Vägledning till eIDAS

Om eIDAS och att ansluta till Sweden Connect
Reviderad version: Januari 2024

Sveriges Kommuner och Regioner

Vägledning till eIDAS

2019 utkom Sveriges Kommuner och Regioner (SKR) med *Vägledning för anslutning till eIDAS: Inloggning till svenska digitala tjänster med utländska e-legitimationer*. Initiativet till vägledningen grundade sig i att det vid den tidpunkten endast var ungefär en tredjedel av Sveriges kommuner och en femtedel av regionerna som var anslutna till den svenska landsnoden för eIDAS.

Målbilden som beskrevs i den vägledningen var att samtliga kommuners och regioners offentliga tjänster skulle acceptera utländska e-legitimationer för autentisering till e-tjänster. Vägledningen riktade sig till personer med ett övergripande ansvar för implementering av e-legitimationslösningar hos kommuner och regioner.

Sedan vägledningen publicerades har ny lagstiftning tillkommit som ökar kravet på kommuner och regioner att kunna konsumera utländska e-legitimationer. Det har även identifierats ett behov av att komplettera vägledningen avseende juridiken som ligger till grund för kraven, samt den tekniska implementeringen.

Vid skrivande stund (november 2023) är ungefär två tredjedelar av kommunerna och knappt hälften av regionerna anslutna till den svenska landsnoden för eIDAS[1] som återfinns i Myndigheten för digital förvaltning (Digg) federation Sweden Connect. Denna vägledning är framtagen för att hjälpa de organisationer som ännu inte har anslutit sig, att uppfylla den lagstadgade skyldigheten.

[1] Uppskattningen är baserad på metadata i Sweden Connect i november 2023.

Innehåll

Inledning

Syftet med denna vägledning är att på överskådlig nivå beskriva eIDAS samt ett antal alternativa vägval som kommuner och regioner kan välja för att ansluta till den svenska eIDAS-noden i Sweden Connect.

Vägledningen riktar sig till dig som är beslutsfattare, utvecklingschef, CIO, IT-ansvarig eller motsvarande samt nyckelpersoner som arbetar med e-legitimering och e-tjänster i kommuner och regioner.

Målbilden är att kommunernas och regionernas offentliga e-tjänster accepterar utländska e-legitimationer som anmälts till EU-kommissionen genom att "Foreign eID", läggs till i listan över de e-legitimationer som användaren kan välja mellan.

Exempel från Region Gotland

En användare som har en utländsk e-legitimation, som är godkänd enligt eIDAS-kraven, kommer att välja Foreign eID. Användaren kommer därefter till en sida där EUs medlemsstater listas, och väljer det land som hen har skapat sin e-legitimation i. Därefter visas det landets olika e-legitimationer som kan användas och inloggningen sker därefter i de olika legitimeringstjänsterna för respektive e-legitimation.

SKR:s målbild är också att alla av staten godkända e-legitimationer ska accepteras.

Avgränsning

eIDAS-förordningen reglerar i huvudsak två områden, elektronisk identifiering och betrodda tjänster. Denna vägledning fokuserar främst på elektronisk identifiering och de skyldigheter som kommuner och regioner har när det kommer till att konsumera e-legitimationer från andra medlemsstater. Vidare ges praktiskt vägledning i hur kommuner och regioner kan ansluta till Sweden Connect.

Vägledningen kommer inte att beröra betrodda tjänster, dvs digitala underskrifter, stämplar eller certifikat, och inte heller frågor kopplade till att bli en leverantör av e-legitimationer, eller att få en e-legitimation anmäld till EU-kommissionen. EU:s förordning om en gemensam digital ingång behandlas inte närmare än att beskriva vad förordningen är och den koppling som finns till eIDAS-förordningen.

Vägledningen berör inte heller eventuella dataskyddsfrågor som kan aktualiseras vid konsumtion av e-legitimationer.

Om eIDAS-förordningen

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS) är en EU-förordning som syftar till att inom unionen skapa en enhetlig och säker ram för elektroniska identifieringar och betrodda tjänster. Förordningen trädde i kraft den 1 juli 2016 och ersatte därmed det tidigare signaturdirektivet.

Några viktiga aspekter av eIDAS-förordningen:

1. **Elektronisk identifiering:** eIDAS fastställer regler för säker och interoperabel elektronisk identifiering. Det innebär att medborgare, företag och offentliga myndigheter ska kunna använda elektroniska identiteter från ett medlemsland för att genomföra affärs-transaktioner och få tillgång till offentliga tjänster i ett annat medlemsland.

2. **Betrodda tjänster:** Förordningen definierar ramen för betrodda tjänster, vilket inkluderar tjänster för elektroniska underskrifter, stämplar, tidsstämplar och andra tjänster som bidrar till att säkerställa autenticitet, integritet och ursprung hos elektroniska dokument och transaktioner.

3. **Interoperabilitet:** eIDAS främjar interoperabilitet genom att fastställa tekniska standarder och krav för elektroniska identifiering och betrodda tjänster. Detta gör det möjligt för medlemsländerna att integrera sina system och möjliggör smidigare gränsöverskridande transaktioner.

4. **Ansvarsfördelning:** Förordningen tydliggör ansvarsfördelningen mellan de olika parterna som är involverade i tillhandahållandet av

elektronisk identifiering och betrodda tjänster, inklusive förlitande parter och tjänsteleverantörer.

5. **Nationella kontaktpunkter:** Varje medlemsland har behövt inrätta en nationell kontaktpunkt för att underlätta samarbete och informationsutbyte mellan medlemsländerna.

eIDAS-förordningen är avsedd att främja förtroende för elektroniska transaktioner över gränserna inom EU genom att skapa en gemensam ram för elektronisk identifiering och tillitstjänster. Det underlättar för företag och medborgare att bedriva affärer och använda offentliga tjänster över nationsgränserna på ett säkert och effektivt sätt.

Om e-identitetsplånboken

I slutet av 2023 tecknades en överenskommelse kring en uppdatering av förordningen, dvs ett tillägg till den tidigare förordningen som även fortsättningsvis gäller. Den officiella EU-lagstiftningsprocessen kan antas vara klar under 2024.

Den största nyheten som kommer med uppdateringarna avseende e-legitimationer är införandet av en europeisk e-identitetsplånbok. Plånboken är tänkt som en lösning liknande den som idag finns i många mobiltelefoner och den ska låta användaren lagra olika attribut. Attributen kan utgöras av t.ex. information om användaren så som personnummer, kön och medborgarskap, men kan även vara information om utbildningar, arbetslivserfarenhet och körkort.

Plånboken är tänkt att förenkla gränsöverskridande transaktioner och att öka användarnas kontroll över sina egna uppgifter eget data och hur de delas. Varje medlemsstat kommer att vara skyldig att tillgängliggöra en e-identitetsplånbok för sina medborgare, utan kostnad för användaren.

Ömsesidigt erkännande av e-legitimationer

Med införandet av plånboken kommer även ett krav för offentliga organ att acceptera andra länders plånböcker som autentiseringsmedel. eIDAS ställer krav på att när kommuner och regioner kräver användande av e-legitimation för åtkomst till en nättjänst så ska de godkänna e-legitimationer som utfärdats i en annan medlemsstat, förutsatt att:

- e-legitimationen ingår i den förteckning över e-legitimationer som anmälts (notifierats) till EU-kommissionen,
- tillitsnivån på e-legitimationen motsvarar en tillitsnivå som är lika hög eller högre än den som kommunen eller regionen kräver för åtkomst till tjänsten, förutsatt att tillitsnivån motsvarar väsentlig eller hög,
- kommunen använder tillitsnivå väsentlig eller hög i samband med åtkomst till tjänsten.

Tillitsnivå ”väsentlig” enligt eIDAS motsvarar i praktiken tillitsnivå 3 enligt de svenska tillitsnivåerna för e-legitimation.[2] Tillitsnivå ”hög” enligt eIDAS motsvarar i praktiken tillitnivå 4.

Kravet innebär endast att en e-legitimation ska kunna användas för att autentisera sig till tjänsten. Det är inte ett krav på att tjänsterna även ska kunna användas av personer som autentiserar sig med en utländsk e-legitimation (skäl 14 eIDAS). Kravet gäller oavsett om nättjänsten har målgrupper i andra medlemsstater.

En förteckning över de e-legitimationer som anmälts inom ramen för eIDAS finns på Connecting Europe Facility (CEF) portal[3].

eIDAS lägger ingen vikt vid hur kommuner och regioner konsumerar utländska e-legitimationer. Genom en uppdatering av lag (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

[2] https://www.digg.se/digitala-tjanster/e-legitimering/tillitsnivaer-for-e-legitimering

[3] https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

(kompletteringslagen) 2021 har det dock införts ett krav i svensk lag på att ett offentligt organ, exempelvis en kommun eller region, som tillhandahåller en nättjänst som innebär ett krav på godkännande av utländska e-legitimationer måste ansluta sig till den svenska landsnoden som återfinns i Diggs federation Sweden Connect. De administrativa och tekniska förfarandena för anslutningen beskrivs under rubriken Ansluta till Sweden Connect och eIDAS nedan.

Förordningen definierar inte vad begreppet nättjänster omfattar, men Sverige har i flera utredningar hänvisat till det som i dagligt tal kallas e-tjänster.[4]

Förordningen om en gemensam digital ingång

Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (Single Digital Gateway-SDG) antogs för att inrätta en gemensam digital ingång som syftar till att underlätta tillgången till information, förfaranden samt hjälp- och problemlösningstjänster för medborgare, företag och offentliga myndigheter inom EU. Målet är att skapa en enhetlig och användarvänlig digital plattform för att stödja gränsöverskridande samarbete och informationsutbyte.

I förordningen definieras ett förfarande som en sekvens av handlingar som en användare måste utföra för att uppfylla kraven eller för att erhålla ett beslut från en behörig myndighet för att kunna utöva sina rättigheter. Förfaranden utgör alltså de olika processer som vi går igenom när vi interagerar med myndigheter, så som att registrera ett aktiebolag eller anmäla adressändring.

Några viktiga aspekter av SDG-förordningen:

[4] . Se exempelvis Användning av e-legitimation i tjänsten i den offentliga förvaltningen, SOU 2021:62, s. 57f.

1. **En gemensam digital ingång:** Förordningen fastställer skapandet av en gemensam digital ingång som är en onlineplattform för tillhandahållande av information och tjänster på ett enhetligt sätt över medlemsländerna.[5]
2. **Tillhandahållande av information:** SDG ger användare tillgång till relevant information om deras rättigheter, skyldigheter och möjligheter inom EU. Det inkluderar information om företags- och arbetslivsrelaterade frågor samt andra områden.
3. **Förfaranden och tjänster:** Plattformen ger användare möjlighet att utföra förfaranden och få tillgång till tjänster elektroniskt. Detta underlättar gränsöverskridande transaktioner och förenklar samarbetet över medlemsländernas gränser.
4. **Hjälp- och problemlösningstjänster:** SDG innehåller mekanismer för att ge stöd och hjälp till användare, inklusive hjälp- och problemlösningstjänster för att hantera eventuella problem eller frågor som kan uppstå under användning av plattformen.

SDG-förordningen kan ses som en förlängning av eIDAS vad det gäller e-tjänster. SDG-förordningen utökar skyldigheten för tillhandahållare av vissa e-tjänster att inte enbart möjliggöra för användare med e-legitimationer från andra medlemsländer att kunna autentisera sig till tjänsten, utan att även kunna nyttja tjänsten. Det finns en skyldighet för medlemsstaterna att göra de tjänster som pekas ut i SDG-förordningen[6] tillgängliga för användare i gränsöverskridande situationer, oavsett vem som tillhandahåller e-tjänsten inom medlemsstaten. Beroende på vilka e-tjänster som tillhandahålls kan det finnas en skyldighet att anpassa tjänsten till SDG-förordningens krav. En analys måste göras av de e-tjänster som organisationen tillhandahåller, och om dessa omfattas av SDG.

Kraven i SDG-förordningen kan leda till behov av att förändra hur e-tjänster tillhandahålls och de förfaranden som är kopplade till tjänsten. För de e-tjänster som omfattas av SDG-förordningen är det inte längre möjligt att endast tillhandahålla en autentiseringslösning för att sedan placera användaren i ett digitalt väntrum. Det blir inte längre möjligt att förutsätta att alla användare som ansluter till tjänsten har ett svenskt personnummer eller samordningsnummer. Det kan till exempel leda till att e-tjänsten måste anpassas för att kunna hantera andra identitetsbegrepp. Digg genomför också ett projekt som ska resultera i en

[5] https://europa.eu/youreurope/

[6] Se närmare art. 5 - 7 och bilaga I – II i SDG-förordningen.

lösning för identitetsmatchning som förväntas vara klar under den senare halvan av 2024.[7]

SDG-förordningen ställer även krav på att den som tillhandahåller en e-tjänst som omfattas tillgängliggör anvisningar för hur e-tjänsten används på ett av unionens officiella språk som i huvudsak förstås av största möjliga antal användare i gränsöverskridande situationer. I vissa fall kan det dock för en tjänst som tillhandahålls på lokal nivå i närheten av en nationsgräns vara lämpligast att tillgängliggöra informationen på förstaspråket i den angränsande medlemsstaten.

Myndighetsansvar och tillsyn

Ansvaret mellan myndigheter avseende eIDAS är idag fördelat på Digg och Post- och Telestyrelsen (PTS). Digg ansvarar i huvudsak för frågor rörande e-legitimationsdelarna i Sverige vad gäller eIDAS, och ansvarar bland annat för den landsnod som möjliggör konsumtion av utländska e-legitimationer samt den tjänst som kommuner de facto ansluter sig till, Sweden Connect. Digg granskar och godkänner svenska e-legitimationer utifrån Tillitsramverket för Svensk e-legitimation, och ansvar även för anmälan av e-legitimationer till kommissionen.

PTS ansvarar i huvudsak för betrodda tjänster vad det gäller eIDAS. Det är till PTS som leverantörer av betrodda tjänster anmäler sin avsikt att bli kvalificerade, och myndigheten har tillsynsansvar över leverantörer av betrodda tjänster. I kompletteringslagen och tillhörande föreskrifter pekas PTS även ut som den myndighet som har tillsynsansvar för efterlevnad av eIDAS och kompletteringslagen. Det innebär att PTS även är skyldig att kontrollera att exempelvis kommuner och regioner i enlighet med kompletteringslagen ansluter sig till Sweden Connect.

[7] https://www.digg.se/digitala-tjanster/identitetsmatchning

Dagens konsumtion av inhemska e-legitimationer

De flesta kommuner och regioner har redan idag en eller i vissa fall flera lösningar för att konsumera inhemska e-legitimationer i egen eller annans regi. Exempel på utfärdare av inhemska e-legitimationer som är godkända av Digg är bland annat:

- Finansiell ID-Teknik BID AB (BankID)
- Freja eID Group AB (Freja eID)
- AB Svenska Pass (Skatteverkets ID-kort)

Digg granskar och godkänner e-legitimationer på alla tillitsnivåer utom den lägsta, tillitsnivå 1. För tillitsnivå 3 och tillitsnivå 4 kan e-legitimationen dessutom erhålla kvalitetsmärket Svensk e-legitimation[8]. Konsumtionen av e-legitimationen i e-tjänsten sker ofta med det tekniska protokollet Security Assertion Markup Language (SAML) v2.0 [9] vilket också används i federationen Sweden Connect.

Ansluta till Sweden Connect och eIDAS

För de organisationer som ännu inte har förmågan att konsumera utländska e-legitimationer som publicerats inom ramen för eIDAS följer här ett antal förslag till väg fram. Förslagen tar utgångspunkt från idag vanligt förekommande lösningar för konsumtion av inhemska e-legitimationer och även konsumtion av egna autentiseringslösningar.

Det är inte ovanligt att en organisation av olika skäl har flera olika lösningar för att konsumera e-legitimationer varför det också kan bli aktuellt att konsolidera

[8] https://www.digg.se/digitala-tjanster/e-legitimering#h-sv-default-anchor
[9] https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

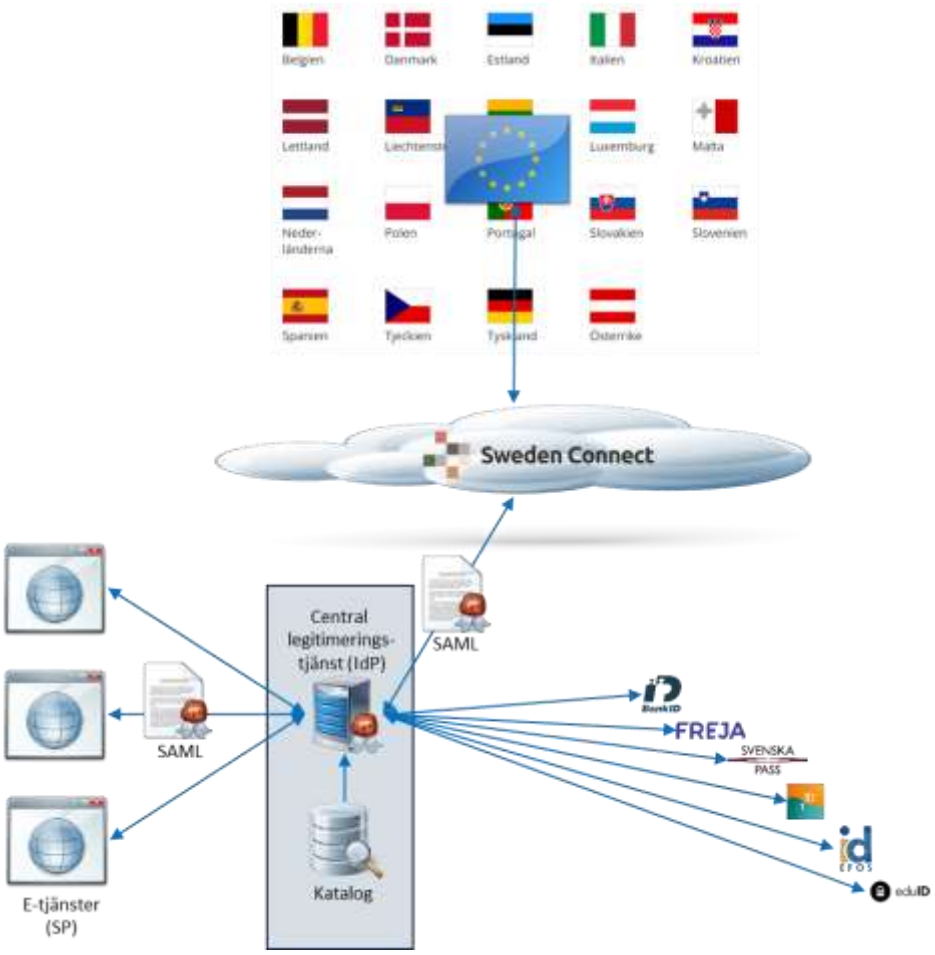
lösningar i samband med en vägvalsdiskussion. Det är sällan något självändamål att ha flera lösningar för att konsumera e-legitimationer.

Resonemangen i vägledningen är allmänt hållna och ska ses som just vägledande. I resonemangen finns det inte några hinder att exempelvis flera kommuner tillsammans hittar en gemensam väg fram för att lösa konsumtion av utländska e-legitimationer. Detta kan i många vara det mest kostnadseffektiva sättet att adressera frågan.

Digg ansvarar för Sweden Connect och den svenska landsnoden för eIDAS. Rekommendation är att kontakta Digg via e-legitimation@digg.se i de fall som det behövs ytterligare stöd.

Fyra alternativ för anslutning till Sweden Connect

Alternativ 1. En egen central legitimeringstjänst som proxy mot Sweden Connect



I detta alternativ har organisationen en central legitimeringstjänst (intygsutfärdare, Identity Provider, IdP) som kommunicerar med det öppna standardiserade protokollet SAML V2.0 med fullständig implementering av SAML. Legitimeringstjänsten har även en förmåga att hantera proprietära

protokoll, som exempelvis BankID Relying Party API[10], för konsumtion av e-legitimationer.

Den centrala legitimeringstjänsten hanteras antingen av den egna organisationen eller av en extern leverantör. Den ansluts direkt till de nationella e-legitimationsutfärdarna som organisationen har valt. För denna organisation rekommenderas en direkt anslutning till den svenska landsnoden i Sweden Connect från den centrala legitimeringstjänsten. På så vis skapas en tillförlitligt kedja hela vägen, dvs från e-tjänsten till tillhandahållarna av de utländska e-legitimationerna. Anvisningen av e-legitimation sker i två steg, först i den centrala legitimeringstjänsten och sen även i den svenska IdP-proxyn i eIDAS-noden.

E-tjänsterna (även kallade förlitande parter eller *Service Provider*, SP) i organisationerna använder den centrala legitimeringstjänsten för att konsumera e-legitimationer, oavsett om de är svenska eller utländska.

Den centrala legitimeringstjänsten förväntas kunna agera som mellanhand, (proxy) i en SAML-kontext. De flesta mjukvaror eller tjänsteleverantörer saknar denna förmåga vilket innebär att kravställningen på rätt förmågor blir väsentlig. Här kan Sweden Connects tekniska ramverk[11] utgöra ett underlag till kravställningen. Om kravställningen inte går att möta så kan Alternativ 2 (nedan) vara en väg framåt.

Anslutningsprocessen på en övergripande nivå

1. Teckna avtal[12] med Digg för anslutning till Sweden Connect.
2. Sätt er in i det tekniska ramverk som ligger till grund för federationen Sweden Connect och undersök er egen organisations förmåga i relation till ramverket.
3. Konfigurera er IdP att agera proxy. Detta innebär bland annat att:
    a. Användare ska kunna påbörja en ny autentisering i en SAML-kontext

[10] https://www.bankid.com/utvecklare/guider/teknisk-integrationsguide

[11] https://www.swedenconnect.se/tekniskt-ramverk

[12] https://www.digg.se/digitala-tjanster/e-legitimering/e-legitimering-for-dig-som-offentlig-aktor/internationell-e-legitimering#h-1TecknaavtalomanslutningSwedenConnect

b. IdP ska kunna vidarebefordra efterfrågade krav på attributsleverans.

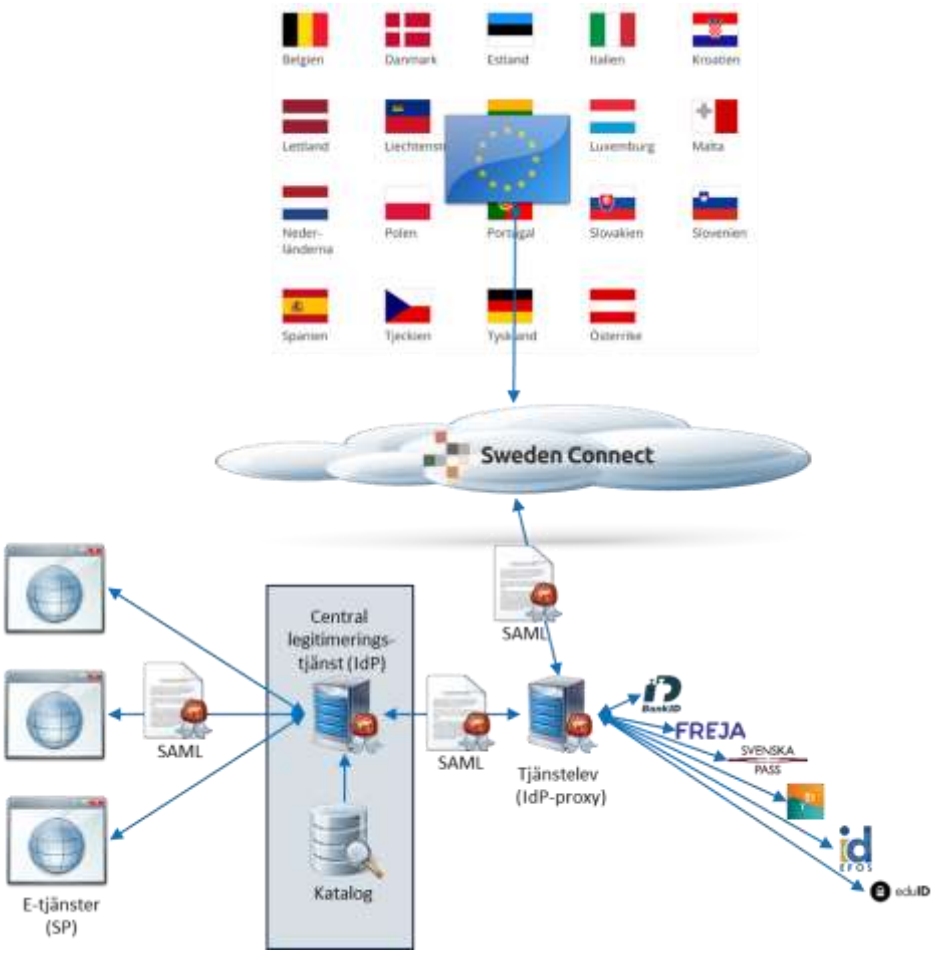
4. Kontrollera SAML-metadata i Sweden Connects valideringstjänst.[13]
5. Ladda upp SAML-metadata i xml-format till Sweden Connects metadataregister. Säkerställ att:
    a. Organisationsinformation är korrekt inlagd
    b. Rätt Entitetskategori är definierad.[14]

Insatsen för att realisera anslutningen till Sweden Connect i detta alternativ uppskattas till ca 2-3 dagar exklusive vänt- och ledtider.

[13] https://validator.swedenconnect.se/

[14] https://www.swedenconnect.se/anslut/saml-metadata/skapa-saml-metadata

Alternativ 2. Ansluta till Sweden Connect via en proxy för de svenska e-legitmationerna



Om organisationen och dess centrala legitimeringstjänst inte med säkerhet har den tekniska förmåga att hantera SAML på det sätt som krävs för att ansluta sig direkt till Sweden Connect, kan anslutningen ofta upprättas via den mellanhand som tillhandahåller inhemska e-legitimationer.

I detta alternativ har organisationen en central legitimeringstjänst (IdP) som kommunicerar med det standardiserade protokollet SAML V2.0. Den centrala legitimeringstjänsten hanteras antingen i egen regi eller av extern organisation och är ansluten via en mellanhand till de inhemska e-legitimationsutfärdare som organisationen har valt att konsumera.

Kommunikationen till mellanhanden sker ofta med det standardiserade protokollet SAML V2.0 vilket förenklar konsumtionen av de inhemska e-legitimationerna, vilket i förlängningen också kan förenkla konsumtionen av de utländska e-legitimationerna genom att förmågan redan är etablerad.

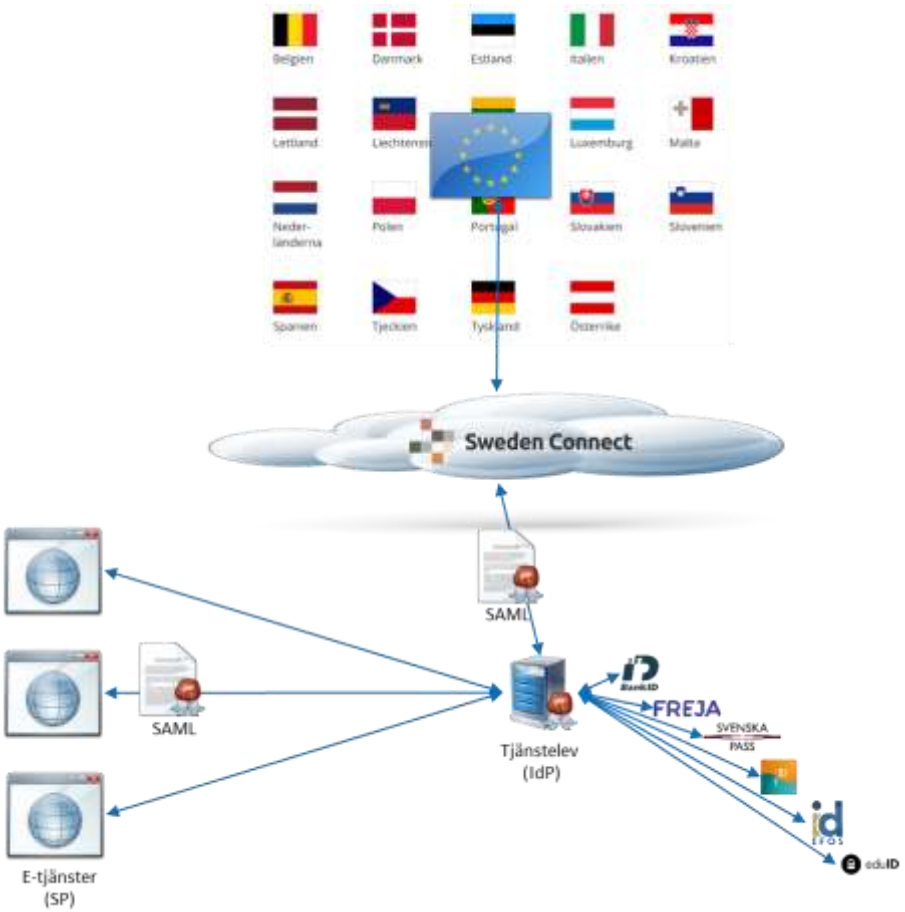
E-tjänsterna i organisationerna använder den centrala legitimeringstjänsten som en proxy vidare till mellanhanden som konsumerar de inhemska e-legitimationerna.

Anslutningsprocessen på en övergripande nivå

1. Bedöm kostnaden och de tekniska förutsättningar för att använda en mellanhand för anslutning till Sweden Connect. Ryms det inom nuvarande avtal eller behöver det upphandlas?
2. Teckna avtal med Digg för anslutning till Sweden Connect.
3. Komplettera eventuellt avtalet med mellanhanden för anslutning till Sweden Connect, alternativt, upphandla eller avropa denna tjänst.
4. Beställ teknisk anslutning till Sweden Connect av mellanhanden.
5. Justera vid behov konfigurationen i er centrala legitimeringstjänst för att hantera autentisering via Sweden Connect.

Insatsen för att realisera anslutningen till Sweden Connect i detta alternativ uppskattas till 1-2 dagar exklusive vänt- och ledtider.

Alternativ 3. Legitimeringstjänst som upphandlad tjänst



I detta alternativ saknar organisationen en egen central legitimeringstjänst (IdP) och har istället köpt tjänsten för att ställa ut identitetsintyg till konsumerande e-tjänster. För denna organisation rekommenderas en anslutning till Sweden Connect via den köpta tjänsten.

Anvisningen av e-legitimation sker i den köpta tjänsten med stöd av Sweden Connects anvisningstjänst avseende de utländska e-legitimationerna.

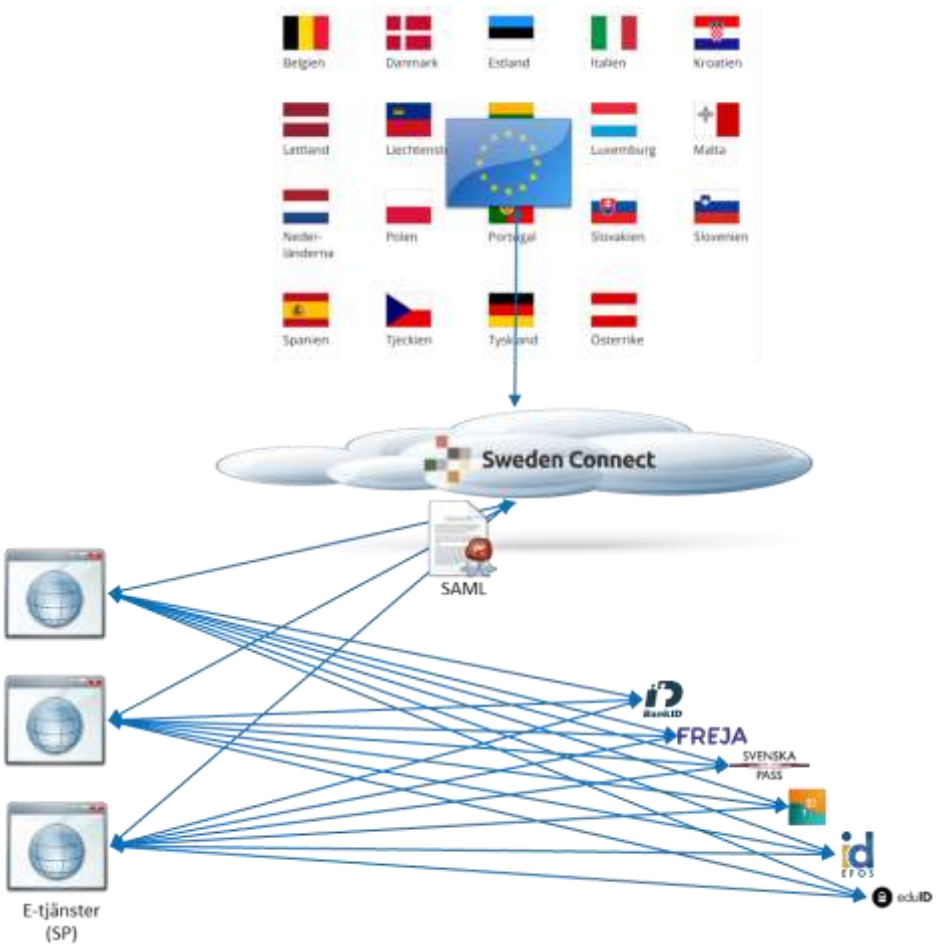
Anslutningsprocessen på en övergripande nivå

1. Bedöm kostnaden och de tekniska förutsättningarna med tjänsteleverantören för anslutning till Sweden Connect. Ryms det inom nuvarande avtal eller behöver det upphandlas?

2. Teckna avtal med Digg för anslutning till Sweden Connect.
3. Komplettera eventuellt avtalet med tjänsteleverantören för anslutning till Sweden Connect, alternativt upphandla eller avropa tjänsten.
4. Beställ teknisk anslutning till Sweden Connect av tjänsteleverantören.

Insatsen för att realisera anslutningen till Sweden Connect i detta alternativ uppskattas till ungefär en (1) dag exklusive vänt- och ledtider.

Alternativ 4. Individuell legitimeringstjänst per e-tjänst



I detta alternativ saknar organisationen en samlad lösning för att konsumera e-legitimationer, varken via en central eller upphandlad tjänst. Organisationen låter varje konsumerande e-tjänst (SP) lösa detta på egen hand.

Rekommendationen är i detta fall att i första hand undersöka möjligheten till att etablera en samlad lösning för att konsumera e-legitimationer i enlighet med tidigare beskrivna alternativ.

Om detta inte är en väg fram så måste varje e-tjänst anpassas för anslutning till Sweden Connect, dvs man kan då inte tillhandahålla en gemensam anvisning av e-legitimationer och Sweden Connect.

Anslutningsprocessen på en övergripande nivå

1. Undersök kostnadsbilden för anpassning av e-tjänsten. Ryms det i befintligt avtal, eller måste det upphandlas?
2. Teckna avtal för anslutning till Sweden Connect direkt med Digg.
3. Genomför anpassning av e-tjänsten.

Insatsen för att realisera anslutningen till Sweden Connect i detta alternativ låter sig inte uppskattas, då insatsen kan vara väldigt omfattande beroende på antal och komplexitet i e-tjänsterna.

Att tänka på

Identitetsbegreppet

En stor mängd e-tjänster som vänder sig till allmänheten använder personnummer eller samordningsnummer som identitetsbegrepp. I många andra EU-länder är identitetsbegreppet långt från lika självklart. Det finns till och med hinder i den nationella lagstiftningen i vissa EU-länder som inte medger permanenta id-begrepp.

Det har gjorts utredningar om kopplingsregister mellan en utländsk e-legitimation och ett svenskt identitetsbegrepp. Slutsatserna i Förslag till handlingsplan för att leva upp till SDG-förordningen (I2019/02438/DF, Diggs ärendenummer 2019-402) visade att Skatteverkets förslag om kopplingsregister visserligen kan fylla en funktion men att det inte i sig kan vara en lösning för att uppfylla SDG-förordningens krav eftersom det förutsätter att användaren har ett svenskt personnummer.

I avsnittet om kraven som följer av SDG-förordningen är det tydligt att det inte längre är möjligt att förutsätta att alla användare som ansluter till tjänsten har ett svenskt personnummer eller samordningsnummer. Det kan till exempel leda till att e-tjänsten måste anpassas för att kunna hantera andra identitetsbegrepp. I det tekniska ramverket för SAMLv2 finns förmåga att skapa permanenta och tillfälliga identitetsbegrepp som kan vara en väg fram. Förmågan att hantera fler identitetsbegrepp än bara de typiskt svenska identitetsbegreppen i de aktuella e-tjänsterna bör övervägas.

Väntrummet

I de flesta fall i Sverige idag kan en innehavare av en utländsk e-legitimation inte få åtkomst till någon e-tjänst då utländska identitetsbegrepp saknar koppling till svenska personnummer eller samordningsnummer. Detta ger till följd att för användaren så misslyckas inloggningen med ett generiskt felmeddelande eller så hänvisas användaren till ett väntrum. Väntrummet bör så långt det är möjligt placeras och hanteras i e-tjänsten, eller med fördel i en central e-tjänst för väntrum, och inte i som i vissa fall redan i legitimeringstjänsten.

Det är viktigt att göra väntrummet informativt, inte bara beklaga det inträffade. Det är viktigt att notera att för att uppfylla förordningen ska ett övervägande ha gjorts på den aktuella tjänsten och att det finns verkliga skäl till att användare inte släpps in. Väntrummet bör därför innehålla information om

- vem som har loggat in
- varför vi inte kan släppa in just den användaren till den här tjänsten
- hur användaren löser ärendet på annat sätt.

Single sign-on (SSO)

Det är fullt möjligt att etablera single sign-on för e-legitimationsinnehavarna i de alternativ som vägledningen presenterar. Det är dock viktigt att tänka på att en organisation kan ha flera olika lösningar för att konsumera e-legitimationer vilket tydliggörs i några av alternativen. Det är heller inte ovanligt att en organisation har implementerat flera av alternativen som presenteras i vägledningen. Det försvårar onekligen en övergripande användarupplevelse av single sign-on för e-legitimationsinnehavaren. Det tillhör dessutom ovanligheten att flera olika lösningar för att konsumera e-legitimationslösningar samverkar, utan de uppträder oftast som enskilda öar. Detta blir särskilt kännbart om det finns en önskan att etablera single sign-on i en lösning som inte är homogen, vilket särskilt behöver beaktas. Inte minst i en vägvalsdiskussion. Rekommendationen även här är att ha så få lösningar som möjligt för att konsumera e-legitimationer.

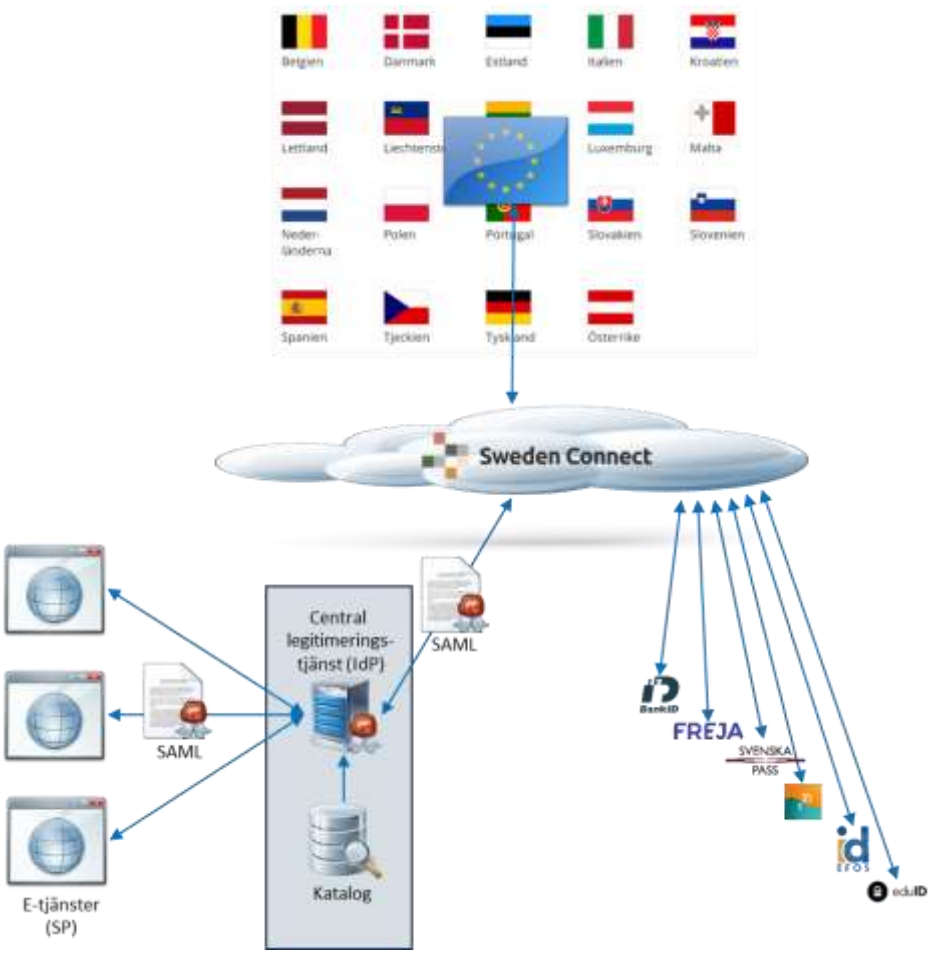
Sweden Connect för konsumtion av inhemska e-legitimationer

Det finns inte några tekniska hinder att Sweden Connects register över betrodda parter även innehåller SAML-metadata för de inhemska e-legitimationerna och att de också inkluderas i Sweden Connects anvisningstjänst. För Valfrihetssystemet, som nu ersätts av Auktorisationssystemet, är det Diggs tänkta väg fram. I skrivande stund (november 2023) är det dock få e-legitimationsutfärdare anslutna, men fler är att vänta. Inte minst som en följd av auktorisationssystemet och förslaget till en statlig e-legitimation.

En klar fördel med denna utveckling är att när det tillkommer nya e-legitimationer, och även när e-legitimationer avvecklas, sker detta dynamiskt. Det behöver alltså inte ske någon manuell konfiguration per e-legitimationstjänst utan den som litar på Sweden Connects register över betrodda parter och använder Sweden Connects anvisningstjänst får denna dynamik på köpet.

Egen central legitimeringstjänst

För organisationer med en central legitimeringstjänst (IdP) som har en fullödig implementation av SAML innebär utökningen av Sweden Connects roll att behovet av mellanhänder minskar. Det är bara i de fall som e-legitimationsutfärdare inte använder standardiserade protokoll likt SAML som det kan bli aktuellt med en mellanhand eller en förmåga i egen IdP att hantera de proprietära protokoll som förekommer idag.



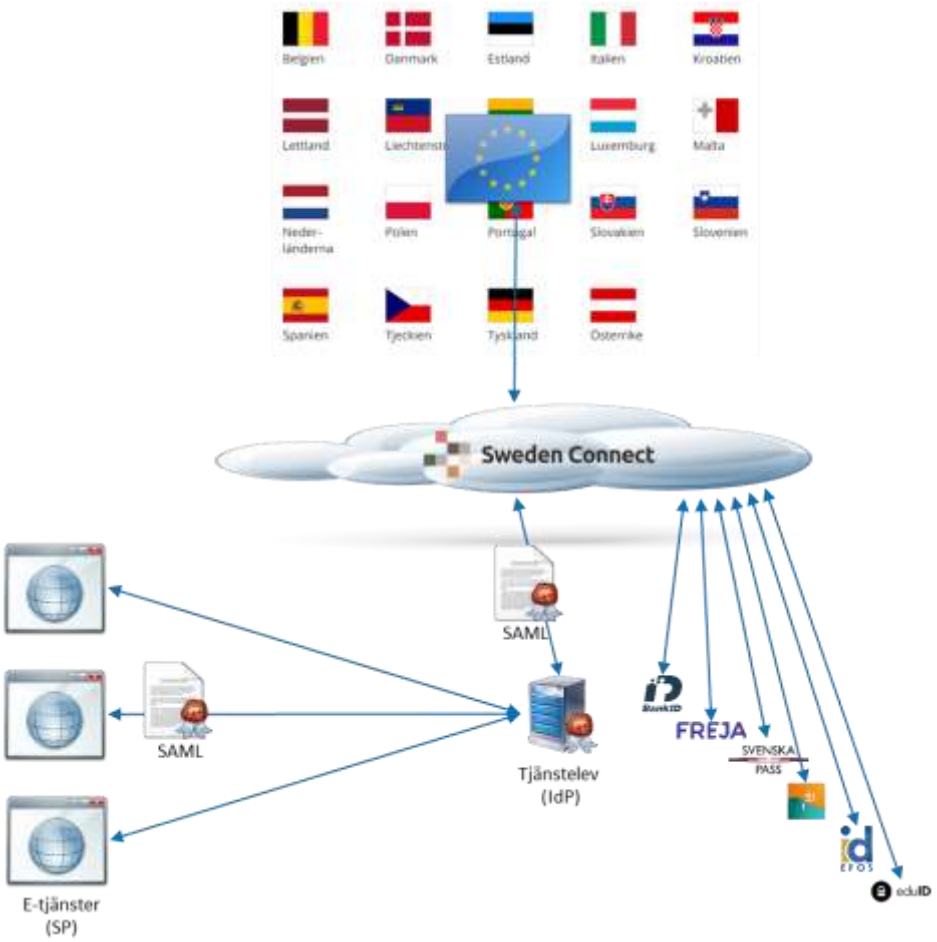
Bilden ovan visar en målbild där alla e-legitimationsutfärdare använder standardiserade protokoll likt SAML. Det finns inte några hinder att en legitimeringstjänst som konsumerar e-legitimationer via SAML även erbjuder modernare protokoll för konsumtion, exempelvis OpenID Connect (OIDC)[15], som komplement till SAML. Det ska snarast ses som en nödvändig utveckling för att möta e-tjänsternas behov av modernare protokoll.

Intygsutfärdare (IdP) som tjänst

I detta alternativ saknar organisationen helt en egen central legitimeringstjänst (IdP) och har istället köpt tjänsten för att ställa ut identitetsintyg till

[15] https://openid.net/developers/discover-openid-and-openid-connect/

konsumerande e-tjänster. För tjänsteleverantören är det enklare att producera tjänsten om e-legitimationer kan konsumeras på ett likartat sätt.



Bilden ovan är ett exempel där alla e-tjänster konsumerar e-legitimationer med standardiserade protokoll som exempelvis SAML. Det finns inte några hinder att en legitimeringstjänst som konsumerar e-legitimationer via SAML även erbjuder OIDC som komplement till SAML. Det ska snarast ses som en nödvändig utveckling för att möta e-tjänsternas behov.

Vägledning till eIDAS

2019 utkom Sveriges Kommuner och Regioner (SKR) med *Vägledning för anslutning till eIDAS: Inloggning till svenska digitala tjänster med utländska e-legitimationer*. Sedan vägledningen publicerades har ny lagstiftning tillkommit som ökar kravet på kommuner och regioner att kunna konsumera utländska e-legitimationer. Det har även identifierats ett behov av att komplettera vägledningen avseende den juridik som ligger till grund för kraven, samt den tekniska implementeringen. Denna vägledning är främst framtagen för att hjälpa organisationer som ännu inte har anslutit sig till eIDAS.

Upplysningar om innehållet

Torbjörn Karlsson, torbjorn.karlsson@skr.se
Lotta Nordström, lotta.nordstrom@skr.se

Sveriges Kommuner och Regioner, 2024
ISBN: 978-91-8047-220-3
www.skr.se

ISBN 978-91-8047-220-3
Post: 118 82 Stockholm | **Besök:** Hornsgatan 20
Telefon: 08-452 70 00 | www.skr.se
Beställ eller ladda ner på skr.se/publikationer

Sveriges Kommuner och Regioner