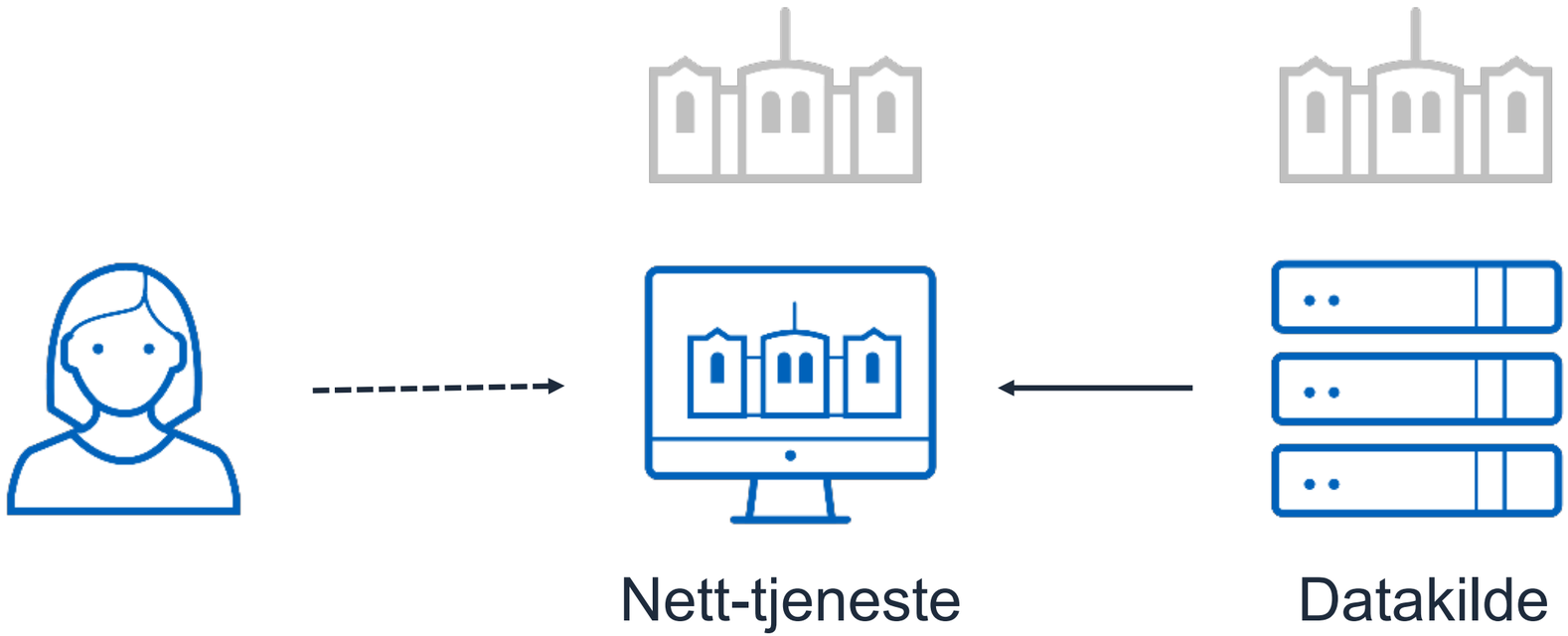
Digdir

digdir.no

Brukerstyrt datadeling i ID-porten

Gir bruker **råderett** over egne data



Fordeler med brukerstyrt datadeling

- Sluttbruker har kontroll på deling av sine data
- Datakilde slipper å eksponere hele datasettet sitt
- Andre kan integrere dine tjenester i sine løsninger

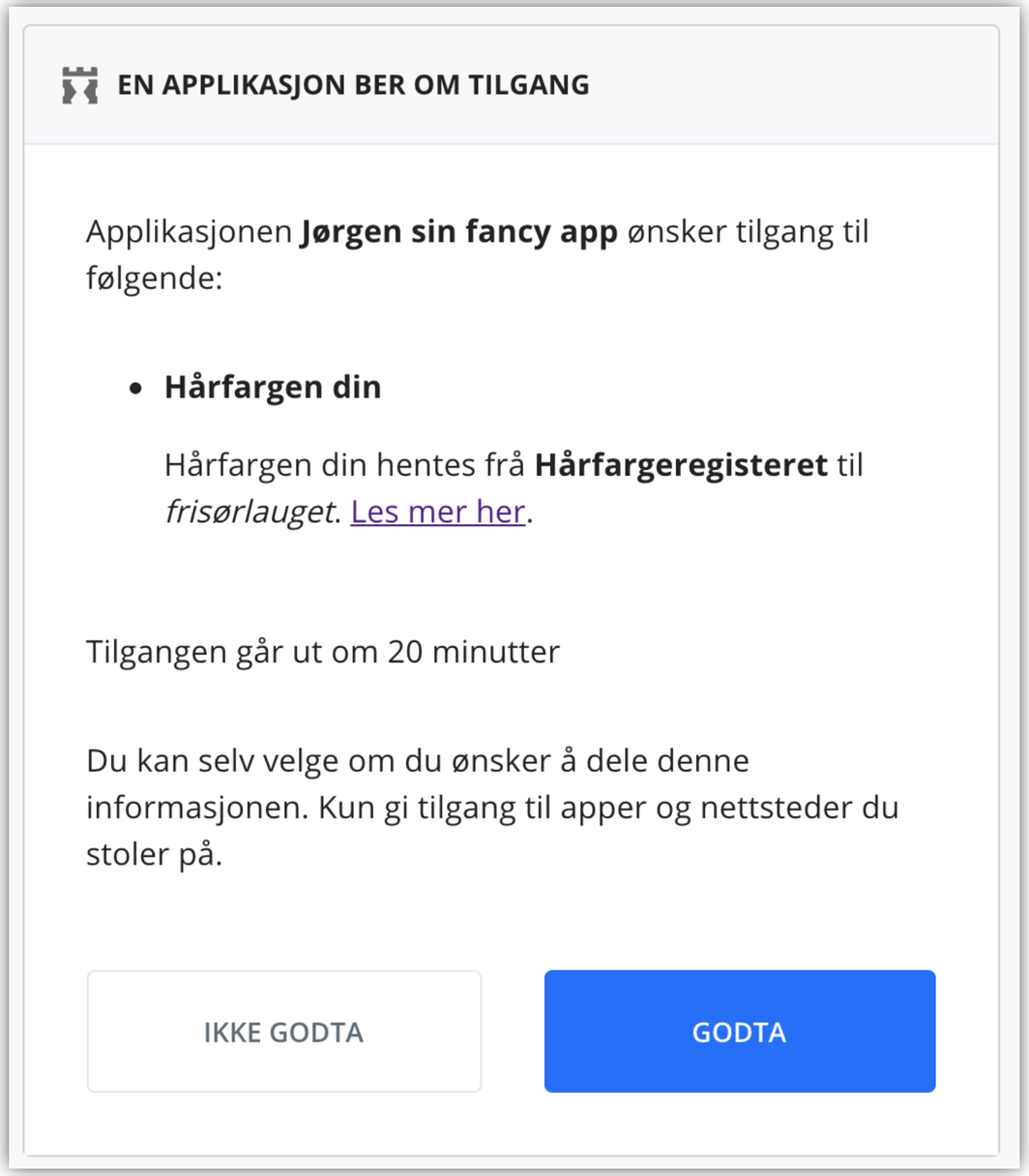
Tilgangsdialog

client.name →

scope.description →

scope.long_description →

min(scope.authorization_max_lifetime, client.authorization_lifetime) →



Tilgangsdialog støtter oversettelser

GET /scopes?scope=testtilgang:nr1


```
{
    "description": "Hårfargen din",
    "description#en": "Your hair colour",

    "long_description": "Hårfargen din hentes frå **Hårfargeregisteret** til *frisørlauget*. [Les mer her](https://www.digdir.no/).",
    "long_description#en": "Your hair color will be fetched from the **Hair Registry** run by the *Hairdresser's association*. [Read more](https://www.digdir.no/)",
}
```

Oppsett for tilbyder

`allowed_integration_types`	Sett til [API_KLIENT] for å unngå at klienter bruker Maskinporten
`requires_user_consent`	Hvis true, så vil tilgangsdialogen bli vist
`requires_user_authentication`	Tving fram ny innlogging sjølv om bruker har aktiv SSO-sesjon i ID-porten
`requires_psedonymous_tokens`	id_ og access_token vil mangle fødselsnummer. Du som tilbyder kan hente fødselsnummer ved å introspecte access_tokenet.

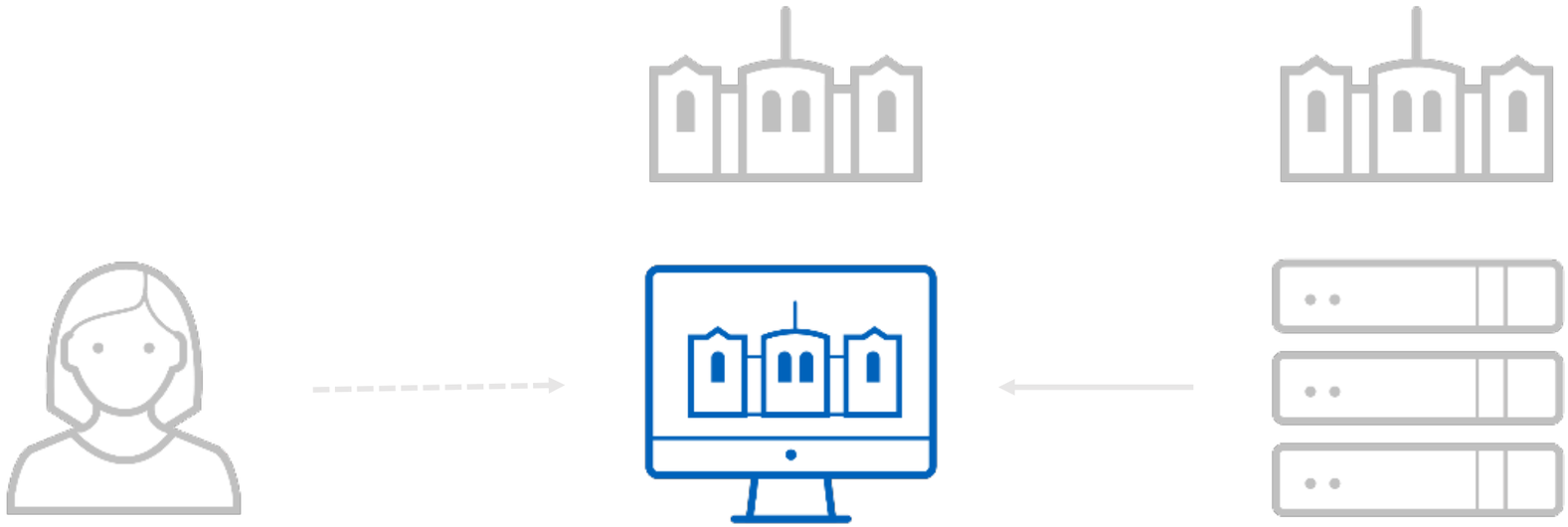
Tilgangstyring som for Maskinporten

- `accessible_for_all`

eller

- Gi eksplisitt tilgang til org.nummer

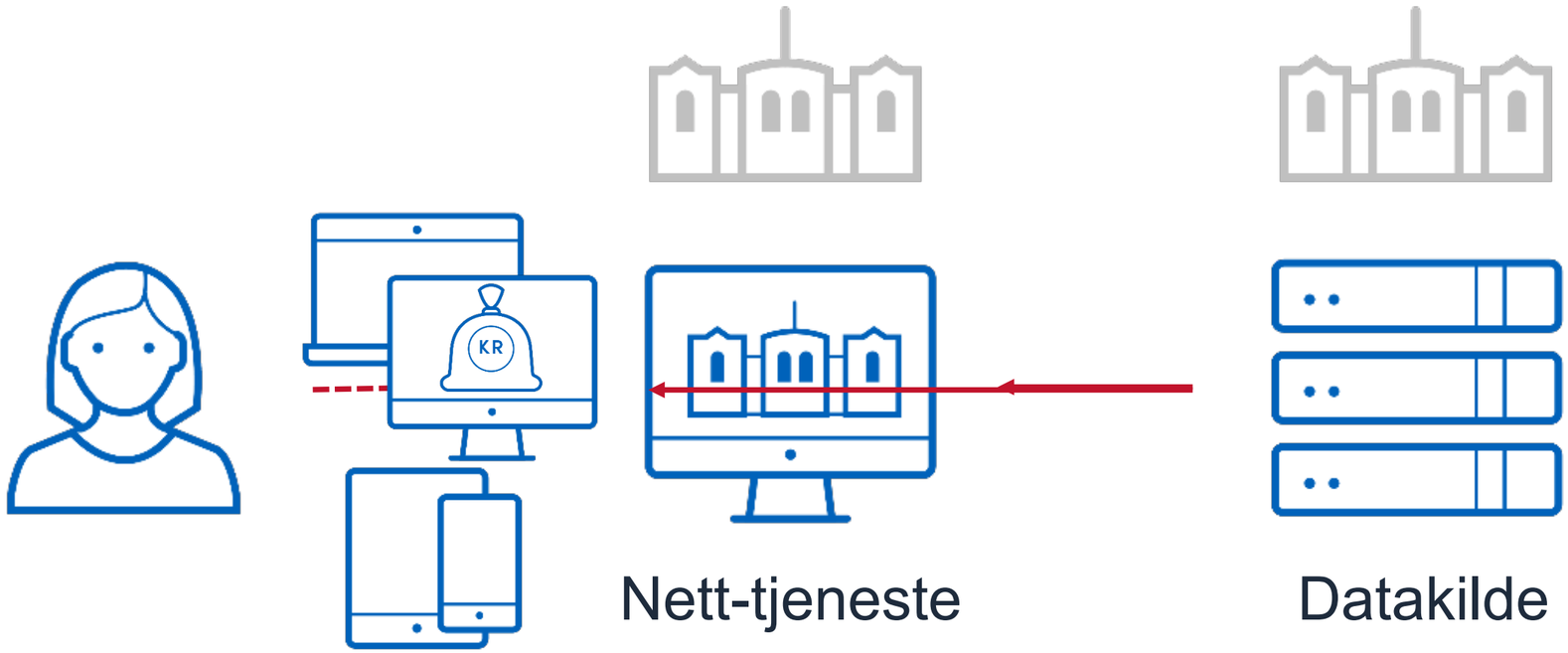
For **konsument**



Konsumenter lager klienter som vanlig

- Må vere integrasjonstype `API_KLIENT`
- Registrere aktuelt oauth2 scope
- Velger selv mellom
  - app,
  - tykk-klient,
  - javascript eller
  - nett-tjeneste
- uansett: authorization code-flyt + PKCE

App’er og tykke klienter er et spesialtilfelle…



Registrering av tykke klienter

- `application_type=native`
  `=> token_endpoint_auth_method=none`
- Felles `client_id`, og ingen `client_secret`
- Må bruke PKCE og state (og nonce, dersom OIDC)
- Kan / bør bruke loopback interface redirection:

	redirect_uri
Registrering	http://127.0.0.1:**0**/callback
Ved runtime	http://127.0.0.1:**45123**/callback

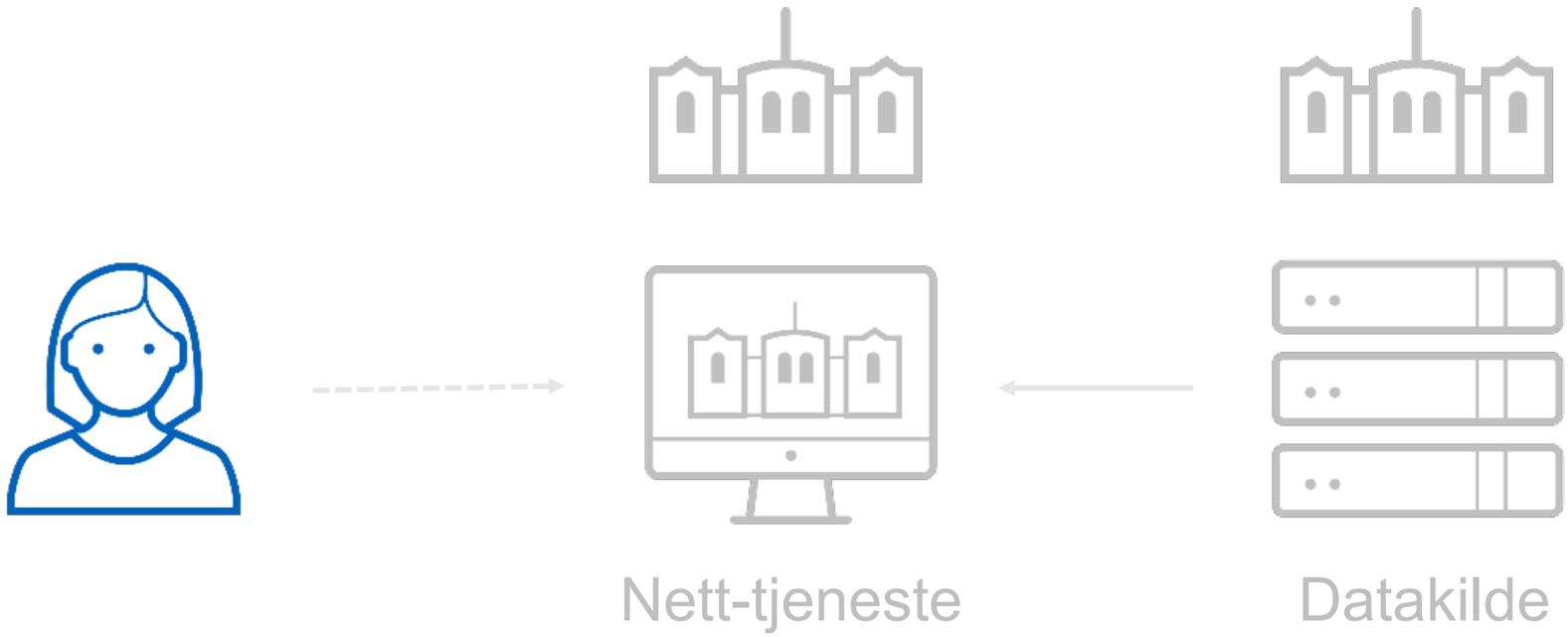
(app: typisk private-use URI: no.idporten.app:/callback)

Konsument bare mot egne APIer?

- Er du sikker? Andre kan ha nytte av dine tjenester!

- Dersom API er sikra av ID-portens access_token direkte:
  - bruke egne scopes, ikke bare “openid profile”
    - ellers så kan alle gyldige ID-porten-innlogginger til alle andre tjenester også brukes mot ditt API
  - bruk audience-begrensa tokens
    - der aud-verdien settes lik URL til API-endepunktet

For **sluttbruker**



Innsyn og revokasjon

- brukerprofil.idporten.no
- eller over API for
  - dine klienter og/eller
  - dine scopes