UH Sak tilgangsstyring

Hvordan vil det fungere?

UH Sak samling - Scandic Solli

20. september 2023

Hvorfor tilgangsstyring?

Sikre at de riktige personene
får de riktige tilgangene
til riktig tid
av riktig grunn

Sak- og arkivsystemet inneholder både personsensitive og virksomhetssensitive data.

UH Sak

Premisser

- ❑ UH Sak leverer byggeklossene for tilgangsstyring
- ❑ Institusjonene må selv tegne ferdig tegningen – og bygge huset
- ❑ Institusjonene er selv ansvarlige for forsvarlig tilgangsstyring i løsningen

Valg av modell for tilgangstyring

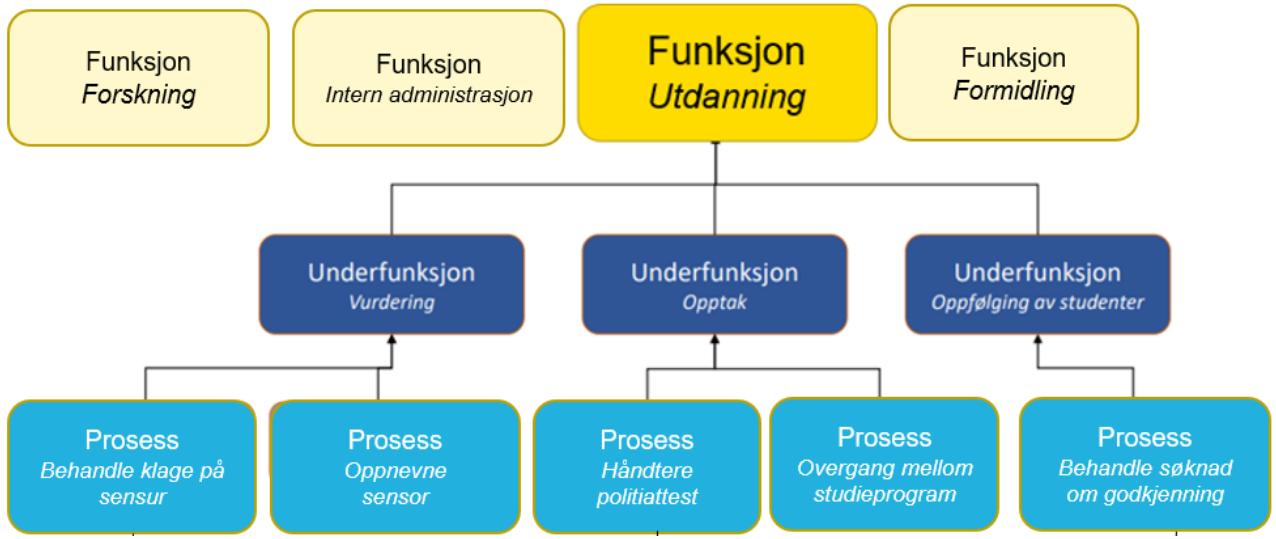
- **Først av alt:** Din institusjon må ta stilling til hvilken tilnærming dere har til rolle- og tilgangsstyring og lage en modell som reflekterer dette (granulering, arv, åpenhet)

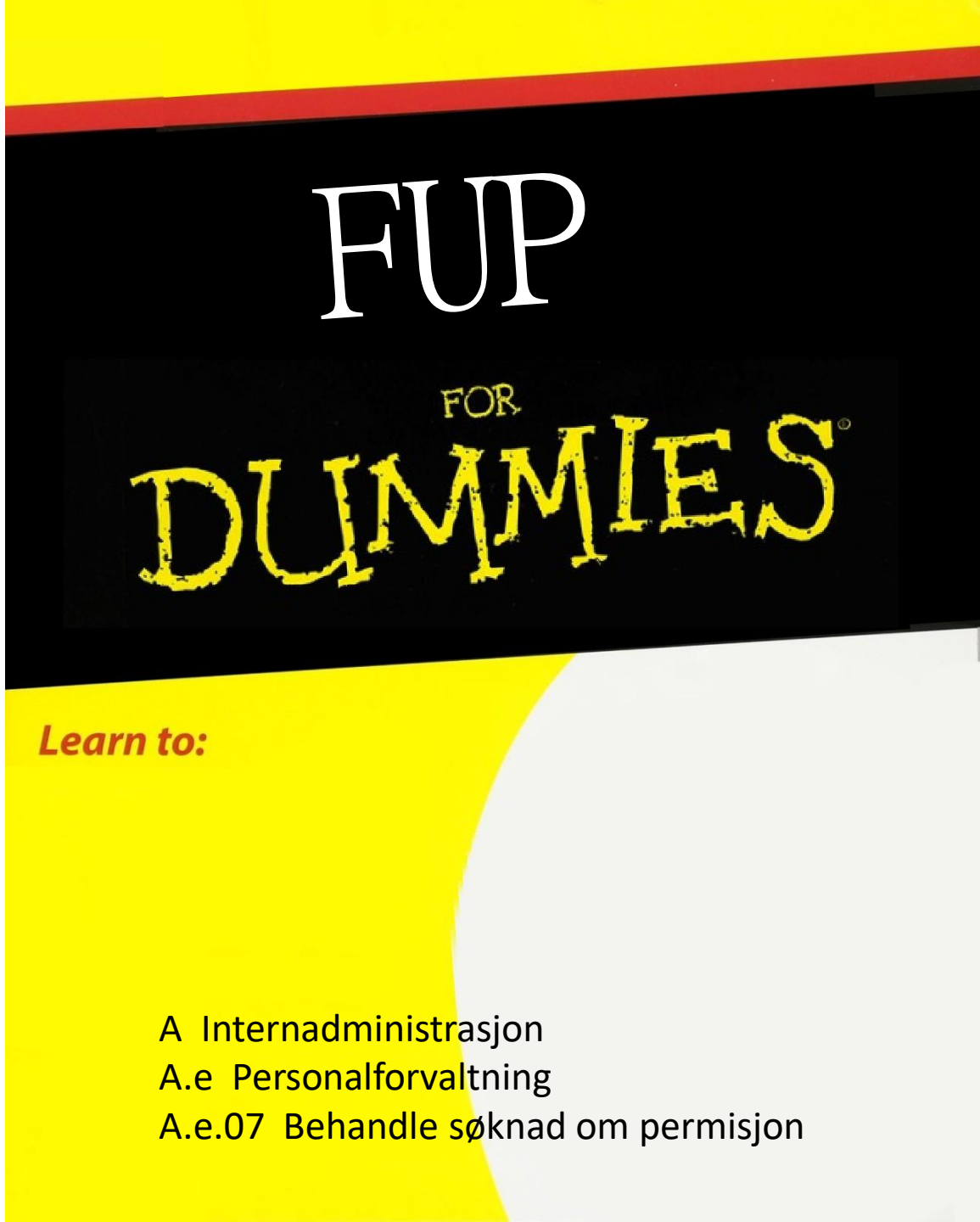
Mekanismer som må forstås for å velge modell:

- Funksjonsbasert tilgangsstyring
- Forretningsroller i fellestjenesten
- Arv
- ROLF-roller plassering styrer smal/bred tilgang
- Shit in – shit out – kvalitet i datakilder

UH Sak

Saksområder

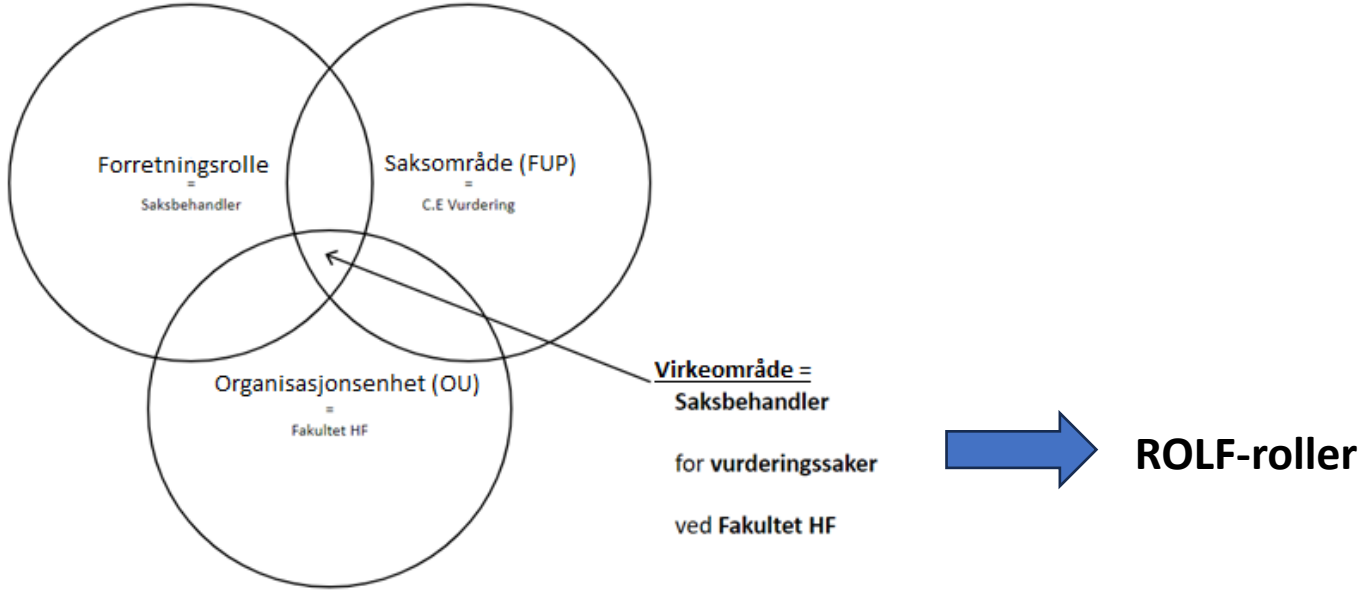




A Internadministrasjon
A.e Personalforvaltning
A.e.07 Behandle søknad om permisjon

Funksjonsbasert tilgangsstyring i UH Sak

- **Hvem** er brukeren i denne sammenhengen (opererer som **forretningsrolle** Leder, Saksbehandler, Godkjenner, Dokumentasjonsforvalter etc.). (alltid **1** per virkeområde).
- Hvilket **saksområde** skal brukeren arbeide innenfor (**1 eller flere** funksjon(er), underfunksjon(er), prosess(er))?
- **Hvor er oppgaven** plassert (hvilken organisasjonsenhet (**1 eller flere**))?



Forretningsroller i fellestjenesten

Forretningsrolle	Avgrensning		Bruksområde
	OU	FUP	
Leder	✓		Leder av organisasjonsenhet, kan hentes automatisk fra SAP/UBW. Godkjenne nye utvalg, kan fordele og omfordele saker, kan være eskaleringspunkt
Godkjenner	✓	✓	Person som kan godkjenne saker, kan også gis til personer uten formell lederrolle. Valgbar som godkjenner av dokumenter, beslutninger, kan opprette presedens.
Saksfordeler	✓		Person som varsles når det mangler tildelingsgruppe eller saksbehandler på sak. Kan fordele saker til tildelingsgrupper for videre «plukking», eller tildele direkte til person.
Saksbehandler	✓	✓	Rolle som kreves for å være valgbar som saksbehandler eller medsaksbehandler. Saksansvarlig for en sak i Documaster. Kan utnevne medsaksbehandler på en sak. Kan initiere gjestetilgang til eksterne bidragsytere.
Dokumentasjons-forvalter	F (arkiv) eller U (arkivdel)		Tilgang til alle saker og registreringer i SN og DM innenfor sine F eller U, uavhengig av om sak eller prosess er tilgangsbegrenset.

Forretningsroller – uten avgrensning på OU/FUP

Forretningsrolle	Bruksområde
Rolleadministrator	Administrere roller. Har oversikt over alle eksisterende ROLF-roller og hvem som er medlem. Kan opprette nye ROLF-roller, utpeke eier, moderatorer og medlemmer.
Prosessdesigner	Utvikle og teste prosesser i ServiceNow. Flytte prosesser mellom institusjonens ServiceNow-instanser. Konfigurere saksområder.
Malforvalter	Opprette og forvalte maler.
Redaktør	Opprette og vedlikeholde kunnskapsartikler.
Tilgangskontrollør	Rolle for tilgangskontroll og internrevisjon. Ser alle saker, kan administrere brukertabellen. Basert på Dokumentasjonsforvalter, uten avgrensning på saksområde.

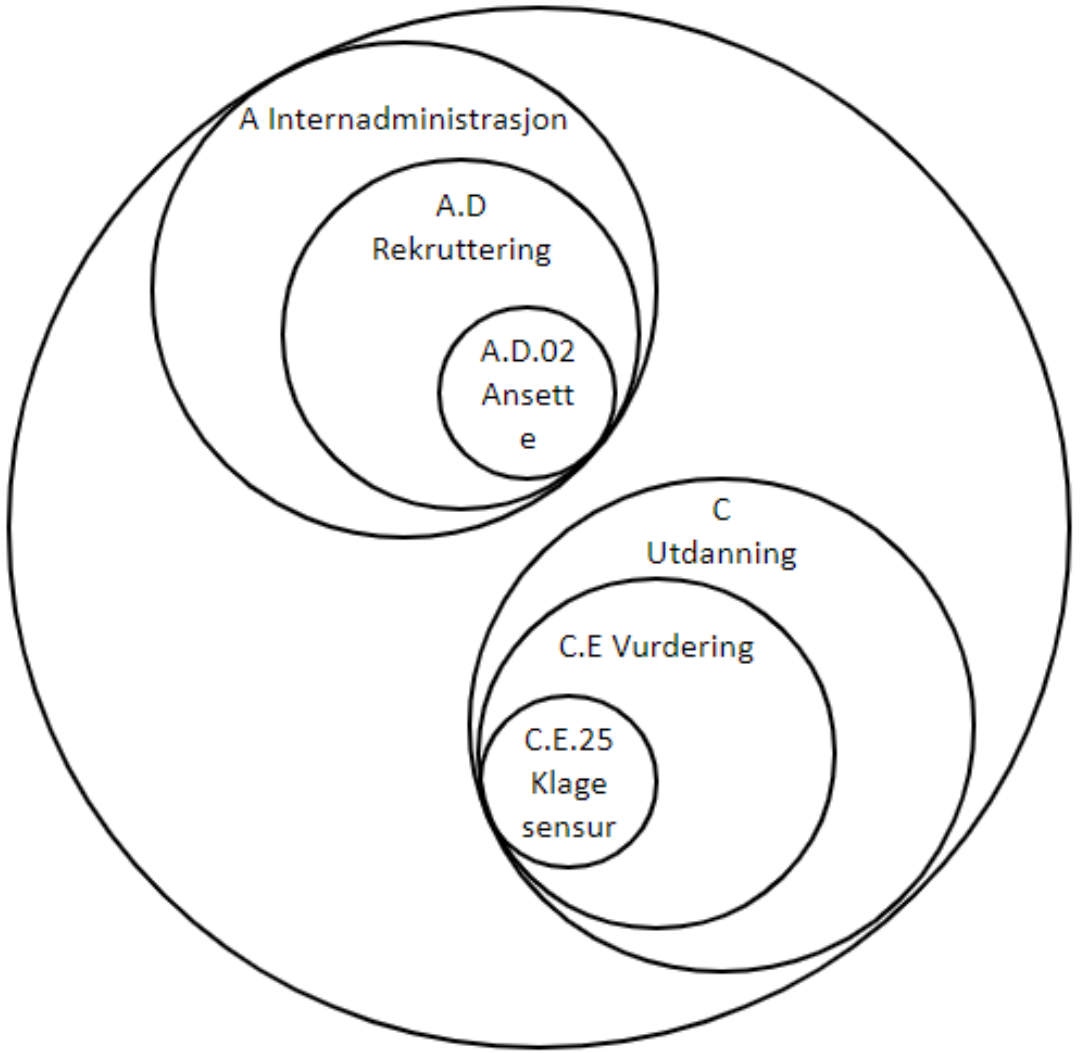
Arv

- Tilganger arves fra topp til bunn i to dimensjoner: **Saksområde- (FUP)** og **Organisasjonsenhet (OU)**
- God kontroll på arvereglene er avgjørende for å forstå konsekvenser av ulike oppsett for tilgangsstyring
- ROLF-rollenes plassering (FUP+OU) avgjør hvor bredt rollene favner (direkte eller gjennom arv)

Arv i Saksområde (FUP)-dimensjonen

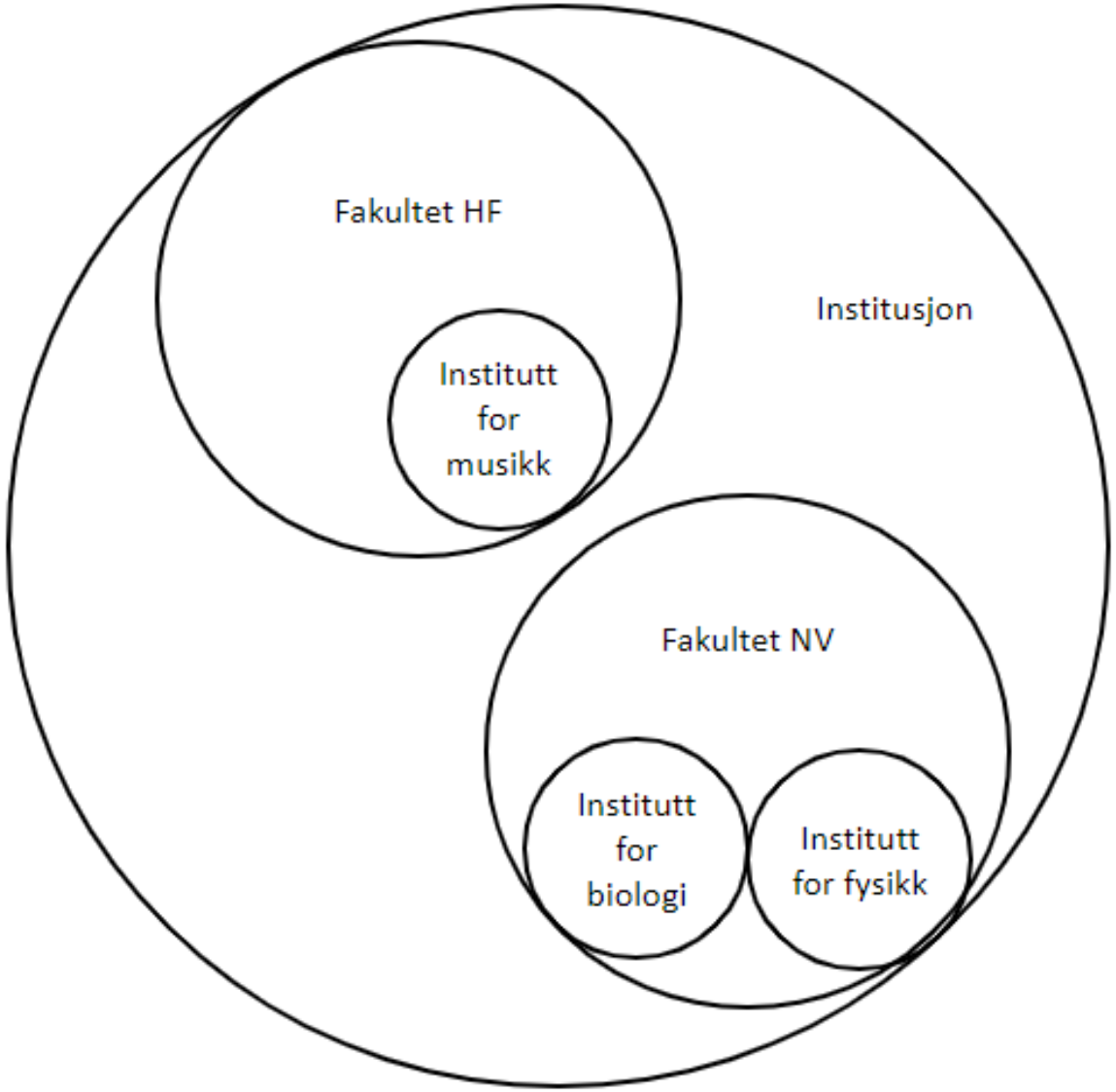
- Plassering av ROLF-rolle på **funksjons-** eller **underfunksjons**nivå gir arv til alle prosesser som ikke spesifikt har blitt unntatt fra arv

- OBS! Det kan unntas fra arv innenfor Saksområde (FUP)-dimensjonen ved å definere en prosess som **tilgangsbegrenset**



Arv i Organisasjonsenhet (OU)-dimensjonen

- Plassering av ROLF-rolle på **Institusjon**snivå gir arv til alle **fakulteter** og **institutter** og andre enheter
- Plassering av ROLF-rolle på et spesifikt **fakultet** gir arv til **institutter og andre enheter** som ligger under fakultetet
- Oppsett i OrgReg styrer hvilke enheter som gis tilgang basert på arv
- Forretningsrollene Leder og Saksfordeler har ikke arv på OU
- Det kan IKKE unntas fra arv på OU for forretningsrollene Saksbehandler og Godkjenner.



Tilgangsbegrensede prosesser

- Tilgangsbegrensede prosesser blir **unntatt fra arv** i Saksområde (FUP)-dimensjonen
- Dersom en hel prosess blir tilgangsbegrenset må det opprettes ROLF-roller tilknyttet prosessen.
  F.eks. *«Saksbehandler – C.b.22 – Håndtere politiattest - NTNU»*

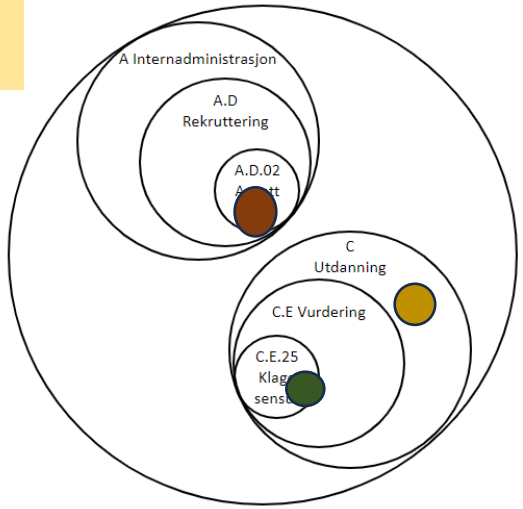
ROLF-rollenes plassering

Høyt i FUP og OU:
- Gir færre roller som må forvaltes
- Kan bety at mange personer får tilgang til for mye

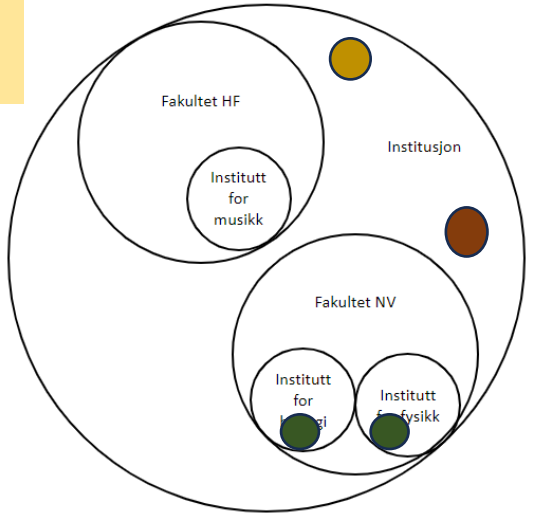
Lavt nivå i FUP og høyt i OU:
- Muliggjør sentralisert behandling og matrisebehandling av saker tilhørende en prosess
- Arv på OU kan gi tilgang til mer enn intendert

Lavt nivå i FUP og OU:
- Begrenser mulighet for at personer har bredere tilgang enn nødvendig
- Potensielt krevende kartleggingsprosess (opprettelse og evt. pre-populering)
- Kan gi økt informasjonssikkerhet i løsningen, men vil samtidig gi behov for mer vedlikehold

FUP

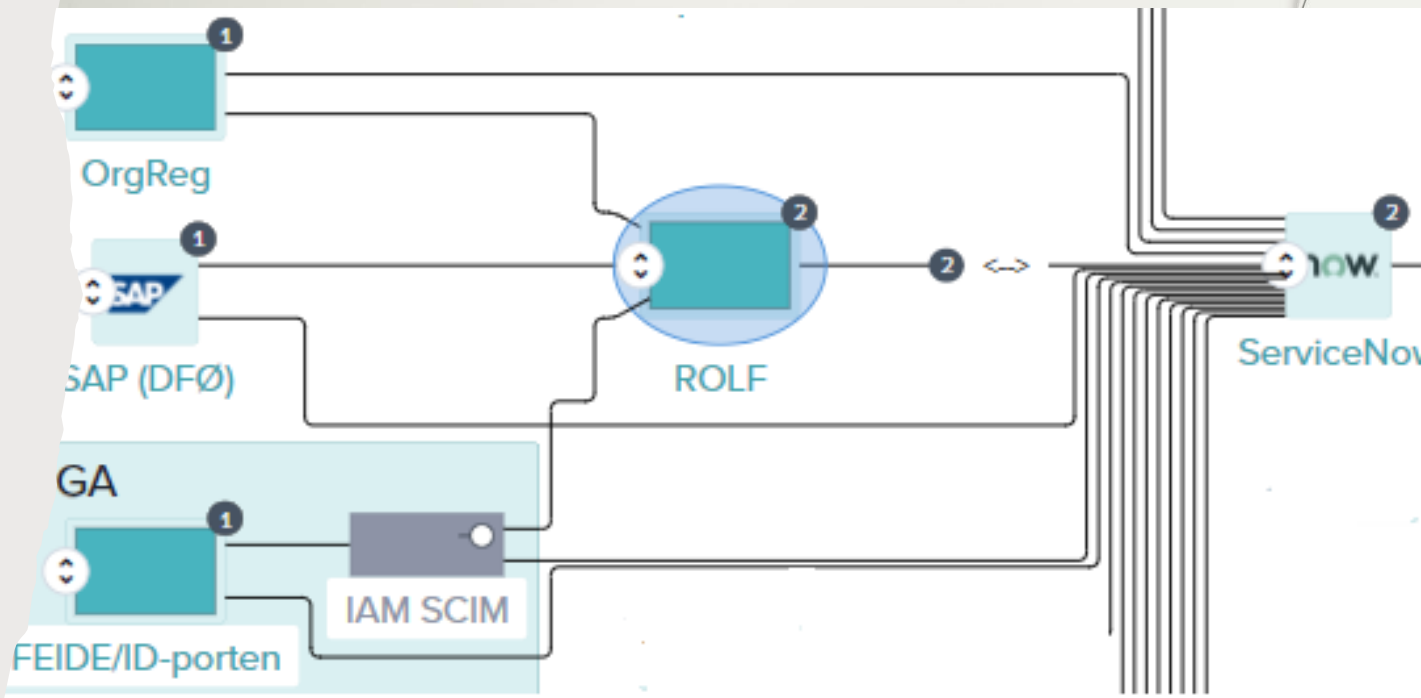


OU



Viktigheten av kvalitet på data i datakildene som benyttes

- ✓ OrgReg: **Organisasjonsenheter** blir tilgjengelig for saksbehandling og saksruting i UH Sak
- ✓ SAP(/UBW): **Ledere** for organisasjonsenhetene [vil kunne] hentes automatisk
- ✓ IAM SCIM: **Brukere** ved institusjonen hentes inn til ServiceNow



Du har valgt modell – hva må gjøres etter det?

- Vurdere hvilke prosesser som skal unntas fra arv (tilgangsbegrenses)
- Vurdere hvilke prosesser som skal ha fast forslag til skjermingshjemmel
- Definere RoLF-rollene: Pre-lastet med forretningsroller, saksområde(r), organisasjonsenhet(er)
- Vurdere i hvilken grad tilgjengelige datakilder skal benyttes for automatisk pre-populering (ledere, godkjennere etc.)
- Knytte brukeridentiteter til RoLF-roller

SKISSE

Hvordan knytte brukeridentiteter til ROLF-roller?

1) Utforme **modell** som skal gjelde for rolle- og tilgangsstyring ved institusjonen (granulering, arv, åpenhet)

2) Opprette initielle **ROLF-roller** basert på den valgte modellen

3) **Innlasting av ledere** som forretningsrolle Leder for ROLF-roller tilknyttet organisasjonsenhetene

4) Ledere gis tilgang til **tilgangsadministrasjon for ledere**, der leder får oversikt over personer tilknyttet organisasjonsenheten, og kan knytte personer mot virkeområder (ROLF-roller)

5) Sluttbrukere gis tilgang til **selvbetjeningsportal**, og kan velge/bestille tilgang til eventuelle virkeområder (ROLF-roller) som mangler

Pågående arbeid knyttet til tilgangsstyring

- Tilgangsstyring historiske baser/arkiv
- Tilgangsstyring direktearkivering fra fagsystemer
- Løsning for uthenting av ledere (og evt. andre) fra SAP(/UBW)
- Selvbetjeningsportal (for ledere og sluttbrukere)
- Opprettelse av gjest i GREG direkte fra ServiceNow