

Inledning och generell beskrivning

Innehåll

Inledning och generell beskrivning	1
Syfte och målgrupp	2
Översikt av VGR behörighetsportal	2
Övergripande arkitektur och integrationsprinciper	3
Anslutningsmodeller till VGR behörighetsportal	3
Styrning av behörigheter i VGR behörighetsportal	5
Beställnings- och godkännandeprocess	5
Tilldelningspolicy och automatisering	5
Process för anslutning till VGR behörighetsportal	5
Val av anslutningsmodell	6
Relaterade dokument och nästa steg	7

Syfte och målgrupp

Detta dokument ger en övergripande beskrivning av VGR behörighetsportal och de huvudsakliga möjligheterna för att ansluta nya system. Syftet är att ge systemägare, projektledare, arkitekter och leverantörer en gemensam förståelse för anslutningsprinciper, rekommenderade integrationsvägar och övergripande kravbild.

Dokumentet fungerar som en introduktion och vägledning inför anslutningsarbete och upphandling. För detaljerade tekniska instruktioner hänvisas till respektive anslutningsguide och kompletterande kravdokument.

Översikt av VGR behörighetsportal

Vad är VGR behörighetsportal

VGR behörighetsportal är Västra Götalandsregionens centrala plattform för styrning och administration av identiteter och behörigheter. Lösningen baseras på Omada Identity och utgör regionens stöd för Identity Governance and Administration (IGA) för hantering av konton, roller och åtkomsträttigheter i anslutna system.

Plattformen möjliggör automatiserad livscykelhantering av identiteter, policybaserad tilldelning av behörigheter, beställnings- och godkännandeprocesser samt uppföljning och granskning. Syftet är att säkerställa att rätt personer har rätt åtkomst vid rätt tidpunkt, i enlighet med gällande regelverk och säkerhetskrav.

Grundläggande begrepp

VGR behörighetsportal bygger på ett antal centrala begrepp inom Identity Governance and Administration. Med identitet avses en digital representation av en person. Ett konto är en teknisk representation av identiteten i ett system. Resurser utgör behörigheter eller åtkomsträttigheter, exempelvis grupper eller applikationsroller, som kan tilldelas ett konto.

System delas in i logiska system, exempelvis applikationer, och fysiska system, exempelvis katalogtjänster där konton och behörigheter lagras. Tilldelning av behörigheter kan ske via roller eller policyer och hanteras genom automatiserad eller manuell provisionering, baserat på fastställda regler och godkännandeprocesser.

Övergripande arkitektur och integrationsprinciper

Masterdata och styrande informationskällor

VGR behörighetsportal bygger på att identitets- och organisationsdata är korrekt och strukturerat enligt regionens masterdata. KIV utgör masterkälla för identitet, organisation och engagemang, och dessa uppgifter ligger till grund för styrning av behörigheter i plattformen.

Tilldelningspolicyer styrs av definierade attribut, exempelvis primärt engagemang, anställningsform och AID-kod. Utifrån dessa kriterier tilldelas behörigheter automatiskt. För att undvika övertilldelning krävs att attribut är korrekt definierade och konsekvent tillämpade i masterdata.

Principer för anslutning

Anslutning av system till VGR behörighetsportal ska i första hand baseras på etablerade och standardiserade integrationsmönster. Befintliga och redan konfigurerade integrationer, exempelvis mot Active Directory, ska nyttjas där det är möjligt för att minska komplexitet och införandetid.

Anslutningen ska utformas så att behörighetsstyrning sker centralt i VGR behörighetsportal, med så liten grad av systemspecifik anpassning som möjligt. Standardprotokoll och konfigurationsbaserade lösningar ska prioriteras framför kundspecifik utveckling.

Anslutningsmodeller till VGR behörighetsportal

Rekommenderad anslutningsmodell – via Active Directory (AD)

Anslutning via AD är i nuläget den primärt rekommenderade modellen. VGR behörighetsportal har en etablerad och fungerande integration mot AD, vilket möjliggör hantering av behörigheter genom medlemskap i definierade AD-grupper.

Genom att anslutande system bygger sin behörighetsmodell på AD-grupper kan införandet ske med kortare ledtid och lägre teknisk komplexitet. Modellen förutsätter att systemet kan konsumera behörighet via gruppmedlemskap samt att grupper utformas enligt gällande krav, exempelvis avseende grupptyp och namngivningsstandard.

Anslutning via AMU

För applikationer som använder administrativa medarbetaruppdrag (AMU) sker behörighetsstyrningen genom att VGR behörighetsportal 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 och används av applikationer som underlag för åtkomst, roller eller funktioner.

Denna anslutningsmodell är relevant för system som är anpassade för att använda AMU som behörighetsbärare. Detaljerade tekniska krav framgår av Anslutningsguide AMU.

Direktanslutning via API och standardprotokoll

Utöver AD och AMU finns möjlighet att ansluta system direkt till VGR behörighetsportal via API och etablerade standardprotokoll, exempelvis SCIM 2.0, REST, OData, SOAP, LDAP eller SQL. Plattformen har stöd för både import av data och provisionering till anslutande system.

Direktanslutning förutsätter att systemet har dokumenterat integrationsstöd och att tekniska förutsättningar analyseras innan arbetet påbörjas. Det behöver verifieras att systemet kan hantera relevanta objekt såsom användarkonton, resurser, exempelvis roller, behörighetsobjekt eller grupper, samt resurstilldelningar, det vill säga kopplingar mellan konto och behörighet.

Beroende på systemets arkitektur, datamodell och integrationsmöjligheter kan denna anslutningsmodell innebära varierande grad av anpassning och utvecklingsinsats. Omfattning och komplexitet fastställs i samband med analysfasen.

Manuell provisionering (kommer att finnas på plats längre fram)

I de fall ett system saknar tekniskt integrationsstöd för automatiserad provisionering kan behörighet hanteras genom manuell process. Beställning och godkännande sker då via VGR behörighetsportal, medan själva tilldelningen genomförs manuellt i det anslutande systemet enligt fastställd rutin.

Även vid manuell provisionering tillämpas samma krav på beställnings- och attestprocess samt spårbarhet. Denna modell bör betraktas som ett undantag och är aktuell när teknisk integration inte är möjlig eller inte bedöms vara ändamålsenlig.

Styrning av behörigheter i VGR behörighetsportal

Beställnings- och godkännandeprocess

All tilldelning av behörigheter i VGR behörighetsportal föregås av en strukturerad beställnings- och godkännandeprocess. Åtkomst kan beställas via självservice, av chef eller av administrativ funktion, beroende på roll och ansvar.

Godkännande kan konfigureras i ett eller flera steg och utförs exempelvis av linjechef, systemägare eller resursägare. Processen säkerställer att behörigheter endast tilldelas efter formell prövning och att beslut är spårbara.

Tilldelningspolicy och automatisering

Utöver beställningsstyrd tilldelning kan behörigheter tilldelas automatiskt genom definierade tilldelningspolicyer. Policyer baseras på styrande attribut från masterdata, exempelvis primärt engagemang, anställningsform eller AID-kod, och aktiveras när angivna kriterier är uppfyllda.

Automatiserad tilldelning är en central princip i VGR behörighetsportal och används för att förenkla administrationen, minska manuell hantering och säkerställa en konsekvent tillämpning av regelverk. Målsättningen är att i så hög utsträckning som möjligt styra behörigheter genom policybaserade mekanismer snarare än genom individuella beställningar.

Denna modell möjliggör effektiv livscykelhantering i samband med förändringar såsom nyanställning, byte av uppdrag eller avslut. Korrekta och strukturerade masterdata är en förutsättning för att undvika övertilldelning och säkerställa att behörigheter speglar faktisk organisatorisk tillhörighet.

Process för anslutning till VGR behörighetsportal

Initiering

Anslutning av ett nytt system till VGR behörighetsportal initieras genom en formell beställning via Serviceportalen enligt gällande rutin. Beställningen ska innehålla relevant underlag om systemets funktion, behörighetsmodell och tekniska integrationsmöjligheter.

Efter mottagen beställning genomförs en inledande dialog och prioritering. Syftet är att fastställa lämplig anslutningsmodell och planera fortsatt analys- och genomförandearbete.

Analys och genomförande

Efter initiering genomförs en analys av systemets behörighetsmodell, tekniska förutsättningar och integrationsmöjligheter. Analysen syftar till att fastställa lämplig anslutningsmodell, identifiera eventuella anpassningsbehov och bedöma omfattning och komplexitet.

Utifrån analysens resultat konfigureras VGR behörighetsportal och, vid behov, anpassas det anslutande systemet för att möjliggöra styrd och spårbar hantering av konton och behörigheter. Målsättningen är att i första hand använda konfigurationsbaserade och standardiserade lösningar.

Val av anslutningsmodell

Val av anslutningsmodell ska baseras på systemets behörighetsmodell, tekniska integrationsmöjligheter och krav på automatisering. Nedanstående principer utgör vägledning vid val av modell.

- **Active Directory (AD)** ska väljas när systemet kan hantera behörigheter via AD-grupper. Detta är den rekommenderade modellen då integrationen är etablerad och förvaltningsbar, bygger på en standardiserad gruppbaserad behörighetsstruktur och normalt medför lägre teknisk komplexitet samt kortare införandetid.
- **AMU** är lämpligt när systemet använder Administrativa medarbetaruppdrag enligt HSA-modellen och är anpassat för att konsumera AMU som grund för behörighetsstyrning inom VGR:s gemensamma behörighetsinfrastruktur.
- **Direktintegration via API och standardprotokoll** behöver analyseras när behörighetsstyrning inte kan ske via AD eller AMU och systemet erbjuder ett dokumenterat integrationsgränssnitt för strukturerad hantering av konton och behörigheter.

Manuell hantering är aktuell när teknisk integration inte är möjlig eller inte bedöms vara ändamålsenlig. Även i dessa fall ska beställning, godkännande och spårbarhet ske via VGR behörighetsportal. (Arbetas på en lösning, ej på plats i dagsläget)

Slutligt val av anslutningsmodell fastställs efter genomförd analys av systemets förutsättningar.

Relaterade dokument och nästa steg

Detta dokument utgör en övergripande introduktion till anslutning av system till VGR behörighetsportal. För detaljerade tekniska krav och genomförandeanvisningar hänvisas till separata anslutningsguider.

I nuläget finns anslutningsguider för Active Directory (AD) och AMU, vilka beskriver respektive anslutningsmodell mer ingående.

Dokumentationen kommer att kompletteras med ytterligare styrande material, bland annat avseende anslutning via standardprotokoll samt tekniska krav vid upphandling av nya IS/IT-tjänster.