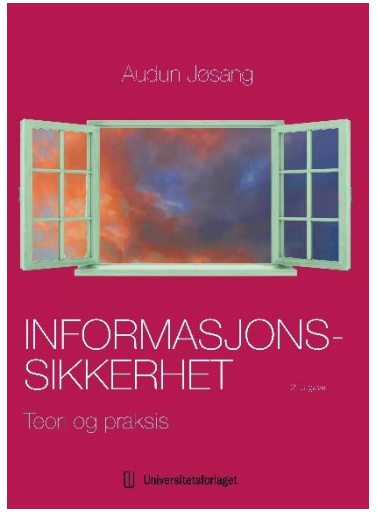
Kapittel 9:
IAM: Identitets- og tilgangshåndtering

Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utg. 2023

Universitetsforlaget



Oversikt

- Hva er IAM (Identity and Access Management)
  - Identitets- og tilgangshåndtering
- Hva er identitet
- Silomodellen for identitetshåndtering
- Føderert modell for identitetshåndtering
  - Brukerautentisering som tjeneste
- Tilgangskontroll

IAM - definisjon

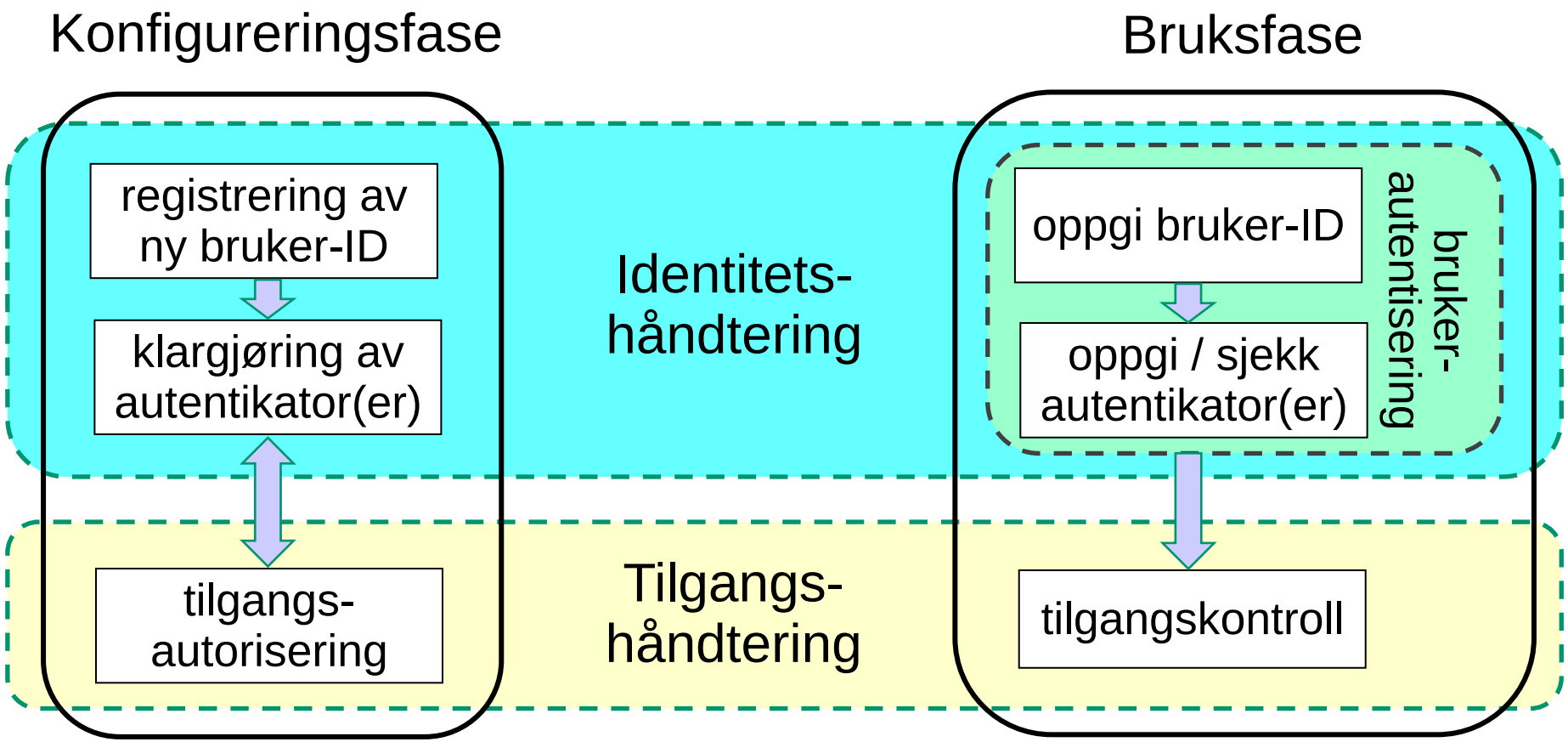
- Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

- *Identitets- og tilgangshåndtering (IAM) er sikkerhetsdisiplinen som gjør det mulig for de rette individene å få tilgang til de riktige ressursene til rett tid, og for riktige hensikter.*

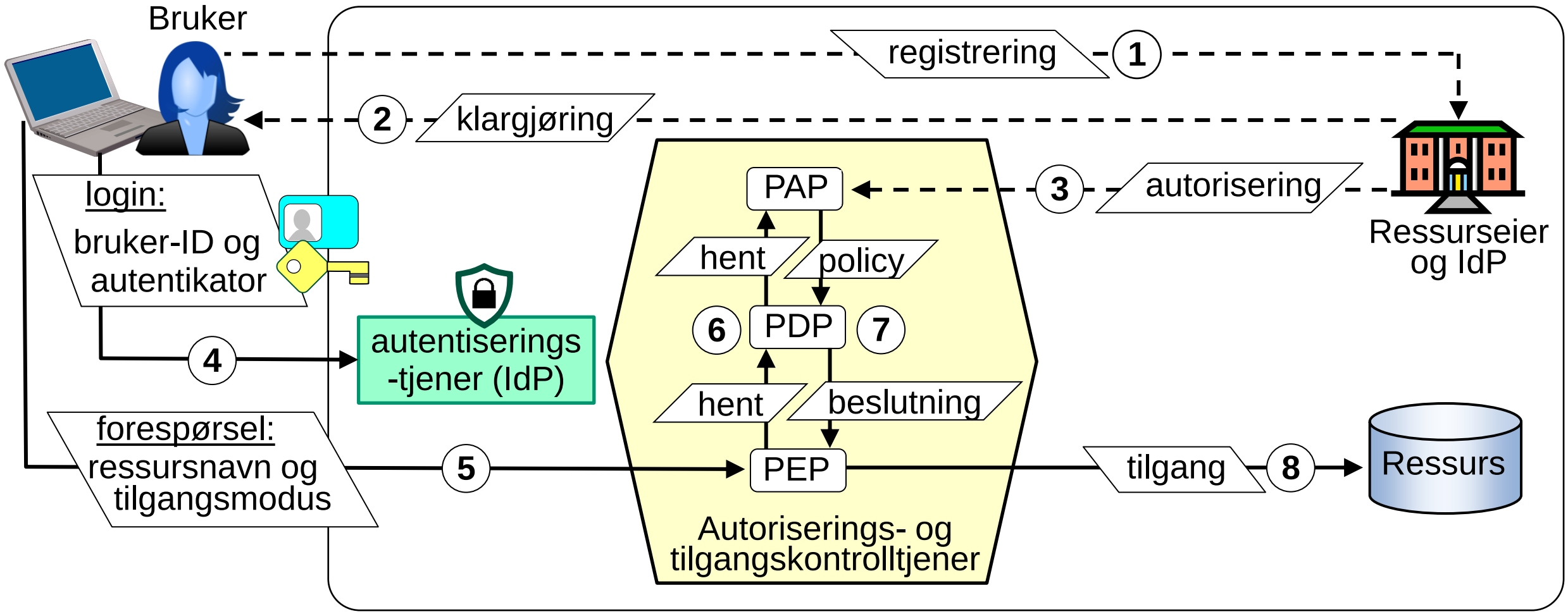
Gartner, security glossary

https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

Identitets- og tilgangshåndtering
IAM
Identity and Access Management

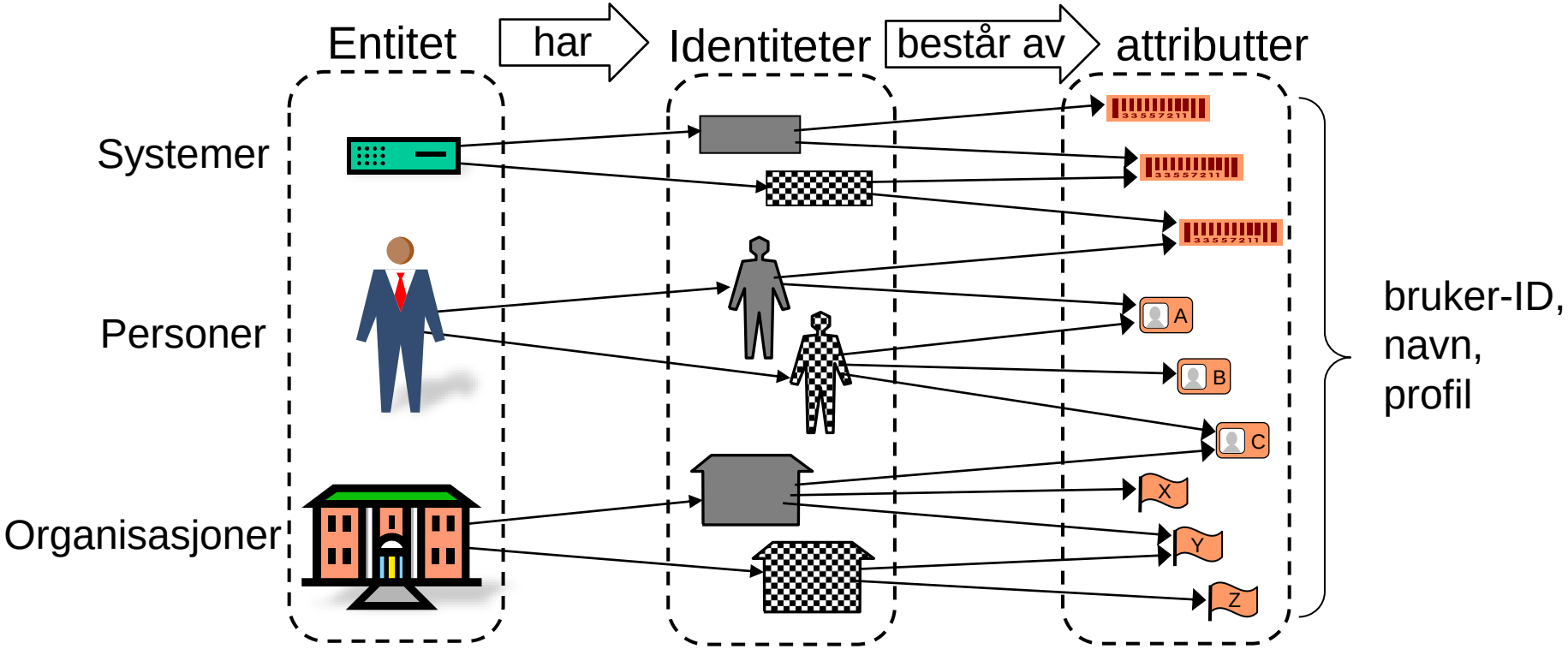


IAM scenario



PAP: Policy Administration Point
PDP: Policy Decision Point
PEP: Policy Enforcement Point
IdP: Identity Provider
konfigureringsfase
bruksfase

Identitet som begrep



Konsepter relatert til identitet

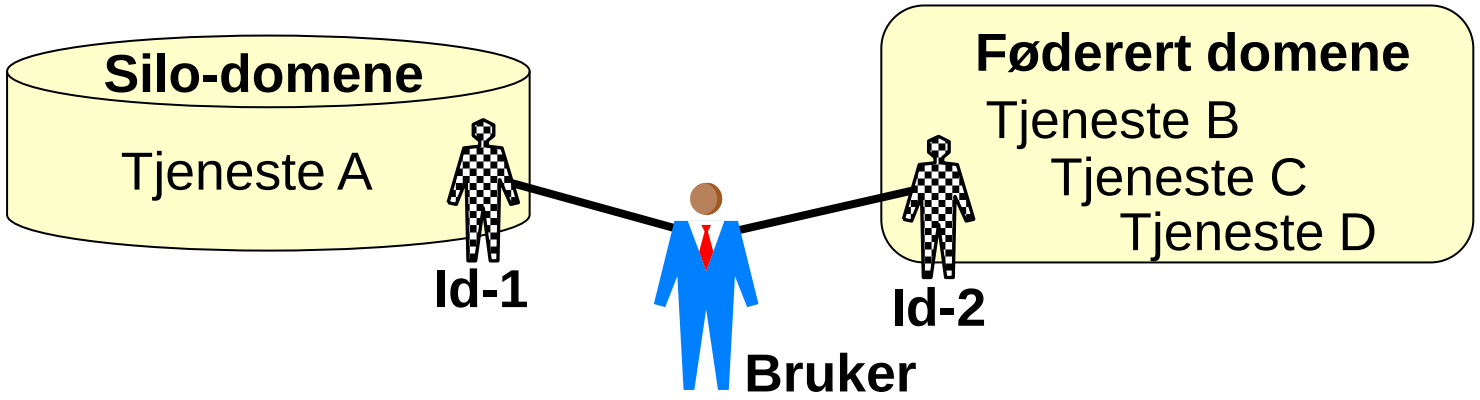
- Entitet
  - En person, organisasjon, agent, system, økt, prosess osv.
- Identitet
  - Et sett med navn / attributter for entiteten i et bestemt domene
  - En entitet kan ha identiteter i flere domener
  - En entitet kan ha flere identiteter i samme domene
- Digital identitet
  - Digital representering av navn / attributter på en måte som er egnet for digital behandling
- Navn og attributt til entiteter, kan være
  - entydig eller tvetydig innenfor et domene
  - kortvarig eller permanent,
  - selvdefinert eller definert av autoritet,
  - behandlet av mennesker og / eller computere
  - osv.
- En identifikator er et entydig unikt navn

Identitet – opprettelse - registrering

- Etymologi (opprinnelig betydning av ord)
  - “Identitet” = “samme som forrige gang”.
- Autentisering forutsetter at en identitet er registrert
- Kan ikke autentiseres uten identitet
  - fordi det ikke er noen "forrige gang"
  - fordi identiteten først må opprettes og registreres
- Registrering kan skje på to måter:
  - pre-autentisering, ny identitet basert på tidligere identitet som f.eks. pass
  - opprettelse av ny entitet, f.eks. nyfødt baby, med tilhørende ny identitet

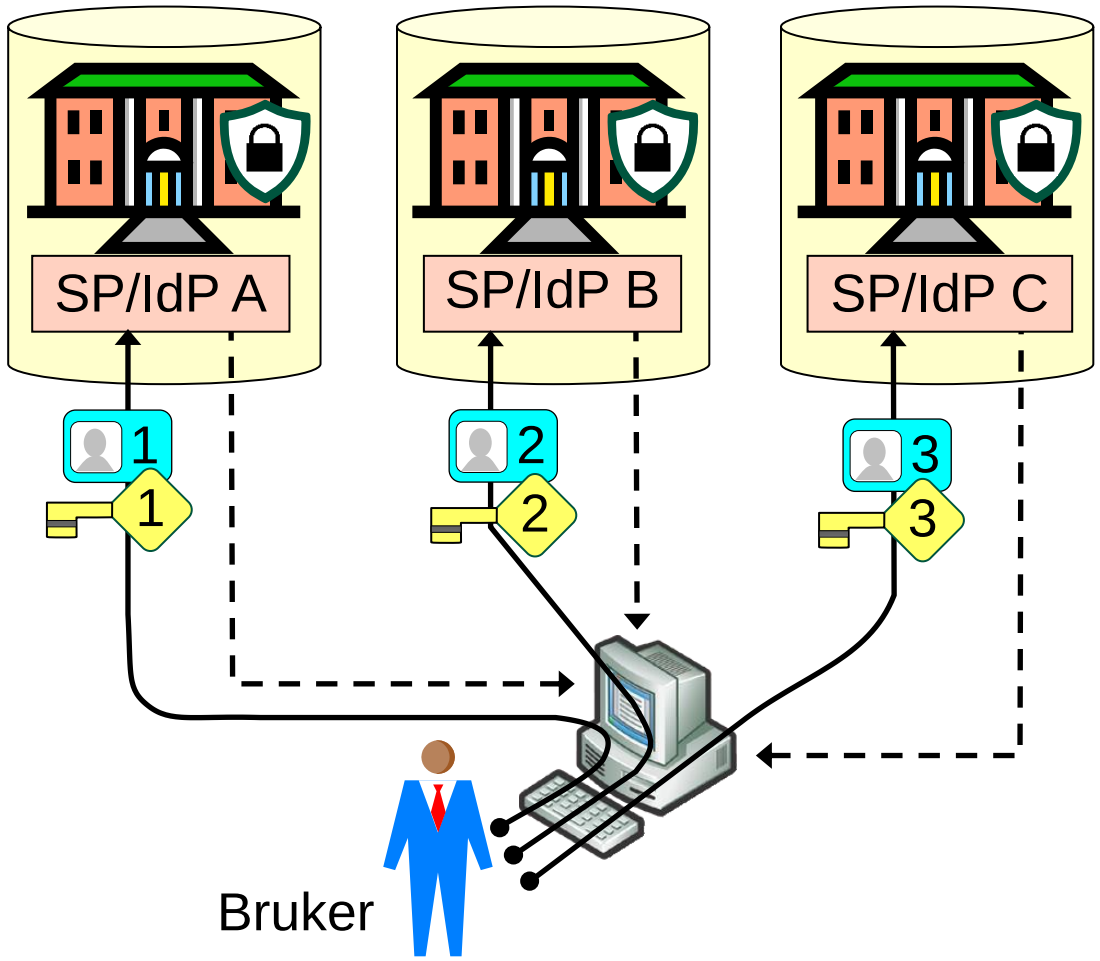
Identitetsdomener

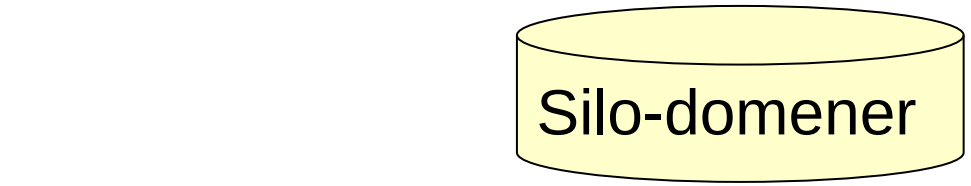
- Et identitetsdomene har et navnerom med unike navn
  - Samme bruker kan ha separate identiteter i ulike domener
  - Samme bruker har normal bare en identitet i et domene, men det er fullt mulig at samme bruker kan ha flere identiteter i et domene.



- Silodomene med én autoritet, f.eks. bedriftsnettverk
- Føderterte identitetsdomener
  - Identitetsdomenet kan brukes av mange forskjellige tjenestetilbydere
  - Krever samarbeid om identitetspolicy mellom tjenestetilbydere

Silo-identitetshåndtering

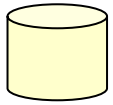


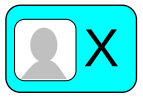


Forklaring:

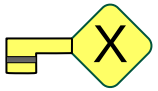

SP (tjenestetilbyder)


IdP (autentiseringstjener)


silo identitetsdomene

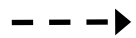


bruker-ID

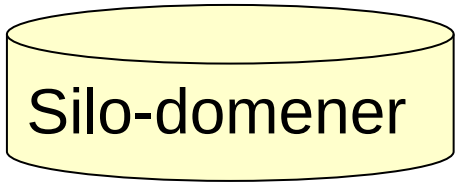


autentikator


login/forespørsel


tjeneste

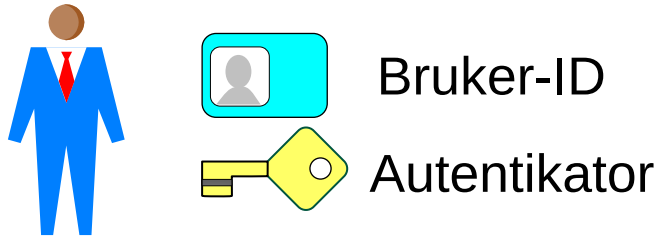
Silo-identitetshåndtering



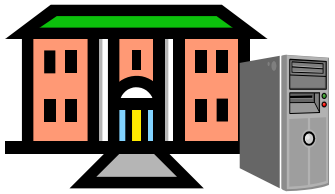
- SP (tjenestetilbyder) = IdP (autentiseringstjener):
  - SP styrer navnerommet og foretar autentisering
- Entydig unike identifikatorer tildelt hver bruker
- Fordeler
  - Enkel å sette opp, lave startkostnader
  - Potensielt godt grunnlag for sterkt personvern
- Ulemper
  - Identitetsoverlast for brukere, dårlig brukervennlighet, dårlig integrasjon av tjenester mellom tilbydere
  - Lav aksept av nye tjenester med separat ID og autentikator
  - Brukere må oppgi samme informasjon til mange tjenesteleverandører
  - For tjenesteleverandører: Barriere mot innsamling av brukerdata

Aktører i føderert identitetshåntering

- Bruker
  - Har bruker-ID og autentikator(er)
  - Ønsker å bruke tjenester fra ulike SP-er.



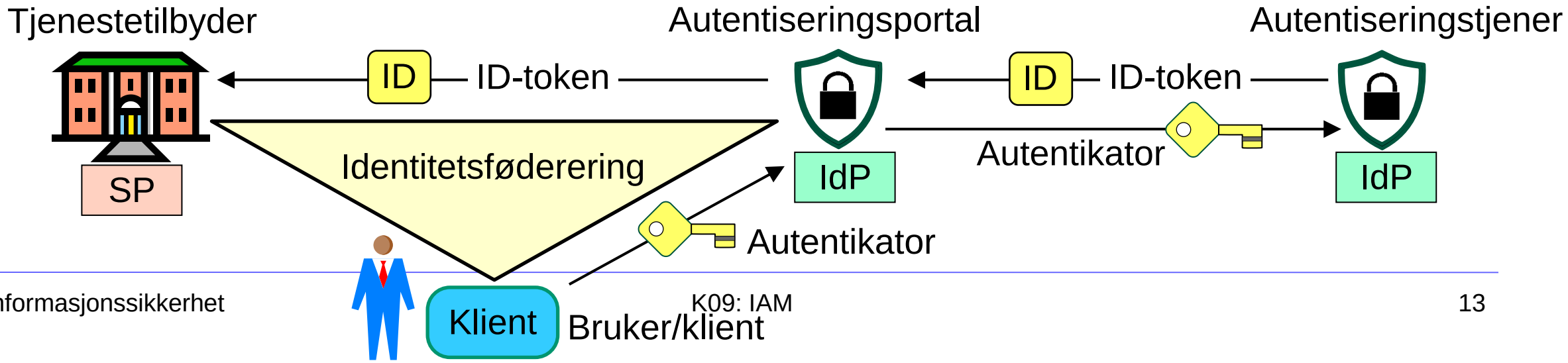
- Tjenestetilbyder (SP: Service Provider), også kalt Relying Party
  - Har register over bruker-ID-er
  - Har avtale med en eller flere IdP-er for brukerautentisering



- Autentiseringstjener (IdP: Identity Provider), kalles ofte eID-leverandør innen e-forvaltning
  - Har avtale med SP-er
  - Gir/selger brukerautentisering som tjeneste til SP-er

Protokoller / standarder for ID-føderering

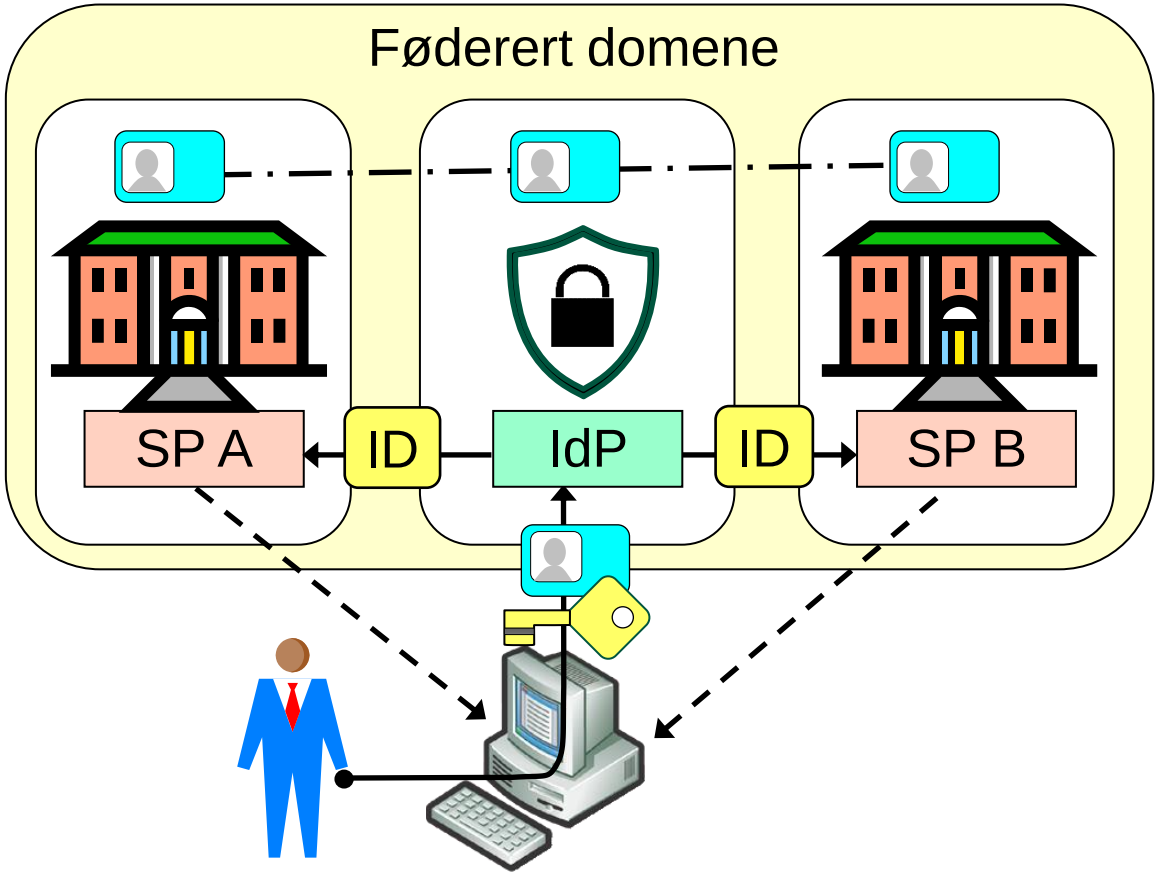
- Involverer flere entiteter
  - Bruker/nettleser, IdP, SP, og noen ganger en broker/autentiseringsportal (f.eks. ID-porten)
- IdP autentiserer bruker, genererer og sender digitalt signert ID-token til SP.
- SP mottar ID-token som bevis på at bruker er autentisert.
- Standarder:
  - OAuth (Open Authorization)
  - OIDC (OpenID Connect), som er basert på OAuth
  - SAML (Security Assertions Markup Language),
    - SAML var en tidligere utbredt standard for ID-føderering, men ordninger går over til OIDC.



ID-føderering – fordeler og ulemper

- Fordeler
  - bedre brukervennlighet
  - Lar SP-er fokusere på tjenester, slipper å håndtere autentikatorer
  - Lar IdP-er samle informasjon om bruksmønster for brukere
  - Skalerer godt innen en sektor, gir god kvalitet i autentisering
- Ulemper
  - Teknisk og juridisk kompleksitet
  - Tillitskrav mellom aktører
    - Hver aktør kan potensielt kompromittere sikkerheten
  - Problemer for personvern,
    - Massiv innsamling/utveksling av data mellom SP og IdP er en trussel mot personvernet
  - Begrenset skalerbarhet mellom ulike sektorer/domener,
    - Begrenset av politiske og økonomiske begrensninger
    - Et føderert domene kan bli en ny form for silo i forhold til andre domener

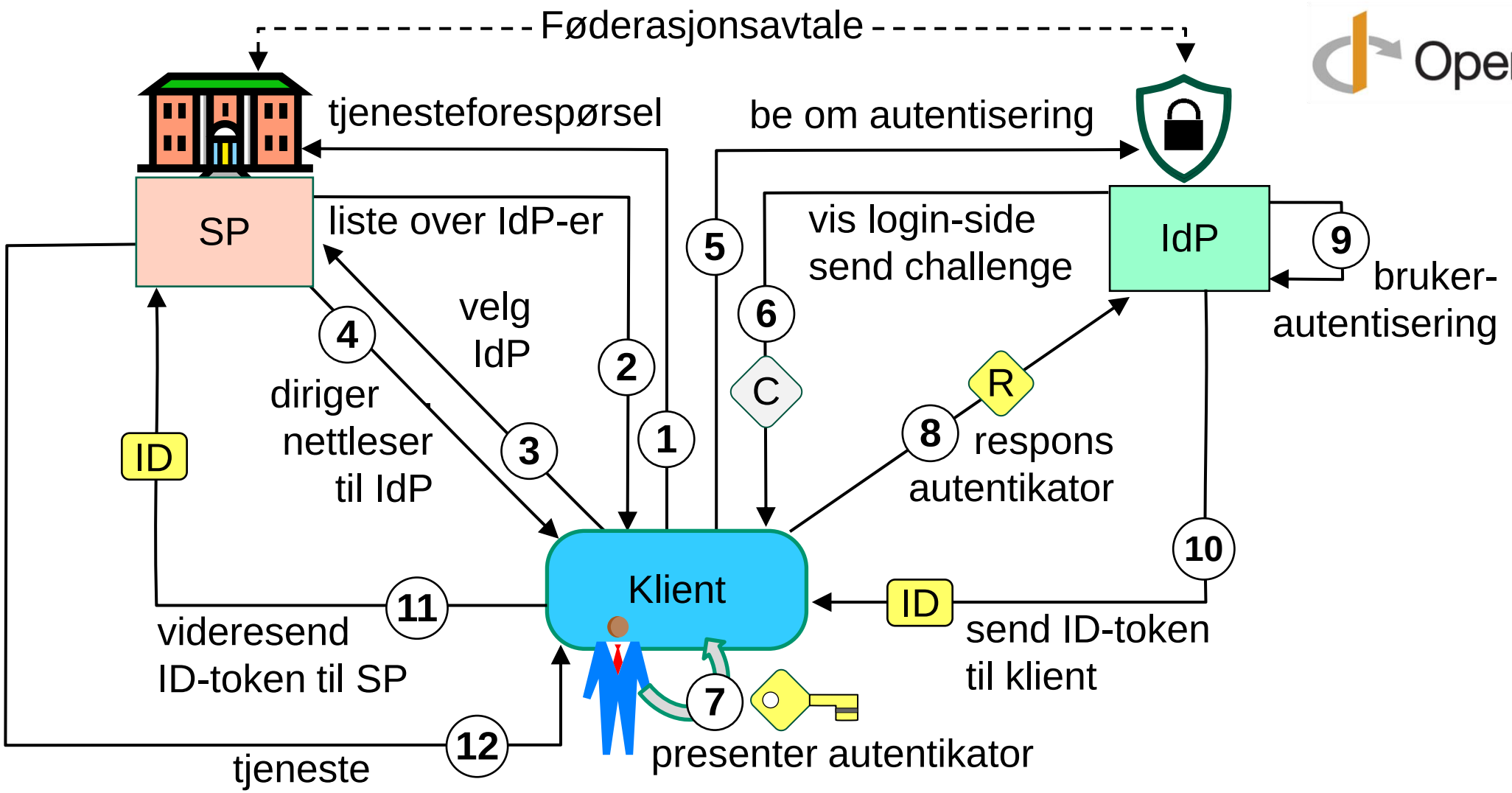
ID-føderering use-case



Forklaring:

- SP (tjenestetilbyder)
- IdP (autentiseringstjener)
- identitetsdomene
- bruker-ID
- autentikator
- ID-token/sikkerhetstoken
- login
- tjeneste
- føderert ID

OIDC føderert autentisering



OIDC

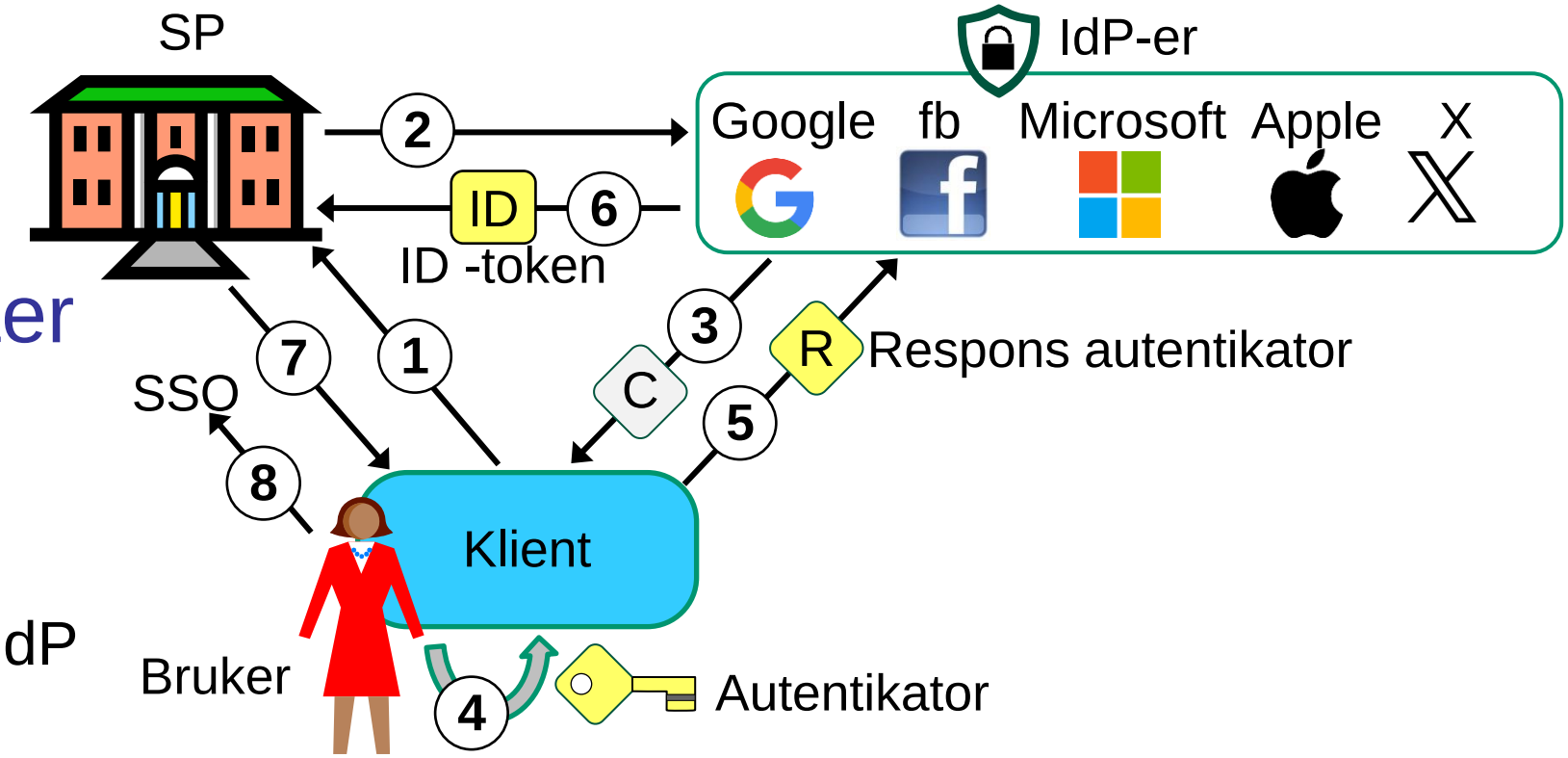
OAuth (Open Authorization)

- OIDC er basert på OAuth 2.0 spesifikasjonen
  - SP-er etablerer føderasjonsavtaler med IdP-er gjennom OAuth
  - f.eks. Airbnb (SP) med facebook (IdP)

- OIDC (OpenID Connect) brukes i

- F.eks. er IAM for norsk helsesektor basert på OIDC
  - Helsepersonell får brukeridentitet (HelseID) av arbeidsgiver
  - Forbindelse mellom personnummer og identiteter i OIDC eksisterer, men er beskyttet

Identitetsføderering og Single-Sign-On (SSO) med google, facebook, microsoft, apple og twitter



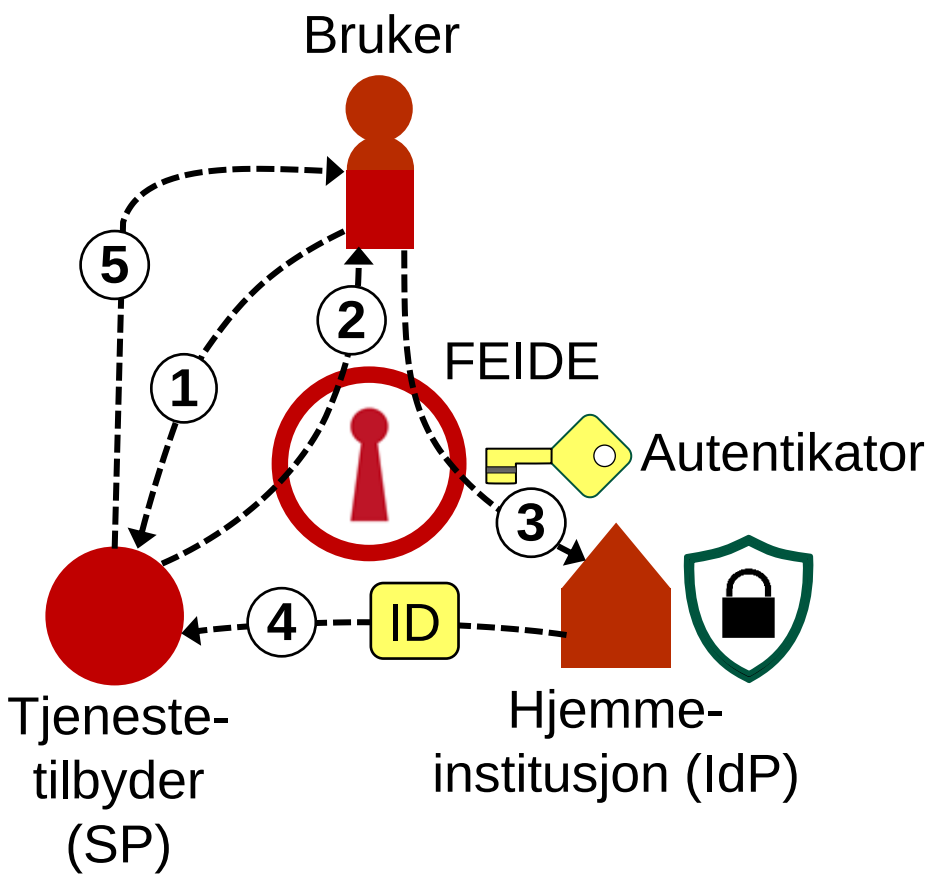
<u>Forenklet IODC-scenario</u>

1. Bruker forespør tjeneste
2. Rediriger nettleser til valgt IdP
3. Presenter login-side fra IdP
4. Bruker oppgir ID og autentikator(er)
5. Bruker-ID og autentikator sendes til IdP som autentiserer brukeren
6. ID-token sendes til SP (egentlig via nettleser)
7. SP gir tjeneste til bruker
8. Klienten har SSO (trenger ikke autentisere) til alle SP-er som benytter samme IdP

FEIDE (Felles Elektronisk Identitet)

- FEIDE er ID-føderasjon for den nasjonale utdanningssektoren.
- Brukere registreres med brukernavn og passord hos egen hjemmeorganisasjon (IdP)
- Brukere autentiserer seg til egen IdP via FEIDEs sentraliserte portal
- Tjenestetilbyder (SP) mottar sikkerhetsbillett og brukerattributter fra brukerens hjemme-institusjon (IdP)
- Andre tjenestetilbydere (SP) enn brukerens hjemme-institusjon (IdP) trenger ikke å motta brukerens passord/autentikator, de mottar bare sikkerhetsbillett og attributter som de trenger å for å kunne tilby tjenesten.

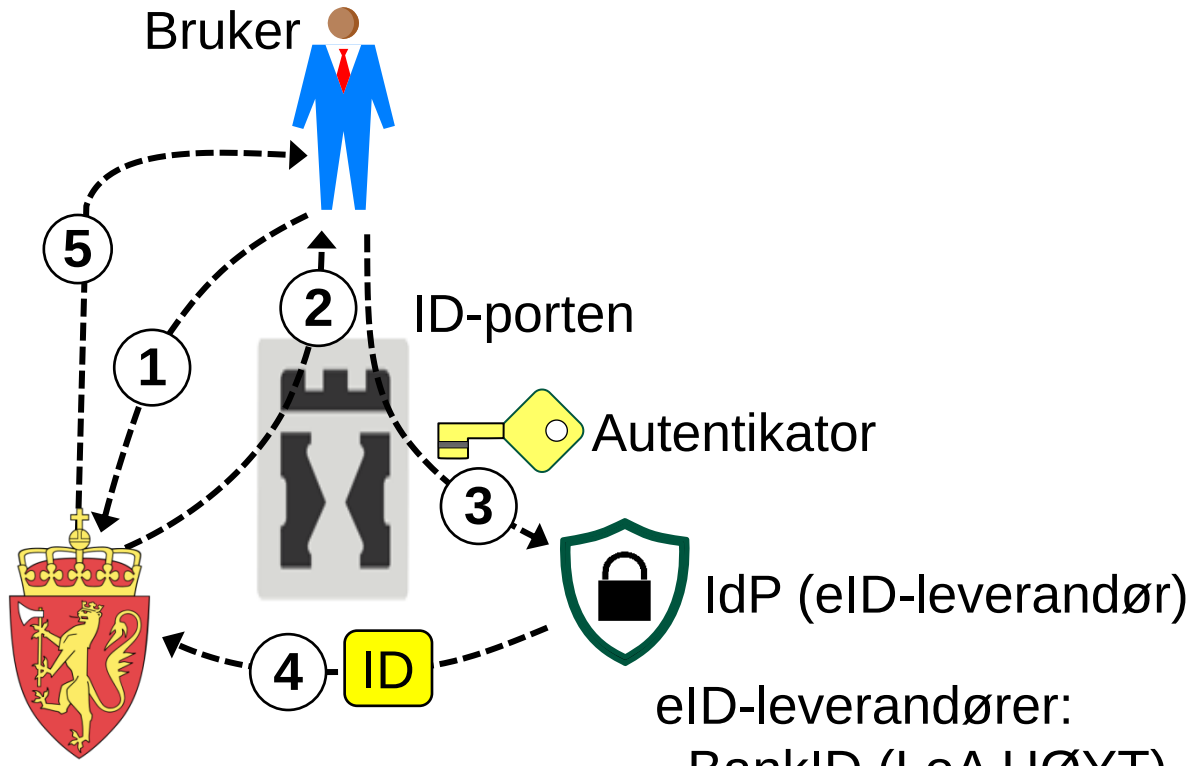
FEIDE Scenario



Forenklet FEIDE-scenario

1. Bruker ber om tilgang til tjenesten hos SP
2. Tjenestetilbyder ber brukeren velge hjemme-institusjon (IdP) for autentisering.
3. Bruker skriver inn navn og autentikator(er) i login-vindu fra hjemme-institusjon.
4. Hjemme-institusjon autentiserer, sender ID-token og brukerattributter til SP.
5. Tjenestetilbyder SP sjekker sikkerhetsbillett og brukerattributter, og gir tjenester i henhold til policy.

Scenario



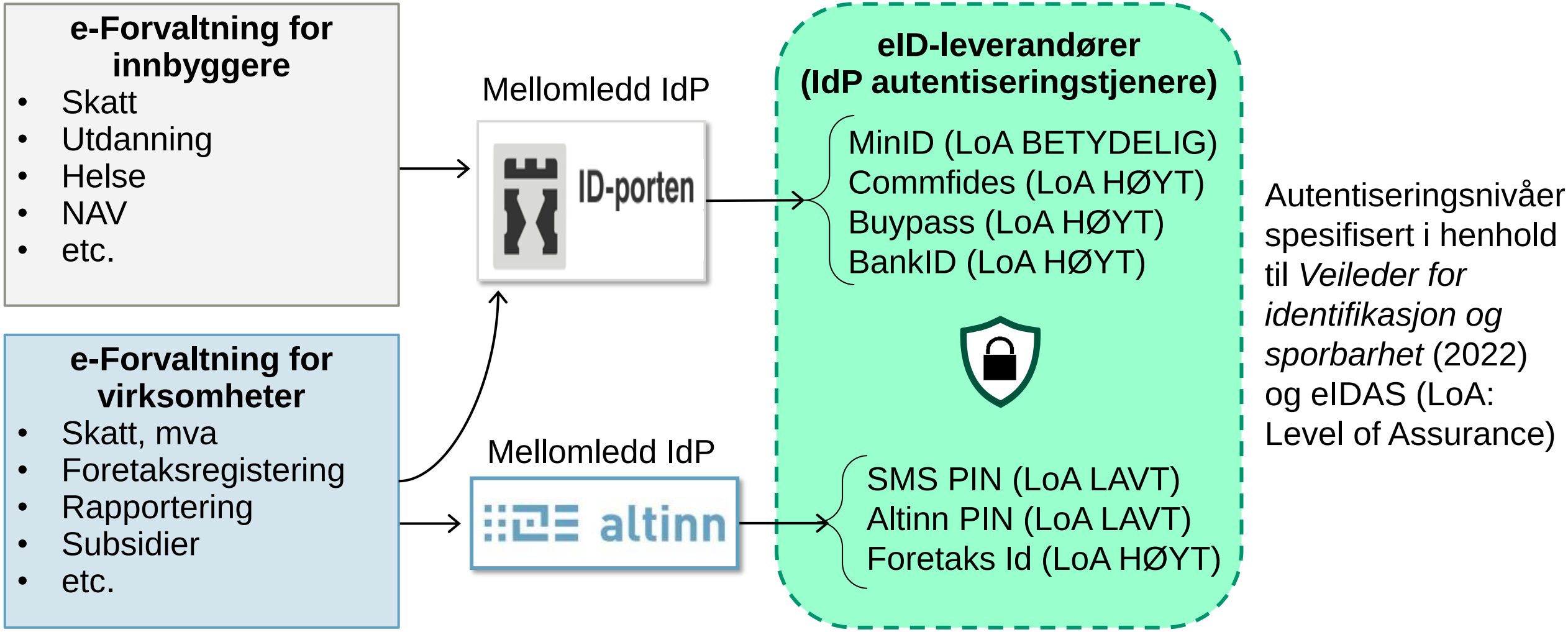
Offentlige e-forvantnings-tjenester (SP)

eID-leverandører:
- BankID (LoA HØYT)
- Commfides (LoA HØYT)
- Buypass (LoA HØYT)
- MinID (LoA BETYDELIG)

Forenklet scenario med ID-porten

1. Bruker ber om tjeneste
2. Tjenestetilbyder omdirigerer autentiseringsforespørsel til ID-porten, og viser ID-portens login-vindu til bruker.
3. Bruker velger autentiseringstjener (IdP), oppgir autentikator(er) (og person-nummer) i påloggingsvinduet, som sendes for validering til autentiseringstjeneren (IdP).
4. Autentiseringstjener (IdP) autentiserer bruker og sender ID-token og brukerattributter til SP.
5. Tjenestetilbyder (SP) sjekker sikkerhetsbillett og attributter, og leverer tjenester i henhold til policy.

Identitetsføderering i e-forvaltningen



Autentiseringsnivåer spesifisert i henhold til *Veileder for identifikasjon og sporbarhet* (2022) og eIDAS (LoA: Level of Assurance)

Identitetsføderering – kategorier

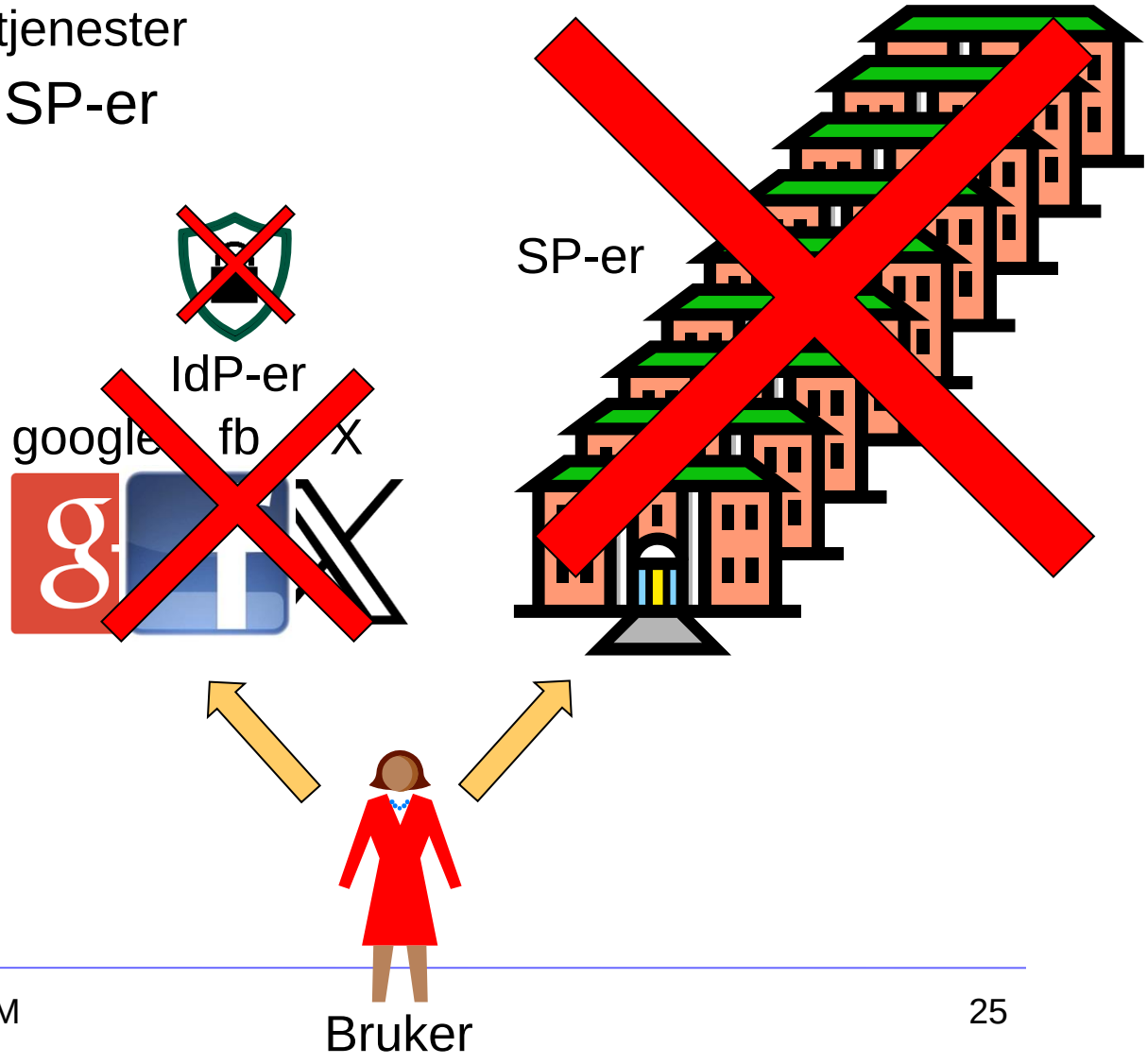
Kategori av føderering	Sentralisert navnerom	Distribuert navnerom
Sentralisert autentisering	Tysk eID  	 
Distribuert autentisering	 ID-porten  HelseID	Google Microsoft X  fb Apple  Europeisk eID

Føderert identitetshåndtering - eksempler

- Tysk eID er sentralisert
  - BSI både forvalter navnerommet og foretar autentisering
- Aadhaar (India) er sentralisert
  - Aadhaar både forvalter navnerommet og foretar autentisering
- FEIDE og Eduroam har distribuert navnerom, men sentralisert autentisering
  - ulike aktører forvalter hver sine navnerom
  - en enkelt bruker kan bare autentiseres av hjemme-institusjon, som dermed er sentralisert
- ID-porten, Altinn og HelseID har sentralisert navnerom og distribuert autentisering
  - identiteter er fødselsnummer/helse-ID, som forvaltes av staten
  - flere private leverandører av autentikatorer og autentisering, som dermed er distribuert
- ID-føderasjoner på internett har distribuert navnerom og distribuert autentisering
  - brukernes identiteter (som er vanlige e-postadresser) forvaltes distribuert
  - bruker kan velge ulike IdP-er for autentisering, som dermed er distribuert
- Secure European e-Identity
  - EU-initiativ under planlegging. Kommer til å ha distribuert navnerom og distribuert autentisering.

IdP-avhengighet

- Facebook falt ut i 6 timer den 4. oktober 2021
  - Millioner av brukere kunne ikke logge på online tjenester
- Antall IdP-er er svært lavt i forhold til antall SP-er
- IdP-avhengighet er et problem
- Behov for alternativ innlogging



Tilgangskontroll

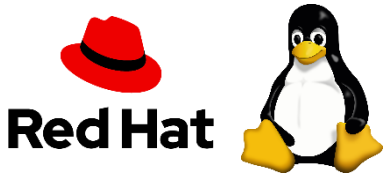
Modeller og metoder

Modeller for tilgangskontroll

- Hensikt
  - *Hvordan skal man definere hvilke subjekter (brukere) som skal ha tilgang til hvilke objekter (ressurser) med hvilken tilgangsmodus (lese, skrive, utføre)?*
- Tre klassiske modeller
  - Discretionary Access Control (DAC)
    - Navnebasert tilgangskontroll
  - Mandatory Access Control (MAC)
    - Merkebasert (labelbasert) tilgangskontroll
  - Role-Based Access Control (RBAC)
- Moderne og generell modell for tilgangskontroll:
  - Attribute-Based Access Control (ABAC)
    - Generalisering av DAC, MAC og RBAC

DAC – Discretionary Access Control
Navnebasert tilgangskontroll

- Tilgangsautorisering spesifiseres og håndheves basert på brukerenes (subjekt) navn og ressursenes (objekt) navn.
- Implementeres med ACL (Access Control Lists) som spesifiserer hvilke subjekter som er autorisert for tilgang til hvilke objekter med hvilke tilgangsmoduser
- Metadata for ACL kan lagres i subjektprofil eller objektprofil
- DAC er «discretionary» i den betydning at eieren av ressursen etter eget skjønn (discretion) kan bestemme hvem som er autorisert for tilgang, ved å spesifisere navn i en ACL.
- DAC er en klassisk modell som bl.a. brukes av:
  - Windows, Mac OS og Linux



objekt-navn

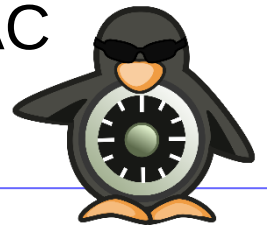
ACL

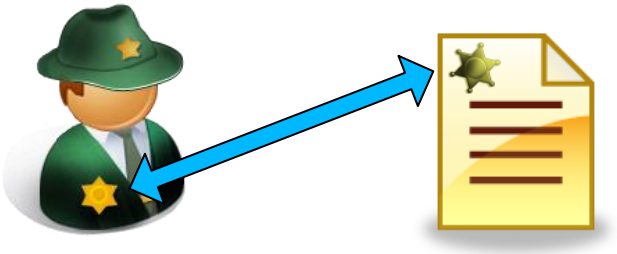
	HR	Sales
John	r, w	
Mary		r, w

subjekt-navn

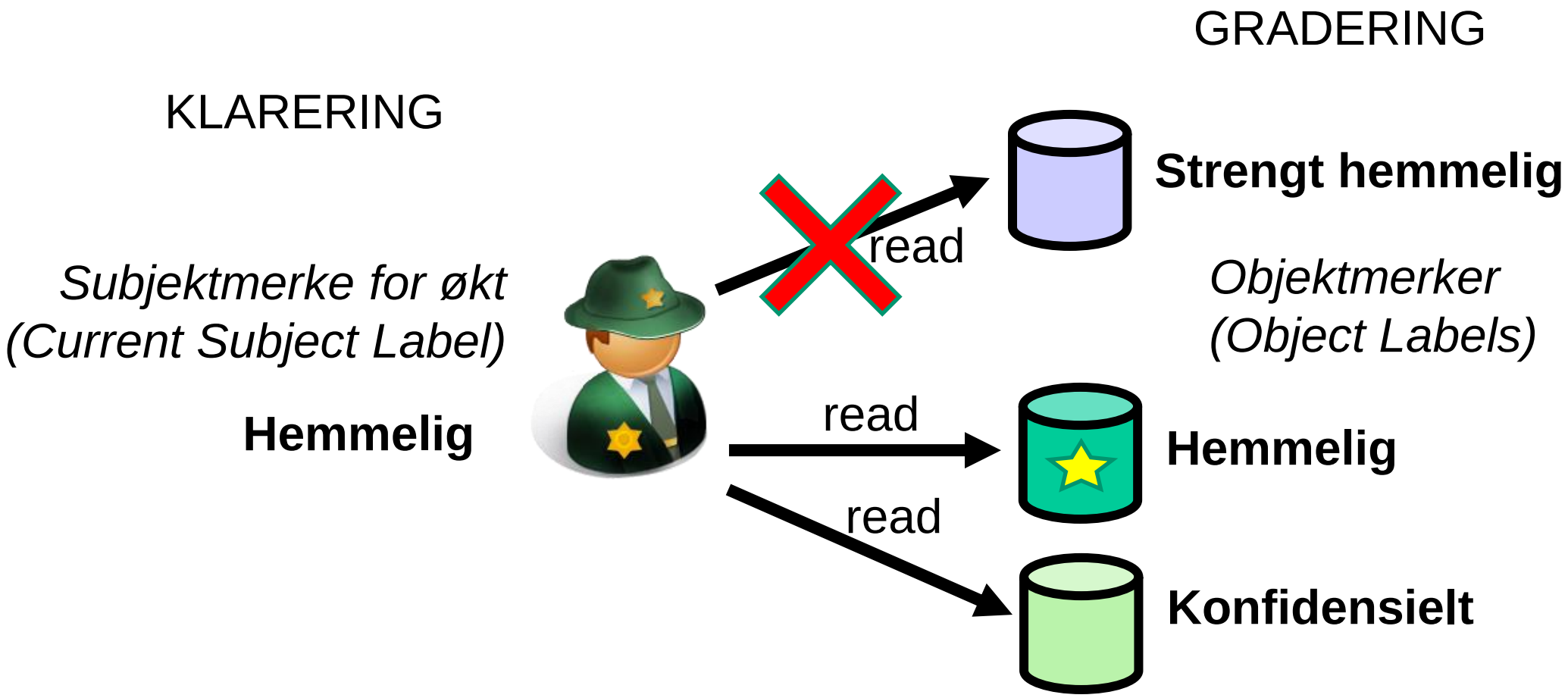
MAC – Mandatory Access Control
Merkebasert (labelbasert) tilgangskontroll

- Sikkerhetsmerking av subjekter og objekter
  - Sikkerhetsklarering for brukere (subjekter)
  - Klassifiseringsnivå for ressurser (objekter)
- Tilgangskontroll gjøres ved å sammenligne merker på bruker og ressurs
- Brukere har et klareringsnivå, men kan velge et lavere nivå for hver økt.
- MAC er «mandatory» i den forstand at tilgangsautorisasjon til ressurser er bestemt av en «mandatory» (obligatorisk) policy for sikkerhetsmerking, og **ikke** er bestemt av brukeren selv
- Hvor brukes MAC?
  - SE (Security Enhanced) Linux støtter MAC
  - Noen militære systemer bruker MAC

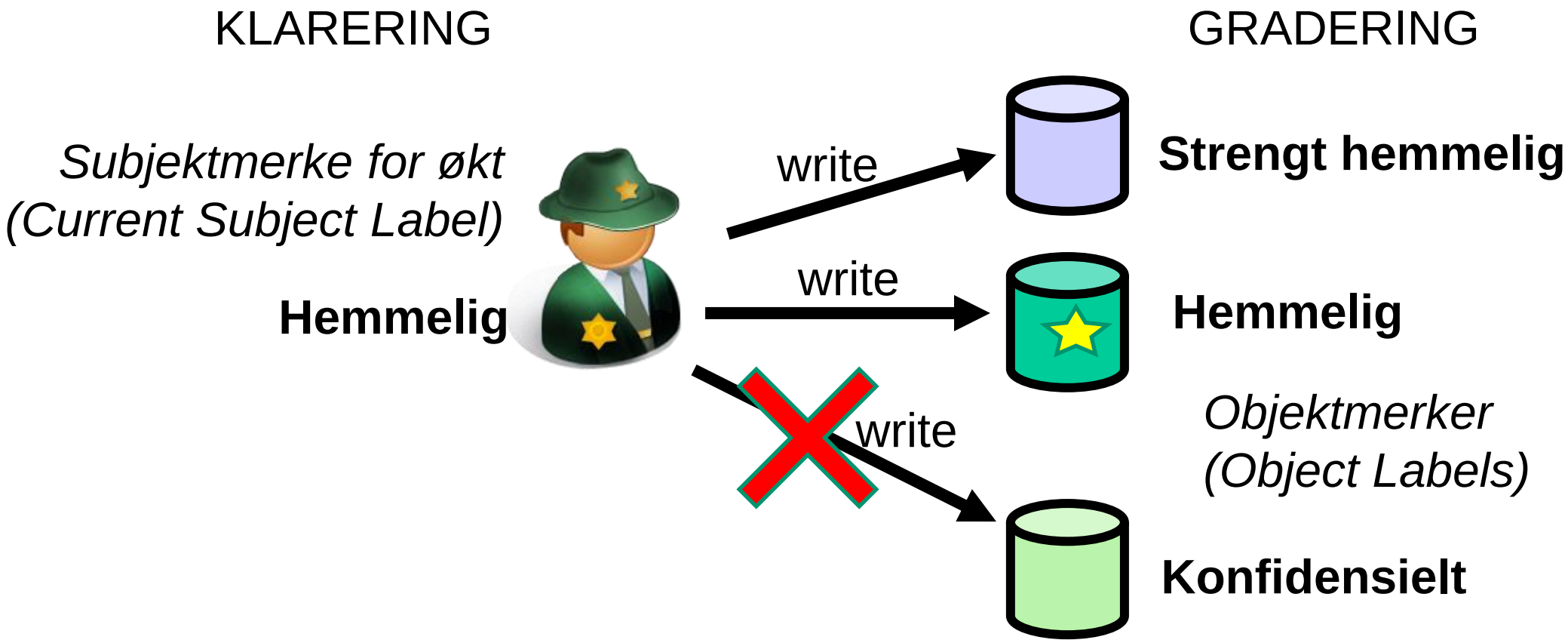




Bell-LaPadula (MAC model) No Read Up

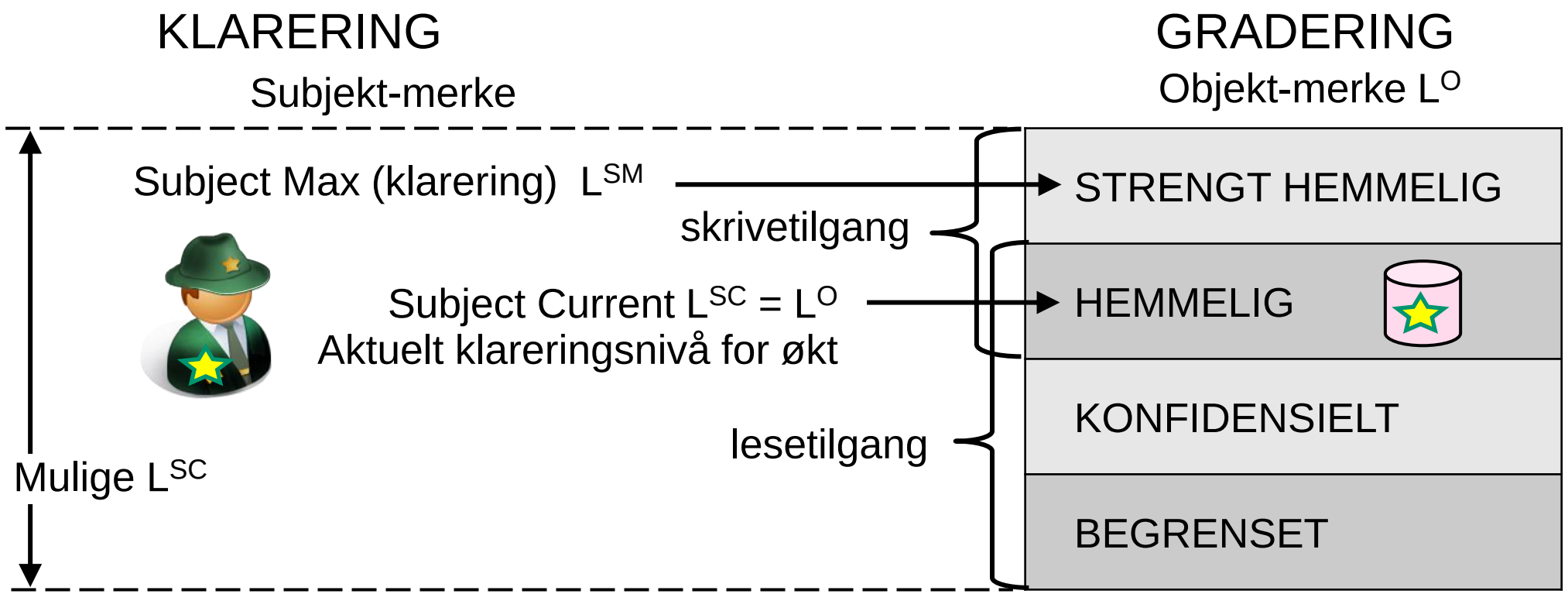


Bell-LaPadula (MAC model) No Write Down



Bell-LaPadula (MAC-modell) Klareringsnivå for økt

- For praktisk å kunne redigere dokumenter kan en bruker (subjekt) velge et aktuelt klareringsnivå for en spesifikk økt på samme eller lavere nivå enn sitt egentlige klareringsnivå. Brukeren kan alltid redigere dokumenter med samme gradering som sitt aktuelle klareringsnivå.

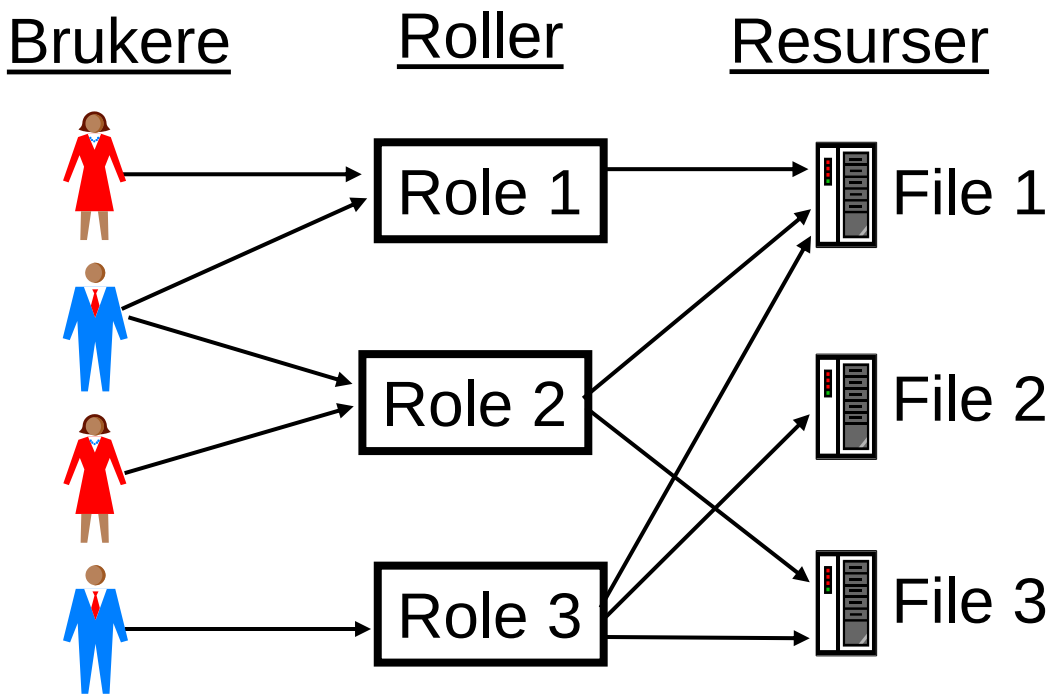


RBAC: Role Based Access Control

- En bruker har tilgang til ressurser basert på brukerens arbeidsrolle.
- Roller defineres ut fra jobbfunksjoner.
- En bruker kan bli autorisert to å velge forskjellige roller.
- Brukere har vanligvis kun en rolle om gangen.
- Hensikten med RBAC er å forenkle tildeling av autorisasjoner.
- Problemet med RBAC er rolle-eksplosjon, dvs. at det defineres svært mange forskjellige roller.

RBAC – Role Based Access Control
Rollebasert tilgangskontroll

Ansatte kommer og går ofte.
Roller er (kanskje) mer stabile.



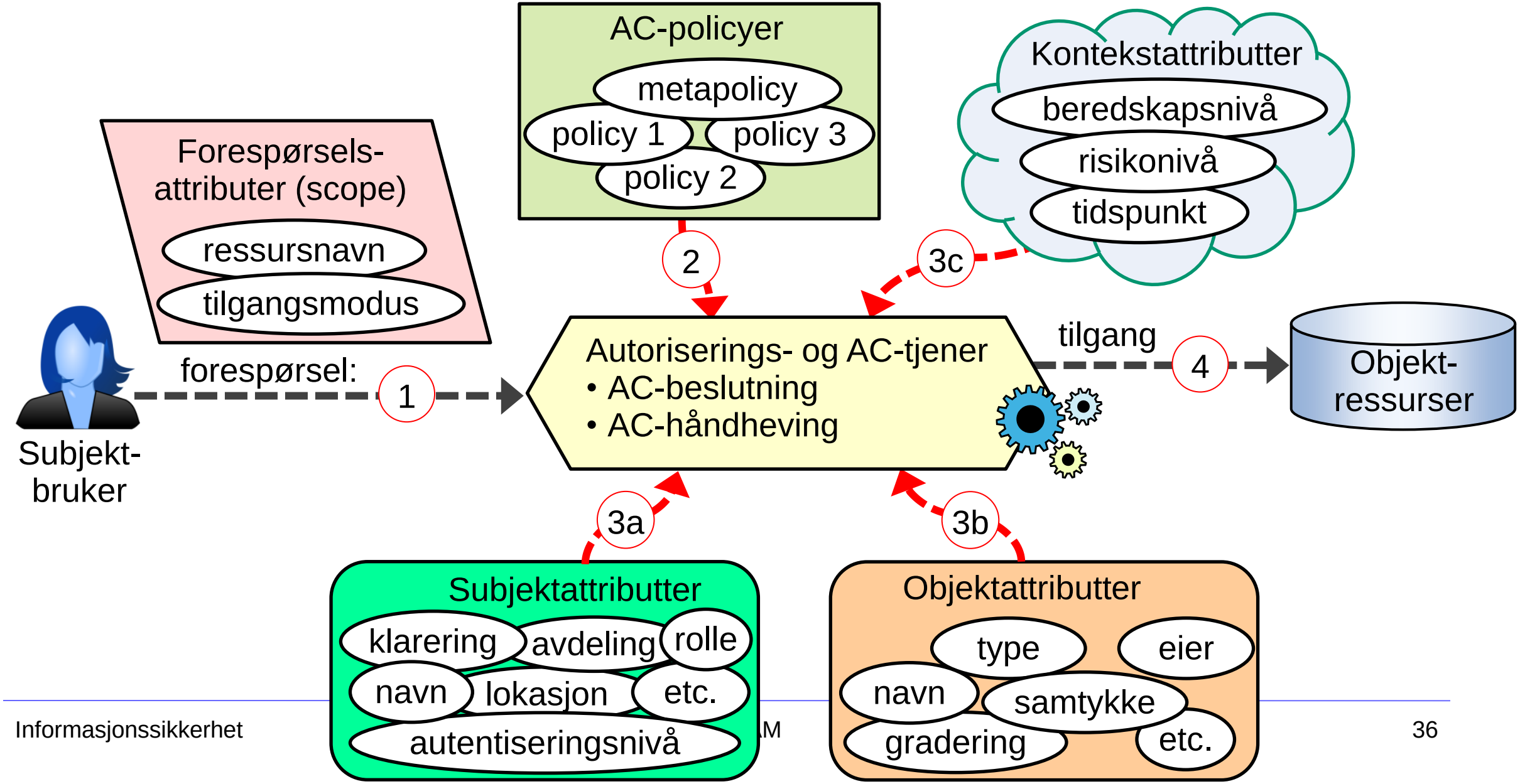
- RBAC kan konfigureres som DAC eller MAC

ABAC, XACML og JSON

ABAC = Attribute Based Access Control

- ABAC spesifiserer tilgangsautorisasjoner og håndhever tilgang gjennom policyer kombinert med attributter. Policyer kan bruke alle typer attributter (brukerattributter, ressursattributt, kontekstattributter osv.).
- ABAC-attributter og policyer kan uttrykkes på ulike måter
  - JSON (JavaScript Object Notation) Schema brukes i implementeringer basert på OAUTH og OIDC.
  - XACML er XML-basert (Extensible Markup Language) og brukes i implementeringer basert på SAML (Security Assertion Markup Language).
- Begge språkene kan brukes til å definerer hvordan systemet skal ta beslutning om tilgang i henhold til reglene definert i policyer.

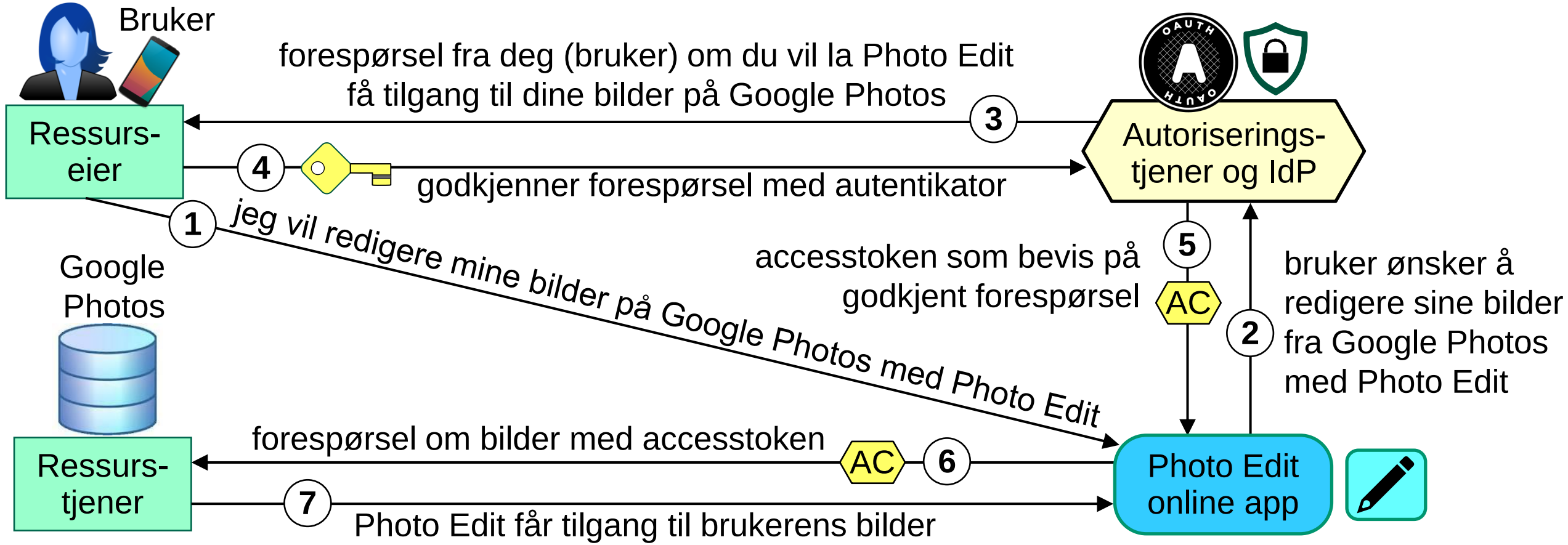
ABAC – Attribute Based Access Control



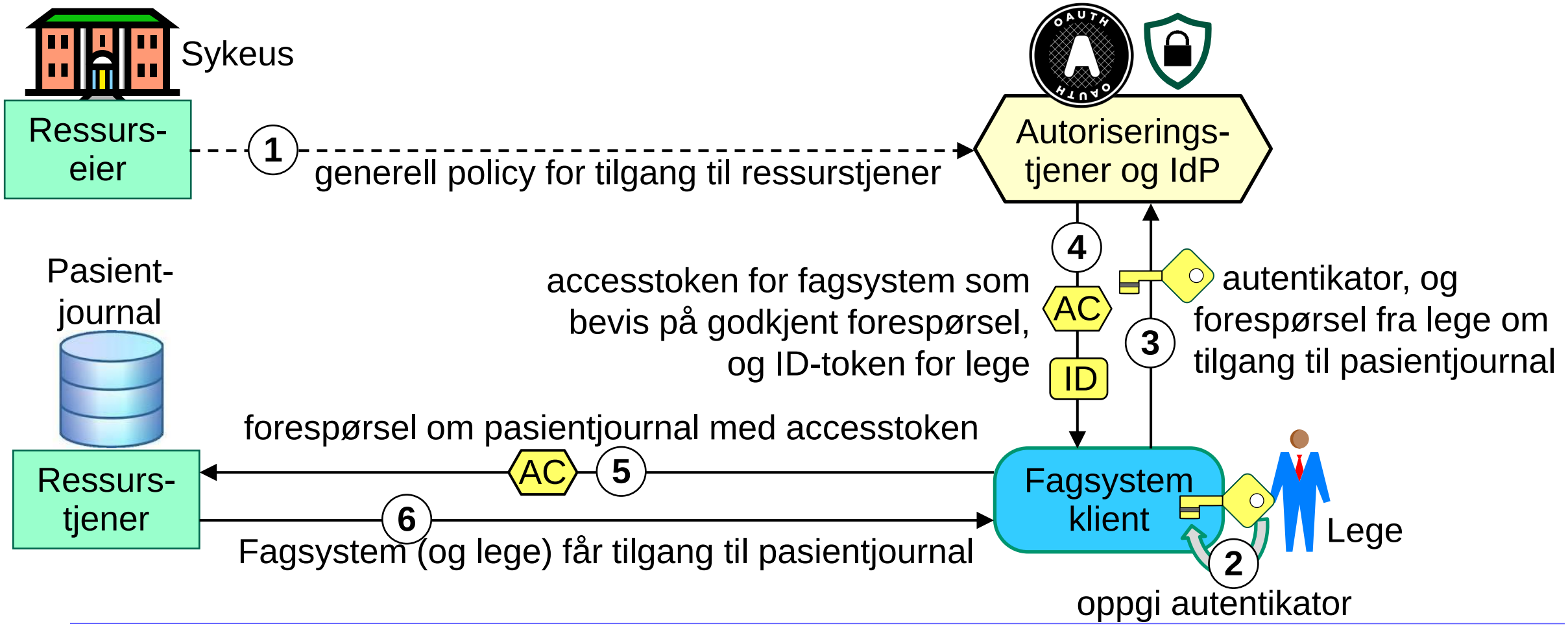
Distribuert tilgangskontroll med OAuth

- I moderne applikasjoner er ressurs-eier og resurs-tjener ofte separate fysiske, logiske og juridiske entiteter.
- Det er ofte ønskelig at tilgangskontroll (beslutning om tilgang) gjøres av ulike entiteter, avhengig av arkitektur.
- OAuth (Open Authorization) er en standard for å definere ulike arkitekturer for tilgangsautorisering og tilgangskontroll.
- OAuth omfatter, og brukes sammen med, OIDC (Open ID Connect).

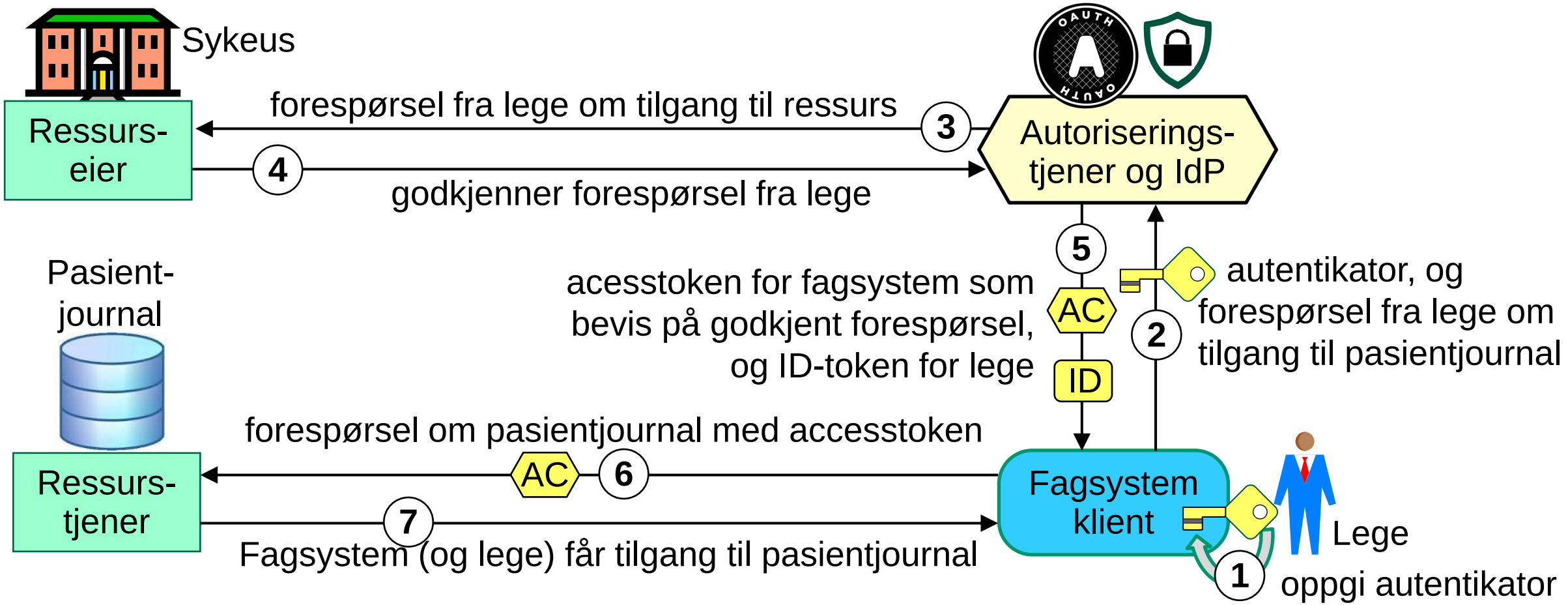
Distribuert tilgangskontroll på internet med OAuth



Tilgangsstyring for samhandling i forvaltning med generell tilgangspolicy



Tilgangsstyring for samhandling i forvaltning med spesifikk tilgangspolicy



Slutt på presentasjonen