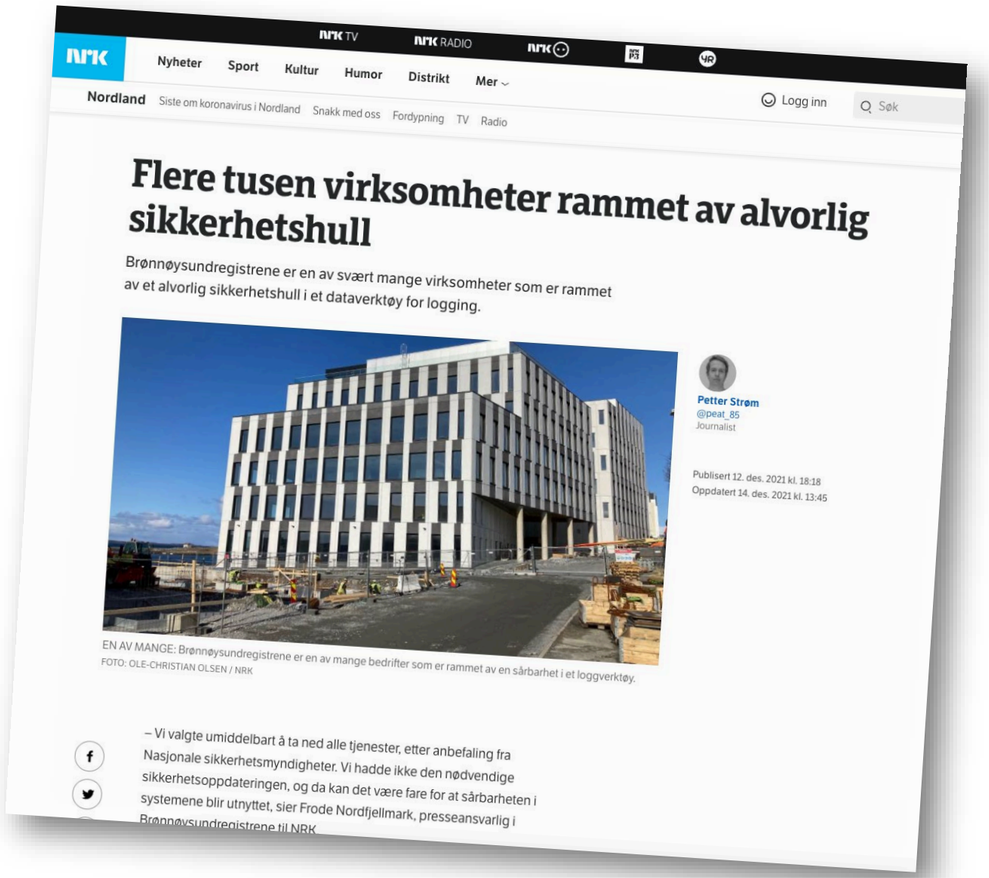
Samfunnskritisk «over natta»

Ukontrollerbare verdikjeder

ID-porten skaper verdi gjennom verdikjeder der Digdir kun har kontroll på ein liten del av disse.

Krever kontinuerlig tilpassing til omgivelsane:

- Endra behov frå kundane
- Endringar i leverandørane sine tjenester
- Rask handtering av sårbarheiter og endringar i rammeverk og 3dje-parts programvare



NRK TV NRK RADIO

NRK Nyheter Sport Kultur Humor Distrikt Mer

Nordland Siste om koronavirus i Nordland Snakk med oss Fordypning TV Radio

Logg inn Søk

Flere tusen virksomheter rammet av alvorlig sikkerhetshull

Brønnøysundregistrene er en av svært mange virksomheter som er rammet av et alvorlig sikkerhetshull i et dataverktøy for logging.

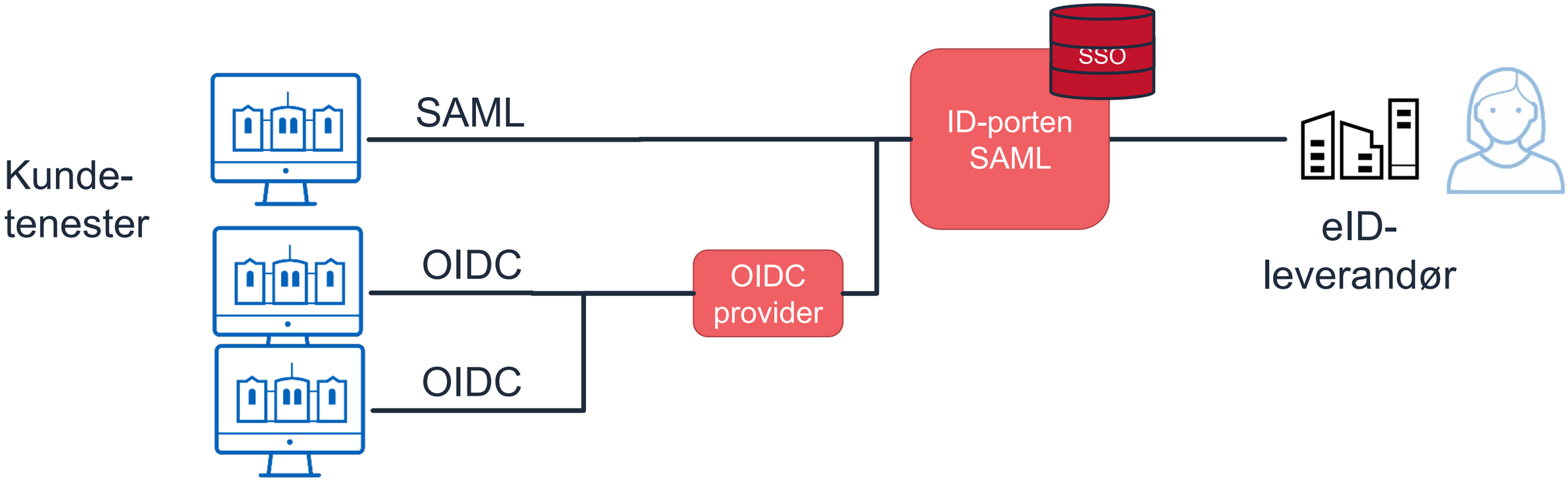
EN AV MANGE: Brønnøysundregistrene er en av mange bedrifter som er rammet av en sårbarhet i et loggverktøy.
FOTO: OLE-CHRISTIAN OLSEN / NRK

Petter Strøm
@peat_85
Journalist

Publisert 12. des. 2021 kl. 18:18
Oppdatert 14. des. 2021 kl. 13:45

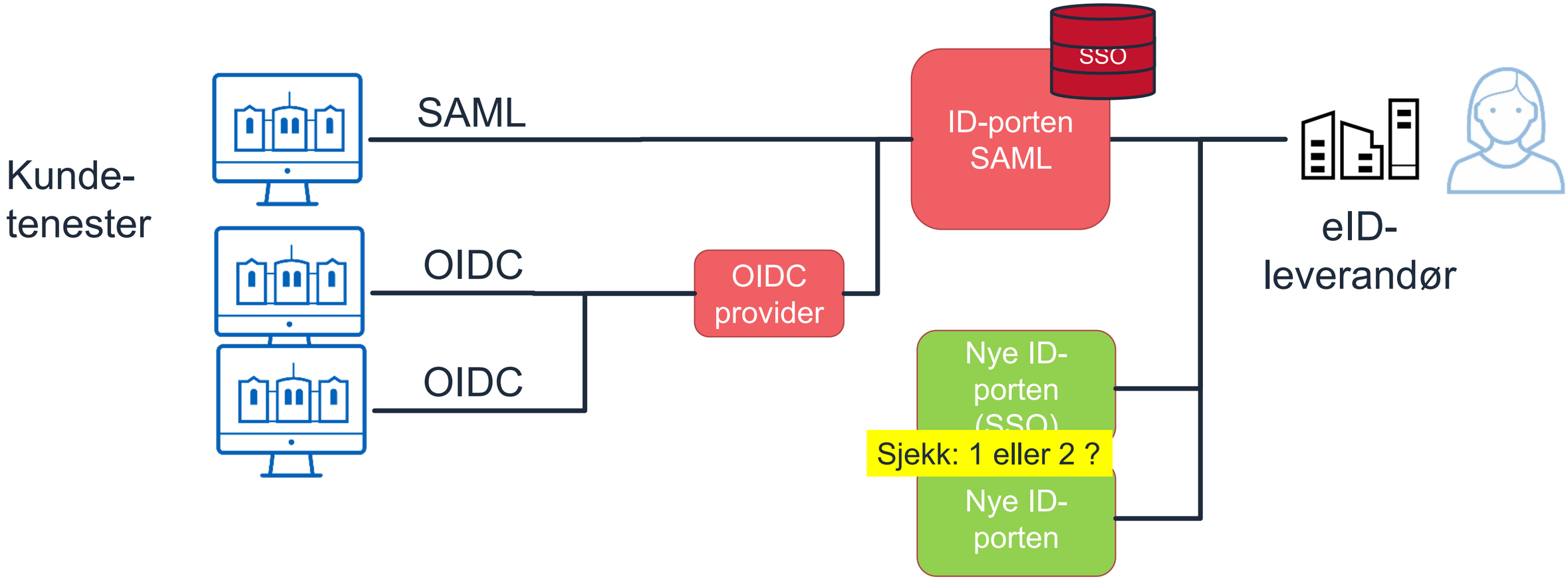
– Vi valgte umiddelbart å ta ned alle tjenester, etter anbefaling fra Nasjonale sikkerhetsmyndigheter. Vi hadde ikke den nødvendige sikkerhetsoppdateringen, og da kan det være fare for at sårbarheten i systemene blir utnyttet, sier Frode Nordfjellmark, presseansvarlig i Brønnøysundregistrene til NRK.

Idag


Kunde-
tenester
SAML
OIDC
OIDC
OIDC
provider
ID-porten
SAML
SSO
eID-
leverandør

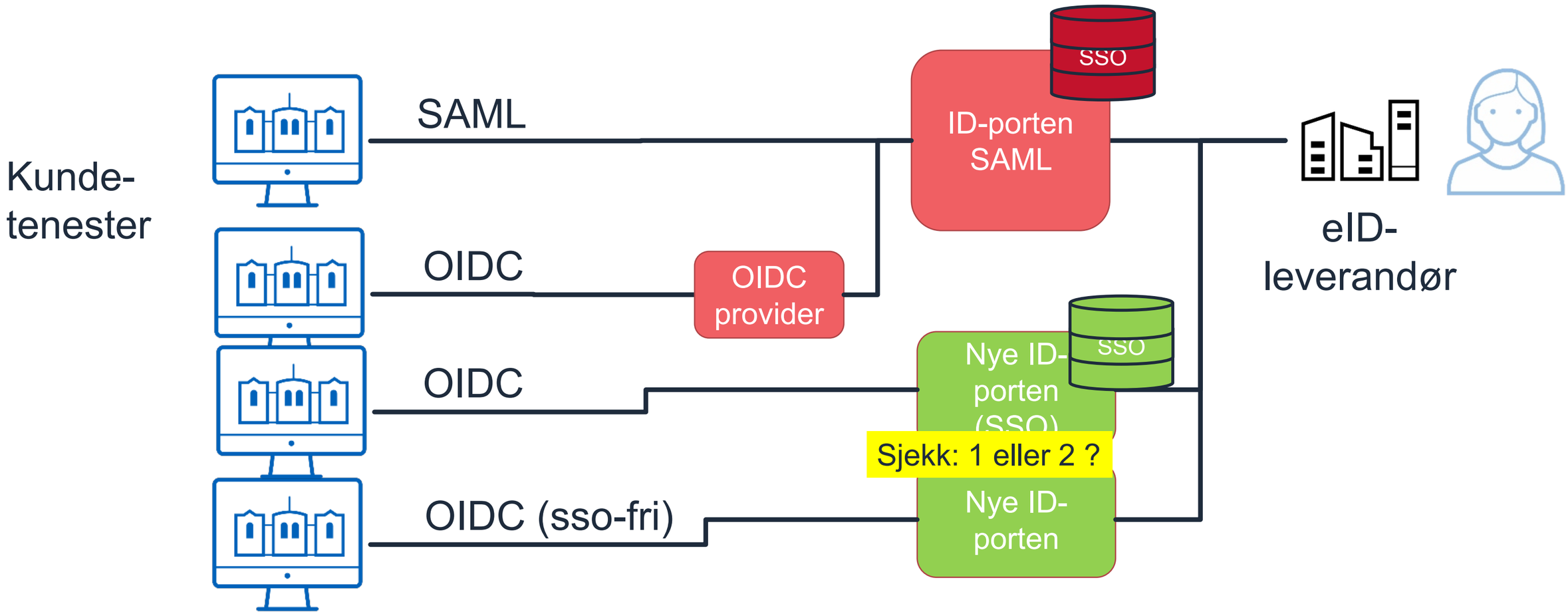
November 2022: **Nye ID-porten lanserast**

- prøvedrift; frivillig for tidleg-brukarar, og pålagt for nye integrasjonar



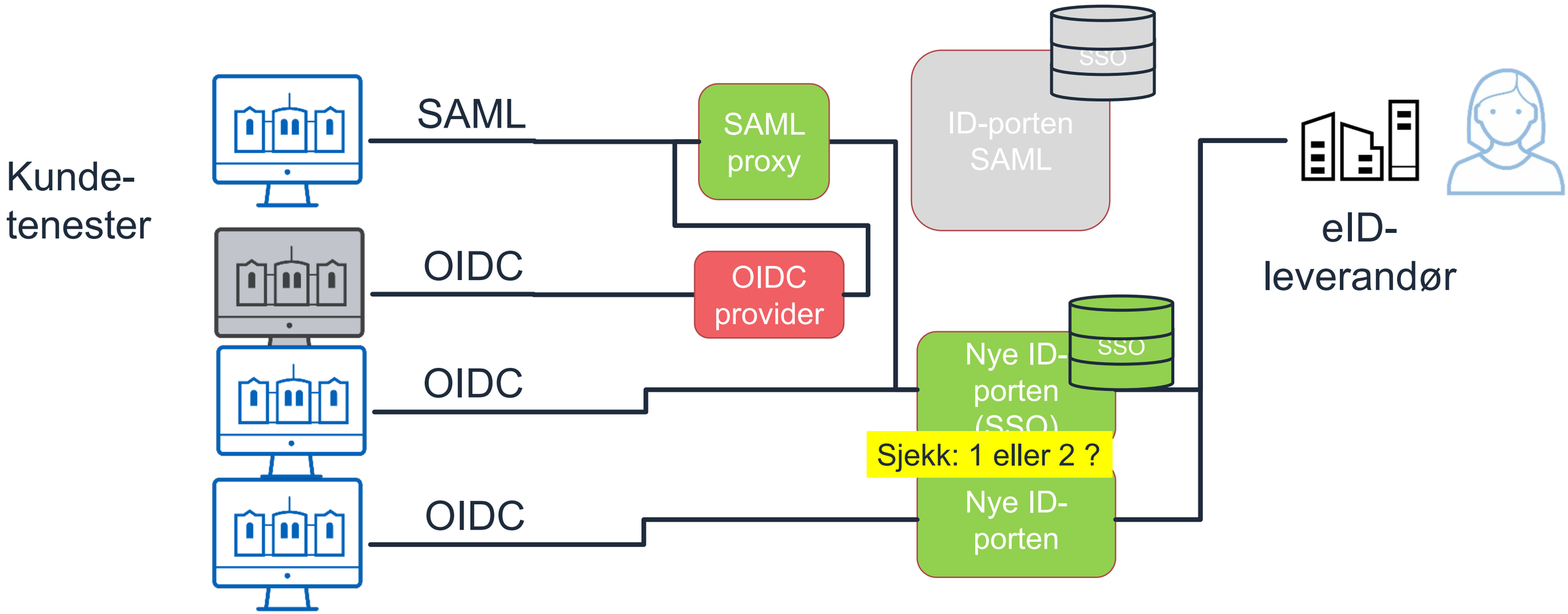
Mars 2023: **Migreringsperiode startar**

- ikkje SSO mellom gamal og ny løysing



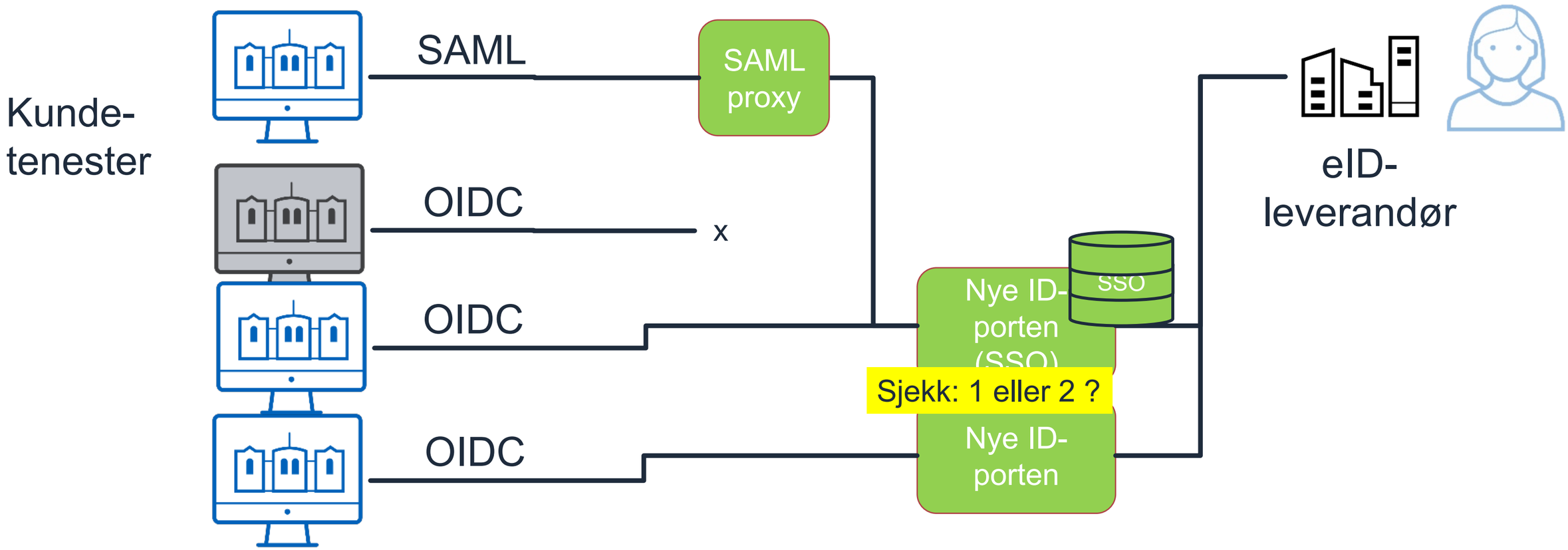
Juni 2023: **SAML vert flytta**

- dei som treng SSO til Altinn/andre SAML-tenester kan starte migrasjon no



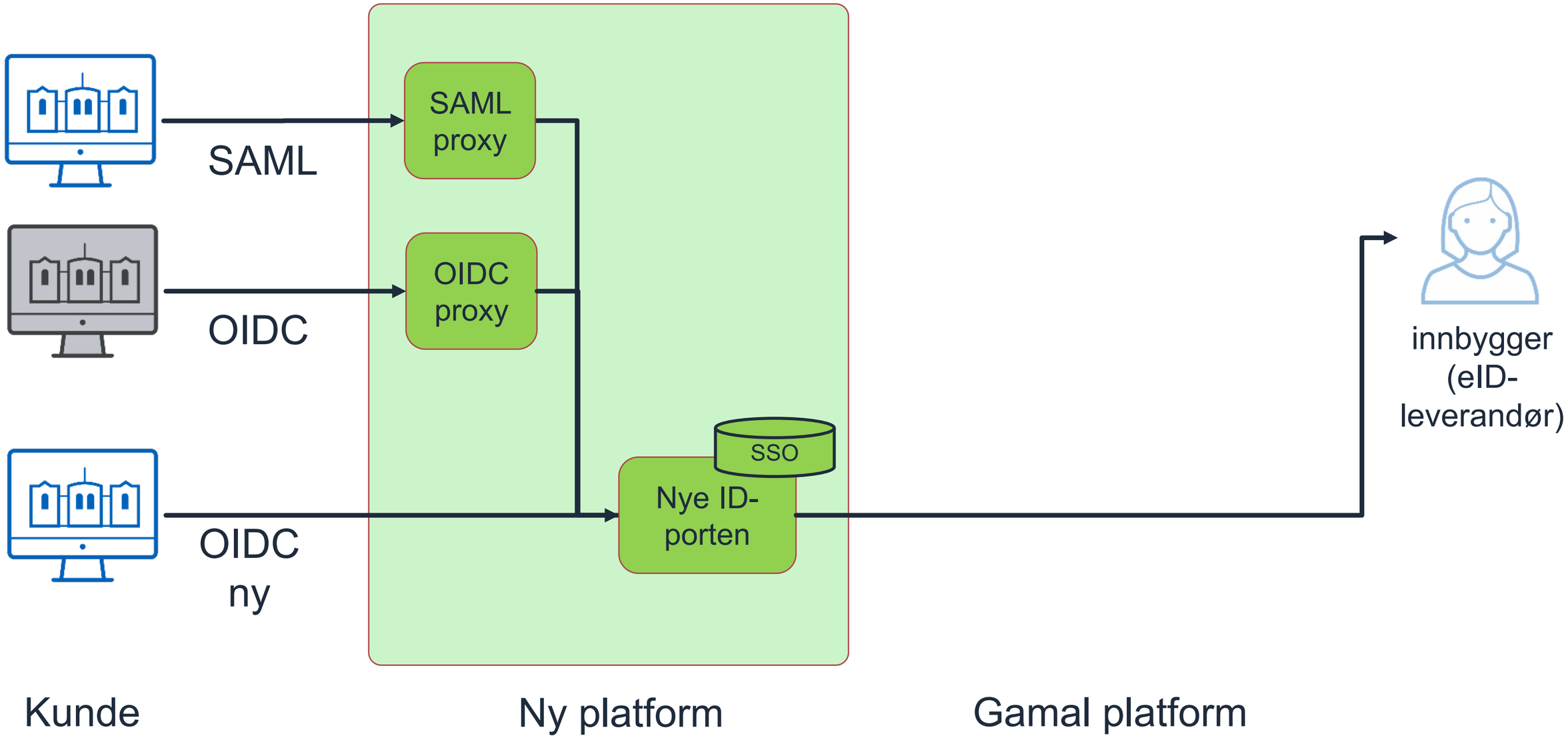
September 2023: **Det gamle vert skrudd av**

- har du ikkje flytta OIDC-integrasjonen din enno, vil den slutte å virke



Desember 2023: **OIDC vert flytta**

- OIDC-proxy er ei midlertidig løysing, for å kunne fase ut gamal platform



Bakgrunn - ny systemarkitektur

- Utgåande IAM-produkt for identitetshandtering
  - Sentral del av ID-porten
- Forventar fortsatt kraftig auke i transaksjonsvolum
  - Gjeld alle fellesløysingar
- Noverande driftsavtalar for fleire eigenutvikla fellesløysingar utgår september 2022
- Ønske om raskare og smidigare syklusar frå idé til produksjon
- Trender i marknaden: Meir bruk av teknologi og tenester i sky. DevOps som arbeidsmetodikk.

Effektmål

Fleksible driftsavtalar som tar høgde for Digdirs behov over tid

Stabil drift med høg oppetid

Fremtidsretta teknologi

Skalerbare på ytelse og ny funksjonalitet

Tilrettelegge for auka endringstakt og innovasjons-evne

Støtte visjon og produktstrategi for dei enkelte fellesløysingane