Sveriges Kommuner och Regioner

VÄGLEDNING

Vårt dnr:
Xx

2025-12-09

Kenneth Zetterberg

Vägledning för hantering av behörighetsattribut

Sammanfattning

Denna vägledning beskriver en gemensam och standardiserad struktur för hur kommuner kan hantera behörighetsattribut inom ramen för modern identitets- och behörighetshantering. Modellen bygger på en tydlig separation mellan identitet och behörighet och kombinerar rollbaserad (RBAC) och attributbaserad (ABAC) styrning i en hybrid som ger både stabilitet och flexibilitet.

Utgångspunkten är att varje individ beskrivs genom identitet, engagemang och roller, kompletterat med domänspecifika attribut där så krävs. Roller baseras på AID-systemet, vilket ger en nationellt harmoniserad rollstruktur och minskar behovet av lokala definitioner. Engagemanget – exempelvis anställd, förtroendevald eller elev – fungerar som ramen där roller och behörigheter knyts samman.

Modellen följer Ena:s nationella domänstruktur och gör det möjligt för kommuner att återanvända etablerade attributlistor, i denna version med fokus på Health-domänen. Samtidigt minskar den beroendet av personnummer, genom att rekommendera organisationsutfärdade identiteter och pseudonyma identifierare som teknisk grund för IAM.

Vägledningen ger också rekommendationer för hur kommuner kan inventera sina attribut, införa AID-roller, modellera engagemang och förbereda sig för framtida domäner. Arbetet med att skapa en nationell namespace-lösning pågår, med målsättning att publicera och förvalta attribut genom Ena.

Tillsammans erbjuder modellen en robust, interoperabel och framtidssäker grund för kommunernas IAM-arbete och skapar förutsättningar för säkrare åtkomst, effektivare förvaltning och enklare samverkan med andra aktörer.

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315

Innehåll

1 Inledning 4
1.1 Avgränsningar 5
2 Bakgrund och kontext 5
2.1 Varför en gemensam struktur för behörighetsattribut 5
2.2 Fragmentering i kommunal sektor idag 6
2.3 Nationellt samordnad modell 6
2.4 Koppling till Ena och nationella domäner 7
2.5 En hybridmodell: Kombinationen av RBAC och ABAC 7
2.5.1 RBAC – Rollbaserad styrning som stabil grund 8
2.5.2 ABAC – Attribut för specificera behörigheter 8
2.5.3 Hybridmodellen i praktiken 8
2.5.4 Varför hybridmodellen är nödvändig i kommunal sektor 9
3 Grundläggande begrepp 9
3.1 Identitetsattribut vs behörighetsattribut 9
3.2 Vad är en roll? 10
3.3 Vad är ett engagemang? 10
3.4 Vad är en domän? 11
3.5 Objekt: Människa vs maskin 11
3.6 Översikt – hur allt hänger ihop 11
4 Övergripande arkitektur för behörighetsattribut 12
4.1 Den nationella vertikala strukturen (Ena-domänerna) 12
4.2 Den kommunala horisontella strukturen (engagemang & roller) 13
4.3 Matrisen: där vertikalt och horisontellt möts 14
4.4 Illustration av tvådimensionell modell 15
5 Grundstruktur för behörighetsattribut i en kommun 16
5.1 Indelningen Human vs Machine 16
5.2 Personattribut (globala attribut) 16
5.3 Engagemang (anställd, förtroendevald, elev, konsult) 17
5.4 Engagemangsspecifika attribut 18
5.5 AID-baserade roller 18

5.6 Rekommenderad modell: 0..n roller per engagemang 19
5.7 Domänspecifika attribut (exempel: Health) 19
5.8 Kommunspecifika attribut 20
6 Domän: Health – referensmodell 20
7 Attribut och identitet utan personnummer 21
7.1 Varför undvika personnummer i attribut 21
7.2 Organisationsutfärdade identiteter 22
7.3 orgAffiliation som unik identifierare 22
7.4 GUID-baserade interna ID:n 23
7.5 Rekommenderad policy för användning av personnummer 23
8 Namespace och publiceringsmodell 24
8.1 Varför attribut behöver namnrymder 24
8.2 Tre alternativ: IANA, egen domän, Ena 24
8.3 Pågående arbete: publicering via Ena 26
9 Implementationsrekommendationer för kommuner 26
9.1 Hur börja: attributinventering 26
9.2 Hur modellera engagemang 27
9.3 Hur införa AID-baserade roller 27
9.4 Hur ordna maskinidentiteter 28
10 Bilagor 28

1 Inledning

Kommuner och regioner är i snabb takt på väg mot en mer sammanhållen digital infrastruktur där identitet, åtkomst och behörighet behöver hanteras på ett enhetligt sätt. I dag varierar arbetssätten kraftigt mellan olika kommuner, vilket leder till onödig komplexitet, höga förvaltningskostnader och svårigheter att uppnå säker och spårbar åtkomst till information. Samtidigt växer de nationella och europeiska kraven på interoperabilitet, exempelvis genom Diggs arbete med Ena – Sveriges digitala infrastruktur – och det kommande europeiska ramverket kring EUDI-wallet.

Det här dokumentet är en rekommendation från SKR till kommuner (och i relevanta delar även regioner) om hur behörighetsattribut bör struktureras och användas i IAM-lösningar. Syftet är att ge tekniskt förankrad vägledning som kan ligga till grund för kravställning, lokal implementation och förvaltning av roller och behörigheter.

Det arbete som ligger till grund för denna struktur och denna rekommendation har haft ett tydligt fokus: att ta fram en gemensam och standardiserad modell för de behörighetsattribut som behövs inom socialtjänsten. Dokumentet gör därför inte anspråk på att omfatta alla attribut som kan förekomma i kommunal verksamhet. I många andra verksamhetsområden pågår utveckling inom Ena eller lokalt i kommunerna, och dessa attribut kommer med tiden att behöva kompletteras och integreras i samma modell.

Dokumentet beskriver den föreslagna attributstrukturen utifrån tre centrala utgångspunkter:

- En gemensam modell för objekt och engagemang: hur en kommun skiljer mellan människa och maskin, och hur olika typer av engagemang – som anställd, förtroendevald, konsult eller elev – representeras på ett enhetligt sätt.
- Roller baserade på AID-systemet: hur kommunernas befintliga yrkeskoder och ansvarsnivåer kan användas som grund för roll- och behörighetsstyrning och därmed minska behovet av lokalt definierade roller.
- Domänspecifika behörighetsattribut: hur kommunsektorn kan använda de attribut som tas fram inom Ena:s nationella domäner, med särskilt fokus på Health-domänen, och hur dessa integreras i kommunernas egna IAM-modeller.

En del i rekommendationen är att minska beroendet av personnummer som teknisk identifierare. Dokumentet beskriver därför hur kommuner kan använda organisationsutfärdade identiteter, pseudonyma identifierare och alternativa attribut utan att tappa spårbarhet eller säkerhet.

Rekommendationen riktar sig främst till IAM-arkitekter, katalogförvaltare, tekniska specialister, leverantörer och andra som ansvarar för identitets- och behörighetshantering i kommuner. Texten kan även fungera som stöd för regionala aktörer som behöver förstå hur kommunerna strukturerar sina attribut, exempelvis i gränssnitt mot socialtjänst, hemsjukvård eller elevhälsa.

Dokumentet är en del av arbetet inom Handslaget – Identitet och behörighet, SKR:s initiativ för att stärka kommunernas förmåga att möta nationella krav och skapa mer enhetliga förutsättningar för digital samverkan.

Dokumentet avses förvaltas och uppdateras på årsbasis.

1.1 Avgränsningar

Denna vägledning beskriver en struktur för behörighetsattribut med fokus på kommunal verksamhet. Arbetet har i denna version avgränsats till de behov som finns inom socialtjänstens område, där attributmodellen har utvecklats och testats. Andra verksamhetsområden inom kommunen, liksom behörighetsattribut för maskinella identiteter och systemtjänster, omfattas därför inte av denna version.

När fler domäner inom Ena utvecklas och när kommunerna tar fram behov i andra delar av sin verksamhet kommer vägledningen att kunna kompletteras och utökas i kommande versioner.

2 Bakgrund och kontext

2.1 Varför en gemensam struktur för behörighetsattribut

Kommuner använder i dag ett stort antal digitala system med egna behörighetslösningar med inbyggda definitioner av roller. När varje system lever sitt eget liv uppstår snabbt en komplex och svårförvaltad miljö där:

- samma person får olika roller i olika system,
- attribut saknar enhetliga namn och betydelse,
- behörigheter blir oöverskådliga eller duplicerade,
- kravställning vid upphandling blir inkonsekvent
- säkerhetsnivån varierar beroende på hur varje leverantör implementerar åtkomstkontroller.

En gemensam struktur för behörighetsattribut gör det möjligt att:

- skapa tydliga och återanvändbara roller,
- införa likvärdiga behörighetsmodeller i hela kommunen,
- minska kostnader för integration och förvaltning,
- förenkla spårbarhet och loggning, och
- samverka bättre med andra kommuner, regioner och statliga aktörer.

Målet är att kommunerna ska kunna effektivisera IAM arbetet och hålla gör säkerhet.

2.2 Fragmentering i kommunal sektor idag

Fragmenteringen märks på flera nivåer:

- **Olika katalogstrukturer och begrepp**
  Varje kommun har historiskt skapat sin egen identitets- och behörighetsmodell. Resultatet är tusentals lokala varianter av roller, grupper, attribut, benämningar och struktur för behörighet. Det gör att två kommuner kan beskriva identiskt arbete på helt olika sätt ur ett IAM-perspektiv.
- **Systemleverantörer som definierar roller själva**
  Många verksamhetssystem kräver att kommunen anpassar sig efter leverantörens egen rollmodell. Det innebär att kommunen tvingas förvalta dubbla strukturer: en intern IAM-modell och systemens lokala roller.
- **Ingen tydlig koppling till verksamhetslogik**
  Roller och behörigheter är ofta uppbyggda utifrån historik, personberoende kunskap och tekniska begränsningar snarare än faktiska arbetsuppgifter eller yrkesroller.
- **Hög förvaltningsbelastning**
  Utan gemensamma strukturer måste varje systemförvaltare och katalogförvaltare lösa samma problem på egen hand – vilket leder till onödig administration, svaga möjligheter till automation och risk för felbehörigheter.

2.3 Nationellt samordnad modell

Den föreslagna modellen innebär ett skifte till en gemensam attributstruktur för alla kommuner som grund för behörighetsstyrning med domänspecifika attribut från Ena i en tvådimensionell modell där kommunens engagemang möter Ena:s nationella domäner. Det innebär inte att varje kommun blir identisk — men att man använder en delad, stabil referensmodell som gör IAM enklare, säkrare och mer förutsägbart.

När kommunerna utgår från samma attributmodell blir det möjligt att nå effekter som:

- kravställa system på ett likvärdigt sätt
- integrera verksamhetssystem snabbare
- skapa automatiserade flöden för onboarding/offboarding
- dela tekniska lösningar och erfarenheter
- ansluta till nationell digital infrastruktur utan lokal specialanpassning.

2.4 Koppling till Ena och nationella domäner

Ena är Sveriges nationella digitala infrastruktur. Inom Ena utvecklas:

- domäner
- gemensamma begrepp
- standardiserade funktioner för identitet och behörighet
- gemensamma attributlistor.

Health-domänen är den första domänen där behörighetsattribut utvecklats nationellt. Andra domäner (t.ex. utbildning, miljö, socialtjänst) kommer successivt att byggas ut.

Den kommunala modellen bygger direkt på Ena:s principer där Ena bidrar med *vertikal* struktur: attribut per domän och kommunerna bidrar med *horisontell* struktur: engagemang och roller. Tillsammans bildar de en *matris* där varje befattning får sina domänspecifika attribut.

För kommunerna innebär detta:

- stabilare grund för IAM
- mindre behov av lokala attributlistor
- bättre förutsättningar att samverka med regioner och statliga aktörer
- enklare anpassning till framtida europeiska ramverk (t.ex. EUDI-wallet).

2.5 En hybridmodell: Kombinationen av RBAC och ABAC

Kommunal verksamhet är komplex. En och samma person kan samtidigt vara anställd, utföra uppdrag inom olika verksamheter, ha särskilda funktioner (t.ex. skyddsombud), arbeta på flera enheter och dessutom ha domänspecifika uppgifter som kräver särskilda behörigheter. Inget enskilt behörighetsmönster räcker för att hantera denna variation på ett robust och förutsägbart sätt.

Därför bygger SKR:s rekommendation på en *hybridmodell*, som kombinerar styrkorna i både rollbaserad och attributbaserad behörighetsstyrning:

2.5.1 RBAC – Rollbaserad styrning som stabil grund

Roller utgör kärnan i kommunernas behörighetshantering.
SKR rekommenderar att kommunerna använder:

- AID-koder för att beskriva yrkesrollen (t.ex. socialsekreterare, sjuksköterska, barnskötare).
- Ansvarskoder (B, C, L, F) för att uttrycka ansvarsnivå (chef, ledning, samordning).

Detta skapar en gemensam och återanvändbar rollmodell som är konsekvent över kommunens samtliga verksamheter och system. RBAC-delen av modellen ger stabilitet och gör det enkelt att automatisera onboarding/offboarding, grupptillhörighet, behörighetspaket och åtkomst till verksamhetssystem.

2.5.2 ABAC – Attribut för specificera behörigheter

Kommuner behöver ofta mer detaljstyrning än vad en roll ensam kan uttrycka. Därför kompletteras RBAC-lagret med attributbaserad styrning. Det kan handla om:

- organisatorisk placering
- arbetsenhet (t.ex. CFAR)
- funktioner som jouransvarig eller skyddsombud
- domänspecifika attribut från Ena (t.ex. HSA-ID, förskrivarkod, vårdenhet).

Attributen gör det möjligt för system att ta mer precisa åtkomstbeslut utifrån aktuell kontext, utan att skapa tusentals roller. Det ger flexibilitet samtidigt som rollmodellen hålls ren och hanterbar.

2.5.3 Hybridmodellen i praktiken

I praktiken innebär hybridmodellen:

1. **Engagemanget** (anställd, förtroendevald, elev, konsult) beskriver *vilket uppdrag* personen har i kommunen.
2. **AID-roll + ansvarskod** beskriver *yrkesrollen och ansvarsnivån*.
3. **Domänspecifika attribut** anger *vilka uppgifter i en viss verksamhetsdomän* personen får utföra (t.ex. Health).

4. **Organisatoriska attribut** uttrycker *var personen arbetar, i vilken enhet och i vilken funktion*.

5. Systemen använder **attributen** för att besluta exakt vilka data och funktioner personen får åtkomst till.

Detta kombinerar det bästa av två världar:

- **RBAC:** förutsägbarhet, automation och administrativ enkelhet.
- **ABAC:** flexibilitet, kontextkänslighet och precision vid åtkomstbeslut.

2.5.4 Varför hybridmodellen är nödvändig i kommunal sektor

Kommunal verksamhet förändras snabbt – personal byts ut, uppdrag förändras, arbetsuppgifter flyttas och utvecklas. Genom en hybridmodell kan kommunen:

- undvika rollinflation,
- standardisera roller över hela organisationen,
- samtidigt skapa exakt så detaljerade behörigheter som behövs,
- integrera sömlöst med Ena:s domäner och nationella attributlistor,
- bättre möta framtida krav från EUDI-wallet och digital samverkan med andra huvudmän.

Resultatet är en modern, skalbar och interoperabel behörighetsmodell som fungerar i både dagens verksamhetssystem och morgondagens nationella digitala infrastruktur.

3 Grundläggande begrepp

En gemensam förståelse för centrala IAM-begrepp är nödvändig för att kunna arbeta enhetligt med behörighetsattribut i kommunal sektor. Det här kapitlet beskriver de grundläggande byggstenar som modellen bygger på: identitetsattribut, behörighetsattribut, roller, engagemang, domäner och objekttyper. Tillsammans utgör de strukturen som sedan används för att forma en konsekvent, skalbar och interoperabel behörighetsmodell.

3.1 Identitetsattribut vs behörighetsattribut

Identitetsattribut handlar om *vem* en individ eller maskin är. De beskriver själva identiteten och används framför allt för autentisering, spårbarhet och för att koppla samman identiteter med katalogobjekt. Exempel är namn, orgAffiliation, tekniska identifierare, och ibland även personnummer eller

PRID. De är stabila över tid och är inte kopplade till vad personen får göra i system.

Behörighetsattribut beskriver däremot *vad* identiteten får göra. Här ryms allt som är kopplat till arbetsuppgifter, funktioner, organisatorisk placering eller specifika domänbehörigheter. Det är dessa attribut som system använder för att besluta om åtkomst. I kommunal verksamhet kan det handla om allt från yrkesroll och ansvarsnivå till förskrivarkod, arbetsenhet eller särskilda funktioner som jouransvarig.
I den modell som SKR rekommenderar hålls identitets- och behörighetsattribut tydligt isär, vilket gör både datastrukturen och säkerhetsarbetet mer överskådliga.

3.2 Vad är en roll?

En roll är en strukturerad beskrivning av vilka arbetsuppgifter en individ har i organisationen. I kommunal verksamhet är detta ofta nära knutet till yrkesfunktionen. SKR rekommenderar därför att roller definieras med hjälp av AID-systemet, där AID-koden beskriver yrkesrollen och ansvarskoden (B, C, L eller F) beskriver vilken nivå av ansvar som ingår i uppdraget.

Med den kombinationen blir rollen en nationellt standardiserad beskrivning av individens arbetsfunktion. Det ger en stabil grund som fungerar lika bra för tekniska kataloger som för kravställning gentemot leverantörer.
Eftersom en person kan ha flera roller samtidigt – vilket är vanligt i kommuner – stödjer modellen parallella uppdrag utan att skapa onödigt många lokala roller.

3.3 Vad är ett engagemang?

Engagemanget beskriver individens relation till kommunen. Det är ett begrepp som ligger ovanför rollerna och förklarar *vilken typ av uppdrag eller tillhörighet* personen har. En individ kan exempelvis vara anställd, förtroendevald, elev eller konsult. Varje engagemang fungerar som en "ram" som innehåller roller, organisatoriska attribut och domänspecifika uppgifter.

Det är genom engagemanget som modellen kan hålla isär exempelvis en medarbetares tjänst, ett politiskt uppdrag och en elevs roll i skolan, även om samma individ förekommer i flera av dessa sammanhang.
Engagemanget är därför en kärnkomponent i den horisontella delen av SKR:s modell.

3.4 Vad är en domän?

En domän representerar ett verksamhetsområde med egna processer, begrepp och behörighetsbehov. Inom Ena utvecklas domäner nationellt. Health är det första fullständigt definierade området, men fler domäner – exempelvis inom utbildning, social service eller miljö – kommer gradvis att tas fram.

Domänspecifika attribut beskriver sådant som är relevant endast i ett visst verksamhetsområde. I Health-domänen kan det till exempel handla om förskrivarkod, legitimationstyp eller vårdgivarens organisationsidentifierare. Dessa attribut läggs ovanpå rollen och engagemanget och ger en mer precis behörighetsmodell som verksamhetssystemen kan använda vid auktorisationsbeslut. Domänerna utgör därmed modellens vertikala struktur.

3.5 Objekt: Människa vs maskin

I en modern IAM-miljö behöver man skilja mellan två typer av objekt: människor och maskiner.
Ett människa-objekt representerar en fysisk person i ett eller flera engagemang, med roller, organisatoriska attribut och domänspecifika uppgifter. Ett maskin-objekt representerar i stället systemtjänster, API-klienter, robotar eller integrationskomponenter. Maskiner har tekniska identiteter som exempelvis clientId eller certificateDn och ges specifika systembehörigheter snarare än roller.

Genom att hantera människor och maskiner separat blir både säkerheten och modellen mer hanterbar.

3.6 Översikt – hur allt hänger ihop

SKR:s modell består av flera lager som tillsammans bildar en sammanhållen struktur. Identitetsattributen ligger till grund för själva katalogobjektet. Engagemanget beskriver vilken relation personen eller maskinen har till kommunen. Roller och organisatoriska attribut placeras inom engagemanget och uttrycker arbetsuppgifter, ansvar och organisatorisk kontext. Därefter kompletteras modellen med domänspecifika attribut som endast är relevanta inom vissa verksamhetsområden. Sist finns systemspecifika rättigheter som används i enskilda applikationer.

Tillsammans bildar dessa lager en tydlig helhet där varje person eller maskin kan beskrivas på ett konsekvent och återanvändbart sätt – och där

både RBAC och ABAC kan tillämpas utan att strukturen blir otydlig eller svår att förvalta.

4 Övergripande arkitektur för behörighetsattribut

SKR:s rekommenderade arkitektur bygger på en tydlig och systematisk indelning av behörighetsattribut i två kompletterande dimensioner: en vertikal struktur som kommer från de nationella verksamhetsdomänerna inom Ena, och en horisontell struktur som beskriver kommunernas engagemang och roller. När dessa två dimensioner kombineras skapas en matris som gör det möjligt att uttrycka behörigheter på ett enhetligt och samtidigt verksamhetsnära sätt.

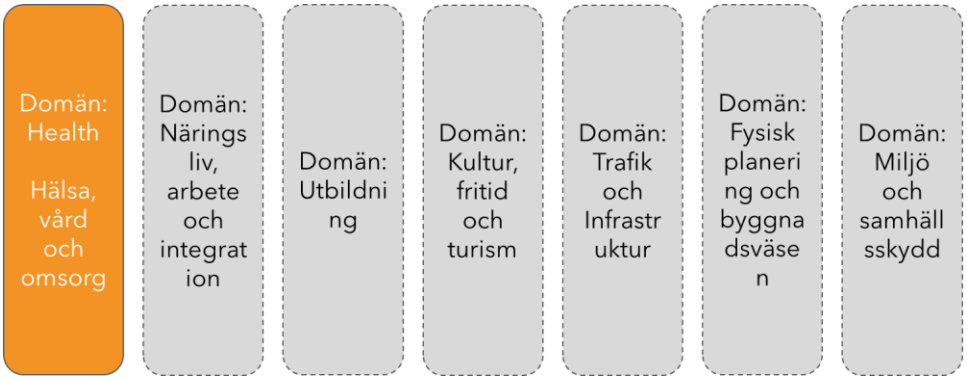
Arkitekturen är framtagen för att fungera tillsammans med både dagens federationslösningar (SAML/OIDC) och morgondagens europeiska strukturer, inklusive EUDI-wallet. Målet är att skapa en modell som är stabil, interoperabel och möjlig att införa oavsett kommunens tekniska plattform.

4.1 Den nationella vertikala strukturen (Ena-domänerna)

Ena utvecklar verksamhetsdomäner på nationell nivå. Varje domän definierar gemensamma begrepp, informationsmodeller, API:er och – i vissa domäner – behörighetsattribut. Health är den domän som kommit längst och som redan har en officiell attributlista. Andra domäner kommer successivt att utvecklas på samma sätt.

Den vertikala strukturen beskriver *vad som gäller i en viss verksamhetskontext*. Ett attribut som “förskrivarkod” eller “vårdenhets-ID” är endast relevant inom Health och tillhör därför den domänen. Det innebär att kommunerna kan återanvända nationellt förvaltade attribut istället för att skapa egna varianter.

Det viktiga här är att domänerna inte beskriver hur kommunerna organiserar sig, utan vilka egenskaper eller rättigheter en person måste ha för att utföra en viss typ av verksamhet. Domänerna är därför ett verksamhetslager som ligger ovanpå kommunens egen organisationsstruktur och roller.



Figur 1 Nationell vertikala domäner

Notera i Figur 1 att endast Healths domänen är del av Enas arbete i nuläget. Övriga domäner är antagande inspirerade av Arkitekturgemenskapens förmågeanalys[1].

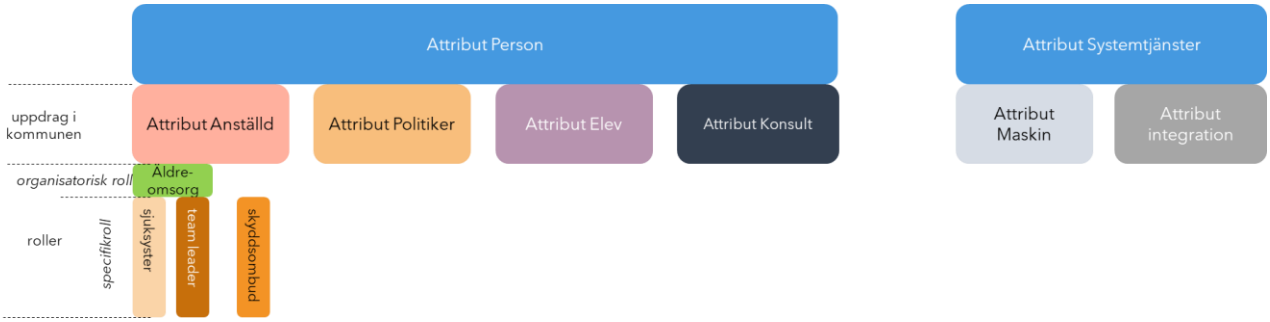
4.2 Den kommunala horisontella strukturen (engagemang & roller)

Parallellt med den vertikala domänstrukturen behöver kommunerna beskriva sina egna organisatoriska och relationella perspektiv – det som i modellen blir den horisontella dimensionen. Här ligger två centrala byggstenar:

- *Engagemang* – relationen en person har till kommunen, exempelvis anställd, förtroendevald, konsult eller elev. Engagemanget är den kontext i vilken behörighetsattribut får betydelse. En person kan förekomma i flera engagemang samtidigt.
- *Roller* – den arbetsuppgift eller funktion individen har inom sitt engagemang. SKR rekommenderar att roller baseras på AID-koder, eftersom det ger en nationellt standardiserad grund. Ansvarskoder kan användas för att uttrycka nivåer av ansvar och ledning inom samma yrkesroll.

Den horisontella strukturen fångar det kommunerna själva är bäst på: att beskriva sina yrkesroller, uppdrag och organisatoriska placeringar. Det är också den struktur som förändras när verksamheten förändras.

[1] Inera, Arkitekturgemenskapens förmågeanalys



Figur 2 Kommunala horisontella struktur

Roller i Figur 2 ska ses som exempel.

4.3 Matrisen: där vertikalt och horisontellt möts

När domänernas vertikala attributstruktur kombineras med kommunernas horisontella struktur skapas en matris. Det är i denna matris som behörighetsmodellen blir konkret och användbar.

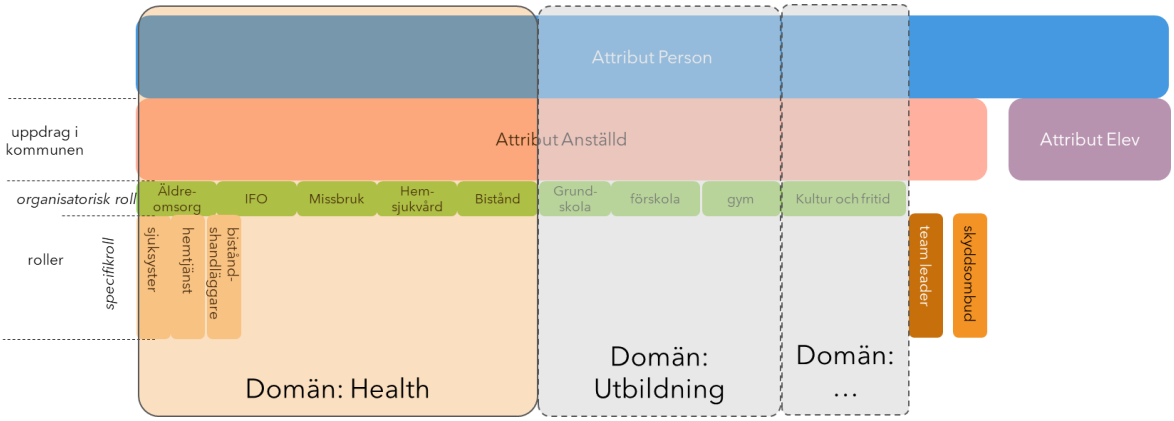
Man kan se matrisen som ett rutnät:

- *Vertikalt*: Ena-domäner (Health, Utbildning, Kultur och fritid m.fl.)
- *Horisontellt*: Engagemang och roller (anställd *har* AID-kod *har* ansvarskod)

I varje ruta i matrisen finns just de behörighetsattribut som är relevanta för en viss roll i en viss domän.
Exempel:

- En socialsekreterare (AID 351008) i socialtjänsten behöver andra attribut än en parkskötare.
- En elev har inga Health-behörigheter, men kan ha attribut inom utbildningsdomänen.
- En förtroendevald saknar domänspecifika attribut men har engagemangsbaserade behörigheter kopplade till sina uppdrag.

Matrisen gör det möjligt för kommunen att bygga sina behörighetsmodeller på ett sätt som är både standardiserat och verksamhetsnära. Varje individ får en profil som består av alla relevanta delar: identitet, engagemang, roller och domänspecifika attribut.



Figur 3 Attributstruktur i matris

Roller och domäner i Figur 3 ska ses som exempel.

4.4 Illustration av tvådimensionell modell

Den tvådimensionella modellen kan sammanfattas som en struktur där:

- den vertikala axeln följer vad nationella aktörer definierar som giltigt inom en domän,
- den horisontella axeln utgår från kommunens egen verksamhet, organisation och yrkesroller,
- och skärningspunkten mellan dessa axlar anger vilka behörighetsattribut som i praktiken ska skickas till ett verksamhetssystem för att avgöra åtkomst.

Modellen möjliggör:

- att kommunerna kan återanvända nationella definitioner där sådana finns,
- att behörigheter förankras i faktiska yrkesroller och uppdrag,
- att attribut kan kombineras utan att skapa komplexa och svårförvaltade rollstrukturer,
- och att både RBAC och ABAC kan tillämpas på ett konsekvent sätt.

På detta sätt blir modellen framtidssäker, skalbar och redo att samverka med både nya nationella tjänster och framtida europeiska lösningar.

5 Grundstruktur för behörighetsattribut i en kommun

SKR:s rekommenderade modell för behörighetsattribut bygger på att varje kommun beskriver människor och maskiner på ett enhetligt, strukturerat och återanvändbart sätt. Modellen utgår från ett antal lager – identitet, engagemang, roller, organisatoriska attribut och domänspecifika attribut – som tillsammans formar en komplett behörighetsprofil för varje individ eller system.

Den här strukturen är avsedd att fungera i alla kataloglösningar och är framtagen för att stödja både nationell interoperabilitet och lokal verksamhetseffektivitet.

5.1 Indelningen Human vs Machine

En grundläggande princip är att skilja mellan mänskliga identiteter och maskinella identiteter.

Människa (Human) representerar individer som har en faktisk relation till kommunen: anställda, förtroendevald, elever eller konsulter. Dessa identiteter har personattribut, engagemang och roller, samt – när det behövs – domänspecifika behörigheter.

Maskin (Machine) representerar systemtjänster, integrationer, API-klienter och robotar. Maskinobjekt har aldrig roller eller engagemang. De beskriver endast *teknisk åtkomst*, vanligtvis med attribut som clientId, certificateDn eller systemspecifika rättigheter.

Denna separation gör åtkomstmodellen tydligare, säkrare och enklare att automatisera.

Exempel på maskinidentiteter ges endast för att förklara strukturen. Denna vägledning specificerar inte en komplett attributmodell för maskiner.

5.2 Personattribut (globala attribut)

Personattributen är de identitetsattribut som gäller oavsett vilken roll individen har och oavsett vilken domän hen arbetar inom. De är det ”globala lagret” som ligger överst i alla mänskliga identiteter.

Typiska personattribut är:

- **sn** (efternamn)
- **givenName** (förnamn)
- **displayName**

- **personalIdentityNumber** (personnummer – används restriktivt)
- **orgAffiliation** (unik organisationsutfärdad identitet)

De globala attributen gör att man kan identifiera, autentisera och spåra en individ utan att blanda ihop dessa grundläggande uppgifter med vilka behörigheter personen har.

5.3 Engagemang (anställd, förtroendevald, elev, konsult)

Ett engagemang beskriver *vilken relation* en individ har till kommunen. Engagemang är därför en central byggsten i den horisontella delen av attributmodellen. En person kan ha flera engagemang samtidigt, exempelvis vara både anställd och förtroendevald, eller konsult och elev.

Vanliga engagemangstyper i kommuner är:

- Anställd
- Förtroendevald
- Elev
- Konsult

Engagemanget fungerar som behållaren där roller, organisatoriska attribut och domänspecifika attribut grupperas. Det gör att varje person kan representeras på ett tydligt och förutsägbart sätt.

I SKR:s rekommendation Identitet och behörighetshantering[2] beskrivs också hur engagemang bör hanteras ur identitetsperspektiv. När en person har flera engagemang i kommunen rekommenderas det att varje engagemang representeras av en egen e-identitet. Syftet är att skapa en tydlig separation mellan olika uppdrag och att säkerställa att behörigheter inte blandas mellan engagemangen.

En individ som både är anställd och elev ska exempelvis inte få åtkomst till system och information som rör anställningen när hen agerar i sin roll som elev. Genom att skilja identiteterna åt blir både åtkomstkontrollen och informationssäkerheten mer robust. Det leder också till effektivare och säkrare processer för onboarding och offboarding, eftersom behörigheter kopplade till ett engagemang kan avslutas utan risk för att oönskade rättigheter ligger kvar via ett annat. Uppdelningen gör därmed behörighetshanteringen både mer förutsägbar och mindre sårbar.

[2] SKR, Identitets- och behörighetshantering

5.4 Engagemangsspecifika attribut

Utöver de globala personattributen behöver varje engagemang kompletteras med uppgifter som är relevanta bara i den kontexten. Ett engagemang ”Anställd” kan till exempel innehålla:

- tjänsteställe eller enhet
- organisatorisk placering
- arbetsfunktioner och lokala uppdrag
- kontaktuppgifter (telefon, mobil, tjänstemejl)
- anknytningar till HR- eller lönesystem

För ett elevengagemang kan helt andra attribut vara relevanta, såsom skolform, årskurs eller klass.

Engagemangsspecifika attribut hjälper systemen att förstå i vilken organisatorisk och verksamhetsmässig kontext individen verkar.

5.5 AID-baserade roller

Rollerna är en av de mest centrala delarna av modellen. SKR rekommenderar att kommunerna använder AID-koder som grund för sina roller, eftersom AID är ett nationellt system som täcker hela kommunsektorns arbetsroller.

Vad är AID-koder?

AID (Arbetsidentifikation)[3] är SKR:s nationellt framtagna system för att klassificera arbeten, yrkesroller och befattningar inom kommuner och regioner. Varje roll har en AID-kod som beskriver vilken typ av arbete individen utför, och en etikett som beskriver funktionen på ett begripligt sätt. Systemet kompletteras med ansvarskoder (t.ex. B, C, L och F) som uttrycker om rollen har lednings-, chef-, samordnings- eller specialistansvar. Den är inte obligatorisk för alla roller.

AID gör att roller kan beskrivas på ett standardsatt sätt i hela landet. Det innebär att en ”socialsekreterare” eller ”undersköterska” alltid kan identifieras på samma sätt i IAM, oavsett kommun eller system.

AID-systemet underlättar också kravställning och interoperabilitet eftersom verksamhetssystem och leverantörer kan förväntas förstå samma rollstruktur. Det minskar behovet av lokalt definierade roller och minskar risken för rollinflation.

[3] SKR, Arbetsidentifikation (AID)

AID-koden beskriver yrkesrollen. Lokala befattningsbenämningar kan behövas som komplement.

I Bilaga 3 redovisas aktuella AID-koder för Arbete inom individ-, familje- och äldreomsorg m.m. (från hösten 2025).

5.6 Rekommenderad modell: 0..n roller per engagemang

I kommunal verksamhet är det vanligt att en individ kombinerar flera arbetsuppgifter. En person kan exempelvis vara både socialsekreterare, samordnare och handledare. Därför rekommenderas modellen *0..n roller per engagemang*.

Det innebär att ett engagemang kan innehålla:

- ingen roll (ovanligt men möjligt, t.ex. ny onboarding)
- exakt en roll
- flera roller (t.ex. kombinationstjänster eller dubbla funktioner)

Denna flexibilitet är en av styrkorna i modellen. Rollen beskriver *vad personen gör*, medan engagemanget beskriver *i vilken relation personen gör det*. När flera roller kombineras bibehålls en tydlig struktur tack vare AID-systemets standardisering.

5.7 Domänspecifika attribut (exempel: Health)

Domänspecifika attribut beskriver sådant som bara är relevant inom ett visst verksamhetsområde. De definieras nationellt inom Ena och gör det möjligt för kommunerna att återanvända etablerade och standardiserade begrepp.

Health-domänen är i dag den mest utvecklade och innehåller attribut som:

- HSA-ID
- olika legitimationstyper
- förskrivarkod
- vårdgivarens organisationsnummer
- vårdenhetsnamn och enhetsidentiteter
- systemroller och kommissionsuppdrag

När en person har en roll som är verksam i en viss domän läggs domänens attribut till just det engagemanget. På så sätt får exempelvis en sjuksköterska sina Health-attribut, medan en lärare får attribut från utbildningsdomänen när dessa utvecklats nationellt.

5.8 Kommunspecifika attribut

Många attribut behövs i en nationell federations kontext. Utöver dessa behöver kommuner ytterligare behörighetsattribut för sin lokala verksamhet. Det kan handla om:

- befattningsnamn
- arbetsområden eller team
- ansvarsområden
- geografiska placeringar (t.ex. för fastighet eller gata/park)
- funktioner som saknar AID-kod, t.ex. skyddsombud eller arkivansvarig

Det viktiga är att kommunspecifika attribut hålls separerade från de nationella och domänspecifika, så att kommunerna inte bygger beroenden som blir svåra att förvalta över tid.

6 Domän: Health – referensmodell

Health är den första verksamhetsdomänen inom Ena som har en nationellt framtagen och förvaltad lista över behörighetsattribut. Attributen beskriver de egenskaper som krävs för att utföra arbete inom hälso- och sjukvård, exempelvis legitimationer, förskrivarkoder, vårdenhetsidentiteter och systemroller.

I kommunal verksamhet används delar av dessa attribut i socialtjänst, hemsjukvård och andra områden där kommunen bedriver hälso- och sjukvårdsuppgifter. SKR:s rekommendation är att kommunerna utgår från Ena:s officiella attributlista för Health.

Den fullständiga specifikationen, inklusive beskrivningar, definitioner och tekniska format, hanteras inom Ena. Kommuner bör alltid hänvisa till och använda den information som finns i Ena:s dokumentation, eftersom dessa attribut kan utvecklas och förändras över tid.[4]

I denna rekommendation redovisar vi därför endast hur Health-attributen placeras i kommunens struktur (engagemang → roll → domän), inte innehållet i varje attribut. Det gör att modellen förblir stabil även när den nationella domänen förändras eller byggs ut.

[4] När detta dokument skrivs har attributlistan för Ena:s Health domän inte publicerats.

7 Attribut och identitet utan personnummer

Personnummer har historiskt varit ett centralt identitetsbärande attribut i kommunernas system. I moderna IAM-lösningar skapar det dock flera utmaningar: integritetsrisker, onödiga beroenden, bristande interoperabilitet och svårigheter vid pseudonymisering. SKR:s rekommendation är därför att personnummer inte ska vara ett primärt tekniskt identitetsattribut i IAM, och att det endast ska användas när det är nödvändigt för en specifik verksamhetsprocess.

För att stödja detta behöver kommunerna använda tekniska identifierare som är stabila, unika och oberoende av personuppgifter.

Personnummer kan fortsatt användas för matchning i källsystem och verksamhetsprocesser, men ska inte användas som primär teknisk identifierare i IAM.

7.1 Varför undvika personnummer i attribut

Det finns flera skäl att undvika personnummer i attribut för identitet och behörighet.

Integritet:
Personnummer är en känslig personuppgift enligt GDPR. Onödig spridning i kataloger och federationsutbyte innebär risker, särskilt vid loggning och systemintegrationer.

Interoperabilitet:
Nationella och europeiska ramverk – inklusive EUDI-wallet – bygger inte på personnummer som teknisk nyckel.

Principen om dataminimering:
IAM ska bära *minsta möjliga mängd personuppgifter* för att kunna fungera säkert och effektivt.

Minskat värde vid cybersäkerhets incidenter:
Personuppgiftskänslig information får ett lägre värde om informationen i sig inte avslöjar VEM informationen är kopplad till.

Av dessa skäl bör personnummer betraktas som ett verksamhetsattribut, inte ett IAM-attribut.

7.2 Organisationsutfärdade identiteter

I stället för personnummer bör kommunerna använda organisationsutfärdade identiteter enligt standarden ELN-AP-OrgPerson-01[5]. Detta attribut-set är framtaget för att skapa unika identiteter inom en organisation utan att avslöja personens civila identitet.

Attribut set: `ELN-AP-OrgPerson-01`

`URI: http://id.elegnamnden.se/ap/1.0/org-person-01`

Attributsetet innehåller bland annat:

- `orgAffiliation` – en unik identifierare som kombinerar ett lokalt ID med kommunens organisationsnummer
- `organizationIdentifier` – organisationsnummer för den juridiska personen
- `o` – organisationens namn
- `displayName` – (frivillig) personens visningsnamn

OrgPerson-01 fungerar i federationer, fungerar i kataloger och fungerar i `tillitsramverket`. Det är dessutom oberoende av personnummer, vilket gör det stabilt över tid.

7.3 orgAffiliation som unik identifierare

`orgAffiliation` är det viktigaste attributet i modellen för teknisk identitetshantering. Det kombinerar ett lokalt unikt ID med kommunens organisationsnummer, enligt formatet:

`<lokalt-uid>@<organisationsnummer>`

Det lokala uid:t kan vara ett GUID, ett katalog-ID eller annat internt ID. Kombinationen säkerställer global unikhet inom federationslösningar och gör att identiteten blir oberoende av personuppgifter.

[5] Utfärdat av E-leg nämnden, numera Digg, publicerat i Sweden Connect - Attribute Specification for the Swedish eID Framework

Fördelarna är:

- unikt inom och mellan kommuner
- stabilt över tid
- ingen koppling till personnummer
- fungerar utmärkt i SAML- och OIDC-flöden
- lämpar sig för maskininläsningar och loggning

I praktiken är `orgAffiliation` den rekommenderade primärnyckeln för alla mänskliga identiteter i IAM.

7.4 GUID-baserade interna ID:n

Ett GUID (globally unique identifier) är en av de mest robusta metoderna för att skapa referenser till en individ i interna system. När ett GUID används som lokalt uid i orgAffiliation får individen en stabil och icke-personrelaterad identitetsnyckel.

Tillsammans med OrgPerson-01 ger GUID-modellen en modern grund för identitetsförvaltning som klarar kommande krav.

7.5 Rekommenderad policy för användning av personnummer

SKR rekommenderar följande principer:

1. **Personnummer ska inte vara primärt identitetsattribut i IAM.** Det ska inte användas som nyckel, inte ingå i tekniska identifierare och inte ingå i attribut som förs över i federation.
2. **Personnummer får användas där verksamheten kräver det.** Exempelvis vid journalföring, myndighetsutövning eller processer med lagkrav, men då inte som nyckelattribut för identifiering.
3. **I IAM bör personnummer användas restriktivt.** I de fall det måste finnas i katalogen bör det behandlas som ett känsligt attribut med strikt åtkomstkontroll.
4. **Ersätt alltid personnummer med organisationsutfärdade identiteter i federationsflöden.**
5. **Vid identitetsbyte** (t.ex. skyddad identitet) ska IAM hantera ändringen utan beroende av personnummer. Detta är endast möjligt om personnummer inte är teknisk nyckel.

Genom dessa principer kan kommunen skapa ett IAM som är både säkert, modernt och kompatibelt med nationella och europeiska identitetsramverk.

8 Namespace och publiceringsmodell

Ett gemensamt ramverk för behörighetsattribut kräver att varje attribut har en stabil, unik och spårbar namnrymd, ett så kallat namespace. Namnrymden gör det möjligt för system att förstå vad ett attribut betyder, var det hör hemma och vem som ansvarar för dess förvaltning. Utan en tydlig namespace-struktur riskerar attributen att få lokala varianter, dubbla definitioner eller oklara ägare — något som försvårar interoperabilitet inom kommunsektorn och mellan kommuner, regioner och statliga aktörer.

SKR har därför analyserat tre möjliga alternativ för hur behörighetsattribut kan publiceras och versionshanteras.

8.1 Varför attribut behöver namnrymder

Ett namespace fyller tre centrala funktioner:

1. Unikhet - Det säkerställer att två olika organisationer inte råkar definiera samma attribut med samma namn men med olika betydelser. En global namnrymd skapar entydighet.

2. Stabilitet över tid - Attribut måste kunna användas i kataloger, federationer och API:er under lång tid utan att länkar eller definitioner förändras eller försvinner.

3. Tydlig förvaltning - Ett attribut blir inte bara ett tekniskt fält, utan en del av en styrd struktur där ansvar, ägarskap, ändringshantering och dokumentation är definierad.

Utan namespace blir attributlistor snabbt fragmenterade och svåra att integrera, särskilt i federationslösningar.

8.2 Tre alternativ: IANA, egen domän, Ena

SKR:s analys visar att det finns tre realistiska sätt att publicera behörighetsattribut på ett korrekt och långsiktigt hållbart sätt.

Alternativ 1: Publicering via IANA (URN-format)

Att registrera en global URN-namnrymd via IANA är det mest formellt internationella alternativet. Det ger global stabilitet och tydlig standardkoppling.
Nackdelar:

- Ansökningsprocessen är omfattande
- Förvaltningskraven är höga
- Kompetensen måste finnas långsiktigt hos förvaltande organisation

- Mindre flexibelt vid förändringar

Bedömning: Tekniskt möjligt, men tungrott och svårmotiverat för kommunsektorn.

Alternativ 2: Egen URL-domän för kommunsektorn

Här skulle SKR eller en neutral aktör (exempelvis Inera i en ren förvaltarroll) registrera en domän, t.ex. `id.municipality.se`, där attribut kan publiceras i URL-form.

Detta ger:

- stor flexibilitet
- möjlighet att snabbt publicera och uppdatera attribut
- enkel dokumentation via webbsidor

Nackdelar:

- risk för att kommunsektorn hamnar vid sidan av Ena
- förvaltningen blir kommunernas ansvar
- risk för framtida parallellstrukturer med statliga normkällor

Bedömning: Ett fungerande alternativ, men mindre långsiktigt robust.

Alternativ 3: Publicering via Ena (rekommenderat alternativ)

Ena har redan etablerat namespace och publiceringsstruktur för domänspecifika attribut, t.ex. genom URL-strukturen:

`https://id.ena-infrastructure.se/attributes/<domän>/<attribut>`

Att publicera kommunernas behörighetsattribut via Ena skulle:

- ge nationell legitimitet
- minska kommunernas förvaltningsbörda
- säkerställa en enhetlig nationell struktur
- underlätta framtida interoperabilitet med statliga och regionala aktörer
- placera kommunsektorn i linje med övriga nationella digitala standarder

Bedömning: Det tekniskt och organisatoriskt bästa alternativet på sikt.

8.3 Pågående arbete: publicering via Ena

SKR arbetar i denna version av vägledningen utifrån ambitionen att kommunala behörighetsattribut ska kunna publiceras och förvaltas inom Ena:s nationella namespace-struktur. Det är det alternativ som ger högst grad av interoperabilitet och stabilitet och som mest effektivt knyter samman kommunernas IAM-lösningar med den nationella digitala infrastrukturen.

Arbetet kommer att kräva styrning, samordning och beslut på nationell nivå och kommer därför att ta tid. Under tiden behöver kommunerna följa strukturen i denna vägledning, men bör avvakta med att etablera egna lokala namespaces som riskerar att bli överflödiga.

I kommande versioner av vägledningen kommer arbetet med namespace att kunna preciseras när Ena:s processer är förtydligade och beslutade.

9 Implementationsrekommendationer för kommuner

Att införa en strukturerad och standardiserad modell för behörighetsattribut är en förändring som påverkar flera delar av kommunens IT– och verksamhetslandskap. Den kräver samverkan mellan IAM-funktion, HR, verksamhetssystemens förvaltare och informationssäkerhet. Nedan följer rekommenderade steg för hur kommuner praktiskt kan påbörja arbetet — i linje med SKR:s vägledning *Identitet och behörighet*.

9.1 Hur börja: attributinventering

Det första steget är att skapa överblick över nuläget. De flesta kommuner har idag hundratals, ibland tusentals, lokalt definierade roller, grupper och attribut. Ett strukturerat startläge underlättar all fortsatt modellering.

Rekommenderat arbetssätt:

1. **Inventera befintliga kataloger och grupper.**
   Lista alla attribut, grupper och rollobjekt i kataloger (AD, Azure AD, IAM-plattformar). Identifiera dupliceringar och oklara namn.

2. **Kartlägg attribut som skickas i federationer.**
   Detta visar vilka attribut som “läcker ut” till externa parter — ofta mer än kommunen tror.

3. **Identifiera attribut som är verksamhetskritiska.**
   Vad används vid inloggning? Vad används i verksamhetssystemens behörighetsmodeller?

4. **Rensa bort lokala attribut som saknar ägare eller inte används.**
   Onödig komplexitet är en av de största bromsklossarna i IAM.

Inventeringen ska ge en lista över vilka attribut som bör migreras, konsolideras eller ersättas av gemensamma attribut enligt denna modell.

9.2 Hur modellera engagemang

Engagemang är ryggraden i kommunens horisontella struktur. Varje person ska kunna beskrivas i flera engagemang, där varje engagemang har egna roller och attribut.

Rekommenderat arbetssätt:

- Definiera kommunens engagemangstyper (anställd, förtroendevald, konsult, elev).
- Säkra datakällor för varje engagemang (HR, nämndadministration, elevdatasystem).
- Inför principen att varje engagemang representeras av en egen e-identitet, enligt SKR:s rekommendation.

Syftet är att skapa tydliga avgränsningar: en person ska inte få anställdas rättigheter via sitt elev- eller politiska engagemang.

En tydlig modell för engagemang gör onboarding, offboarding och förändrade uppdrag mycket enklare att automatisera.

9.3 Hur införa AID-baserade roller

Rollerna är navet i behörighetsstyrningen. Genom att använda AID-systemet får kommunen en standardiserad och nationellt harmoniserad rollmodell.

Steg för införande:

1. **Kartlägg dagens roller och befattningar.**
   Matcha dem mot AID-systemets koder och etiketter.

2. **Fastställ ansvarskoder** (B, C, L, F) för roller som har lednings- eller specialfunktioner.

3. **Definiera regler för 0..n roller per engagemang.**
   Kommuner bör undvika “kombinationsroller” och i stället ge individen flera separata roller när det behövs.

4. **Inför rollen som katalogobjekt eller attribut i IAM.**
   Rollen ska vara tekniskt mappbar till federationsattribut.

När AID-rollerna är etablerade blir det möjligt att kravställa system så att de förstår och utnyttjar dessa roller.

9.4 Hur ordna maskinidentiteter

Även om maskiner inte ingår i denna version av vägledningen behöver kommunen ändå säkerställa en grundläggande struktur för sina maskinobjekt.

Rekommenderade principer:

- Maskiner ska aldrig ha roller eller engagemang.
- Maskiner ska ha identiteter baserade på certifikat, clientId eller andra tekniska attribut.
- Maskinidentiteter ska separeras från mänskliga identiteter i katalogen.
- Behörigheter för maskiner uttrycks som entitlements (t.ex. app-roller, scopes), inte som AID-koder eller domänattribut.
- Maskiner ska ingå i lifecycle-hantering med tydlig ägare och tidsbegränsning.

En ren separation mellan människa och maskin är en förutsättning för en säker IAM-miljö.

10 Bilagor

Bilaga A: Lista över Ena Health-attribut
Bilaga B: SKR:s rekommenderade attributlista för kommuner
Bilaga C: AID-koder och ansvarsnivåer - För socialtjänsten

Bilaga 1

Lista över Enas behörighetsattribut. Nedan visas exempel, inte en komplett lista. Fullständig information finns hos Digg (Ena).

Name	Friendly Name	Description
urn:oid:2.5.4.4	sn	Surname
urn:oid:2.5.4.42	givenName	Given name
urn:oid:2.16.840.1.113730.3.1.241	displayName	Display name
urn:oid:1.2.752.29.4.13	personalIdentityNumber	National civic registration number/code
urn:oid:2.5.4.20	telephoneNumber	Telephone number
urn:oid:0.9.2342.19200300.100.1.41	mobile	Mobile number
urn:oid:0.9.2342.19200300.100.1.3	mail	E-mail address
urn:oid:1.2.752.29.6.2.1	employeeHsaId	HSA-ID
urn:oid:2.5.4.10	o	Organization name
urn:oid:2.5.4.97	organizationIdentifier	Organizational identifier code
urn:oid:1.2.752.201.3.1	orgAffiliation	@ (<unik id>@<orgnr>.se)
urn:oid:1.2.752.201.3.2	transactionIdentifier	Unique identifier for the transaction
https://id.ena infrastructure.se/attributes/health/healthcareProfessionalLicenseIdentityNumber	healthcareProfessionalLicenseIdentityNumber	Professional legitimation code
https://id.ena-infrastructure.se/attributes/health/personalPrescriptionCode	personalPrescriptionCode	Personal prescription code
https://id.ena-infrastructure.se/attributes/health/healthcareProfessionalLicense	healthcareProfessionalLicense	Professional license
https://id.ena-infrastructure.se/attributes/health/occupationalCode	occupationalCode	Extended occupational code

https://id.ena-infrastructure.se/attributes/health/groupPrescriptionCode	groupPrescriptionCode	Group prescription code
https://id.ena-infrastructure.se/attributes/health/pharmacyIdentifier	pharmacyIdentifier	Pharmacy GLN code
https://id.ena-infrastructure.se/attributes/health/healthcareProviderId	healthcareProviderId	Healthcare provider organization number
https://id.ena-infrastructure.se/attributes/health/healthcareProviderHsaId	healthcareProviderHsaId	Healthcare provider HSA-id
https://id.ena-infrastructure.se/attributes/health/healthcareProviderName	healthcareProviderName	Healthcare provider name
https://id.ena-infrastructure.se/attributes/health/healthcareUnitName	healthcareUnitName	Healthcare unit name
https://id.ena-infrastructure.se/attributes/health/healthcareUnitHsaId	healthcareUnitHsaId	Healthcare unit HSA-id
https://id.ena-infrastructure.se/attributes/health/commissionName	commissionName	Commission name
https://id.ena-infrastructure.se/attributes/health/commissionPurpose	commissionPurpose	Commission purpose
https://id.ena-infrastructure.se/attributes/health/commissionRight	commissionRight	Commission right
https://id.ena-infrastructure.se/attributes/health/systemRole	systemRole	System role
https://id.ena infrastructure.se/attributes/health/healthcareProfessionalLicenceSpeciality	healthcareProfessionalLicenceSpecialty	Professional license specialty

Bilaga 2

SKR:s rekommenderade attributlista för kommuner

```
Object
├─ objectType: human | machine
│
├─ Human
│   └─ personalAttributes (globala OID/LDAP-attribut)
│       ├─ sn (urn:oid:2.5.4.4)
│       ├─ givenName (urn:oid:2.5.4.42)
│       ├─ displayName (urn:oid:2.16.840.1.113730.3.1.241)
│       ├─ personalIdentityNumber (urn:oid:1.2.752.29.4.13)
← använd sparsamt
│       │
│       └─ affiliation (engagemang/uppdrag)
│           ├─ employee (0..n anställningar/uppdrag)
│           │   │
│           │   ├─ organizationalPersonIdentity – ELN-AP-OrgPerson-
01 (attribute set)
│           │   │   ├─ orgAffiliation (urn:oid:1.2.752.201.3.1)
← REQUIRED, format: <uid>@<orgnr>
│           │   │   │     • <uid> = lokalt unikt ID (t.ex. GUID)
│           │   │   │     • <orgnr> = svenskt org.nr enligt SKV
709, 10 siffror utan bindestreck
│           │   │   ├─ o – Organization name (urn:oid:2.5.4.10)
← REQUIRED
│           │   │   ├─ organizationIdentifier (urn:oid:2.5.4.97)
← RECOMMENDED (juridiskt org.nr)
│           │   │   └─ displayName
(urn:oid:2.16.840.1.113730.3.1.241)← REQUIRED (tillfredsställs av
personattributet)
│           │   │
│           │   ├─ employmentAttributes (oberoende av domän)
│           │   │   ├─ telephoneNumber (urn:oid:2.5.4.20)
│           │   │   ├─ mobile (urn:oid:0.9.2342.19200300.100.1.41)
│           │   │   ├─ mail (urn:oid:0.9.2342.19200300.100.1.3)
│           │   │   ├─ cFARUnit – CFAR valfri,
identifikationsnummer för ett arbetsställe som tilldelas av
Statistiska centralbyrån (SCB)
│           │   │   ├─ organizationalUnitAssignment (0..n, hr)
│           │   │   ├─ financialResponsibilityCode (0..n,  ekonomi)
│           │   │   └─ employmentId (lokal referens)
│           │   │
│           │   └─ role - In this model, AID code represents a job
role. It is expressed as a ‘role’ attribute in the RBAC layer, in
line with international IAM terminology
│           │       ├─ aidCode (t.ex. 351008)
│           │       ├─ aidLabel (t.ex. ”Socialsekreterare, barn och
unga, myndighetsutövning”)
```

```
│           │       ├─ responsibilityCode(s) (B | C | L | F)
│           │       ├─ function (valfri; t.ex. “Jouransvarig”)
│           │       ├─ serviceDomain (t.ex. socialservice | health
| education | …)
│           │       ├─ validFrom
│           │       ├─ validTo
│           │       │
│           │       ├─ municipalRoleAttributes - kommunspecifika
org-rollattribut
│           │       │    ├─ jobTitle - befattning
│           │       │    ├─ facility - fastighet
│           │       │    ├─ responsibilityArea - ansvarsområde
│           │       │    └─ workLocation - plats
│           │       │
│           │       └─ domainSpecificAttributes - domänspecifika
org-rollattribut (aktiveras när domain=health)
│           │           ├─ employeeHsaId (urn:oid:1.2.752.29.6.2.1)
│           │           ├─
healthcareProfessionalLicenseIdentityNumber
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/healthcareProfessionalLicenseI
dentityNumber)
│           │           ├─ personalPrescriptionCode
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/personalPrescriptionCode)
│           │           ├─ healthcareProfessionalLicense
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/healthcareProfessionalLicense)
│           │           ├─ occupationalCode
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/occupationalCode)
│           │           ├─ groupPrescriptionCode
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/groupPrescriptionCode)
│           │           ├─ pharmacyIdentifier (GLN)
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/pharmacyIdentifier)
│           │           ├─ healthcareProviderId – vårdgivarens
orgnr
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/healthcareProviderId)
│           │           ├─ healthcareProviderHsaId
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/healthcareProviderHsaId)
│           │           ├─ healthcareProviderName
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/healthcareProviderName)
│           │           ├─ healthcareUnitName
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/healthcareUnitName)
│           │           ├─ healthcareUnitHsaId
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/healthcareUnitHsaId)
```

```
│           │           ├─ commissionName
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/commissionName)
│           │           ├─ commissionPurpose
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/commissionPurpose)
│           │           ├─ commissionRight (multi)
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/commissionRight)
│           │           ├─ systemRole (multi; app-nära)
│           │           │   (https://id.ena-
infrastructure.se/attributes/health/systemRole)
│           │           └─ healthcareProfessionalLicenceSpeciality
(multi)
│           │               (https://id.ena-
infrastructure.se/attributes/health/healthcareProfessionalLicenceS
peciality)
│           │
│           ├─ electedOfficial (0..n politiskt uppdrag)
│           ├─ contractor  (0..n konsult uppdrag)
│           └─ student (elev)
│
└─ Machine (systemtjänst/robot)
   ├─ clientId / certificateDn
   ├─ domain
   └─ entitlements[]
```

Bilaga 3

AID-roller inom socialtjänstens område

Nedan listas de AID-roller som ingår i etikettområdet *Arbete inom individ-, familje- och äldreomsorg m.m*, i kompakt form. För respektive AID-kod finns fördjupande ansvarskoder etc på skr.se. Källa: https://extra.skr.se/skr/arbetsgivarekollektivavtal/lonebildning/arbetsidentifikationaid/etikettlistaaid.80445.html

Socialtjänst – myndighetsutövning och utredning

Socialsekreterare, barn och unga, myndighetsutövning
Utreder, planerar, analyserar eller utvärderar ärenden inom området barn och unga.
Kod: 351008

Socialsekreterare, ekonomiskt bistånd
Utreder, planerar och fattar beslut inom ekonomiskt bistånd.
Kod: 351009

Socialsekreterare, övrigt
Utreder och planerar inom individ- och familjeomsorgen.
Kod: 351010

Fältsekreterare
Uppsökande och förebyggande arbete riktat mot barn och unga.
Kod: 351011

Socialsekreterare, biståndsbedömare
Bedömer och utvärderar hjälpbehov inom IFO, äldreomsorg och funktionsnedsättning.
Kod: 351012

Familjerådgivare
Ger stöd, rådgivning och konfliktlösning till familjer.
Kod: 351013

Integrationshandläggare
Utreder och bedömer hjälpbehov för flyktingar.
Kod: 351014

Behandling, stöd och pedagogiskt arbete

Behandlingsassistent / Socialpedagog
Socialt förändrings- och motivationsarbete med barn, unga eller vuxna.
Kod: 351015

Arbetsmarknadskonsulent
Planerar och genomför insatser mot arbete för arbetssökande.
Kod: 351016

Funktionsnedsättning – stöd och omsorg

Stödpedagog, funktionsnedsättning
Ger pedagogiskt stöd och individanpassad vägledning.
Kod: 351030

Stödassistent / Vårdare, gruppboende
Ger individanpassat vardagsstöd på grupp- och korttidsboenden.
Kod: 351031

Stödassistent / Vårdare, dagverksamhet
Stödjer personer med funktionsnedsättning i daglig verksamhet.
Kod: 351032

Vårdbiträde / Stödbiträde, funktionsnedsättning
Utför brukarnära omsorgsarbete.
Kod: 351033

Boendestödjare, hemmiljö, funktionsnedsättning
Ger individuellt stöd i hemmiljö eller stödboende.
Kod: 351034

Socialpsykiatri

Skötare / Boendestödjare, hemmiljö, socialpsykiatri
Vård- och stödarbete inom socialpsykiatrisk verksamhet.
Kod: 351035

Personlig assistans och anhörigstöd

Personlig assistent
Ger stöd, service och omvårdnad enligt sociallagstiftning.
Kod: 351040

Anhörigvårdare
Ger omvårdnad i hushållsgemenskap med funktionsnedsatt person.
Kod: 351041

Övriga roller

Socialt arbete, annat
Används endast när ingen annan etikett är rimlig.
Kod: 351090

Kurativt arbete

Kurator
Kurativt stödarbete.
Kod: 352010

Kurativt arbete, annat
Endast när ingen annan kurativ etikett passar.
Kod: 352090