Sveriges Kommuner och Regioner

VÄGLEDNING

2026-06-03

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

Federationsvägledning 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

Federationsvägledning - 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 SAML-implementationen 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 åtkomst till Klassa 5

Klassa 5 har förmågan att konsumera e-tjänstelegitimering, e-legitimering och andra autentiseringsmetoder via SAML, och på sikt 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 inte några inbyggda autentiseringsförmågor utan förlitar sig helt på att autentisering sker utanför Klassa och att elektroniska intyg inom ramen för SAML och OIDC används för konsumtion av identitet och behörighet.

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 Connect Federation när det realiseras på bredare front i Sverige.

Organisationen är informationsägare av innehållet i Klassa och med det följer ansvaret att besluta om vilken minsta nivån av tillit till e-tjänstelegitimationen/e-legitimationen eller motsvarande som krävs för att få åtkomst till organisationens informationsinnehåll i Klassa.

Identitetsbegrepp och attribut

Identitetsbegrepp

I många organisationer förekommer redan användningen av unika identitetsbegrepp såsom EPPN, HSAid, orgid, mejladress, GUID och andra persistenta pseudonymer vika 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 bör vara standardiserat. Exempelvis:

- *eduPersonPrincipalName* för EPPN.
- *personalIdentityNumber* för person- och samordningsnummer.

Det fungerar också att förpacka identitetsbegreppet i *subject-id*.

Attribut

Vi rekommenderar även följande attribut till Klassa:

- *mail* för mejladress
- *givenName* för förnamnet
- *sn (surname)* för efternamnet

Mejladressen används som intern identifierare i Klassa och även 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.

Vägval för åtkomst

I första han rekommenderas anslutning via någon av de nationella federationerna för åtkomst till Klassa som tjänst:

Vill du ansluta via Sweden Connect?

Federationen Sweden Connect som tillhandahålls av Digg har flera ändamål. För de flesta är Sweden Connect sannolikt mest känd som Sveriges eIDAS-nod där e-legitimationer inom EU som anmälts inom ramen för eIDAS-förordningen kan konsumeras. Det innebär att många av de som använder Klassa också redan har en avtalsrelation med Digg för det syftet.

Förmågan att konsumera e-legitimationer inom ramen för eIDAS är den anslutningen som de allra flesta gjort till Sweden Connect. Rent tekniskt innebär det att organisationen visar upp ett e-tjänstegränssnitt (Service Provider, SP) för Sweden Connects eIDAS-nod som uppträder som en intygsutfärdare (Identity Provider, IdsP).

För åtkomst till Klassa krävs att organisationen ansluter sin intygsutfärdare (IdP) i rollen som just IdP, inte i rollen som e-tjänst (SP) till Sweden Connect. Det är ett större steg att ansluta en intygsutfärdare (IdP) till Sweden Connect då det kräver följsamhet mot Sweden Connects tekniska ramverk.

Information för anslutning till Sweden Connect finns här.

Kontakta info@digg.se för mer information.

Är din organisation ansluten till Sambi eller Skolfederation?

Om organisationen är medlem i Sambi eller Skolfederation och avtal är tecknat med Internetstiftelsen för tjänsten *Svenska federationer* samt *Federation för kommunal verksamhet* så tillgängliggörs SAML-metadata för Klassa.

I de fall organisationen är med i Skolfederation eller Sambi, men inte vill dela just det SAML-metadatat med Klassa så är det möjligt för Internetstiftelsen att tillgängliggöra annat SAML-metadata för Klassa. Skicka det till info@svenskafederationer.se. Uppge även organisationsnamn och kontaktuppgifter.

Osäker på om ni är medlemmar? Kolla här eller här.

Det krävs ytterligare ett aktivt val för att tillgängliggöra SAML-metadata för Klassa och det är att SAML-metadata i organisationens intygsutfärdare (IdP) taggas. Det är dels för att organisationen även tekniskt ska ge sitt

medgivande, men också för att i ett scenario med flera intygsutfärdare (IdP:er) tagga den eller de intygsutfärdare (IdP) som ska dela sitt metadata med Klassa.

Taggningen 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>
```

Är din organisation inte ansluten till Sambi eller Skolfederation men vill ansluta federativt?

Det är också möjligt för dem som inte är medlem i Sambi eller Skolfederation att teckna avtal med Internetstiftelsen för tjänsten *Svenska federationer* samt *Åtkomstlösning till Klassa* för att tillgängliggöra SAML-metadata för Klassa.

All information och avtal finns på https://svenskafederationer.se/klassa

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.

Är din organisation inte ansluten till någon av ovanstående federationer och vill ansluta utan att federera?

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.

För organisationer som använder en lokal installation av Klassa, Klassa onprem, är en bilateral lösning sannolikt den rätta vägen fram. För Klassa onprem finns en särskild vägledning som går in på djupet i SAML-implementationen i Klassa.

Se https://klassa.skr.se/sidor/stodmaterial/a-klassa-5-vagledning.

SAML-metadata utbyte för Klassa som tjänst

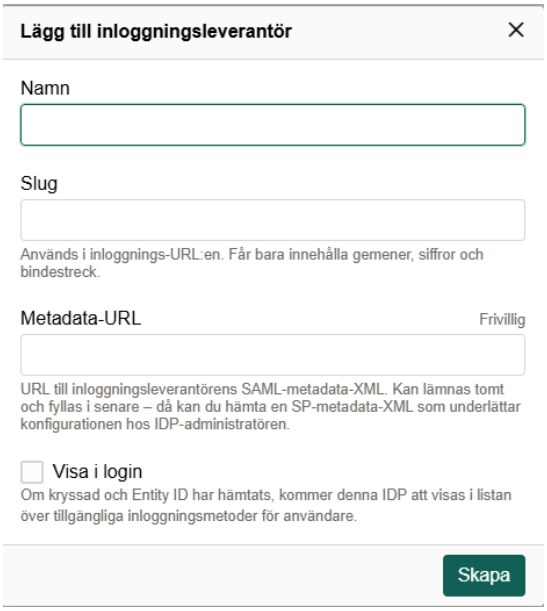
För att etablera en bilateral relation med tjänsten Klassa utgår en administrativ avgift från Adda på 10.000 SEK för att etablera organisationstillit och per tillfälle när SAML-metadata utbyts.

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 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 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

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