VGR behörighetsportal, teknisk dokumentation v.1.0
Datum

Anslutningsdokument - administrativa medarbetaruppdrag (AMU)

Innehåll

Anslutningsdokument - administrativa medarbetaruppdrag (AMU) 1

Sammanfattning 2

Så här funkar det 3

Applikation, domän och onboarding 4

AMU och applikationsroller 4

Beställning och godkännande 4

Tilldelning och livscykel 4

Uppföljning och spårbarhet 5

Så här gör du – steg för steg 5

Applikationsroller (AMU) 8

Frågor och vidare information 12

VÄSTRA GÖTALANDSREGIONEN

VGR behörighetsportal (Omada Identity) hanterar beställning, godkännande och tilldelning av behörigheter till verksamhetens IT-system. För applikationer som använder administrativa medarbetaruppdrag (AMU) sker behörighetsstyrningen genom att behörighetsportalen hanterar medlemskap i AMU och förmedlar dessa vidare till VGR:s gemensamma behörighetsinfrastruktur.

AMU används inom VGR för att styra administrativa behörigheter som inte omfattas av patientdatalagen och bygger på den nationella behörighetsmodellen inom HSA. Ett AMU tillhör ett behörighetsområde (domän) och används av applikationer som underlag för åtkomst, roller eller funktioner.

När en applikation ansluts till VGR behörighetsportal för AMU innebär det att applikationens behörigheter görs beställningsbara i portalen. Behörighetsportalen säkerställer då att rätt uppdrag tilldelas rätt person, efter fastställda godkännandeflöden, och att tilldelning och borttag av AMU sker automatiskt i de gemensamma katalog- och behörighetstjänster som applikationen förlitar sig på.

Syftet med detta dokument är att ge en tydlig och praktisk vägledning för hur en applikation som använder AMU ansluts till VGR behörighetsportal. Dokumentet beskriver vad som behöver vara på plats inför anslutning, vilket underlag som krävs från systemägare och applikationsansvariga, samt vad anslutningen innebär i form av standardiserad behörighetsbeställning, spårbarhet, godkännanden och automatiserad livscykelhantering av AMU-medlemskap.

Sammanfattning

- Vad & varför: Dokumentet beskriver hur en applikation som använder administrativa medarbetaruppdrag (AMU) ansluts till VGR behörighetsportal (Omada Identity) för att säkerställa en enhetlig, spårbar och kontrollerad hantering av administrativa behörigheter genom hela livscykeln.
- Vem: Riktar sig till t.ex. informationsägare, systemägare, applikationsansvariga samt berörda resursägare som ansvarar för applikationens behörighetsmodell, användning av AMU och

koppling till VGR:s gemensamma behörighets- och katalogtjänster.

- Hur: Applikationens behörigheter modelleras som applikationsroller i VGR behörighetsportal och kopplas till ett eller flera AMU inom en definierad domän. behörighetsportalen hanterar beställning, godkännande samt tilldelning och borttag av medlemskap i AMU enligt fastställda godkännandeflöden samt regler och policys som kan baseras på olika verksamhetsattribut.
- När: Processen startar när en applikation ska börja använda VGR behörighetsportal för hantering av AMU och genomförs i fyra steg:
  Förberedelser → Beställning → Konfiguration → Test & driftsättning.

Var: Grunddata för AMU, såsom domäner och vilka uppdrag som ska vara beställningsbara, hanteras i KIV. Dessa uppgifter görs tillgängliga i VGR behörighetsportal, där beställning, godkännande och livscykelhantering av AMU-medlemskap sker. Anslutning av en ny applikation initieras via Serviceportalen.

Resultat: Anslutningen ger en standardiserad och centraliserad hantering av AMU, inklusive självservicebeställning, stöd för godkännandeflöden samt automatisk tilldelning och borttag av AMU-medlemskap baserat på fastställda regler och policys. Lösningen ger full spårbarhet samt underlag för uppföljning och återkommande granskning av behörigheter.

Så här funkar det

Översikt

När en applikation ansluts till VGR behörighetsportal för hantering av Administrativa medarbetaruppdrag (AMU) innebär det att tilldelning och borttag av medlemskap i AMU hanteras centralt och enhetligt genom VGR behörighetsportal. Själva definitionen av AMU och tillhörande domäner förvaltas i KIV, medan VGR behörighetsportal

används för att styra vem som ska ha vilket uppdrag och under vilka förutsättningar.

Applikation, domän och onboarding

För varje ansluten applikation skapas en applikation i VGR behörighetsportal som motsvarar en AMU-domän. Applikationen kopplas till ett hsaDomainCode och utgör därmed en förutsättning för att AMU ska kunna exponeras och hanteras via VGR behörighetsportal.
Applikationen behöver vara ansluten till VGR behörighetsportal innan AMU inom motsvarande domän görs beställningsbara och tillgängliga för behörighetsportalen i KIV.

AMU och applikationsroller

AMU definieras i KIV, där det även styrs vilka uppdrag som ska vara möjliga att beställa. När AMU görs beställningsbara i KIV skapas motsvarande applikationsroller automatiskt i VGR behörighetsportal. Varje applikationsroll motsvarar ett AMU, och beställning av en roll innebär tilldelning av medlemskap i det tillhörande AMU.

Beställning och godkännande

VGR behörighetsportal fungerar som det gemensamma gränssnittet för beställning, godkännande och livscykelhantering av AMU-medlemskap. När en användare beställer en applikationsroll och beställningen godkänns enligt fastställda godkännandeflöden, säkerställer VGR behörighetsportal att användaren tilldelas rätt AMU-medlemskap.

Tilldelning och livscykel

Tilldelning och borttag av AMU-medlemskap sker via VGR behörighetsportal baserat på beviljade beställningar och kan även styras av regler och policys som tar hänsyn till exempelvis organisatorisk tillhörighet, roll eller andra verksamhetsattribut. Detta möjliggör både manuell hantering med godkännandeflöden och

automatisering av tilldelning och återkallelse när förutsättningarna för åtkomst förändras.

Vid manuell beställning kopplas medlemskapet i AMU till den förvaltning som anges vid beställningstillfället. Om användarens koppling till förvaltningen upphör återkallas även medlemskapet i AMU, och behörigheten behöver i så fall beställas på nytt vid behov. Detta säkerställer att AMU-medlemskap alltid är kopplade till ett aktuellt och giltigt organisatoriskt sammanhang.

Uppföljning och spårbarhet

Genom att använda VGR behörighetsportal för hantering av AMU-medlemskap får applikationen stöd för hela behörighetslivscykeln, från kontrollerad tilldelning till återkallelse, med full spårbarhet samt underlag för uppföljning och återkommande granskning av behörigheter.

Så här gör du – steg för steg

Anslutning av en applikation som använder Administrativa medarbetaruppdrag (AMU) till VGR behörighetsportal genomförs i ett antal tydliga steg. Processen beskriver hur anslutningen initieras, sätts upp, testas och tas i drift utifrån VGR:s gemensamma arbetssätt. Test- och produktionsprocessen följer samma principer och ordning för att säkerställa ett korrekt och förutsägbart resultat.

Steg 1 – Förberedelser

Innan anslutning påbörjas behöver följande vara på plats:

- Applikationen ska använda AMU som grund för sin behörighetsstyrning
- Applikationen ska utgöra en egen AMU-domän och ha ett definierat hsaDomainCode
- Systemägare och relevanta kontaktpersoner för applikationen ska vara identifierade.

AMU kan skapas och förvaltas i KIV i detta skede, men får inte göras beställningsbara innan applikationen är korrekt ansluten till VGR behörighetsportal.

Steg 2 – Beställ anslutning

Anslutning av applikationen initieras genom en beställning via Serviceportalen enligt VGR:s ordinarie process för anslutning till VGR behörighetsportal.

Beställning görs via kunskapsartikel (KB).
Beställningen ska innehålla:

- ifylld Excel-fil *”Ansökan anslutning VGR behörighetsportal.xlsx”*
- information om applikationen enligt formulärets fält
- angivet hsaDomainCode
- systemägare samt kontaktperson(er) för anslutningen

Excel-filen bifogas i ärendet och utgör det formella underlaget för anslutningen.

Steg 3 – Onboarding i VGR behörighetsportal

När beställningen är mottagen och komplett genomförs onboarding av applikationen i VGR behörighetsportal. Detta innebär att:

- applikationen skapas i VGR behörighetsportal
- koppling till angivet hsaDomainCode etableras

Applikationen måste vara ansluten till i VGR behörighetsportal innan AMU inom motsvarande domän görs beställningsbara och tillgängliga för behörighetsportalen i KIV.

Steg 4 – Förberedelser inför test

När applikationen är ansluten till VGR behörighetsportal kan arbetet med testförberedelser påbörjas. Detta sker i **testmiljö** och omfattar:

- verifiering av att applikationen finns korrekt upplagd i VGR behörighetsportal testmiljö
- säkerställande av att testmiljön är ansluten till KIV testmiljö
- förberedelse för mottagande av AMU från KIV testmiljö

Steg 5 – Konfiguration i testmiljö

När förberedelserna är klara genomförs konfiguration i VGR behörighetsportal testmiljö, enligt samma principer och ordning som senare används i produktionsmiljön.

I detta steg:

- konfigureras applikationen i testmiljön med korrekt hsaDomainCode
- konfigureras mottagande av AMU från KIV testmiljö
- konfigureras godkännandeflöden baserat på VGR:s standardstöd samt de uppgifter som angivits i beställningen

När applikationen är korrekt skapad och konfigurerad i testmiljön kan AMU inom applikationens domän markeras som beställningsbara i KIV testmiljö, vilket gör dem tillgängliga för test i VGR behörighetsportal (test).

Steg 6 – Test och verifiering

Test och verifiering genomförs i VGR behörighetsportal testmiljö, i samverkan mellan:

- teamet för VGR behörighetsportal
- KIV-teamet
- representanter för den anslutande applikationen

Syftet är att gemensamt verifiera att:

- AMU läses in korrekt från KIV testmiljö
- AMU skapas som applikationsroller i VGR behörighetsportal
- beställning och godkännande fungerar enligt konfigurerade flöden
- medlemskap i AMU tilldelas och återkallas korrekt
- applikationen konsumerar AMU enligt avsett arbetssätt

Testmiljön används för att säkerställa att flöden, ordning och beteende motsvarar den kommande produktionssättningen. När samtliga parter bedömer att lösningen fungerar enligt förväntan kan driftsättning godkännas.

Steg 7 – Driftsättning och beställningsbarhet i produktion

Efter godkänd test och verifiering genomförs driftsättning i **produktionsmiljön**. Detta sker enligt samma process som i testmiljön och innebär att:

- Applikationen skapas och konfigureras i VGR behörighetsportal produktionsmiljö,
- Godkännandeflöden etableras enligt VGR:s standardstöd och uppgifterna i beställningen,
- AMU inom applikationens domän markeras som beställningsbara i KIV produktionsmiljö.

Först efter detta steg blir AMU tillgängliga för beställning i VGR behörighetsportal (produktion), och tilldelning och borttag av AMU-medlemskap sker för verkliga användare.

Tekniska riktlinjer

Applikationsroller (AMU)

Tilldelning av medlemskap i Administrativa medarbetaruppdrag (AMU) i VGR behörighetsportal kan ske på två huvudsakliga sätt: automatisk tilldelning via policy eller manuell beställning med godkännande. Båda sätten kan användas parallellt beroende på applikationens och verksamhetens behov.

Automatisk tilldelning via policy

Automatisk tilldelning via policy rekommenderas när det finns tydliga och stabila regler för vilka personer som ska ha ett visst AMU. Genom att använda tilldelningspolicys minimeras behovet av manuella beställningar och risken för felaktiga eller kvarhängande behörigheter.

Tilldelningspolicys konfigureras i VGR behörighetsportal och:

- bygger på identitetsattribut från KIV
- gäller alltid utan godkännande och utan undantag
- ska ha dokumenterad målpopulation, logik och ägare

Logiken för tilldelningspolicys baseras på en kombination av identitetsvy och/eller kontext, vilka tillsammans avgör vilka personer som träffas av policyn. För AMU innebär detta att policyn automatiskt tilldelar och återkallar medlemskap i ett eller flera AMU när villkoren är uppfyllda.

Exempel på information som kan användas i policys:

- organisatorisk tillhörighet
- roll eller uppdrag
- kontext, såsom förvaltningstillhörighet

Manuell beställning

Manuell beställning används när medlemskap i AMU kräver ett aktivt godkännande eller när tilldelningen avviker från generella regler. Beställning sker via VGR behörighetsportal och följer konfigurerade godkännandeflöden.

Manuell beställning är lämplig exempelvis när:

- behörigheten är känslig eller särskilt skyddsvärd
- tilldelningen är tidsbegränsad eller undantagsbaserad
- verksamheten kräver individuell prövning av åtkomst

Vid manuell beställning kopplas medlemskapet i AMU till den kontext (förvaltning) som anges vid beställningstillfället, vilket påverkar hur livscykel och återkallelse hanteras.

Rådgivning kring policys

Möjligheterna för automatisk tilldelning via policy är flexibla och kan anpassas efter olika behov och förutsättningar. Om ni har frågor kring vad som är möjligt, eller vill diskutera olika alternativ och upplägg för policys kopplat till AMU, är ni välkomna att kontakta VGR behörighetsportal: behorighetsportal@vgregion.se

Godkännandeflöde (AMU)

Vid manuell beställning av medlemskap i Administrativa medarbetaruppdrag (AMU) används godkännandeflöden för att säkerställa att tilldelning av behörighet sker med rätt kontroll och ansvar. För varje applikation väljs ett godkännandeflöde, alternativt en kombination av flera flöden i sekvens, till exempel att en beställning först godkänns av linjechef och därefter av systemägare.

Val av godkännandeflöde görs per applikation och baseras på verksamhetens behov samt de uppgifter som angivits vid anslutning.

Tillgängliga godkännandeflöden

I VGR behörighetsportal finns i nuläget följande typer av godkännanden som kan användas för AMU:

- Linjechef
- Systemägare
- Resursägare

Dessa kan användas var för sig eller kombineras i flerstegsgodkännande.

Linjechef

Linjechef avser den närmaste chefen för den person som beställningen avser, baserat på personens primära engagemang i KIV. Detta godkännandeflöde livscykelhanteras automatiskt och kräver ingen manuell uppdatering vid organisationsförändringar, under förutsättning att informationen om chef och engagemang hålls uppdaterad i KIV.

Resursägare (AMU-specifikt)

För AMU finns ett särskilt stöd för resursägare genom att attributet hsaAdminCommissionResponsiblePerson läses in automatiskt från KIV och används som resursägare i VGR behörighetsportal. Detta är en central del av AMU-lösningen och har tagits fram för att möta verksamhetens behov av tydligt och korrekt ansvar för administrativa uppdrag.

- Endast en person kan anges som hsaAdminCommissionResponsiblePerson i KIV.
- Denna person livscykelhanteras automatiskt via KIV och kräver ingen manuell uppdatering i VGR behörighetsportal.

Utöver den automatiskt inlästa resursägaren är det även möjligt att i VGR behörighetsportal lägga till ytterligare manuella resursägare. Dessa livscykelhanteras inte automatiskt, vilket innebär att applikationsansvariga ansvarar för att hålla informationen uppdaterad vid förändringar, till exempel när:

- en person slutar eller byter roll

- nya resursägare tillkommer
- befintliga resursägare ska tas bort

Systemägare

Systemägare kan användas som godkännare i ett eller flera steg i godkännandeflödet. Det är möjligt att ange en eller flera personer som systemägare för en applikation.

Till skillnad från linjechef och resursägare via hsaAdminCommissionResponsiblePerson livscykelhanteras systemägare inte automatiskt. Det är därför applikationsägarens ansvar att säkerställa att information om systemägare är korrekt och att meddela VGR behörighetsportal vid förändringar, till exempel när:

- en systemägare slutar eller byter roll
- ansvaret flyttas till annan person
- ytterligare systemägare tillkommer eller tas bort

Sammanfattning av ansvar och livscykelhantering

- Linjechef: livscykelhanteras automatiskt via KIV
- Resursägare via hsaAdminCommissionResponsiblePerson: livscykelhanteras automatiskt via KIV
- Manuella resursägare: kräver manuell uppdatering
- Systemägare: kräver manuell uppdatering

Godkännandeflöden är endast aktuella vid manuell beställning. Vid automatisk tilldelning via policy används inga godkännanden.

Revision

Revision används för att regelbundet granska och bekräfta att manuellt tilldelade medlemskap i Administrativa medarbetaruppdrag (AMU) fortfarande är motiverade och korrekta. Syftet är att säkerställa att behörigheter inte kvarstår längre än nödvändigt och att ansvariga tar ställning till fortsatt behov.

I VGR behörighetsportal finns stöd för att sätta upp revisioner där utpekade personer får i uppgift att besluta om ett AMU-medlemskap ska:

- behållas

- återkallas

  Revision är främst relevant för manuellt beställda AMU-medlemskap, eftersom automatiskt tilldelade medlemskap via policy redan styrs kontinuerligt av uppsatta regler och attribut.

  Vilka som deltar i revisionen (t.ex. linjechef, systemägare eller resursägare) samt hur ofta granskning ska ske konfigureras enligt verksamhetens behov.

  För att sätta upp eller ändra revision för AMU i VGR behörighetsportal, kontakta behörighetsteamet: behorighetsportal@vgregion.se

  Frågor och vidare information

  - **Beställning:**
    Kunskapsdokument (KB) KB0028399 – VGR behörighetsportal – ansökan om anslutning
    Excelunderlag:
    Ansökan anslutning VGR behörighetsportal.xlsx
    (finns som bifogad fil i KB0028399)
  - **Kontakt:**
    behorighetsportal@vgregion.se
  - **Insidan:**
    https://insidan.vgregion.se/forvaltningar/koncernkontoret/stod-och-tjanster/system-a-o/vgr-behorighetsportal/