Sveriges Kommuner och Regioner

VÄGLEDNING

2026-10-16

Vårt dnr:
Klicka eller tryck här för att ange text.

Åtkomstvägledning KLASSA 5

Att identifiera alla de informationsmängder som finns inom en verksamhet kan vara svårt. Men genom att utgå från t.ex. de informationstillgångar eller system som en organisation använder (eller planerar att införa) kan man strukturera upp informationsmängderna och lättare hantera eventuella risker och hot.

KLASSA är ett självskattningsverktyg som fungerar som en länk mellan verksamhetens behov av skydd och tekniken som kan säkerställa detta skydd. Skydden kan vara såväl tekniska som organisatoriska och benämns ofta säkerhetsåtgärder (exempelvis i NIS2) eller skyddsåtgärder (exempelvis i GDPR).

Med hjälp av KLASSA:s kravkataloger och automatiserade flöden underlättas arbetet med att värdera de informationsmängder, system eller motsvarande tillgångar som en verksamhet har. Därmed blir det också enklare att skapa handlingsplaner med de identifierade säkerhetsåtgärder som behöver vidtas för att hålla verksamheten trygg, samt säkerställa relevant regelefterlevnad.

Genom att använda KLASSA kan verksamheten också sammanställa behovet av säkerhet avseende sina informationsmängder, inför upphandlingar av nya system eller verktyg.

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

Åtkomstvägledning KLASSA 5 1
Innehåll 2
Åtkomstvägledning - KLASSA 5 3
Om federerad åtkomst till KLASSA 5 3
Identitetsbegrepp och attribut 4
Identitetsbegrepp 4
Attribut 4
Vägval för åtkomst 5
Anslutning via Svenska federationer 5
Anslutning via Sweden Connect 6
Anvisningstjänst vid federativ anslutning 7
Bilateral anslutning 7
Skillnader mellan KLASSA som tjänst och onprem 2
Behov av ytterligare stöd 2

Åtkomstvägledning - KLASSA 5

Denna vägledning för åtkomst till KLASSA kan tillämpas både för åtkomst till tjänsten KLASSA och när KLASSA körs som lokal installation, även kallad KLASSA onprem.

För KLASSA onprem finns en särskild vägledning som går in på djupet i implementationen av detta i KLASSA.

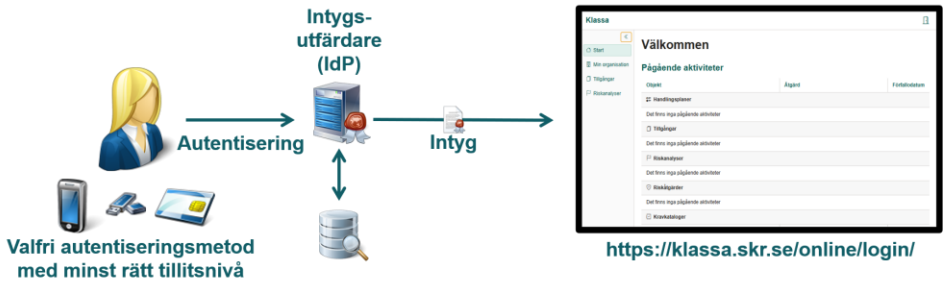
För användarna av KLASSA finns en användarvägledning som stöttar användare genom inloggningen och vidare in i KLASSA.

Alla vägledningar för KLASSA finns här:
https://klassa.skr.se/sidor/stodmaterial/a-klassa-5-vagledning.

Om federerad åtkomst till KLASSA 5

KLASSA 5 har stöd för legitimering med e-legitimation, e-tjänstelegitimation samt andra metoder för delegerad åtkomst via Security Assertion Markup Language (SAML), och på sikt OpenID Connect (OIDC), helt i enlighet med:

- Diggs förslag om en sammanhållen infrastruktur för identitet & behörighet som går under namnet Ena
- SKR:s rekommendation för identitet & behörighet
- Ineras referensarkitektur för identitet & åtkomst



Dessa ramverk har gemensamt att varje organisation själv ansvarar för sin förmåga att autentisera användarna och ställa ut elektroniska intyg. I praktiken realiseras detta med en intygsutfärdare (IdP), en eller flera autentiseringsmetoder samt en tillförlitlig källa för attribut.

KLASSA har en auktorisationsförmåga som förlitar sig helt på att autentisering sker utanför KLASSA. Beslut om åtkomst grundas på elektroniska intyg och attribut inom ramen för de federationer som KLASSA ingår i.

KLASSA är följsam mot de tekniska ramverk som reglerar användningen av SAML inom respektive federation. I bilaterala sammanhang, där en ömsesidig tillit etableras mellan KLASSA och organisationens intygsutfärdare (IdP), används klassisk SAML WEBSSO med implementationsprofilen saml2int som inspiration.

På sikt kommer OIDC att implementeras och i förlängningen OpenID Federation när det realiseras på bredare front i Sverige.

Organisationen är informationsägare av innehållet i KLASSA och med det följer ansvaret att besluta om tillitsnivåer på de e-legitimationer eller motsvarande identifieringsmetoder som krävs för åtkomst till organisationens information i KLASSA.

Identitetsbegrepp och attribut

Identitetsbegrepp

I många organisationer förekommer redan etablerade identitetsattribut, såsom subject-id, EPPN, HSAid, orgid, GUID och andra persistenta pseudonymer vilka alla fungerar i KLASSA.

Det går också att använda personnummer och samordningsnummer även om exponeringen av dessa bör om möjligt minimeras med respekt för den personliga integriteten.

KLASSA är att betrakta som en allätare vad gäller identitetsbegrepp. Det viktiga är att identitetsbegrepp är globalt unika och unika över tid. Det är inte ett unikt krav från KLASSA utan det är gängse för identitetsbegrepp.

Identitetsbegreppet förpackas i för ändamålet lämpligt attribut som ska vara standardiserat. KLASSA stödjer idag följande attribut:

- *subject-id* (urn:oasis:names:tc:SAML:attribute:subject-id)
- *eduPersonPrincipalName* (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)
- *employeeHsaId* (urn:oid:1.2.752.29.6.2.1)
- *personalIdentityNumber* (urn:oid:1.2.752.29.4.13)

Det rekommenderade attributet är *subject-id*.

Attribut

Vi rekommenderar även användning av följande attribut till KLASSA:

- *mail* (urn:oid:0.9.2342.19200300.100.1.3)
- *givenName* (urn:oid:2.5.4.42)
- *sn* (urn:oid:2.5.4.4)

Mejladressen används när KLASSA vill påkalla på uppmärksamhet i form av avisering. Förnamn och efternamn används i användardialogen. Om dessa uppgifter saknas kommer användaren vid första registreringen att få ange dessa uppgifter. Hur en användare ansluts första gången till KLASSA beskrivs i användarvägledningen för KLASSA.

Teknisk specifikation om dessa attribut finns här:

- Attribute Specification for the Swedish eID_Framework (Digg)
- Common Attributes for SAML Federation (Internetstiftelsen)

Vägval för åtkomst

I första hand rekommenderas anslutning via någon av de nationella federationerna för åtkomst till KLASSA som tjänst. De alternativ som står till buds är:

- Anslutning via Svenska federationer (Internetstiftelsen)
- Anslutning via Sweden Connect (Digg)

Det är också möjligt att ansluta bilateralt till KLASSA.

Anslutning via Svenska federationer

Internetstiftelsen är federationsoperatör för de federationer som finns under Svenska federationer. För åtkomst till KLASSA finns dels "Federation för kommunal verksamhet" (Fedkom) samt "Åtkomstlösning till KLASSA" (Access), skillnaden är vilken slags organisationstyp ni är.

Information om avtal, priser och anslutning till Svenska federationer finns här.

För organisationer som är medlemmar i någon av Internetstiftelsens andra federationer; Sambi eller Skolfederation, ges en rabatt på den del av medlemskapet i Svenska federationer och samma SAML-metadata kan tillgängliggöras för åtkomst till KLASSA, efter att avtal har tecknats med Internetstiftelsen.

Kolla här (Skolfederation) eller här (Sambi) ifall din organisation redan är medlem.

Utöver det rent administrativa krävs ytterligare ett aktivt val för att tillgängliggöra SAML-metadata för KLASSA. SAML-metadata i organisationens intygsutfärdare (IdP) behöver tekniskt ge sitt medgivande genom deklaration i metadata.

Deklarationen görs enligt följande:

```
<md:EntityDescriptor … >
  <md:Extensions>
    <mdattr:EntityAttributes>
      <saml:Attribute Name="https://id.openfed.se/entityattributes/opt-in"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>https://id.openfed.se/entityattributes/opt-in/yes
        </saml:AttributeValue>
    </saml:Attribute>
  </mdattr:EntityAttributes>
</md:Extensions>
```

Klassas SAML-metadata hittar ni här:

- https://md.openfed.se/prod/md/metadata_set1_sp_01.xml (Fedkom)
- https://md.openfed.se/prod/md/metadata_set2_sp_01.xml (Access)

Vill ni inte dela befintligt SAML-metadata eller är ny som medlem så tillgängliggör ni helt enkelt nytt metadata enligt anvisningarna på https://svenskafederationer.se/klassa. Det är Internetstiftelsen som är operatör och dem ni kontaktar om ni har frågor kring t.ex metadatat som ska tillgängliggöras.

Här hittar ni all information ni behöver om Svenska federationer, kontakta info@svenskafederationer.se för mer information.

Anslutning via Sweden Connect

Federationen Sweden Connect, som tillhandahålls av Myndigheten för digital förvaltning (Digg), är sannolikt mest känd för sin roll som Sveriges infrastruktur för gränsöverskridande e-legitimering inom eIDAS. Genom Sweden Connect kan svenska e-tjänster använda e-legitimationer från andra EU- och EES-länder som anmälts enligt eIDAS-förordningen.

Sweden Connect är också en frivillig identitetsfederation som möjliggör användning av svenska e-legitimationer, inklusive e-tjänstelegitimationer, som uppfyller tillämpliga krav och är anslutna till federationen. Rent tekniskt innebär det att en förlitande part kan använda dessa e-legitimationer via ett standardiserat SAML-gränssnitt, där den förlitande parten agerar Service Provider (SP) eller IdP-proxy.

Sweden Connect har ännu inte etablerats som den naturliga federationen för åtkomst till e-tjänster i tjänsten. Inom ramen för initiativet Samordnad identitet och behörighet utvecklar Digg en gemensam svensk infrastruktur för identitet, behörighet och åtkomst över organisations- och sektorsgränser. Målet är att ge medarbetare enklare och säkrare åtkomst till digitala tjänster och information.

Lösningen är fortfarande under uppbyggnad och ännu inte öppen för anslutning. Ambitionen är att ansluta KLASSA när förutsättningarna finns och lösningen är tillgänglig.

Anvisningstjänst vid federativ anslutning

KLASSA har en inbyggd anvisningstjänst för dem som ansluter vi ovan nämnda federationer. För åtkomst till KLASSA som tjänst anges följande URL https://klassa.skr.se/online/login/.



Där visas en lista över tillgängliga intygsutfärdare (IdP). I listan väljer ni er intygsutfärdare för inloggning till KLASSA varpå er webbläsare styrs till er intygsutfärdare (IdP). Efter en lyckad inloggning styrs er webbläsaren till startsidan i KLASSA. Användarvägledningen stöttar användare genom inloggningen och vidare in i KLASSA. Se https://klassa.skr.se/sidor/stodmaterial/a-klassa-5-vagledning.

Namnet på intygsutfärdaren (IdP) i listan hämtas från *mdui:DisplayName* i SAML-metadata från er intygsutfärdare (IdP). Om namnet ser märkligt ut i listan behöver ert SAML-metadata uppdateras med avseende på detta.

Bilateral anslutning

Vägen via de nationella federationerna är förstahandsvalet för åtkomst till KLASSA som tjänst.

För de organisationer som av olika anledningar inte önskar använda de nationella federationerna för åtkomst till KLASSA som tjänst finns möjlighet att upprätta en bilateral relation mellan organisationens intygsutfärdare (IdP) och KLASSA som tjänst.

För att etablera en bilateral relation med tjänsten KLASSA utgår en administrativ avgift från Adda på 10.000 SEK för att etablera organisationstillit.

Organisationen ansvarar för livscykelhanteringen av det kryptografiska nyckelmaterialet som är en del av SAML-metadata vilket också styr intervallet hur ofta SAML-metadata byts.

En URL till organisationens SAML-metadata skickas till klassa@skr.se. Uppge även organisationsnamn och kontaktuppgifter.

Adda/SKR kommer att verifiera att det finns ett avtal tecknat för KLASSA och för bilateral tillit samt säkerställa tilliten till organisations SAML-metadata.

Därefter kommer Adda/SKR att lägga upp organisationens intygsutfärdare (IdP) i KLASSA som tjänst:



Namn är ett administrativt namn för att skilja organisationerna åt i KLASSA.

Slug representerar en del av den URL som används som åtkomst. Exempelvis om *Slug* anges till *adda* blir URL för inloggningen https://klassa.skr.se/online/org/adda. När ni ansluter till denna URL styrs er webbläsare till er intygsutfärdare (IdP). Efter en lyckad inloggning styrs er webbläsaren vidare till startsidan i KLASSA.

Metadata-URL är den URL där organisationens intygsutfärdare (IdP) exponerar aktuellt SAML-metadata för den bilaterala relationen. KLASSA läser in SAML-metadata löpande vilket innebär att ni kan göra förändringar av ert SAML-metadata utan att behöva kontakta Adda/SKR.

När organisationens intygsutfärdare (IdP) är registrerad i KLASSA som tjänst skapas en *Metadata-URL* som organisationen adderar i sin intygsutfärdare (IdP). Exemplet ovan ger följande URL för SAML-metadata:
https://klassa.skr.se/online/saml2/managed-sp-metadata/klassa-adda.

Skillnader mellan KLASSA som tjänst och onprem

Denna vägledning beskriver i huvudsak åtkomst till KLASSA som tjänst. Den är tillämpningsbar även för KLASSA onprem, med den skillnaden att den första SAML-konfigurationen inte kan göras via användargränssnittet av förståeliga skäl. Detta beskrivs närmare i installationsvägledningen för onprem som finns på https://klassa.skr.se/sidor/stodmaterial/a-klassa-5-vagledning.

En ytterligare skillnad är att KLASSA onprem kan fånga användarens organisationstillhörighet genom att uttrycka organisationsnumret i attributet *OrgID*. Det är också möjligt att tilldela roller via attributet *klassa_[roll]*. Attributen har företräde framför det som är angivet i KLASSA.

Behov av ytterligare stöd

Adda/SKR tillhandahåller administrativt stöd via klassa@skr.se

Har ni behov av djupare tekniskt stöd rekommenderar Adda/SKR att avropa konsultstöd inom ramen för ramavtal IT-konsulttjänster 2021 vid dynamisk rangordning inom kompetensområdet IT-, informations- och cybersäkerhet.

Se avropsvägledningen för ytterligare information:
https://klassa.skr.se/sidor/stodmaterial/a-klassa-5-vagledning