VGR behörighetsportal, teknisk dokumentation v.1.0
Datum

Anslutningsdokument - direktintegration via API och standardprotokoll

Innehåll

Anslutningsdokument - direktintegration via API och standardprotokoll 1

Sammanfattning 6

När ska denna anslutningsguide användas? 6

Målgrupp och ansvar 8

Så här funkar det 11

- Översikt 12
- Direktintegration jämfört med AD och AMU 13
- Konton, resurser och tilldelningar 14
- Import, provisionering och avstämning (reconciliation) 15
- Automatiserad, manuell och vidarebefordrad provisionering 16
- Önskat och faktiskt läge 17

Rekommenderad logisk datamodell för anslutning 19

- Grundprinciper 19
- Konto 20
- Behörighetsresurs 22

Resurstilldelning 23
Kontext, organisatoriskt sammanhang 24
Identifierare och livscykel 25
Tillämpning per anslutningstyp 26
Val av integrationsmodell 28
Anslutningsätt och protokoll 29
SCIM 2.0, rekommenderat förstahandsval där det är möjligt 30
REST API 31
SOAP 32
OData 33
LDAP 34
SQL 36
Filbaserad import 37
Manuell eller vidarebefordrad provisioning 38
Så här gör du steg för steg 40
Kontrollera om AD eller AMU kan användas 40
Beställ anslutning 40
Kartlägg behörighetsmodellen 41
Kartlägg tekniska integrationsförutsättningar 41
Välj integrationsmodell 41
Ta fram lösningsdesign och kravbild 42
Konfiguration i testmiljö 42
Test och verifiering 42
Driftsättning 43

Förvaltning och förändring 43
Det här behöver vi från dig 43
Det här får du automatiskt 44
Tekniska riktlinjer, kortversion 45
Rekommendationer vid upphandling 48
Teknisk kravbilaga, detaljerade specifikationer 50
Frågor och mer information 56

VGR behörighetsportal (Omada Identity) hanterar beställning, godkännande, tilldelning och borttag av behörigheter till verksamhetens IT-system. I de fall en applikation inte lämpligen kan anslutas via Active Directory (AD) eller administrativa medarbetaruppdrag (AMU) kan direktintegration via API eller standardprotokoll vara ett alternativ.

Direktintegration innebär att VGR behörighetsportal integrerar direkt med det anslutande systemet, eller med ett integrationslager framför systemet, för att läsa in och/eller provisionera konton, behörighetsresurser och resurstilldelningar. Exempel på möjliga anslutningssätt är SCIM 2.0, REST API, SOAP, OData, LDAP, SQL och filbaserad import. Vilket anslutningssätt som är lämpligt beror på systemets behörighetsmodell, tekniska integrationsstöd, säkerhetskrav och krav på automatisering.

Denna anslutningsmodell används när behörighetsstyrning behöver hanteras mer direkt mot målssystemet än vad som är möjligt via AD eller AMU. Det kan till exempel vara aktuellt när systemet har en egen intern behörighetsmodell, när behörigheter behöver hanteras som applikationsroller eller resurser i systemet, eller när det finns behov av att läsa och stämma av aktuellt behörighetsläge direkt från systemet.

Syftet med detta dokument är att ge en tydlig och praktisk vägledning för hur ett system kan anslutas till VGR behörighetsportal genom direktintegration. Dokumentet beskriver hur systemets behörighetsmodell bör analyseras, vilka tekniska förutsättningar som behöver vara på plats och hur olika anslutningssätt kan användas på ett sätt som är standardiserat, förvaltningsbart och långsiktigt hållbart.

Vid direktintegration rekommenderas i första hand att använda etablerade standarder och konfigurationsbaserade integrationsmönster. SCIM 2.0 bör väljas där det är möjligt, eftersom standarden är framtagen för identitetshantering och har en tydlig modell för användare, grupper och resurser. Även andra anslutningssätt, exempelvis REST, SOAP, OData, LDAP eller SQL, kan

vara lämpliga om de ger en stabil och tydlig modell för konton, resurser och tilldelningar.

Oavsett tekniskt anslutningssätt bör integrationen utformas så att VGR behörighetsportal kan arbeta mot en logisk och begriplig behörighetsmodell. Det innebär att systemets interna tekniska komplexitet, exempelvis interna tabeller, koder, signaturer, grupper, roller eller relationsmodeller, så långt som möjligt bör kapslas in i systemet, API eller ett integrationslager. Målet är att portalen ska kunna styra vem som ska ha vilken åtkomst, och vid behov i vilket organisatoriskt sammanhang, utan att behöva hantera onödig systemspecifik logik.

Direktintegration kan omfatta både import av data från systemet och provisionering till systemet. Import används för att läsa in aktuellt läge, till exempel befintliga konton, behörigheter och tilldelningar. Provisionering används för att skapa, uppdatera eller ta bort konton och behörighetstilldelningar i målssystemet. I vissa fall kan anslutningen införas stegvis, till exempel genom att börja med import eller manuell provisionering och senare gå vidare till mer automatiserad hantering.

Eftersom direktintegration kan se olika ut beroende på systemets förutsättningar behöver anslutningen alltid föregås av en analys. Analysen ska fastställa vilken integrationsmodell som är lämplig, vilka objekt och behörigheter som ska hanteras, hur livscykel och återkallelse ska fungera, vilka säkerhetskrav som gäller samt vilken lösning som är mest kostnadseffektiv och förvaltningsbar över tid.

Den övergripande målsättningen är att skapa en anslutning som möjliggör centraliserad, spårbar och kontrollerad behörighetshantering i VGR behörighetsportal, samtidigt som lösningen hålls så enkel, standardiserad och hållbar som möjligt.

Sammanfattning

Denna guide beskriver hur system kan direktintegreras med VGR behörighetsportal när behörighetsstyrning inte lämpligen kan realiseras via AD-grupper eller administrativa medarbetaruppdrag (AMU).

Direktintegration kan ske via exempelvis SCIM 2.0, REST API, SOAP, OData, LDAP eller SQL, men kan även bygga på filbaserad import och manuell eller vidarebefordrad provisionering när full teknisk integration inte är möjlig eller lämplig. SCIM 2.0 rekommenderas som förstahandsval där ett lämpligt stöd finns, men andra etablerade och supporterade integrationssätt kan vara fullt lämpliga beroende på systemets förutsättningar.

Guiden beskriver hur systemets behörighetsmodell bör mappas till en gemensam logisk modell för konton, behörighetsresurser och resurstilldelningar, hur import, provisionering och avstämning kan utformas samt vilka tekniska och förvaltningsmässiga krav som bör beaktas.

En anslutning ger förutsättningar för central styrning och uppföljning av behörigheter, kontroll över vem som har åtkomst till vad, korrekt tilldelning och återkallelse samt stöd för regelefterlevnad och minskad manuell behörighetshantering.

När ska denna anslutningsguide användas?

Denna anslutningsguide ska användas när ett system ska anslutas till VGR behörighetsportal genom direktintegration via API, standardprotokoll eller annat överenskommet integrationssätt.

Guiden är aktuell när behörighetsstyrning inte lämpligen kan realiseras genom medlemskap i AD-grupper eller genom administrativa medarbetaruppdrag (AMU), och när systemet har, eller kan tillhandahålla, ett tekniskt gränssnitt som kan användas för att läsa information om konton, behörigheter och tilldelningar samt, där provisionering ska automatiseras, skriva förändringar tillbaka till systemet.

Det kan till exempel handla om SCIM 2.0, REST API, SOAP, OData, LDAP, SQL eller filbaserad import. Vilket anslutningssätt som är lämpligt beror på systemets behörighetsmodell, tekniska integrationsstöd, säkerhetskrav, krav på automatisering och hur lösningen ska förvaltas över tid.

Innan direktintegration väljs ska det alltid kontrolleras om behörighetsstyrningen kan realiseras via AD-grupper eller AMU:

- Active Directory (AD-grupper) ska i första hand användas när systemet kan styra åtkomst via gruppmedlemskap.
- AMU ska användas när systemet bygger sin behörighetsstyrning på administrativa medarbetaruppdrag.

Om AD-grupper eller AMU inte är lämpliga eller tillräckliga analyseras direktintegration enligt denna guide.

Direktintegration är ofta mer flexibel än AD- och AMU-baserad anslutning, men innebär också att fler frågor behöver analyseras innan anslutningen kan genomföras. Det behöver bland annat klarläggas hur systemet hanterar konton, vilka behörigheter eller resurser som ska kunna styras, hur tilldelningar representeras, vilka tekniska gränssnitt som finns och om integrationen ska användas för import, provisionering eller båda delarna.

Guiden kan användas både vid anslutning av befintliga system och som stöd vid kravställning av nya system. Vid upphandling eller vidareutveckling bör systemets stöd för standardiserad integration, tydlig behörighetsmodell, stabila identifierare, import, provisionering och avstämning beaktas tidigt. Det minskar risken för specialanpassningar och ger bättre förutsättningar för en långsiktigt förvaltningsbar lösning.

Om systemet saknar tekniskt stöd för direktintegration, till exempel API, standardprotokoll, databasgränssnitt eller filbaserad export/import, kan guiden ändå användas som stöd för att bedöma möjliga alternativ. Det kan exempelvis vara manuell provisionering, vidarebefordrad provisionering eller andra arbetssätt där beställning,

godkännande och spårbarhet hanteras i VGR behörighetsportal även om den tekniska förändringen i målssystemet sker på annat sätt.

Slutligt val av anslutningsmodell görs efter analys av systemets behörighetsmodell, tekniska förutsättningar, säkerhetskrav, förvaltningsbarhet och verksamhetens behov av automatisering.

Målgrupp och ansvar

Detta dokument riktar sig till de roller som är involverade i analys, beslut, anslutning och förvaltning av system som ska direktintegreras med VGR behörighetsportal via API, standardprotokoll eller annat överenskommet integrationssätt.

Eftersom direktintegration kan se olika ut beroende på systemets behörighetsmodell och tekniska förutsättningar behöver både verksamhetsmässiga och tekniska roller vara involverade tidigt. Det behöver vara tydligt vem som ansvarar för vad åtkomsten innebär, hur den ska styras, hur den tekniskt kan hanteras och hur lösningen ska förvaltas över tid.

Beroende på systemets storlek och komplexitet kan en och samma person inneha flera av rollerna nedan. Alla roller behöver inte heller användas separat i varje anslutning. Det viktiga är att relevanta ansvar är identifierade inför anslutning och att kontaktuppgifter och ansvar hålls uppdaterade över tid. Systemägaren ansvarar för att detta säkerställs.

Följande roller är vanligt förekommande involverade:

Systemägare
Här avses rollen "Systemägare" i VGR behörighetsportal. Systemägaren ansvarar för systemet ur ett verksamhets- och säkerhetsperspektiv. Det innebär bland annat att säkerställa att systemets behörighetsmodell är korrekt beskriven, att rätt behörigheter görs tillgängliga för styrning via VGR behörighetsportal och att åtkomst kan motiveras utifrån verksamhetens behov.

Systemägaren ansvarar även för att besluta vilka behörigheter som ska kunna beställas manuellt, vilka som eventuellt ska tilldelas

automatiskt via policy och vilka godkännandeflöden som ska användas. Systemägaren kan även ingå som godkännare vid tilldelning av behörigheter och som ansvarig vid uppföljning eller återcertifiering.

Applikationsansvarig / produktägare

Applikationsansvarig eller produktägare ansvarar normalt för den operativa samordningen av anslutningen. Rollen tar fram eller samordnar det underlag som behövs för analys och implementation, till exempel beskrivning av systemets behörighetsmodell, kontaktvägar till leverantör, teknisk dokumentation och information om miljöer.

Applikationsansvarig ansvarar också för att säkerställa att det anslutande systemet kan använda den valda integrationsmodellen och att systemets funktion verifieras i test innan driftsättning. I praktiken innebär detta ofta ett nära samarbete med systemägare, leverantör och teamet för VGR behörighetsportal.

Informationsägare

Informationsägaren ansvarar för att åtkomst till informationstillgångar i systemet är korrekt utifrån verksamhetens krav, informationsklassning och gällande regelverk. Rollen behöver säkerställa att behörighetsmodellen är förenlig med krav på informationssäkerhet, sekretess och spårbarhet.

Informationsägaren kan behöva bidra till bedömningen av vilka behörigheter som är särskilt känsliga, vilka som kräver godkännande och om det finns behov av regelbunden uppföljning eller återcertifiering.

Resursägare

Resursägare är en mer granulär ansvarsnivå som kan användas när det finns behov av särskilt ansvar för en specifik behörighetsresurs, applikationsroll eller motsvarande objekt i VGR behörighetsportal.

Resursägare behöver inte alltid anges separat. För enklare system, eller där behörighetsmodellen är begränsad, kan ansvar för behörigheter normalt hanteras av systemägare, applikationsansvarig

eller produktägare. Resursägare är främst relevant när ett system har flera behörigheter med olika verksamhetsansvar, när vissa behörigheter är särskilt känsliga eller när godkännande och återcertifiering behöver göras av någon annan än systemägaren.

När resursägare används kan rollen ingå i godkännandeflöden och återcertifieringar. Resursägaren ansvarar då för att ta ställning till tilldelning och fortsatt behov av åtkomst för de resurser som rollen ansvarar för.

För direktintegration är det särskilt viktigt att det är tydligt vad en behörighetsresurs innebär i det anslutande systemet. Namn och beskrivningar på resurser behöver därför vara begripliga ur verksamhetens perspektiv och inte enbart spegla tekniska koder, interna rollnamn eller systembegrepp.

Teknisk systemförvaltare / integrationsansvarig
Teknisk systemförvaltare eller integrationsansvarig ansvarar för systemets tekniska förutsättningar för anslutning. Det omfattar exempelvis API, standardprotokoll, databasgränssnitt, filbaserade gränssnitt, autentisering, nätverk, testmiljöer, felhantering, loggning och teknisk dokumentation.

Rollen behöver kunna beskriva hur systemet hanterar konton, behörigheter, tilldelningar och livscykel, samt om systemet kan stödja import, provisionering eller båda delarna. Om systemet har en komplex intern behörighetsmodell behöver teknisk systemförvaltare bidra till hur denna kan förenklas eller kapslas in i ett integrationsgränssnitt.

Leverantör
Leverantören kan behöva medverka när systemets integrationsstöd, datamodell eller tekniska begränsningar behöver analyseras. Leverantören ansvarar för att beskriva vilka gränssnitt som finns, hur de är avsedda att användas, vilka delar som är supporterade och vilka konsekvenser olika integrationsalternativ får för drift, support och framtida uppgraderingar.

Vid behov av nyutveckling, anpassning eller wrapper ansvarar leverantören normalt för att ta fram lösningsförslag, estimat och teknisk implementation enligt överenskommen kravbild.

Teamet för VGR behörighetsportal

Teamet för VGR behörighetsportal ansvarar för att stödja analys, design, konfiguration, test och driftsättning av anslutningen i VGR behörighetsportal. Teamet bistår med vägledning kring lämplig anslutningsmodell, datamodell, tilldelningssätt, godkännandeflöden, provisionering och uppföljning.

Teamet ansvarar även för att konfigurera relevanta delar i VGR behörighetsportal utifrån godkänt underlag och att samordna test och verifiering tillsammans med berörda roller.

Systemägaren ansvarar för vad åtkomst innebär och vem som ska kunna få den. Applikationsansvarig, teknisk systemförvaltare och leverantör ansvarar för hur åtkomsten kan realiseras tekniskt. Teamet för VGR behörighetsportal ansvarar för hur anslutningen konfigureras och styrs i portalen utifrån överenskommen modell.

Så här funkar det

Direktintegration innebär att VGR behörighetsportal kopplas direkt till ett system, eller till ett integrationslager framför systemet, för att styra och följa upp konton och behörigheter. Till skillnad från AD- och AMU-baserade anslutningar finns det inte en enda standardiserad teknisk modell som alltid används. Anslutningen behöver därför utformas utifrån systemets behörighetsmodell, tekniska gränssnitt och verksamhetens behov av styrning, automatisering och uppföljning.

Gemensamt för direktintegrationer är att VGR behörighetsportal behöver kunna förstå vilka konton, behörighetsresurser och resurstilldelningar som finns i systemet, samt hur dessa ska skapas, uppdateras, tas bort eller stämmas av. I guiden används begreppet behörighetsresurs som ett samlingsnamn för den åtkomst som kan styras i ett anslutet system. Det kan till exempel vara roller, grupper, behörighetsprofiler, åtkomstnivåer, funktioner eller behörighetskoder.

Integration kan ske via exempelvis SCIM 2.0, REST API, SOAP, OData, LDAP, SQL eller filbaserad import. I vissa fall används full automatisering, medan andra system kan anslutas stegvis genom import, manuell provisionering eller vidarebefordrad provisionering.

Målet är att behörigheter ska kunna styras centralt i VGR behörighetsportal med tydligt ansvar, spårbarhet och kontrollerad livscykelhantering, samtidigt som den tekniska lösningen hålls så enkel och förvaltningsbar som möjligt.

Översikt

När ett system kopplas till VGR behörighetsportal via direktintegration skapas en modell i portalen som beskriver systemet och de behörigheter som ska kunna hanteras. Behörigheterna kan motsvara roller, grupper, behörighetsprofiler, åtkomstnivåer eller andra behörighetsresurser i det anslutande systemet.

En direktintegration kan omfatta ett eller flera av följande flöden:

- Import av konton, behörighetsresurser och resurstilldelningar från systemet till VGR behörighetsportal.
- Provisionering av konton, behörighetsresurser och resurstilldelningar från VGR behörighetsportal till systemet, där detta stöds och är lämpligt.
- Avstämning mellan önskat läge i VGR behörighetsportal och faktiskt läge i systemet.
- Manuell eller vidarebefordrad provisionering när full teknisk automation inte är möjlig eller lämplig.

I en automatiserad lösning kan VGR behörighetsportal tilldela eller återkalla åtkomst genom att skriva förändringar till målssystemet. I en enklare eller stegvis införd lösning kan portalen i stället användas för beställning, godkännande, spårbarhet och uppföljning, medan den tekniska ändringen i målssystemet sker manuellt eller via ett annat system.

Vilken nivå av integration som är lämplig fastställs i analysfasen. Då bedöms bland annat vilka objekt som ska hanteras, hur systemets

behörighetsmodell ser ut, vilket tekniskt gränssnitt som finns, vilka säkerhetskrav som gäller och hur lösningen ska förvaltas över tid.

Direktintegration jämfört med AD och AMU

Anslutning via AD och AMU bygger på etablerade modeller där VGR behörighetsportal styr behörighet genom befintliga behörighetsbärare. För AD innebär det normalt att åtkomst realiseras genom medlemskap i AD-grupper. För AMU innebär det att åtkomst styrs genom administrativa medarbetaruppdrag som används av applikationen som underlag för behörighet.

Direktintegration skiljer sig från dessa modeller genom att VGR behörighetsportal integrerar mer direkt med det anslutande systemets egen behörighetsmodell. Det kan innebära att portalen läser och, där det är lämpligt, skriver konton, behörighetsresurser och resurstilldelningar via ett API, ett standardprotokoll, ett databasgränssnitt, filbaserad import eller ett integrationslager.

AD och AMU bör användas när systemet är byggt för att konsumera dessa modeller, eftersom de normalt ger en enklare och mer etablerad anslutning. Direktintegration är aktuell när systemets behörigheter inte kan eller bör styras via AD-grupper eller AMU, till exempel när systemet har egna applikationsroller, interna grupper, behörighetsprofiler, åtkomstnivåer eller andra resurser som behöver hanteras direkt.

Direktintegration ger större flexibilitet, men kräver också mer analys. Det behöver bland annat klarläggas hur systemet representerar konton, vilka behörigheter som ska kunna styras, hur tilldelningar fungerar, vilka tekniska gränssnitt som finns och hur livscykeln för åtkomst ska hanteras. Det behöver också bedömas om integrationen ska omfatta import, provisionering, avstämning eller en kombination av dessa.

Målet är inte att välja den mest avancerade integrationsmodellen, utan den modell som ger bäst balans mellan verksamhetsnytta, säkerhet, automatisering, införandekostnad och långsiktig förvaltningsbarhet. Om AD eller AMU kan uppfylla behovet på ett

enkelt och hållbart sätt bör dessa modeller normalt prioriteras. Om de inte är tillräckliga används denna guide som stöd för att analysera och utforma en lämplig direktintegration.

Konton, resurser och tilldelningar

För att ett system ska kunna direktintegreras med VGR behörighetsportal behöver systemets behörighetsmodell kunna beskrivas på ett strukturerat sätt. I praktiken handlar det om att förstå vilka konton som finns i systemet, vilka behörighetsresurser som kan tilldelas och hur kopplingen mellan konto och behörighet ser ut.

Ett konto är den tekniska representationen av en användare i det anslutande systemet. Kontot kan till exempel motsvara ett användarkonto, en systemanvändare eller annan kontotyp som systemet använder för åtkomst. I många fall behöver kontot kunna kopplas till en identitet i VGR behörighetsportal, till exempel genom en stabil identifierare.

En behörighetsresurs är den åtkomst som kan styras i systemet. Det kan till exempel vara en roll, grupp, behörighetsprofil, åtkomstnivå, funktion, behörighetskod eller annan rättighet. Behörighetsresurser bör ha tydliga namn och beskrivningar så att systemägare, godkännare och beställare kan förstå vad åtkomsten innebär.

En resurstilldelning är kopplingen mellan ett konto och en behörighetsresurs. Det är resurstilldelningen som anger att ett visst konto har en viss åtkomst. Vid direktintegration är det ofta resurstilldelningen som skapas, ändras eller tas bort när en användare får eller förlorar behörighet.

Samma grundmodell kan tillämpas oavsett tekniskt anslutningssätt. I ett SCIM- eller REST-baserat API kan konton, resurser och tilldelningar exponeras som objekt eller endpoints. I LDAP kan motsvarande modell uttryckas genom användarobjekt, grupper och gruppmedlemskap. I SQL kan modellen motsvaras av tabeller, vyer eller relationer. I SOAP eller OData kan den uttryckas genom operationer, entiteter eller relationer i systemets gränssnitt.

Det viktiga är inte att alla system använder exakt samma tekniska struktur, utan att behörighetsmodellen går att översätta till en modell som VGR behörighetsportal kan styra, följa upp och förvalta. Om systemets interna modell är komplex bör komplexiteten i första hand kapslas in i systemet, API eller ett integrationslager, så att VGR behörighetsportal kan arbeta mot en tydlig och stabil modell för konton, behörighetsresurser och resurstilldelningar.

Import, provisionering och avstämning (reconciliation)

En direktintegration kan omfatta både informationsflöden från det anslutande systemet till VGR behörighetsportal och förändringar från VGR behörighetsportal tillbaka till systemet. Import, provisionering och avstämning är centrala delar för att VGR behörighetsportal ska kunna förstå aktuellt behörighetsläge och styra vilket läge som ska gälla.

Import innebär att information hämtas från det anslutande systemet till VGR behörighetsportal. Det kan exempelvis vara konton, behörighetsresurser och resurstilldelningar. Importen ger portalen information om hur systemet faktiskt ser ut och är en viktig grund för bland annat spårbarhet, uppföljning, återcertifiering och avstämning. Import kan ske automatiserat via ett tekniskt gränssnitt eller, när detta inte är möjligt eller lämpligt, genom exempelvis filbaserad import.

Provisionering innebär att VGR behörighetsportal initierar förändringar i det anslutande systemet för att realisera det behörighetsläge som ska gälla. Det kan exempelvis innebära att skapa eller uppdatera ett konto, skapa eller uppdatera en behörighetsresurs eller tilldela och återkalla en behörighet. Provisionering kan ske automatiserat direkt mot systemet, vidarebefordras till ett annat system eller genomföras manuellt beroende på systemets förutsättningar och vald integrationsmodell.

Avstämning (reconciliation) innebär att information om det faktiska läget i det anslutande systemet jämförs med det läge som VGR behörighetsportal förväntar sig. Syftet är att identifiera

skillnader, exempelvis behörigheter som finns i målssystemet men inte motsvaras av en giltig tilldelning i VGR behörighetsportal, eller förändringar som inte har genomförts som avsett. Hur identifierade avvikelser ska hanteras beror på systemets behörighetsmodell och vald integrationslösning.

Import och provisionering behöver inte använda samma tekniska anslutningssätt och behöver inte heller införas samtidigt. Ett system kan exempelvis börja med import för att ge VGR behörighetsportal insyn i befintliga konton och behörigheter och senare kompletteras med automatiserad provisionering. På motsvarande sätt kan automatiserad import kombineras med manuell eller vidarebefordrad provisionering.

Målbilden bör, där systemets förutsättningar medger det, vara att VGR behörighetsportal både har tillförlitlig information om det faktiska läget och kan styra det önskade läget. Detta ger bäst förutsättningar för automatiserad livscykelhantering, spårbarhet och kontroll av behörigheter över tid.

Automatiserad, manuell och vidarebefordrad provisionering

Provisionering från VGR behörighetsportal kan genomföras på olika sätt beroende på det anslutande systemets tekniska förutsättningar och verksamhetens behov. Målsättningen bör vara att automatisera provisioneringen där det är möjligt och lämpligt, men även system som inte stödjer full automatisering kan anslutas och omfattas av portalens styrning av behörigheter.

Automatiserad provisionering innebär att VGR behörighetsportal automatiskt genomför förändringen i det anslutande systemet via det valda tekniska gränssnittet. När en behörighet tilldelas eller återkallas i portalen provisioneras förändringen till systemet utan att en administratör behöver utföra motsvarande åtgärd manuellt. Beroende på integrationsmodell kan automatiserad provisionering även omfatta skapande, uppdatering och inaktivering av konton samt hantering av behörighetsresurser.

Automatiserad provisionering är den rekommenderade modellen där systemets förutsättningar medger det. Den ger bäst förutsättningar för snabb och konsekvent hantering, minskar behovet av manuella åtgärder och gör det möjligt att automatisera hela livscykeln från tilldelning till återkallelse.

Manuell provisionering innebär att VGR behörighetsportal hanterar styrningen av förändringen, men att den slutliga åtgärden i målssystemet utförs manuellt. En administratör eller annan ansvarig får då en uppgift om vilken förändring som ska genomföras och bekräftar därefter att åtgärden är utförd.

Manuell provisionering kan användas när systemet saknar lämpligt tekniskt stöd för automatiserad provisionering eller när vissa förändringar av andra skäl behöver utföras manuellt. Beställning, eventuella godkännanden och spårbarhet kan fortfarande hanteras i VGR behörighetsportal även om själva förändringen genomförs manuellt i målssystemet.

Vidarebefordrad provisionering (relayed provisioning) innebär att VGR behörighetsportal vidarebefordrar provisioneringsuppgiften till ett annat system som ansvarar för den fortsatta hanteringen. Inom VGR kan exempelvis Plexus (ServiceNow), som används för IT Service Management (ITSM), vara aktuellt för denna typ av hantering. Plexus kan då ta emot en uppgift eller ett ärende från VGR behörighetsportal för vidare hantering och genomförande av förändringen i målssystemet.

Vidarebefordrad provisionering kan vara lämplig när det anslutande systemet saknar stöd för direkt automatiserad provisionering, eller när etablerade processer innebär att förändringar ska hanteras och följas upp via Plexus. Exakt utformning och grad av automatisering behöver analyseras för respektive anslutning.

Önskat och faktiskt läge

En central princip i VGR behörighetsportal är skillnaden mellan **önskat läge** och **faktiskt läge**. Önskat läge beskriver vilka konton och behörigheter en användare ska ha enligt de beslut, regler och

policyer som gäller i VGR behörighetsportal. Faktiskt läge beskriver vilka konton och behörigheter som vid en viss tidpunkt faktiskt finns i det anslutande systemet.

När en behörighet tilldelas eller återkallas i VGR behörighetsportal förändras det önskade läget. Vid automatiserad provisionering ska integrationen omsätta förändringen till motsvarande åtgärd i målssystemet, exempelvis genom att skapa eller uppdatera ett konto, lägga till en resurstilldelning eller ta bort en behörighet. Målet är att det faktiska läget i systemet ska överensstämma med det önskade läget i VGR behörighetsportal.

Genom import och avstämning kan VGR behörighetsportal samtidigt få information om det faktiska läget i målssystemet. Därmed kan skillnader mellan önskat och faktiskt läge identifieras, exempelvis om en provisionering har misslyckats eller om en behörighet har förändrats direkt i målssystemet utanför VGR behörighetsportal.

Integrationen bör där det är möjligt utformas så att VGR behörighetsportal kan ange vilket slutligt läge som ska gälla utan att behöva känna till alla steg som krävs för att uppnå detta i målssystemet. Systemspecifik logik bör så långt som möjligt hanteras av målssystemet, dess integrationsgränssnitt eller ett integrationslager. Detta minskar systemspecifik komplexitet i VGR behörighetsportal och ger en tydligare och mer förvaltningsbar integration.

För tekniska gränssnitt där samma förändring kan behöva skickas flera gånger är det önskvärt att operationer är idempotenta. Det innebär att samma begäran kan upprepas utan att skapa oönskade sidoeffekter. Exempelvis ska en begäran om att en viss tilldelning ska finnas kunna skickas igen utan att dubbla tilldelningar skapas.

Målet är att VGR behörighetsportal ska vara den styrande källan för de behörigheter som omfattas av anslutningen och att avvikelser mellan önskat och faktiskt läge ska kunna upptäckas och hanteras på ett kontrollerat sätt.

Rekommenderad logisk datamodell för anslutning

För att skapa en enhetlig och förvaltningsbar anslutning rekommenderas att information från det anslutande systemet så långt som möjligt kan beskrivas enligt en gemensam logisk datamodell. Modellen utgår huvudsakligen från konton, behörighetsresurser och resurstilldelningar samt, när det finns behov, organisatoriskt sammanhang i form av kontext.

Den logiska datamodellen är oberoende av vilket tekniskt anslutningssätt som används. Det anslutande systemet behöver därför inte internt vara uppbyggt enligt samma modell. Systemets egna objekt och relationer mappas i stället till den gemensamma modellen vid integrationen. Syftet är att minska systemspecifik komplexitet i VGR behörighetsportal och skapa en tydlig och långsiktigt förvaltningsbar modell för behörighetsstyrning.

Grundprinciper

Den logiska datamodellen ska göra det möjligt för VGR behörighetsportal att hantera olika typer av system på ett enhetligt sätt, oberoende av hur respektive system internt representerar användare och behörigheter. Utgångspunkten är att systemets objekt och relationer så långt som möjligt kan mappas till konton, behörighetsresurser och resurstilldelningar samt, när det finns behov, kontext.

Följande grundprinciper bör tillämpas vid utformning av integrationen:

- **Enkel och tydlig modell:** Den information som exponeras mot VGR behörighetsportal bör vara så enkel som möjligt och endast innehålla den komplexitet som behövs för att styra och följa upp behörigheter.
- **Stabila identifierare:** Konton, behörighetsresurser och andra objekt som hanteras i integrationen ska kunna identifieras entydigt och stabilt över tid. Identifierare bör inte förändras exempelvis vid namnbyte eller andra förändringar av visningsinformation.
- **Separation mellan teknisk struktur och verksamhetsmässig åtkomst:** Tekniska objekt i målssystemet behöver inte motsvara det

som exponeras för beställare och godkännare i VGR behörighetsportal. Behörigheter bör kunna presenteras med tydliga namn och beskrivningar som förklarar vilken åtkomst de faktiskt ger.

- **Systemspecifik komplexitet bör kapslas in:** Om målssystemet har en komplex intern modell bör denna så långt som möjligt hanteras av systemet, dess integrationsgränssnitt eller ett integrationslager. VGR behörighetsportal bör inte behöva innehålla onödig systemspecifik logik för att hantera exempelvis interna tabeller, koder eller relationer.
- **Stöd för hela livscykeln:** Modellen bör kunna hantera relevanta förändringar över tid, exempelvis skapande, uppdatering och inaktivering av konton samt tilldelning och återkallelse av behörigheter.
- **Stöd för både faktiskt och önskat läge:** Där det är möjligt bör modellen stödja både import av det faktiska läget från målssystemet och provisionering av det önskade läget från VGR behörighetsportal.
- **Standardisering och återanvändning:** Etablerade standarder och generella integrationsmönster bör användas framför systemspecifika speciallösningar där det är möjligt. Det förenklar implementation, test, felsökning och framtida förvaltning.

Hur dessa principer tillämpas beror på systemets förutsättningar och valt anslutningssätt. Ett system behöver därför inte stödja exakt samma objekt eller operationer som ett annat system, men integrationen bör så långt som möjligt följa den gemensamma modellen och principerna ovan.

Konto

Ett konto representerar den tekniska användaren i det anslutande systemet. Kontot kopplas till en identitet i VGR behörighetsportal och används som den tekniska bärare som behörighetsresurser och resurstilldelningar knyts till.

Det är viktigt att skilja mellan identitet och konto. En identitet representerar personen i VGR behörighetsportal, medan ett konto representerar personens tekniska åtkomst i ett specifikt system.

Samma identitet kan därför ha konton i flera system och, beroende på behov, även flera olika typer av konton inom samma system.

Kontotyper

VGR behörighetsportal stödjer olika kontotyper (Account Types) för att skilja mellan konton med olika syften. Det kan exempelvis vara personligt konto, administrativt eller privilegierat konto, utbildningskonto eller andra kontotyper som behövs i det anslutande systemet.

Kontotypen används för att säkerställa att en behörighet kopplas till rätt konto. En administrativ behörighet kan exempelvis styras till ett administrativt konto utan att motsvarande behörighet tilldelas personens vanliga personliga konto. Vilka kontotyper som ska användas fastställs utifrån det anslutande systemets behov och modellen bör hållas så enkel som möjligt.

Identifiering och kontonamn

Ett konto behöver kunna identifieras entydigt och stabilt över tid. Identifieringen bör inte baseras enbart på uppgifter som kan förändras, exempelvis namn, e-postadress eller visningsnamn.

För personidentiteter inom VGR finns etablerade identifierare såsom VGR-ID och HSA-ID. Vilken identifierare som ska användas för kopplingen mellan identitet och konto bedöms för respektive system. VGR-ID kan i många fall även användas som kontonamn, medan andra system kan ha egna krav på kontonamn. Kontonamn och den stabila identifierare som används för att koppla kontot till rätt identitet behöver därför inte vara samma värde.

Beroende på systemets behov kan ett konto exempelvis innehålla kontotyp, kontonamn, stabil identifierare, status, giltighetsperiod och andra attribut som krävs för att hantera kontot.

Livscykel

Kontots livscykel bör kunna hanteras på ett tydligt och förutsägbart sätt. Där det är relevant bör integrationen kunna hantera skapande, uppdatering, inaktivering och återaktivering av konton. Fysisk

borttagning är inte alltid lämplig eller möjlig och behöver bedömas utifrån målssystemets funktion och verksamhetens krav.

Om målssystemet har en komplex eller systemspecifik kontomodell bör denna så långt som möjligt kapslas in i systemets integrationsgränssnitt eller ett integrationslager. Målet är att VGR behörighetsportal ska kunna arbeta mot en tydlig och stabil kontomodell där rätt identitet och kontotyp konsekvent kan kopplas till rätt konto och behörigheter.

Behörighetsresurs

En behörighetsresurs (Resource) representerar en behörighet eller annan åtkomst som kan styras genom VGR behörighetsportal. Det kan exempelvis vara en applikationsroll, grupp, behörighetsprofil, funktion, åtkomstnivå eller behörighetskod i det anslutande systemet.

Vilka objekt som ska representeras som behörighetsresurser behöver bedömas utifrån systemets behörighetsmodell och verksamhetens behov. Målet är inte att exponera hela systemets interna tekniska struktur, utan att identifiera de resurser som behöver kunna tilldelas, återkallas, följas upp eller på annat sätt styras genom VGR behörighetsportal.

En behörighetsresurs behöver kunna identifieras entydigt och stabilt över tid. Den tekniska identifieraren bör därför inte vara beroende av exempelvis visningsnamn eller andra uppgifter som kan förändras. Samtidigt bör resursen ha ett tydligt namn och en beskrivning som gör det möjligt för beställare, godkännare, systemägare och andra berörda att förstå vilken åtkomst den innebär.

Behörighetsresurser kan vid behov kopplas till en eller flera kontotyper. Det gör det möjligt att styra vilken typ av konto en viss behörighet får tilldelas till. En administrativ behörighet kan exempelvis begränsas till administrativa konton, medan en vanlig verksamhetsbehörighet kan vara avsedd för personliga konton.

I vissa system kan en verksamhetsmässig behörighet motsvaras av flera underliggande tekniska resurser. Denna komplexitet bör så långt som möjligt hanteras i behörighetsmodellen, målssystemet eller integrationslagret, så att den åtkomst som exponeras och styrs genom VGR behörighetsportal är tydlig och förvaltningsbar.

Målet är att behörighetsresurser ska ge en stabil och begriplig representation av den åtkomst som ska styras, samtidigt som målssystemets interna tekniska struktur kan förändras utan att det i onödan påverkar beställning, tilldelning och uppföljning i VGR behörighetsportal.

Resurstilldelning

En resurstilldelning (Resource Assignment) representerar kopplingen mellan ett konto och en behörighetsresurs. Resurstilldelningen anger därmed att ett visst konto har, eller ska ha, en viss behörighet i det anslutande systemet.

När en användare tilldelas en behörighet genom VGR behörighetsportal skapas eller uppdateras det önskade läget för resurstilldelningen. Vid automatiserad provisionering omsätts detta till motsvarande tilldelning i målssystemet. När behovet av åtkomst upphör tas resurstilldelningen bort, vilket ska leda till att motsvarande behörighet återkallas i målssystemet.

En resurstilldelning behöver normalt kunna kopplas entydigt till både rätt konto och rätt behörighetsresurs. Beroende på systemets behörighetsmodell kan tilldelningen även behöva innehålla ytterligare information, exempelvis giltighetsperiod, organisatorisk avgränsning eller andra attribut som påverkar hur behörigheten ska tillämpas i målssystemet.

Resurstilldelningar kan skapas på olika sätt i VGR behörighetsportal, exempelvis automatiskt genom tilldelningspolicyer eller genom manuell beställning med godkännande. Oavsett hur tilldelningen uppstår bör samma grundläggande modell användas för att styra och följa upp den faktiska åtkomsten i målssystemet.

Vid import behöver befintliga tilldelningar i målssystemet kunna kopplas till rätt konto och behörighetsresurs. Detta möjliggör avstämning mellan faktiskt och önskat läge och gör det möjligt att identifiera exempelvis behörigheter som har tilldelats direkt i målssystemet eller provisionering som inte har genomförts som avsett.

Om målssystemet använder en mer komplex modell för tilldelningar, exempelvis flera interna relationer eller attribut för att realisera en behörighet, bör denna komplexitet så långt som möjligt kapslas in i målssystemets integrationsgränssnitt eller ett integrationslager. VGR behörighetsportal bör kunna arbeta mot en tydlig och stabil resurstilldelning som beskriver vilket konto som ska ha vilken behörighetsresurs, samt vid behov under vilka förutsättningar den gäller.

Kontext, organisatoriskt sammanhang

Kontext används i VGR behörighetsportal när en identitet eller behörighet behöver kopplas till ett visst organisatoriskt eller verksamhetsmässigt sammanhang. Det kan exempelvis vara en förvaltning, organisatorisk enhet, ett uppdrag, projekt eller annan relevant gruppering.

Kontext är ett kompletterande begrepp och behöver inte användas för alla anslutningar. För många system är modellen med konto, behörighetsresurs och resurstilldelning tillräcklig. Kontext blir främst relevant när samma person kan ha olika organisatoriska tillhörigheter eller uppdrag och dessa behöver påverka vilka behörigheter personen ska ha, under vilka förutsättningar de gäller eller hur deras livscykel ska hanteras.

Ett exempel är en användare som har uppdrag inom flera delar av organisationen och där en viss behörighet endast ska gälla så länge användaren har ett specifikt organisatoriskt sammanhang. Genom att koppla behörigheten till rätt kontext kan tilldelningen styras och återkallas utifrån detta sammanhang.

Kontext kan även användas som underlag för tilldelningspolicyer och andra styrregler i VGR behörighetsportal. I AD-guiden används exempelvis kontext tillsammans med identitetsinformation för att avgöra vilka personer som omfattas av en tilldelningspolicy.

För det anslutande systemet innebär detta normalt inte att systemet behöver implementera VGR behörighetsportals kontextmodell. Om systemets egen behörighetsmodell innehåller organisatoriska eller verksamhetsmässiga dimensioner som behöver hanteras i integrationen ska dessa analyseras och vid behov mappas till lämplig kontext eller annan struktur i VGR behörighetsportal.

Vilka kontexter som behöver användas, och om kontextinformation behöver importeras eller provisioneras som en del av integrationen, fastställs därför för respektive anslutning. Modellen bör inte göras mer komplex än vad systemets behörighetsstyrning och verksamhetens behov kräver.

Identifierare och livscykel

För att VGR behörighetsportal på ett tillförlitligt sätt ska kunna importera, provisionera och stämma av information behöver de objekt som hanteras i integrationen kunna identifieras entydigt och stabilt över tid. Detta gäller framför allt konton, behörighetsresurser och resurstilldelningar, men även andra objekt som ingår i den valda integrationsmodellen.

Identifierare bör vara tekniskt stabila och så långt som möjligt oberoende av information som kan förändras under objektets livscykel. Visningsnamn, beskrivningar, e-postadresser, organisatorisk tillhörighet och liknande uppgifter bör därför normalt inte användas som enda identifierare. Ett namn på en roll eller behörighet ska exempelvis kunna ändras utan att VGR behörighetsportal uppfattar den som en ny behörighetsresurs.

Det behöver också finnas en tydlig koppling mellan objekt i målssystemet och motsvarande objekt i VGR behörighetsportal. För konton är det särskilt viktigt att rätt konto kan kopplas till rätt identitet och, när flera kontotyper används, till rätt kontotyp. För

behörighetsresurser och resurstilldelningar behöver motsvarande stabila koppling kunna upprätthållas även när andra attribut förändras.

Objektens livscykel behöver hanteras utifrån målssystemets funktion och verksamhetens behov. Det kan exempelvis innebära att:

- konton skapas, uppdateras, inaktiveras och vid behov återaktiveras
- behörighetsresurser tillkommer, förändras, inaktiveras eller tas ur bruk
- resurstilldelningar skapas när åtkomst beviljas och tas bort när behovet upphör
- förändringar av namn, beskrivningar eller andra attribut kan hanteras utan att objektens identitet eller befintliga kopplingar går förlorade

Fysisk borttagning är inte alltid lämplig eller möjlig. I många system behöver konton eller behörighetsresurser i stället kunna markeras som inaktiva eller avslutade för att historik, spårbarhet och befintliga relationer ska kunna bevaras. Hur detta hanteras fastställs för respektive anslutning.

Integrationen bör även ta hänsyn till återkommande livscykelscenarier, exempelvis att en person avslutas och senare återkommer eller att en tidigare inaktiverad behörighetsresurs åter tas i bruk. Lösningen bör kunna hantera sådana förändringar utan att i onödan skapa nya objekt eller förlora kopplingen till tidigare information.

Målet är att identifierare och livscykelhantering tillsammans ska ge en stabil modell där VGR behörighetsportal kan följa samma objekt över tid och korrekt hantera förändringar i både önskat och faktiskt läge.

Tillämpning per anslutningstyp

Den rekommenderade logiska datamodellen är oberoende av vilket tekniskt anslutningssätt som används. Konton, behörighetsresurser och resurstilldelningar kan representeras på olika sätt i målssystemet och behöver därför mappas till motsvarande objekt i VGR behörighetsportal.

Hur mappningen görs beror på både anslutningstypen och målssystemets egen datamodell. Exempelvis kan:

- **SCIM 2.0** representera konton som Users och behörighetsresurser genom exempelvis Groups och medlemskap.
- **REST API** exponera konton, behörighetsresurser och tilldelningar genom systemspecifika resurser och endpoints.
- **SOAP** exponera motsvarande information genom definierade operationer och objekt enligt tjänstens kontrakt.
- **OData** exponera objekten som entiteter och relationer som kan läsas och, där gränssnittet stödjer det, förändras.
- **LDAP** representera konton och behörighetsresurser som katalogobjekt och tilldelningar exempelvis genom gruppmedlemskap.
- **SQL** representera motsvarande information genom tabeller, vyer och relationer eller andra supporterade databasgränssnitt.
- **Filbaserad import** representera informationen genom strukturerade filer som mappas till motsvarande objekt vid import.

Det finns inget krav på att målssystemet använder samma benämningar eller struktur som VGR behörighetsportal. En roll, grupp eller behörighetskod i ett målssystem kan exempelvis mappas till en behörighetsresurs, medan ett gruppmedlemskap eller en relation mellan två tabeller kan motsvara en resurstilldelning.

Alla anslutningar behöver inte heller hantera samtliga delar av den logiska datamodellen. Ett system kan exempelvis ha konton som redan skapas och livscykelhanteras på annat sätt, medan VGR behörighetsportal endast behöver hantera behörighetsresurser och resurstilldelningar. I andra system kan portalen behöva hantera både konton och behörigheter. Vilka objekt och flöden som ska omfattas fastställs därför för respektive anslutning.

Oavsett anslutningstyp bör målet vara att mappningen blir så enkel, stabil och tydlig som möjligt. Systemspecifik komplexitet bör där det är möjligt hanteras i målssystemets gränssnitt eller ett integrationslager, så att VGR behörighetsportal kan arbeta mot en enhetlig och förvaltningsbar logisk modell.

Val av integrationsmodell

Val av integrationsmodell görs utifrån det anslutande systemets behörighetsmodell, tekniska integrationsmöjligheter, säkerhetskrav och verksamhetens behov av automatisering. Målet är att välja den lösning som ger en så enkel, standardiserad och långsiktigt förvaltningsbar anslutning som möjligt.

När flera alternativ finns bör etablerade standarder och konfigurationsbaserade integrationssätt prioriteras framför systemspecifik utveckling. För direktintegration är SCIM 2.0 rekommenderat förstahandsval där det är möjligt, eftersom standarden är särskilt utformad för identitets- och behörighetshantering och definierar både gränssnitt och datamodell. Om SCIM inte stöds kan andra etablerade anslutningssätt, exempelvis REST API, SOAP, OData, LDAP eller SQL, vara fullt lämpliga beroende på systemets förutsättningar. VGR behörighetsportal har stöd för konfigurationsbaserad anslutning via samtliga dessa anslutningssätt.

Valet bör inte enbart baseras på vilket protokoll eller gränssnitt som finns. Det behöver även bedömas:

- hur väl systemets datamodell kan mappas till konton, behörighetsresurser och resurstilldelningar
- om gränssnittet stödjer både läsning och skrivning av den information som behöver hanteras
- hur autentisering, säker kommunikation, felhantering och spårbarhet kan lösas
- om gränssnittet är dokumenterat, supporterat och stabilt över tid
- vilken utvecklings-, införande- och förvaltningsinsats lösningen innebär

Import och provisionering behöver inte använda samma integrationsmetod. Ett system kan exempelvis importeras via SQL eller fil samtidigt som provisionering sker via ett API eller vidarebefordras via Plexus. Anslutningen kan också införas stegvis, där import etableras först och automatiserad provisionering införs senare.

Det mest tekniskt avancerade alternativet är inte nödvändigtvis det bästa. Valet ska utgå från vilken modell som uppfyller verksamhetens och säkerhetens behov med lägst rimliga komplexitet och ger bäst förutsättningar för en robust och förvaltningsbar integration över tid.

Nästa kapitel beskriver de olika anslutningssätten och deras huvudsakliga egenskaper mer ingående.

Anslutningsätt och protokoll

VGR behörighetsportal kan ansluta till system genom flera olika tekniska gränssnitt och protokoll. Vilket alternativ som är lämpligt beror på målssystemets stöd, datamodell, säkerhetskrav och vilka informationsflöden som ska hanteras.

Följande avsnitt beskriver de vanligaste anslutningssätten och hur de kan användas för integration med VGR behörighetsportal. SCIM 2.0 rekommenderas som förstahandsval där det är möjligt, men även REST API, SOAP, OData, LDAP och SQL kan ge effektiva och långsiktigt förvaltningsbara integrationer. VGR behörighetsportal har även stöd för filbaserad import samt manuell och vidarebefordrad provisionering när full teknisk integration inte är möjlig eller lämplig. Dessa möjligheter ligger i linje med plattformens stöd för flera protokoll, separata flöden för import och provisionering samt olika grader av automatisering.

Import och provisionering kan använda olika anslutningssätt och behöver inte automatiseras i samma omfattning. En anslutning kan exempelvis kombinera automatiserad import via SQL med provisionering via ett API, eller filbaserad import med manuell eller vidarebefordrad provisionering.

Vilket upplägg som väljs fastställs utifrån respektive systems förutsättningar och kan vid behov förändras över tid när förutsättningarna för integration och automatisering förändras.

SCIM 2.0, rekommenderat förstahandsval där det är möjligt

SCIM 2.0 (System for Cross-domain Identity Management) är en öppen standard särskilt framtagen för utbyte och hantering av identitets- och behörighetsinformation mellan system. Vid direktintegration med VGR behörighetsportal är SCIM 2.0 därför det rekommenderade förstahandsvalet när det anslutande systemet har ett lämpligt och tillräckligt SCIM-stöd.

Till skillnad från ett generellt REST API definierar SCIM både hur kommunikationen sker och en standardiserad datamodell. SCIM 2.0 bygger på REST och definierar bland annat standardiserade resurser för Users och Groups, gemensamma attribut och operationer samt mekanismer för att beskriva vilka resurser, scheman och funktioner en SCIM-tjänst stödjer. Standarden är definierad genom IETF RFC 7642, RFC 7643 och RFC 7644.

För VGR behörighetsportal innebär detta att systemets information i många fall kan mappas till den logiska datamodellen med mindre systemspecifik anpassning. Exempelvis kan ett användarkonto representeras som en SCIM User och grupper eller motsvarande behörighetsresurser representeras genom SCIM Groups och medlemskap. SCIM kan även utökas med egna scheman och attribut när standardmodellen inte är tillräcklig.

Ett SCIM-gränssnitt bör, utifrån vad som ska hanteras i den aktuella integrationen, ge stöd för att:

- läsa relevanta konton, behörighetsresurser och tilldelningar
- skapa och uppdatera de objekt som ska provisioneras
- tilldela och återkalla behörigheter
- hantera status och relevant livscykelinformation
- söka och filtrera information på ett effektivt sätt
- använda stabila och unika identifierare
- hantera större datamängder på ett förutsägbart sätt

Att ett system uppges ha stöd för SCIM 2.0 innebär dock inte automatiskt att gränssnittet uppfyller behoven för anslutning till VGR behörighetsportal. SCIM-implementationer kan skilja sig åt avseende

vilka resurser, attribut och operationer som stöds. Det behöver därför verifieras att systemets SCIM-implementation stödjer den behörighetsmodell och de informationsflöden som behövs för den aktuella anslutningen.

Om SCIM 2.0 inte stöds, eller om systemets SCIM-stöd inte täcker behoven, kan andra anslutningssätt vara lika relevanta. Ett väl dokumenterat och stabilt REST API, SOAP-, OData-, LDAP- eller SQL-gränssnitt kan vara ett bättre alternativ än att anpassa lösningen till ett otillräckligt SCIM-stöd.

Målet är därför inte att använda SCIM till varje pris, utan att använda standarden när den ger en enklare, mer standardiserad och långsiktigt förvaltningsbar integration.

REST API

REST API är ett vanligt och flexibelt anslutningssätt för direktintegration med VGR behörighetsportal. REST kan vara ett lämpligt alternativ när systemet saknar tillräckligt stöd för SCIM 2.0 men erbjuder ett dokumenterat och supporterat API som kan användas för att läsa och, där det behövs, förändra konton, behörighetsresurser och resurstilldelningar.

Till skillnad från SCIM definierar REST inte någon standardiserad datamodell för identiteter och behörigheter. Två REST API:er kan därför representera samma information på helt olika sätt. Vid anslutning behöver systemets API och datamodell därför analyseras och mappas till den logiska modell som används av VGR behörighetsportal.

När ett nytt REST API utvecklas eller ett befintligt API kan anpassas rekommenderas att utformningen så långt som möjligt följer samma grundprinciper som beskrivs i denna guide. Konton, behörighetsresurser och resurstilldelningar bör kunna hanteras genom tydliga och stabila objekt, och systemspecifik komplexitet bör så långt som möjligt kapslas in bakom API. Om det är möjligt bör även etablerade principer och datamodeller från SCIM 2.0 återanvändas i stället för att skapa en helt egen modell.

Ett REST API bör, utifrån vad som ska hanteras i den aktuella integrationen, ge stöd för att:

- läsa relevanta konton, behörighetsresurser och resurstilldelningar
- skapa, uppdatera och inaktivera konton där VGR behörighetsportal ska hantera kontolivscykeln
- skapa eller uppdatera behörighetsresurser där detta ingår i integrationen
- skapa och ta bort resurstilldelningar
- använda stabila och unika identifierare
- söka, filtrera och vid större datamängder paginera resultat
- returnera tydliga resultat och fel så att integrationen kan övervakas och felsökas

Ett befintligt REST API behöver inte vara utformat exakt enligt den rekommenderade modellen för att kunna användas. Det avgörande är att nödvändig information och nödvändiga operationer kan mappas på ett tydligt, robust och förvaltningsbart sätt. Om API:t är mycket systemspecifikt eller kräver omfattande orkestrering bör det övervägas om komplexiteten kan kapslas in i API:t eller ett integrationslager i stället för att byggas in i VGR behörighetsportal.

SOAP

SOAP är ett standardiserat protokoll för utbyte av strukturerade meddelanden mellan system och kan användas för direktintegration med VGR behörighetsportal när målssystemet erbjuder ett dokumenterat och supporterat SOAP-baserat webbtjänstegränssnitt.

SOAP använder normalt XML för informationsutbyte och ett WSDL-kontrakt (Web Services Description Language) för att beskriva vilka operationer tjänsten erbjuder, vilka parametrar som kan skickas och vilka datastrukturer som returneras. Det ger ett tydligt kontrakt mellan VGR behörighetsportal och det anslutande systemet.

På samma sätt som för REST definierar SOAP inte någon generell datamodell för identitets- och behörighetshantering. Systemets objekt och operationer behöver därför analyseras och mappas till den

logiska modell som används av VGR behörighetsportal, exempelvis konton, behörighetsresurser och resurstilldelningar.

Ett SOAP-gränssnitt bör, utifrån vad som ska hanteras i den aktuella integrationen, ge stöd för att:

- läsa relevanta konton, behörighetsresurser och resurstilldelningar
- skapa, uppdatera och inaktivera konton där VGR behörighetsportal ska hantera kontolivscykeln
- skapa eller uppdatera behörighetsresurser där detta ingår i integrationen
- skapa och ta bort resurstilldelningar
- använda stabila och unika identifierare
- hantera de datamängder som behöver överföras på ett effektivt sätt
- returnera tydliga resultat och fel så att integrationen kan övervakas och felsökas

Ett befintligt SOAP-gränssnitt behöver inte vara utformat specifikt för identitets- och behörighetshantering för att kunna användas. Det avgörande är att de operationer och den information som behövs kan mappas till VGR behörighetsportals logiska modell på ett tydligt och förvaltningsbart sätt. Om gränssnittet kräver omfattande systemspecifik logik eller många beroende operationer bör det övervägas om komplexiteten kan kapslas in i målssystemet eller ett integrationslager.

OData

OData (Open Data Protocol) är ett standardiserat protokoll för att exponera och hantera strukturerad data via REST-baserade API:er. OData kan användas för direktintegration med VGR behörighetsportal när målssystemet erbjuder ett dokumenterat och supporterat OData-gränssnitt.

OData definierar en gemensam modell för bland annat entiteter, egenskaper, relationer och metadata samt standardiserade sätt att fråga och filtrera data. Det gör det möjligt att beskriva vilka objekt och relationer som finns tillgängliga och att begränsa vilken information som hämtas. Detta kan vara särskilt användbart vid

import och avstämning där VGR behörighetsportal behöver läsa och bearbeta strukturerad information från målssystemet.

OData definierar hur data exponeras och hanteras, men inte någon specifik datamodell för identitets- och behörighetshantering. Målssystemets entiteter och relationer behöver därför analyseras och mappas till den logiska modell som används av VGR behörighetsportal, exempelvis konton, behörighetsresurser och resurstilldelningar.

Ett OData-gränssnitt bör, utifrån vad som ska hanteras i den aktuella integrationen, ge stöd för att:

- läsa relevanta konton, behörighetsresurser och resurstilldelningar
- exponera tydliga relationer mellan relevanta objekt
- använda stabila och unika identifierare
- filtrera och begränsa vilken information som hämtas
- hantera större datamängder på ett effektivt sätt
- skapa, uppdatera eller ta bort information där gränssnittet ska användas även för provisionering
- returnera tydliga resultat och fel så att integrationen kan övervakas och felsökas

Ett befintligt OData-gränssnitt behöver inte vara utformat specifikt för identitets- och behörighetshantering för att kunna användas. Det avgörande är att relevanta entiteter, relationer och operationer kan mappas till VGR behörighetsportals logiska modell på ett tydligt och förvaltningsbart sätt.

LDAP

LDAP (Lightweight Directory Access Protocol) är ett standardiserat protokoll för åtkomst till och hantering av information i katalogtjänster. LDAP kan användas för direktintegration med VGR behörighetsportal när målssystemet exponerar konton, grupper, behörigheter eller annan relevant information genom ett dokumenterat och supporterat LDAP-gränssnitt.

LDAP organiserar information som katalogobjekt med definierade objektklasser, attribut och relationer. Konton kan exempelvis representeras som användarobjekt, behörighetsresurser som grupper eller andra katalogobjekt och resurstilldelningar som gruppmedlemskap eller andra relationer mellan objekten.

Målssystemets katalogstruktur behöver analyseras och mappas till den logiska modell som används av VGR behörighetsportal. Det behöver bland annat vara tydligt vilka objekt och attribut som representerar konton och behörighetsresurser, hur tilldelningar uttrycks och vilka identifierare som kan användas för att stabilt identifiera objekten över tid.

Ett LDAP-gränssnitt bör, utifrån vad som ska hanteras i den aktuella integrationen, ge stöd för att:

- läsa relevanta konton, behörighetsresurser och resurstilldelningar
- använda tydliga objektklasser och attribut för den information som ska hanteras
- använda stabila och unika identifierare
- söka och filtrera relevanta objekt och relationer på ett effektivt sätt
- skapa och uppdatera konton eller behörighetsresurser där detta ingår i integrationen
- skapa och ta bort medlemskap eller andra relationer där LDAP används för provisionering
- hantera de datamängder som behöver importeras och stämmas av på ett effektivt sätt

Ett befintligt LDAP-gränssnitt behöver inte vara utformat specifikt för identitets- och behörighetshantering i VGR behörighetsportal. Det avgörande är att relevanta katalogobjekt, attribut och relationer kan mappas till den logiska modellen på ett tydligt och förvaltningsbart sätt. Mappningen bör begränsas till den information som behövs för behörighetsstyrningen och så långt som möjligt bygga på etablerade objektklasser, attribut och relationer i katalogen.

SQL

SQL kan användas för direktintegration med VGR behörighetsportal när målssystemet tillhandahåller ett dokumenterat och supporterat databasgränssnitt för den information som behöver hanteras. SQL kan användas både för att läsa information från målssystemet och, när systemets integrationsmodell stödjer det, för provisionering.

Vid SQL-baserad integration representeras konton, behörighetsresurser och resurstilldelningar normalt genom tabeller, vyer och relationer i databasen. Målssystemets datamodell behöver därför analyseras och mappas till den logiska modell som används av VGR behörighetsportal.

För import är SQL ofta lämpligt när systemet på ett strukturerat och stabilt sätt kan exponera aktuellt behörighetsläge genom exempelvis tabeller eller särskilt avsedda vyer. Det behöver vara möjligt att identifiera relevanta objekt och relationer entydigt samt att effektivt läsa den information som behövs för import och avstämning.

Ett SQL-baserat gränssnitt bör, utifrån vad som ska hanteras i den aktuella integrationen, ge stöd för att:

- läsa relevanta konton, behörighetsresurser och resurstilldelningar
- använda stabila och unika identifierare
- exponera tydliga relationer mellan relevanta objekt
- filtrera och begränsa vilken information som hämtas
- hantera de datamängder som behöver importeras och stämmas av på ett effektivt sätt
- genomföra nödvändiga förändringar på ett kontrollerat sätt där SQL används för provisionering

Om SQL ska användas för provisionering behöver det finnas ett dokumenterat och supporterat sätt att genomföra förändringar. Det kan exempelvis ske genom särskilt avsedda stored procedures eller andra databasgränssnitt som säkerställer att målssystemets regler och dataintegritet upprätthålls. Direkt skrivning i applikationens interna databastabeller bör undvikas om detta inte uttryckligen är ett av systemleverantören avsett och supporterat integrationssätt.

Ett befintligt SQL-gränssnitt behöver inte vara utformat specifikt för identitets- och behörighetshantering för att kunna användas. Det avgörande är att relevant information och nödvändiga operationer kan mappas till VGR behörighetsportals logiska modell på ett tydligt, stabilt och förvaltningsbart sätt.

Filbaserad import

Filbaserad import kan användas när målssystemet kan exportera relevant information i ett strukturerat filformat men saknar ett lämpligt gränssnitt för automatiserad import, eller när en sådan integration inte är möjlig eller motiverad. Det kan även användas som en övergångslösning innan en mer automatiserad integration etableras.

Vid filbaserad import exporteras information från målssystemet och läses in i VGR behörighetsportal genom strukturerade CSV-filer. Informationen kan innehålla flera olika objekttyper, exempelvis konton, behörighetsresurser och resurstilldelningar, i samma fil eller fördelas över flera filer beroende på vad som är lämpligt för den aktuella anslutningen. Vid behov kan även flera filer användas för samma objekttyp. Informationen mappas vid import till motsvarande objekt i VGR behörighetsportals logiska datamodell.

Filer kan hämtas från en överenskommen nätverksresurs eller via SFTP. Vilket överföringssätt som används fastställs för respektive anslutning utifrån tekniska och säkerhetsmässiga förutsättningar.

Underlaget för filbaserad import ska:

- följa det CSV-format och den filstruktur som fastställts för anslutningen
- innehålla stabila och unika identifierare för relevanta objekt
- innehålla de attribut och relationer som krävs för den aktuella integrationen
- vara konsekvent mellan olika leveranser
- kunna tas fram och göras tillgängligt med överenskommen frekvens
- möjliggöra att aktuellt behörighetsläge kan återskapas och stämmas av på ett tillförlitligt sätt

Detaljer såsom filstruktur, filnamn, separator, teckenkodning, kolumnrubriker, obligatoriska attribut och identifierare fastställs för respektive anslutning. Det överenskomna formatet ska därefter vara stabilt och konsekvent över tid.

Filbaserad import sker som fullständig import. Varje leverans ska därför innehålla den kompletta aktuella mängden objekt för den information som importeras. Deltafiler som endast innehåller förändringar sedan föregående import stöds inte. Det anslutande systemet behöver därför kunna ta fram en fullständig och aktuell export vid varje importtillfälle.

Filbaserad import ger VGR behörighetsportal information om det faktiska läget i målssystemet och kan därmed ge underlag för exempelvis avstämning, uppföljning och återcertifiering. Eftersom filbaserad import i sig inte genomför förändringar i målssystemet behöver provisionering lösas separat om VGR behörighetsportal även ska styra förändringar av konton och behörigheter. Provisioneringen kan exempelvis ske automatiserat genom ett annat tekniskt gränssnitt eller, för vissa system, genom PowerShell. Manuell eller vidarebefordrad provisionering kan också användas när automatiserad provisionering inte är möjlig eller lämplig.

Om förutsättningarna förändras kan en filbaserad integration senare ersättas eller kompletteras med automatiserad import via exempelvis API, LDAP eller SQL. Den logiska datamodellen bör därför så långt som möjligt vara densamma oavsett hur informationen tekniskt överförs.

Manuell eller vidarebefordrad provisioning

När målssystemet saknar ett lämpligt tekniskt gränssnitt för automatiserad provisionering, eller när direkt provisionering av andra skäl inte är lämplig, kan VGR behörighetsportal använda manuell eller vidarebefordrad provisionering (relayed provisioning).

Manuell provisionering innebär att VGR behörighetsportal skapar en provisioneringsuppgift som behöver genomföras av en administratör eller annan ansvarig person. Uppgiften beskriver vilken

förändring som ska göras i målssystemet, exempelvis att skapa eller inaktivera ett konto, tilldela en behörighet eller återkalla en befintlig tilldelning. När åtgärden har genomförts bekräftas detta i provisioneringsflödet.

Manuell provisionering gör det möjligt att behålla styrning, beställning, godkännande och spårbarhet i VGR behörighetsportal även när den tekniska förändringen behöver utföras manuellt. Modellen är främst lämplig när automatiserad provisionering inte är tekniskt möjlig eller när antalet förändringar är begränsat och en automatiserad integration inte är motiverad.

Vidarebefordrad provisionering (relayed provisioning) innebär att provisioneringsuppgiften skickas från VGR behörighetsportal till ett annat system som ansvarar för den fortsatta hanteringen. Inom VGR kan Plexus (ServiceNow) användas för detta. VGR behörighetsportal skapar då ett ärende i Plexus med information om den förändring som ska genomföras. Ärendet hanteras därefter enligt det arbetsflöde som konfigurerats i Plexus för den aktuella typen av förändring.

VGR behörighetsportal följer statusen på ärendet i Plexus genom återkommande statuskontroller. Statusar i Plexus mappas till provisioneringsflödets status, så att portalen kan avgöra om uppgiften fortfarande väntar på hantering, har misslyckats eller är slutförd. När ärendet har slutförts uppdateras provisioneringsstatusen i VGR behörighetsportal och efterföljande avstämning kan verifiera det faktiska läget i målssystemet.

Den faktiska förändringen i målssystemet kan genomföras manuellt eller automatiserat beroende på vilka processer och integrationer som finns bakom Plexus. VGR behörighetsportal behöver därmed inte ha en direkt teknisk integration med målssystemet för att kunna initiera och följa upp provisioneringen.

Manuell och vidarebefordrad provisionering kan även användas som ett första steg vid anslutning av ett system och senare ersättas med

direkt automatiserad provisionering om tekniska och verksamhetsmässiga förutsättningar förändras.

Så här gör du steg för steg

Anslutning genom direktintegration genomförs i ett antal steg, från inledande analys av systemets behov och förutsättningar till konfiguration, test, driftsättning och förvaltning. Eftersom varje system har olika behörighetsmodeller och tekniska integrationsmöjligheter behöver processen anpassas för respektive anslutning.

Följande steg beskriver det rekommenderade arbetssättet och vilket underlag som behöver tas fram för att tillsammans med teamet för VGR behörighetsportal kunna utforma och genomföra en säker, effektiv och långsiktigt förvaltningsbar anslutning.

Kontrollera om AD eller AMU kan användas

Innan direktintegration påbörjas ska det kontrolleras om systemets behörighetsstyrning i stället kan realiseras via AD-grupper eller administrativa medarbetaruppdrag (AMU). Dessa anslutningsmodeller är redan etablerade inom VGR och bör användas när de kan uppfylla systemets behov på ett ändamålsenligt sätt.

Om systemet inte kan eller bör styra sina behörigheter via AD-grupper eller AMU går arbetet vidare med analys av direktintegration enligt följande steg.

Beställ anslutning

Anslutning initieras normalt genom en beställning via Serviceportalen enligt KB0028399. Beställningen ger teamet för VGR behörighetsportal underlag för att inleda dialogen och tillsammans med berörda parter analysera förutsättningarna för anslutningen. Det är inte nödvändigt att den tekniska lösningen är färdigutredd innan beställningen görs.

Kartlägg behörighetsmodellen

Kartlägg hur konton och behörigheter är uppbyggda och hanteras i det anslutande systemet. Identifiera vilka kontotyper som finns, vilka behörighetsresurser som ska styras, exempelvis roller, grupper eller behörighetsprofiler, samt hur tilldelningar mellan konton och behörigheter fungerar.

Kartlägg även hur behörigheter ska tilldelas och återkallas, vilka delar som ska hanteras via VGR behörighetsportal och om det finns organisatoriska eller andra sammanhang som behöver påverka behörighetsstyrningen. Målet är att kunna mappa systemets behörighetsmodell till den rekommenderade logiska datamodellen för anslutning.

Kartlägg tekniska integrationsförutsättningar

Kartlägg vilka tekniska möjligheter systemet har för import och provisionering, exempelvis stöd för SCIM 2.0, REST API, SOAP, OData, LDAP, SQL eller filbaserad import. Ta fram tillgänglig teknisk dokumentation och identifiera vilka objekt, attribut och operationer som gränssnittet stödjer.

Kartlägg även förutsättningar för bland annat autentisering, kommunikation, testmiljö, datamängder, felhantering och övervakning. Målet är att få ett tillräckligt underlag för att kunna välja en säker, robust och förvaltningsbar integrationsmodell.

Välj integrationsmodell

Utifrån kartläggningen av behörighetsmodellen och de tekniska förutsättningarna väljs lämplig integrationsmodell för systemet. SCIM 2.0 bör vara förstahandsval där det finns ett lämpligt stöd, men även REST API, SOAP, OData, LDAP, SQL eller filbaserad import kan vara lämpliga beroende på systemets förutsättningar.

Fastställ samtidigt hur import och provisionering ska genomföras. Dessa kan använda olika anslutningssätt och graden av automatisering kan variera. Målet är att välja den lösning som

uppfyller verksamhetens och säkerhetens behov med så låg komplexitet som möjligt och som är långsiktigt förvaltningsbar.

Ta fram lösningsdesign och kravbild

Utifrån kartläggningen tas en lösningsdesign och kravbild fram **i** samverkan mellan det anslutande systemet och teamet för VGR behörighetsportal. Det anslutande systemet bidrar med kunskap om behörighetsmodell, tekniska gränssnitt och verksamhetens behov, medan teamet för VGR behörighetsportal bidrar med vägledning kring lämplig datamodell, integrationslösning och behörighetsstyrning.

Tillsammans fastställs bland annat vilka objekt och informationsflöden som ska hanteras, hur informationen ska mappas samt hur import, provisionering, avstämning, säkerhet och test ska lösas. Lösningsdesignen dokumenteras på en nivå som är tillräcklig för implementation, test och framtida förvaltning.

Konfiguration i testmiljö

När lösningsdesignen är fastställd konfigureras anslutningen i VGR behörighetsportals testmiljö. Det omfattar de delar som är relevanta för den valda integrationsmodellen, exempelvis anslutning, datamappning, import, provisionering och avstämning samt konfiguration av behörighetsresurser och tilldelningslogik.

Konfigurationen genomförs i samverkan mellan teamet för VGR behörighetsportal och berörda parter för det anslutande systemet. Nödvändiga testmiljöer, testdata och tekniska kommunikationsvägar behöver finnas tillgängliga innan efterföljande test och verifiering kan genomföras.

Test och verifiering

När anslutningen är konfigurerad genomförs test och verifiering tillsammans med berörda parter. Testerna ska säkerställa att integrationen fungerar enligt lösningsdesignen och att rätt information importeras, provisioneras och stäms av mellan VGR behörighetsportal och det anslutande systemet.

Verifieringen ska omfatta relevanta livscykelscenarier, exempelvis skapande och förändring av konton, tilldelning och återkallelse av behörigheter samt hantering av fel och avvikelser. Även beställningsflöden, godkännanden och tilldelningspolicyer testas där dessa används. Både den tekniska funktionen och att behörigheterna motsvarar verksamhetens behov ska vara verifierade innan driftsättning.

Driftsättning

Efter godkänd test och verifiering driftsätts anslutningen i produktionsmiljön. Konfiguration och integrationsflöden etableras enligt den lösning som verifierats i test, och nödvändiga produktionsanslutningar och behörigheter säkerställs.

Inför driftsättning ska berörda parter ha godkänt lösningen och det ska vara tydligt hur anslutningen ska övervakas och förvaltas. Efter driftsättning verifieras att import, provisionering och avstämning fungerar som avsett med produktionsdata och att behörighetsstyrningen fungerar korrekt.

Förvaltning och förändring

Efter driftsättning behöver anslutningen förvaltas och följas upp över tid. Förändringar i målssystemets behörighetsmodell, tekniska gränssnitt, datamodell eller andra förutsättningar som kan påverka integrationen behöver hanteras kontrollerat och vid behov samordnas med teamet för VGR behörighetsportal.

Även förändringar av exempelvis kontotyper, behörighetsresurser, tilldelningsregler och integrationsflöden kan kräva anpassning och test innan de införs. Ansvar och kontaktvägar ska hållas aktuella och större förändringar bör hanteras enligt samma principer för analys, test och verifiering som vid den ursprungliga anslutningen.

Det här behöver vi från dig

För att kunna analysera, utforma och genomföra anslutningen behöver teamet för VGR behörighetsportal underlag och kunskap om

det anslutande systemet. Exakt vilket underlag som behövs beror på systemets behörighetsmodell och vald integrationslösning.

Du behöver normalt kunna bidra med:

- beskrivning av systemet och dess behörighetsmodell, inklusive relevanta kontotyper, behörighetsresurser och tilldelningar
- information om vilka behörigheter som ska styras via VGR behörighetsportal och hur de ska tilldelas och återkallas
- dokumentation av tillgängliga tekniska gränssnitt och integrationsmöjligheter
- information om relevanta test- och produktionsmiljöer samt tekniska kontaktpersoner
- verksamhetsmässiga och tekniska representanter som kan delta i analys, design, test och verifiering
- kontaktuppgifter till systemägare och andra ansvariga roller som behövs för anslutningen

Du behöver inte ha en färdig integrationslösning innan arbetet påbörjas. Lösningsdesign och detaljerad kravbild tas fram i samverkan med teamet för VGR behörighetsportal utifrån systemets behov och förutsättningar.

Det här får du automatiskt

När ett system ansluts till VGR behörighetsportal får det tillgång till portalens gemensamma funktioner för styrning, kontroll och uppföljning av behörigheter. Exakt vilka funktioner som används beror på systemets behörighetsmodell och hur anslutningen utformas.

Anslutningen kan bland annat ge stöd för:

- automatisk tilldelning och återkallelse av behörigheter genom tilldelningspolicyer
- beställning av behörigheter via självservice med konfigurerbara godkännandeflöden
- automatiserad, manuell eller vidarebefordrad provisionering enligt vald integrationsmodell

- import och avstämning av faktiskt behörighetsläge, vilket ger överblick över vilka konton och behörigheter som faktiskt finns i det anslutna systemet
- identifiering och hantering av behörigheter som är felaktiga, saknar giltig grund eller inte längre ska finnas
- automatisk eller beslutad återkallelse av behörigheter när behovet upphör
- central loggning och spårbarhet av beställningar, beslut, tilldelningar och återkallelser
- återcertifiering och återkommande granskning för att säkerställa att befintliga behörigheter fortfarande är motiverade
- livscykelhantering där behörigheter kan förändras eller återkallas när användarens uppdrag, organisatoriska tillhörighet eller andra styrande förutsättningar förändras

Sammantaget ger anslutningen bättre kontroll över vem som har åtkomst till vad och varför, samt möjlighet att upptäcka och åtgärda behörigheter som inte längre är korrekta. Detta ger bättre förutsättningar för informationssäkerhet, spårbarhet och regelefterlevnad.

Tekniska riktlinjer, kortversion

Följande riktlinjer sammanfattar de viktigaste tekniska principerna för direktintegration med VGR behörighetsportal. Exakta krav och utformning fastställs för respektive anslutning utifrån systemets behörighetsmodell, valt anslutningssätt och verksamhetens behov.

- **Standardiserade anslutningssätt:** SCIM 2.0 bör användas som förstahandsval där ett lämpligt stöd finns. REST API, SOAP, OData, LDAP, SQL och filbaserad import kan användas när de ger en lämplig och förvaltningsbar integration. Konfigurationsbaserade och standardiserade lösningar bör prioriteras framför kundspecifik utveckling.
- **Logisk datamodell:** Informationen bör så långt som möjligt kunna mappas till den gemensamma modellen med konton, behörighetsresurser och resurstilldelningar samt, när behov finns,

kontext. Målssystemets interna datamodell behöver inte vara uppbyggd på samma sätt.

- **Stabila identifierare:** Konton, behörighetsresurser och andra relevanta objekt ska kunna identifieras entydigt och stabilt över tid. Namn, beskrivningar och andra föränderliga attribut bör inte användas som enda identifierare.
- **Import och faktiskt läge:** Där det är relevant bör VGR behörighetsportal kunna läsa konton, behörighetsresurser och resurstilldelningar från målssystemet. Informationen ska vara tillräcklig för att kunna följa upp och stämma av det faktiska behörighetsläget.
- **Provisionering och önskat läge:** Där VGR behörighetsportal ska styra förändringar bör integrationen kunna skapa, uppdatera, inaktivera eller återkalla relevanta objekt och tilldelningar. Automatiserad provisionering bör användas där det är möjligt och lämpligt. Manuell eller vidarebefordrad provisionering kan användas när direkt automation inte är möjlig.
- **Idempotens och robust provisionering:** Där det är tekniskt möjligt bör provisioneringsoperationer kunna upprepas utan oönskade sidoeffekter. Integrationen bör så långt som möjligt kunna uttrycka vilket läge som ska gälla utan att vara beroende av en viss sekvens av tidigare operationer.
- **Säker kommunikation och autentisering:** Integrationen ska använda ett för anslutningssättet lämpligt och godkänt sätt för autentisering och säker kommunikation. Tekniska identiteter och integrationskonton ska endast ha de behörigheter som krävs för integrationens funktion.
- **Datamängder och prestanda:** Gränssnittet ska kunna hantera de datamängder som integrationen kräver. Vid större datamängder behöver lämpligt stöd finnas för exempelvis filtrering, paginering eller motsvarande mekanismer beroende på anslutningssätt.
- **Felhantering och övervakning:** Fel vid import och provisionering ska kunna identifieras och felsökas. Gränssnitt och integrationsflöden bör ge tillräcklig information för att avgöra vilken operation eller vilket objekt som har orsakat ett fel och möjliggöra kontrollerad omkörning eller korrigering.

- **Test och förändringshantering:** Anslutningen ska kunna verifieras i testmiljö innan driftsättning. Förändringar i gränssnitt, datamodell, behörighetsmodell eller andra delar som påverkar integrationen behöver hanteras kontrollerat och testas innan de införs i produktion.
- **Supporterat och förvaltningsbart gränssnitt:** Det gränssnitt som används ska vara dokumenterat och avsett för integration med systemet. Lösningen bör utformas så att uppgraderingar och förändringar i målssystemet inte i onödan kräver förändringar i VGR behörighetsportal.

Den tekniska kravbilagan beskriver gemensamma tekniska principer och krav för direktintegration. Anslutningsspecifika detaljer fastställs i samband med analys och lösningsdesign för respektive anslutning.

Rekommendationer vid upphandling

Vid upphandling eller större vidareutveckling av system bör möjligheten att ansluta systemet till VGR behörighetsportal beaktas redan vid kravställningen. Ett system med en tydlig behörighetsmodell och ett standardiserat och väl dokumenterat integrationsstöd ger bättre förutsättningar för automatiserad behörighetsstyrning och minskar behovet av kostsamma specialanpassningar under systemets livscykel.

I första hand bör det utredas om systemets behörighetsstyrning kan realiseras genom VGR:s etablerade anslutningsmodeller via AD-grupper eller AMU. Om dessa modeller inte är lämpliga bör systemet ha ett standardiserat och väl dokumenterat stöd för direktintegration. För direktintegration bör SCIM 2.0 vara förstahandsval där ett lämpligt stöd finns. Om SCIM inte är lämpligt bör systemet erbjuda ett annat dokumenterat och supporterat integrationsgränssnitt, exempelvis REST API, SOAP, OData, LDAP eller SQL. Detta följer de övergripande anslutningsprinciperna där etablerade och standardiserade integrationsmönster ska prioriteras och systemspecifik utveckling begränsas.

Vid kravställning för direktintegration bör följande särskilt beaktas:

- **Standardiserat och supporterat integrationsgränssnitt:** Integrationsgränssnittet ska vara en dokumenterad och supporterad del av systemet och avsett för den typ av integration som ska genomföras. Standardiserade gränssnitt och konfigurationsbaserade lösningar bör prioriteras framför kundspecifika integrationer.
- **Komplett integrationsdokumentation:** Leverantören ska tillhandahålla aktuell och tillräckligt detaljerad dokumentation för det integrationsgränssnitt som ska användas. Dokumentationen ska omfatta relevanta objekt och datamodeller, attribut, operationer, autentisering, felhantering, begränsningar samt filtrering och paginering där det är relevant. För API-baserade gränssnitt bör även exempel på anrop och svar finnas. Dokumentationen ska hållas aktuell och vara tillgänglig för VGR under hela den tid som integrationen används.

- **Stöd för läsning och skrivning:** Gränssnittet bör möjliggöra både läsning av faktiskt behörighetsläge och automatiserad hantering av förändringar. Det bör, utifrån systemets behov, gå att läsa och hantera konton, behörighetsresurser och resurstilldelningar. Om vissa delar inte kan hanteras via gränssnittet ska detta framgå tydligt.
- **Tydlig behörighetsmodell:** Leverantören ska kunna beskriva hur konton, kontotyper, roller, grupper, behörigheter och tilldelningar är modellerade samt hur relevanta delar kan exponeras och hanteras genom integrationsgränssnittet.
- **Stabila identifierare:** Konton, behörighetsresurser och andra relevanta objekt ska ha stabila och unika tekniska identifierare som inte förändras exempelvis vid namnbyte eller ändring av visningsinformation.
- **Livscykelhantering:** Integrationsgränssnittet bör stödja de livscykelhändelser som behövs för systemet, exempelvis skapande, uppdatering, inaktivering och återaktivering av konton samt tilldelning och återkallelse av behörigheter.
- **Säker integration:** Systemet ska stödja lämplig autentisering och säker kommunikation samt möjlighet att begränsa integrationsbehörigheter enligt principen om minsta privilegium.
- **Effektiv import och avstämning:** Gränssnittet ska kunna hantera de datamängder som krävs för att VGR behörighetsportal ska kunna läsa och stämma av faktiskt behörighetsläge. Vid behov ska lämpligt stöd finnas för exempelvis filtrering, paginering eller motsvarande mekanismer.
- **Felhantering och spårbarhet:** Integrationsgränssnittet ska ge tydliga felkoder och felmeddelanden som gör det möjligt att identifiera berörd operation och objekt samt förstå orsaken till felet. Generiska felmeddelanden utan användbar felsökningsinformation ska undvikas.
- **Testbarhet:** Leverantören ska ge VGR möjlighet att testa och verifiera integrationen före produktionssättning. Det ska vara möjligt att verifiera relevanta informationsflöden, behörighetstilldelningar och livscykelscenarier under förhållanden som i tillräcklig grad motsvarar produktionsmiljön.

- **Versionering och förändringshantering:** Leverantören ska ha en tydlig hantering av versionering och förändringar i integrationsgränssnittet. Förändringar som kan påverka integrationen ska kommuniceras till VGR i tillräckligt god tid för att möjliggöra analys, anpassning och test innan förändringen införs.

Kravställningen bör så långt som möjligt beskriva vilka förmågor systemet och integrationsgränssnittet ska erbjuda, snarare än att låsa lösningen till produktspecifika tekniska detaljer. Det ger bättre förutsättningar att behålla en fungerande och förvaltningsbar integration även när VGR behörighetsportal eller det anslutande systemet utvecklas över tid.

För system där behörighetsstyrning är viktig bör integrationsförmågan även ingå som en del av utvärderingen vid upphandling och inte enbart vara ett informationskrav. Leverantören bör vid behov kunna demonstrera hur systemets integrationsgränssnitt stödjer de konton, behörigheter, tilldelningar och livscykelflöden som VGR behöver hantera.

Teknisk kravbilaga, detaljerade specifikationer

Den tekniska kravbilagan beskriver gemensamma tekniska principer och krav för direktintegration med VGR behörighetsportal. Syftet är att ge stöd vid anslutning, lösningsdesign och kravställning samt att skapa förutsättningar för säkra, robusta och långsiktigt förvaltningsbara integrationer.

Kraven är avsiktligt utformade på en produktneutral och stabil nivå. Exakt teknisk implementation, konfiguration och andra anslutningsspecifika detaljer fastställs för respektive system i samband med analys och lösningsdesign.

Integrationsgränssnitt och datamodell

Det anslutande systemet ska tillhandahålla ett dokumenterat och supporterat integrationsgränssnitt för den information och de operationer som omfattas av anslutningen. Standardiserade och etablerade gränssnitt ska prioriteras framför kundspecifika lösningar.

SCIM 2.0 är rekommenderat förstahandsval för direktintegration där ett lämpligt stöd finns. Andra gränssnitt, exempelvis REST API, SOAP, OData, LDAP eller SQL, kan användas när de uppfyller behoven för den aktuella anslutningen. Detta ligger i linje med plattformens stöd för konfigurationsbaserad anslutning via dessa gränssnitt.

Systemets datamodell behöver kunna mappas till den logiska modell som används av VGR behörighetsportal. Beroende på vad anslutningen ska hantera ska relevant information kunna representeras som:

- **konton**, inklusive relevanta attribut och, när behov finns, olika kontotyper
- **behörighetsresurser**, exempelvis roller, grupper, behörighetsprofiler eller andra rättigheter
- **resurstilldelningar**, som beskriver kopplingen mellan konto och behörighetsresurs
- **kontext eller motsvarande organisatoriskt sammanhang**, när detta är relevant för den aktuella behörighetsmodellen

Alla objekt som behöver följas över tid ska ha stabila och unika tekniska identifierare. Identifierare ska inte vara beroende av exempelvis visningsnamn, beskrivningar eller andra attribut som normalt kan förändras under objektets livscykel. Det ska vara möjligt att ändra sådan information utan att objektet uppfattas som ett nytt konto eller en ny behörighetsresurs.

Gränssnittet ska exponera de attribut och relationer som krävs för att VGR behörighetsportal entydigt ska kunna förstå och hantera relevanta objekt. För behörighetsresurser ska det finnas tillräcklig information för att behörigheten ska kunna presenteras och förvaltas på ett begripligt sätt, exempelvis ett tydligt namn och vid behov en beskrivning av vilken åtkomst resursen ger.

Där VGR behörighetsportal ska hantera både faktiskt och önskat läge ska gränssnittet stödja nödvändig läsning och skrivning av relevanta objekt och relationer. Om gränssnittet endast stödjer delar av modellen, exempelvis import men inte provisionering, ska

begränsningen vara tydligt dokumenterad och hanteras i lösningsdesignen.

Målssystemets interna tekniska struktur behöver inte motsvara VGR behörighetsportals logiska datamodell. Om systemet har en komplex intern modell bör integrationsgränssnittet så långt som möjligt exponera en tydlig och stabil struktur och undvika att onödig systemspecifik komplexitet behöver hanteras i VGR behörighetsportal.

Import, provisionering och livscykel

Integrationen ska utformas så att VGR behörighetsportal kan hantera de informationsflöden och livscykelhändelser som krävs för den aktuella anslutningen. Vilka objekt och operationer som omfattas fastställs utifrån systemets behörighetsmodell och verksamhetens behov.

För import ska målssystemet kunna tillhandahålla aktuell information om de objekt som omfattas av anslutningen, exempelvis konton, behörighetsresurser och resurstilldelningar. Informationen ska vara tillräcklig för att objekten ska kunna identifieras, kopplas samman och stämmas av mot informationen i VGR behörighetsportal.

För provisionering ska målssystemet, där automatiserad provisionering ingår i lösningen, stödja de operationer som krävs för att realisera önskat läge. Beroende på vad som omfattas av anslutningen kan detta exempelvis innebära att:

- skapa, uppdatera, inaktivera och vid behov återaktivera konton
- skapa eller uppdatera behörighetsresurser där dessa ska hanteras av VGR behörighetsportal
- skapa och ta bort resurstilldelningar
- hantera relevanta attribut och giltighetsperioder

Provisioneringsoperationer bör där det är tekniskt möjligt vara idempotenta, så att en operation kan upprepas utan att skapa dubbla objekt, tilldelningar eller andra oönskade sidoeffekter. Integrationen bör så långt som möjligt kunna uttrycka vilket läge som ska gälla utan att vara beroende av en viss sekvens av tidigare operationer.

Integrationen ska ge förutsättningar för avstämning mellan faktiskt och önskat läge. Det innebär att VGR behörighetsportal ska kunna läsa tillbaka relevant information från målssystemet och identifiera exempelvis förändringar som inte har genomförts som avsett eller behörigheter som har tillkommit utanför den styrda processen.

Livscykeln för de objekt som omfattas av integrationen ska vara tydligt definierad. Det ska framgå hur exempelvis skapande, förändring, inaktivering, återaktivering och avslut hanteras samt vilka konsekvenser förändringar får för relaterade behörigheter och tilldelningar. Lösningen ska även kunna hantera relevanta återkomstscenarier utan att i onödan skapa nya objekt eller förlora kopplingen till tidigare information.

Gränssnittet ska kunna hantera de datamängder och den förändringstakt som är aktuell för systemet. Vid större datamängder ska lämpligt stöd finnas för exempelvis filtrering, paginering eller motsvarande mekanismer där detta är relevant för valt anslutningssätt.

Import och provisionering behöver inte använda samma tekniska gränssnitt eller ha samma grad av automatisering. Om någon del inte kan automatiseras ska detta vara tydligt dokumenterat och hanteras genom överenskommen alternativlösning, exempelvis manuell eller vidarebefordrad provisionering.

Säkerhet och teknisk robusthet

Integrationen ska utformas så att information och behörighetsförändringar hanteras säkert, tillförlitligt och spårbart. Säkerhetsnivån ska anpassas till informationens skyddsbehov, integrationens risker och VGR:s gällande säkerhetskrav.

Följande principer ska beaktas:

- **Säker kommunikation:** Information som överförs mellan VGR behörighetsportal och målssystemet ska skyddas under överföring med kryptering och andra säkerhetsmekanismer i enlighet med VGR:s gällande säkerhetskrav och informationens skyddsbehov.

- **Autentisering:** Integrationen ska använda en autentiseringsmetod som uppfyller VGR:s gällande säkerhetskrav utifrån informationens skyddsbehov och integrationens risker. Autentiseringsuppgifter, certifikat, nycklar och andra hemligheter ska hanteras säkert under hela sin livscykel.
- **Minsta privilegium:** Tekniska identiteter och integrationskonton ska endast ha de behörigheter som krävs för de operationer integrationen ska utföra. Läs- och skrivbehörigheter ska begränsas till relevanta objekt och information där detta är möjligt.
- **Felhantering och status:** Det anslutande systemet eller integrationsgränssnittet ska ge tillräcklig information om resultat, status och fel för att misslyckade operationer ska kunna identifieras, felsökas och följas upp. Informationen ska vid fel göra det möjligt att identifiera exempelvis berörd operation, objekt och typ av fel, utan att säkerhetskänslig information exponeras.
- **Spårbarhet och loggning:** Det ska finnas tillräcklig loggning i det anslutande systemet för att relevanta integrationsoperationer ska kunna följas upp och för att det ska gå att utreda när och varför fel eller oväntade förändringar har uppstått. Loggningen ska utformas så att känslig information inte exponeras i onödan.
- **Återhämtning vid fel:** Tillfälliga fel eller avbrott ska inte leda till okontrollerade eller dubbla förändringar. Det anslutande systemet och dess integrationsgränssnitt ska ge förutsättningar för att misslyckade operationer kan genomföras på nytt eller på annat sätt återställas på ett kontrollerat sätt.

Exakt utformning av autentisering, kryptering, nätverkskommunikation, loggning och andra säkerhetsmekanismer fastställs för respektive anslutning utifrån VGR:s gällande krav, informationens skyddsbehov och integrationens risker.

Test, dokumentation och förvaltning

Integrationen ska kunna testas, dokumenteras och förvaltas på ett sätt som säkerställer att den fungerar korrekt både vid införande och vid framtida förändringar. Det anslutande systemets

integrationsgränssnitt ska vara en dokumenterad och supporterad del av systemet.

Följande principer ska beaktas:

- **Testbarhet:** Det ska finnas möjlighet att testa integrationen innan driftsättning i produktion. Relevanta operationer, informationsflöden och livscykelscenarier ska kunna verifieras under förhållanden som i tillräcklig grad motsvarar produktionsmiljön.
- **Integrationsdokumentation:** Det ska finnas aktuell och tillräckligt detaljerad dokumentation för det integrationsgränssnitt som används. Dokumentationen ska beskriva relevanta objekt och datamodeller, attribut, relationer och operationer samt autentisering, felhantering, begränsningar och andra förutsättningar som krävs för att implementera och förvalta integrationen.
- **Supporterat gränssnitt:** Integrationsgränssnittet ska vara avsett och supporterat för den typ av användning som integrationen kräver. Lösningen bör inte vara beroende av odokumenterade gränssnitt eller interna strukturer som kan förändras utan hänsyn till externa integrationer.
- **Versionshantering och kompatibilitet:** Det ska vara tydligt hur integrationsgränssnittet versionshanteras och hur olika versioner förhåller sig till varandra. Förändringar bör så långt som möjligt införas på ett sätt som begränsar påverkan på befintliga integrationer.
- **Förändringshantering:** Förändringar i integrationsgränssnitt, datamodell eller funktionalitet som kan påverka integrationen ska kommuniceras i tillräckligt god tid för att möjliggöra analys, anpassning och test innan förändringen införs.
- **Dokumentation över tid:** Integrationsdokumentationen ska hållas aktuell och vara tillgänglig för VGR under hela den tid som integrationen används.

Vid större förändringar eller uppgraderingar som kan påverka integrationen ska det finnas möjlighet att verifiera integrationen i test innan förändringen införs i produktion. Målet är att anslutningen ska kunna förvaltas och vidareutvecklas utan onödigt beroende av enskilda personer, speciallösningar eller odokumenterad kunskap.

Frågor och mer information

För frågor om anslutning, tekniska förutsättningar eller val av integrationsmodell kan du kontakta teamet för VGR behörighetsportal. Ansökan om anslutning och aktuellt underlag finns via Serviceportalen.

- **Ansökan om anslutning:**
  Kunskapsdokument (KB) KB0028399 – *VGR behörighetsportal – ansökan om anslutning*
- **Kontakt:**
  behorighetsportal@vgregion.se
- **Insidan:**
  https://insidan.vgregion.se/forvaltningar/koncernkontoret/stod-och-tjanster/system-a-o/vgr-behorighetsportal/
- **Relaterade anslutningsdokument:**
  Inledning och generell beskrivning
  Anslutningsguide – active directory (AD)
  Anslutningsguide - administrativa medarbetaruppdrag (AMU)