Sveriges Kommuner och Regioner

PM

Vårt dnr:
Xx

2025-12-17

Kenneth Zetterberg

Krav på behörighetshantering vid upphandling av verksamhetssystem

Sammanfattning

Detta dokument ger ett gemensamt stöd för kommuner vid upphandling av verksamhetssystem med krav på identitet- och behörighetshantering. Syftet är att bidra till en enhetlig och säker tillämpning av nationella rekommendationer inom området, i linje med SKR:s arbete i Handslaget för välfärdsutveckling genom digitalisering.

Dokumentet beskriver tekniska grundkrav som stödjer säker autentisering, centraliserad behörighetsstyrning, automatiserad kontohantering och spårbarhet. Kraven är formulerade som SKA- eller BÖR-krav, där varje upphandlande organisation behöver bedöma relevans och rimlighet utifrån eget sammanhang.

En särskild del belyser pseudonymisering av identitetsattribut som en framåtsyftande åtgärd för stärkt integritetsskydd. Tillsammans syftar kraven till att driva marknaden mot ökad standardisering, interoperabilitet och säkerhet i kommuners digitala ekosystem.

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

Innehåll

Inledning 3
Tekniska grundkrav för identitet och åtkomst 4
Pseudonyminsering av identitetsattribut 8

Inledning

Detta dokument är framtaget som ett generiskt stöd för upphandling av verksamhetssystem. Syftet är att ge kommuner en gemensam grund att utgå ifrån vid formulering av krav på identitet- och behörighetshantering vid upphandling.

Syftet som avses är att ge stöd för krav på behörighetshantering i system som hanteras i den egna organisationen. För system som avses hantera behörigheter via federationer med användare från andra organisationer, behöver krav från Enas samordnade identitet och behörighet inväntas[1].

Kraven i dokumentet är formulerade som **SKA**- eller **BÖR**-krav. Dessa markeringar anger vilken nivå av angelägenhet som rekommenderas, men det är alltid upp till varje enskild upphandling att värdera om kravet är lämpligt, rimligt och proportionerligt för det aktuella systemet och sammanhanget.

Ett centralt syfte med kraven är att driva utvecklingen på marknaden. Det kan innebära att vissa krav kan upplevas som utmanande för leverantörer. Samtidigt är det viktigt att beställare gör en avvägning mot praktisk rimlighet – olika marknadssegment har olika förutsättningar och teknisk mognad.

För hårt ställda krav riskerar att begränsa leverantörernas vilja eller möjlighet att lämna anbud vid en upphandling. Ett sätt att hantera denna utmaning, och samtidigt driva marknadens utveckling framåt, är att utforma avtalet så att vissa kravområden behöver uppfyllas inom en definierad tidsperiod efter avtalstecknande. På så sätt kan upphandlingen både främja innovation och säkerställa en stegvis anpassning till den önskade målbilden.

Kraven i detta dokument följer SKR:s rekommendationer i Handslagets arbete inom identitet- och behörighetshantering[2]. De är därför en del av en större samlad strategi för att skapa en långsiktigt hållbar, säker och standardiserad hantering av identitet och behörigheter inom kommuner.

SKR har som ambition att vid behov på årlig basis uppdatera detta dokument.

---

[1] Enas federationsinfrastruktur är ett pågående regeringsuppdrag när denna text skrivs.
[2] Handslagets rekommendationer för identitet och behörighet

Tekniska grundkrav för identitet och åtkomst

Dessa krav är grundläggande för att följa Handslagets rekommendation.

Krav 1:

Tjänsten **SKA** tillhandahålla API:er för extern behörighetshantering, så att roller, grupper och åtkomsträttigheter kan administreras från ett externt system.

Acceptanskriterier:

- Leverantören **SKA** kunna visa dokumentation (t.ex. API-specifikation) som beskriver hur externa system kan administrera roller, grupper och åtkomsträttigheter.
- Leverantören **SKA** kunna visa exempel på anrop som möjliggör administration av dessa objekt via API.
- Funktionaliteten **SKA** kunna verifieras i en test- eller demomiljö på begäran.

Krav 2:

API:er för behörighetshantering **SKA** följa standarden SCIM (System for Cross-domain Identity Management) för att möjliggöra automatiserad provisionering och avprovisionering av användare och grupper.

Acceptanskriterier:

- Leverantören **SKA** tillhandahålla dokumentation som visar att API:erna följer SCIM-standarden.
- Det **SKA** finnas stöd för de vanligaste SCIM-operationerna (Create, Read, Update, Delete) för användare och grupper.
- Följsamhet mot SCIM **SKA** kunna verifieras i test- eller demomiljö, exempelvis genom integration med ett externt IdM-system.

Kommentarer: Krav 1 och Krav 2 är uppdelat eftersom det inom vissa områden finns fungerande standarder och kravet på SCIM kan vara onödig. Samtidigt visar erfarenheten att om alla leverantörer följer SCIM så förenklas den övergripande behörighetshanteringen.

Krav 3:

Tjänsten **SKA** stödja autentisering via en utpekad identity provider (IdP/OP).

Acceptanskriterier:

- Leverantören **SKA** kunna demonstrera konfiguration mot beställarens eller annan utpekad IdP.
- Dokumentation **SKA** tillhandahållas som beskriver hur tjänsten integreras med IdP:n.
- Test av autentisering via IdP **SKA** kunna genomföras i testmiljö.

Kommentarer: Acceptanskriteriet att kunna demonstrera konfiguration mot beställarens eller annan utpekad IdP, kan justeras och i stället demonstrerar leverantören mot egen eller annan IdP.

Krav 4:

Tjänsten **SKA** stödja autentiseringsprotokollen SAML2 och/eller OpenID Connect. Vid användning av SAML2 **SKA** tjänsten kunna ta emot och tolka autentiseringskontext (AuthnContext) enligt tillämplig federationsprofil, exempelvis Sweden Connect. Tjänsten **SKA** därmed kunna avgöra vilken tillitsnivå (Level of Assurance) som använts vid autentiseringen, i enlighet med Digg:s tillitsramverk.

Acceptanskriterier:

- Leverantören **SKA** kunna visa konfiguration och exempel på autentiseringsflöden för SAML2 och/eller OpenID Connect.
- Det **SKA** kunna verifieras att tjänsten kan ta emot en SAML2-respons som innehåller AuthnContextClassRef och tolka den enligt tillämplig federationsspecifikation (t.ex. Sweden Connect).
- Funktionalitet **SKA** kunna testas i en demomiljö genom autentisering med en test-IdP.

Krav 5:

Tjänsten **SKA** stödja Just In Time (JIT) provisionering av användarkonton via autentisering med SAML2 och/eller OpenID Connect (OIDC).

Acceptanskriterier:

- Leverantören **SKA** kunna demonstrera hur ett användarkonto skapas automatiskt när en användare autentiserar sig första gången via en utpekad IdP.
- Det **SKA** vara möjligt att tilldela roller och rättigheter vid kontoskapandet baserat på attribut i autentiseringstoken.

- Funktionaliteten **SKA** kunna verifieras i en test- eller demomiljö.

Kommentar: Använd kravet om JIT-provisionerna där det är önskvärt.

Krav: 6:

Tjänsten **SKA** i SAML2 ”biljett” eller genom OIDC kunna ta emot och hantera en sluttidpunkt för JIT-provisionerade konton, så att konton automatiskt gallras vid den tidpunkten.

Acceptanskriterier:

- Vid JIT-provisionering **SKA** systemet kunna sätta en giltighetstid eller sluttidpunkt för kontot.
- Kontot **SKA** automatiskt avaktiveras eller tas bort när sluttidpunkten passerats.
- Systemet **SKA** logga både skapande och gallring av JIT-provisionerade konton för spårbarhet.

Krav: 7:

Tjänsten **SKA** automatiskt kunna avaktivera användarkonton som varit inaktiva under en konfigurerbar tidsperiod.

Acceptanskriterier:

- Tjänsten **SKA** innehålla en konfigurerbar parameter som anger efter hur lång tids inaktivitet ett konto ska avaktiveras.
- Tjänsten **SKA** kunna notifiera administratör eller annan utpekad funktion innan avaktivering sker.
- När kontot avaktiveras **SKA** det loggas med tidpunkt, användaridentitet (t.ex. GUID) och orsak.
- Leverantören **SKA** kunna visa att automatisk avaktivering fungerar i en test- eller demomiljö.

Kommentar: Automatiserad hantering av inaktiva konton minskar risken för obehörig åtkomst och stärker informationssäkerheten. En flexibel konfiguration gör det möjligt för kommunen att anpassa tidsintervallen efter sina egna säkerhetspolicys och verksamhetsbehov

Krav: 8:

Tjänsten **SKA** inte tillåta att privilegierade behörigheter (t.ex. administratörsroller eller systemägarnivå) tilldelas via JIT-provisionering.

Acceptanskriterier:

- <Leverantören **SKA** kunna visa att JIT-provisionering endast kan användas för vanliga användarroller och att privilegierade roller inte kan skapas eller tilldelas via JIT.
- Det **SKA** finnas kontroller som förhindrar att en användare automatiskt tilldelas privilegierade behörigheter vid JIT-provisionering.
- Eventuella försök att tilldela privilegierade roller via JIT **SKA** loggas och rapporteras.

Krav 9:

Tjänsten **SKA** följa Digg:s tillitsramverk och Sweden Connects tekniska ramverk för SAML2, inklusive krav på att kryptografiskt nyckelmaterial hanteras i en kryptografisk hårdvarumodul (HSM) eller motsvarande säkerhetslösning som uppfyller ramverkets specifikationer.

Acceptanskriterier:

- Leverantören **SKA** tillhandahålla intyg, certifieringar eller revisionsrapporter som styrker att HSM-lösningen uppfyller kraven i Digg:s och Sweden Connects ramverk.
- Beskrivning av hur nyckelmaterial hanteras, roteras och skyddas **SKA** ingå i leverantörens säkerhetsdokumentation.
- Beställaren **SKA** kunna granska dokumentationen och vid behov genomföra stickprov eller revision.

Kommentarer: Krav kan ställas vid upphandling av system som hantera kritiska eller särskilt skyddsvärda informationsmängder. Generellt är det sällsynt krav som endast behöver ställs på ett mycket fåtal system.

Krav 10:

Tjänsten **SKA** logga alla relevanta autentiserings- och behörighetshändelser på ett sätt som möjliggör revision, spårbarhet och uppföljning.

Acceptanskriterier:

- Loggar **SKA** innehålla information om tidpunkt, användaridentitet (t.ex. GUID), utförd åtgärd, resultat (lyckad/misslyckad) och eventuell associerad roll eller behörighet.
- Loggar **SKA** omfatta händelser såsom inloggningar, misslyckade inloggningsförsök, tilldelning eller borttagning av roller, JIT-

provisionering, gallring av konton och ändringar av åtkomsträttigheter.
- Loggar **SKA** vara åtkomliga för beställarens säkerhets- och revisionsfunktioner via ett dokumenterat gränssnitt eller exportfunktion.
- Loggar **SKA** skyddas mot manipulation och rensas enligt fastställda gallringsregler.

***Kommentar*:** Detta krav säkerställer att kommunen kan upptäcka avvikelser, genomföra revision och uppfylla krav på spårbarhet i enlighet med både säkerhetsstandarder och GDPR.

Pseudonyminsering av identitetsattribut

Det finns ingen uttalad rekommendation eller krav från SKR eller annan aktör om allmänt pseudonymisering av identiter, dvs. att personnummer eller annan identitetsattribut ersätts så att användarens riktiga identitet inte avslöjas. Att i IT-system lagra och hantera pseudonymiserad användaridentitet är säkrare. Intrång och stöld av data har visar att stor skada uppkommer om det kopplat till känslig data finns identitetsattribut som gör att en individ kan bli igenkänd. Detta ligger i linje med GDPR:s krav på dataminimering

Eftersom dessa BÖR-krav är att se som nya och tuffa rekommenderas de att bifogas till upphandlingar för att visa marknadsaktörer att det är åt det här hållet som utvecklingen är på väg.

Krav 11:

Systemet **bör** kunna hantera behörigheter, så att identiteten representeras av en unik GUID (Globally Unique Identifier), eller motsvarande, från en separat katalog.

Krav 12:

Systemet **bör** inte använda personnummer som primär identitetsattribut, utan endast använda och lagra GUID, eller likande, som unik identifierare för användare.

Krav 13:

Systemet **bör** stödja att GUID, eller likande, används i alla autentiserings- och behörighetsflöden, inklusive loggning och rapportering, för att stärka integritetsskyddet och underlätta central identitetshantering.

Krav 14:

Systemet **bör** inte lagra personnummer i verksamhetssystemet, för att minska sårbarhet vid dataintrång och förhindra dataläckor.