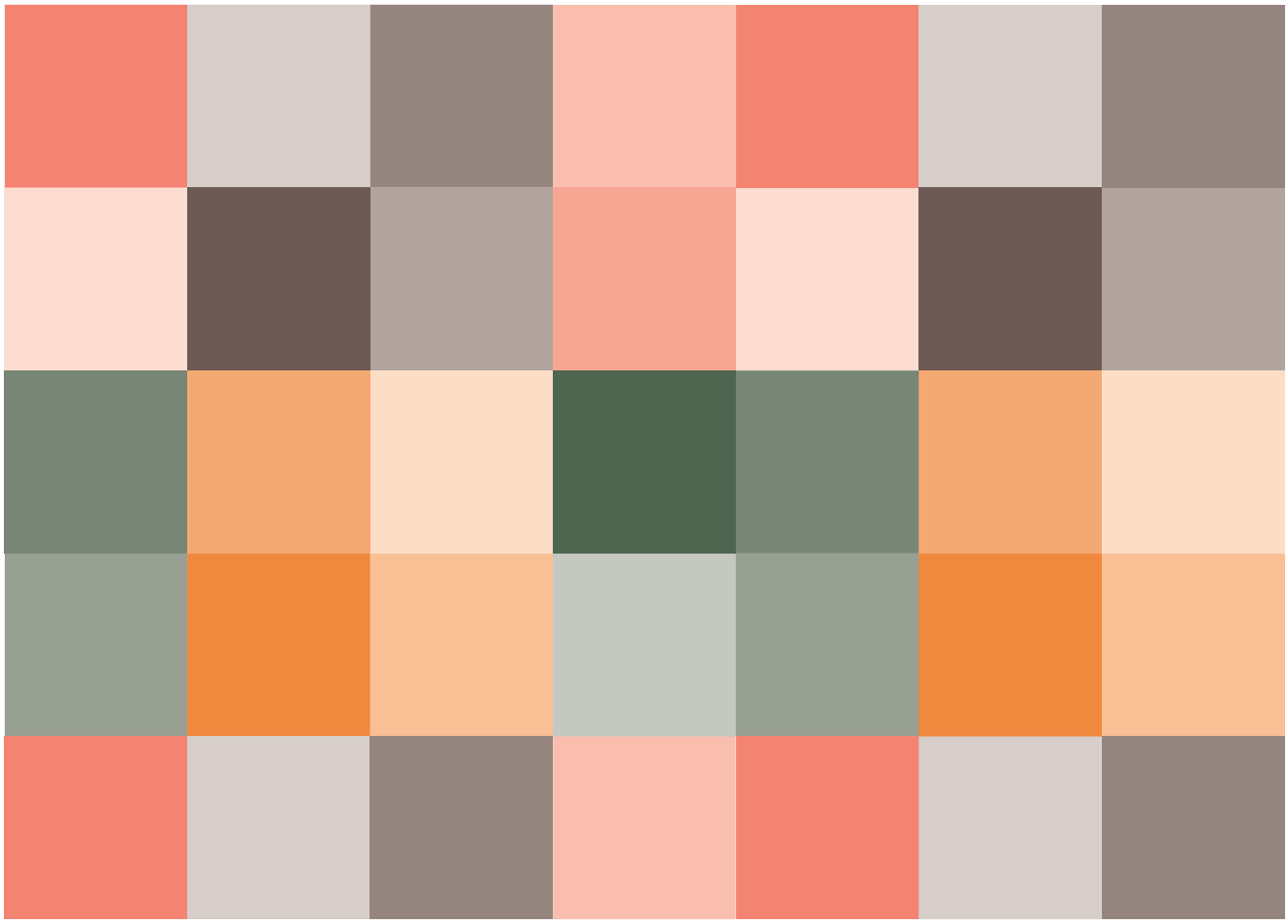

Fördjupad analys av förutsättningar för att tillämpa Samordnad identitet och behörighet i data- och AI-scenarier

Bilaga till Slutredovisning av uppdrag till Myndigheten för digital förvaltning att föreslå en samverkansstruktur för utveckling av tjänster för data och artificiell intelligens

Diarienummer: Fi2026/00137

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Datum: 2026-05-29

I denna bilaga analyseras förutsättningarna för att använda Samordnad identitet och behörighet i praktiken inom samverkansstrukturen för data och AI. Analysen utgår från konkreta användningsfall där en aktör vill få tillgång till data eller köra AI-modeller i en säker behandlingsmiljö, ofta över organisations- och nationsgränser.

Ett typiskt scenario är att ett företag eller en forskningsorganisation vill träna en AI-modell i en regions säkra behandlingsmiljö, där data inte får lämna miljön. Ett annat är att en svensk aktör, exempelvis forskningsmiljön SAFER vid Göteborgs universitet, vill ansluta till ett europeiskt dataområde som Mobility Data Space. I båda fallen krävs att aktörer kan identifiera sig, styrka att de uppfyller vissa krav och bli verifierade av en motpart, ofta maskinellt.

Syftet med analysen är att tydliggöra i vilken utsträckning Samordnad identitet och behörighet stödjer dessa scenarier, samt vilka ytterligare förutsättningar som krävs för att de ska fungera i praktiken.

Samordnad identitet och behörighet definierar en gemensam uppsättning regler, krav och specifikationer för att etablera interoperabla federationer för identitets- och behörighetshantering.

Analysen visar att Samordnad identitet och behörighet skapar förutsättningar för att etablera en eller flera federationer för anslutning av organisationer samt data- och AI-resurser inom olika dataområden. Genom att federationerna utgår från samma gemensamma grund blir de interoperabla med varandra.

Samordnad identitet och behörighet är ett gemensamt regelverk för hur resurser ansluts, identifieras och hur verifierbar information om dem förmedlas inom en federation. Däremot definieras inte verksamhetsspecifika krav på resurser eller vad som krävs för att fatta beslut om åtkomst till data och resurser. Sådana regler definieras inom respektive federation och verksamhetsområde.

Federationer som etableras med stöd av Samordnad identitet och behörighet kan användas för att förmedla information på ett sätt som möjliggör verifiering av informationens ursprung, identitet, behörighet och egenskaper. Det skapar förutsättningar för säker, interoperabel och skalbar åtkomst till data och AI-resurser mellan organisationer. Utan en gemensam standard behöver motsvarande lösningar tas fram självständigt av respektive part, vilket riskerar att leda till fortsatt fragmentering och försvåra informationsutbyte mellan många aktörer och flera dataområden. Detta gäller inte minst i ett europeiskt sammanhang där behovet av

nationella standarder och gemensamma tillämpningar av dessa är en förutsättning för harmonisering och samverkan inom europeiska dataområden och andra gränsöverskridande initiativ.

1. Rollen för samordnad identitet och behörighet i användningsfallen

I de analyserade användningsfallen spelar samordnad identitet och behörighet en central men avgränsad roll. När ett företag vill köra en AI-modell i en säker behandlingsmiljö behöver miljön kunna verifiera vem som ansluter, vilken organisation som står bakom och om det finns giltiga egenskaper som styrker att aktören uppfyller relevanta krav. Samordnad identitet och behörighet tillhandahåller mekanismer för detta genom federerad identitet, förmedling av egenskaper och tillitskedjor.

Åtkomst i dessa scenarier omfattar både tillgång till den säkra behandlingsmiljön och tillgång till de data som används i miljön. Dessa beslut fattas av olika aktörer. Miljöoperatören ansvarar för åtkomst till själva miljön, medan beslut om tillgång till data och användning för exempelvis AI-modellträning fattas av den dataansvariga organisationen eller, i förekommande fall, ett ansvarigt organ för datatillgång (t.ex. HDAB).

Samordnad identitet och behörighet kan stödja båda dessa beslut genom att förmedla verifierbar information om aktörer och deras egenskaper, men fattar inte besluten i sig.

På motsvarande sätt behöver aktören som vill använda miljön kunna verifiera att miljön faktiskt uppfyller de krav som ställs, exempelvis avseende säkerhetsnivå eller regulatorisk efterlevnad. Även här kan samordnad identitet och behörighet bidra genom att möjliggöra verifierbara egenskaper hos miljön.

Samordnad identitet och behörighet svarar därmed på frågorna vem är du och kan jag lita på det du visar. Däremot svarar Samordnad identitet och behörighet inte på frågan vad som krävs för att få åtkomst, eller hur denna information ska uttryckas och tolkas.

Det innebär att även om Samordnad identitet och behörighet kan användas som en grund för att utbyta och verifiera tillitsinformation samt möjliggöra säker åtkomst i dessa scenarier, behövs kompletterande styrning och strukturer för att hantera kravställning, semantik, informationsmodeller och verksamhetsspecifika tillämpningar kopplade till data och AI-resurser.

2. Från upptäckt till åtkomst – vad saknas?

Om man följer användarens resa i dessa scenarier framträder ett antal konkreta gap.

När en aktör söker efter en resurs, exempelvis en säker behandlingsmiljö via Sveriges dataportal, kan denne i bästa fall (se bilaga 3) hitta en beskrivning av miljön och dess villkor. I detta läge saknas dock en tydlig koppling mellan denna beskrivning och den federationsbaserade infrastrukturen. Det innebär att även om en miljö identifieras i en katalog, finns det ingen etablerad mekanism för att maskinellt koppla denna till en verifierbar entitet i samordnad identitet och behörighet. I praktiken stannar därför upptäckbarheten vid information, snarare än att leda vidare till faktisk åtkomst.

När aktören därefter försöker uppfylla kraven för åtkomst uppstår nästa problem. I scenariot där ett företag vill träna en AI-modell i en regions miljö kan kraven exempelvis vara att organisationen ska vara godkänd, att ett visst datatillstånd finns och att den tekniska miljön uppfyller vissa säkerhetskrav. Dessa krav finns ofta definierade, men de uttrycks på olika sätt och i olika format beroende på domän. Det saknas ett enhetligt sätt att beskriva vad kraven är och hur de ska kopplas till verifierbara bevis.

Detta blir särskilt tydligt i maskin-till-maskin-scenarier, där ett system automatiskt ska avgöra om en annan part uppfyller kraven. Utan en gemensam struktur för hur krav och bevis hänger ihop måste varje producent implementera egen logik för att tolka informationen. Resultatet blir begränsad interoperabilitet och svårigheter att skala upp lösningen.

3. Säkra behandlingsmiljöer – ett konkret exempel

I scenariot där en AI-modell tränas i en säker behandlingsmiljö blir behovet av gemensamma strukturer särskilt tydligt. För att producenten ska kunna fatta ett beslut behöver den förstå vilken typ av miljö det är, vilken säkerhetsnivå den uppfyller och hur detta har verifierats.

I dag beskriver olika miljöer dessa egenskaper med olika begrepp, klassificeringar och modeller, vilket försvårar jämförelse och automatiserad hantering mellan aktörer. Även om en miljö kan exponera verifierbara egenskaper via en federation enligt Samordnad identitet och behörighet behövs gemensamma semantiska och informationsmässiga

strukturer för att dessa egenskaper ska kunna tolkas och användas på ett enhetligt sätt.

Konsekvensen blir annars att beslut om åtkomst i praktiken ofta kräver manuell bedömning eller bilaterala överenskommelser. Detta motverkar automatiserad och skalbar datadelning.

4. Hybridmiljöer – när flera modeller möts

I praktiken kommer inte alla aktörer att använda samordnad identitet och behörighet från början. I scenarier som involverar AI och dataområden kommer samordnad identitet och behörighet att samexistera med andra tillitsmodeller, såsom SAML-baserade federationer, EU-noder och fristående lösningar.

I ett scenario där en aktör från Tyskland vill använda en svensk behandlingsmiljö inom ramen för EHDS, kommer tilliten inte etableras direkt mellan de enskilda aktörerna. I stället sker den via nationella kontaktpunkter där land litar på land. Samtidigt behöver den svenska miljön kunna verifiera aktören enligt nationella krav, vilket kräver en intern tillitsinfrastruktur.

Här uppstår ett behov av att koppla samman olika modeller. I dag saknas gemensamma principer för hur identitet och egenskaper ska översättas mellan dessa kontexter. Utan sådana principer riskerar varje koppling att bli en egen lösning, vilket leder till ökad komplexitet och minskad skalbarhet.

5. Europeisk dimension – behovet av en nationell tillitsgrund

De analyserade användningsfallen visar att de i praktiken är nära kopplade till europeiska initiativ. Mobility Data Space, EHDS och andra dataområden ställer alla krav på att aktörer ska kunna identifiera sig och styrka sina egenskaper över nationsgränser.

I dessa sammanhang etableras tillit i regel via nationella kontaktpunkter. Det innebär att varje medlemsstat behöver ha en sammanhållen nationell tillitsgrund som andra länder kan förhålla sig till. Samordnad identitet och behörighet har potential att utgöra en sådan grund, men det saknas i dag en tydlig modell för hur denna ska användas i relation till europeiska strukturer.

I scenariot där SAFER vill ansluta till Mobility Data Space innebär detta att organisationen behöver kunna styrka sina egenskaper på ett sätt som accepteras i det europeiska sammanhanget. Om varje domän eller dataområde utvecklar egna lösningar för detta riskerar resultatet att bli fragmenterat. Ett gemensamt nationellt förhållningssätt blir därför centralt.

6. Relationen till befintliga initiativ

Det finns i dag flera europeiska initiativ som adresserar delar av problematiken. iSHARE visar hur åtkomstregler och delegation kan uttryckas maskinellt. Gaia-X etablerar modeller för hur organisationer och tjänster beskriver sina egenskaper och efterlevnad. SDK möjliggör säker informationsöverföring mellan aktörer.

Dessa initiativ visar att behovet av strukturer ovanpå tillitsinfrastrukturen är välkänt. Samtidigt adresserar de olika lager av problemet och ersätter inte behovet av en sammanhållen nationell modell. I en svensk kontext behöver dessa perspektiv integreras med samordnad identitet och behörighet och Sveriges dataportal.

7. Samlad bedömning

Gapanalysen visar att färdplanen för samordnad identitet och behörighet adresserar den tekniska mekanismen för tillit, men att flera avgörande förutsättningar saknas för att denna mekanism ska kunna användas i praktiken i data- och AI-scenarier.

Det handlar om att kunna uttrycka krav på ett enhetligt sätt, att koppla dessa krav till verifierbara bevis, att möjliggöra samverkan mellan olika tillitsmodeller och att skapa en sammanhållen nationell grund som kan användas i europeiska sammanhang.

Utan dessa kompletterande delar riskerar användningsfallen att lösas genom separata och domänspecifika lösningar, vilket motverkar målet om en samordnad och skalbar samverkansstruktur.

8. Slutsats

Som framgått av analysen är Samordnad identitet och behörighet en nödvändig förutsättning för att möjliggöra säker och skalbar datadelning, men inte tillräckligt i sig eftersom lösningen inte definierar verksamhetsspecifika krav. De analyserade användningsfallen visar att det

krävs kompletterande strukturer för att omsätta funktionaliteten i praktisk tillämpning. Det är dessa strukturer, kopplade till semantik, struktur, samverkan och skala, som motiverar de föreslagna tilläggsuppdragen i huvudrapporten.

9. Identifierade behov i användningsfall

I de analyserade användningsfallen framträder dessa behov tydligt. När en aktör, exempelvis ett företag, vill träna en AI-modell i en regions säkra behandlingsmiljö behöver producenten kunna avgöra om aktören uppfyller de krav som ställs. Dessa krav kan avse organisationens status, tillstånd att använda data eller egenskaper hos den tekniska miljön.

I dag saknas ett enhetligt sätt att uttrycka dessa krav och hur de ska kopplas till verifierbara bevis. Krav definieras inom olika domäner, ofta med olika begrepp och strukturer, medan bevis kan tillhandahållas via olika mekanismer, exempelvis federerade lösningar. Utan en gemensam struktur för hur denna information hänger ihop behöver varje aktör göra egna tolkningar, vilket försvårar automatisering och interoperabilitet.

Motsvarande problem uppstår i gränsöverskridande scenarier. En aktör från en annan medlemsstat kan behöva styrka sina egenskaper för att få tillgång till en svensk resurs, exempelvis inom ramen för EHDS eller ett europeiskt dataområde. Samtidigt behöver den svenska aktören kunna tolka dessa egenskaper i relation till nationella krav. I dag saknas en tydlig modell för hur denna koppling ska göras på ett enhetligt sätt.

Detta innebär att de identifierade behoven inte är begränsade till enskilda användningsfall, utan återkommer i flera scenarier där data och AI-resurser behöver användas mellan organisationer och över nationsgränser. De föreslagna tilläggsuppdragen syftar till att adressera dessa återkommande strukturella behov.

10. Fördjupning av föreslagna uppdrag

De kompletteringar som beskrivs i huvudrapporten kan konkretiseras utifrån de analyserade användningsfallen. I dessa scenarier blir det tydligt att Samordnad identitet och behörighet utgör en nödvändig grund för att verifiera identitet och egenskaper, men att ytterligare strukturer krävs för att denna information ska kunna användas enhetligt i praktiken. Nedan beskrivs vad respektive uppdrag innebär och vilka problem de adresserar.

Uppdrag 1 – Struktur för krav och verifierbara bevis

I de analyserade scenarierna, exempelvis när en aktör vill träna en AI-modell i en säker behandlingsmiljö, behöver producenten kunna avgöra om aktören uppfyller ett antal krav. Dessa krav kan avse organisationstillhörighet, rättsligt tillstånd eller tekniska och säkerhetsmässiga egenskaper.

I dag uttrycks dessa krav på olika sätt beroende på domän, samtidigt som de bevis som ska styrka kraven kan komma från olika tillitsmodeller och i olika format. Samordnad identitet och behörighet möjliggör att sådana bevis kan verifieras, men det saknas en gemensam struktur för hur krav och bevis relaterar till varandra och hur de ska tolkas enhetligt.

Uppdraget innebär därför att etablera en domänneutral struktur för hur krav, aktörer, resurser och verifierbar information hänger ihop. Detta omfattar hur krav kan uttryckas maskinläsbart, hur de kopplas till specifika resurser och hur de kan tillämpas konsekvent mellan olika aktörer. Detta är en förutsättning för att organisationsbehörighet ska kunna tillämpas maskinellt. Uppdraget innebär inte att definiera innehållet i kraven, vilket även fortsättningsvis är en fråga för respektive domän, utan att möjliggöra att dessa krav kan uttryckas och användas inom en gemensam struktur.

Uppdrag 2 – Enhetlig modell för beskrivning av säkra behandlingsmiljöer

I användningsfall där data inte får lämna en kontrollerad miljö blir den säkra behandlingsmiljön en central komponent. För att möjliggöra åtkomst behöver producenten kunna avgöra om en viss miljö uppfyller de krav som ställs.

I dag saknas en enhetlig modell för hur sådana miljöer beskrivs. Olika aktörer använder olika begrepp och klassificeringar, vilket innebär att miljöer inte är direkt jämförbara. Detta försvårar både automatiserade beslut och återanvändning mellan organisationer.

Uppdraget innebär att etablera en gemensam struktur för hur säkra behandlingsmiljöer beskrivs, inklusive hur egenskaper som säkerhetsnivå, användningsbegränsningar och tekniska förutsättningar uttrycks. Strukturen ska möjliggöra att dessa egenskaper kan användas som underlag för åtkomstbeslut och, där det är relevant, kopplas till verifierbara egenskaper via samordnad identitet och behörighet. Ansvaret för att definiera konkreta nivåer och krav ligger även fortsättningsvis hos respektive domän.

Uppdrag 3 – Principer för samverkan mellan tillitsmodeller i en hybridmiljö

I praktiken kommer samordnad identitet och behörighet att samexistera med andra tillitsmodeller, såsom SAML-baserade federationer, EU-noder och fristående lösningar. Detta blir särskilt tydligt i scenarier där aktörer från olika sektorer eller länder behöver samverka.

Samordnad identitet och behörighet skapar möjligheter att etablera federativa lösningar för verifiering av tillitsinformation, och arbete pågår för att möjliggöra samverkan med befintliga identitetsfederationer baserade på äldre federationsteknik, exempelvis SAML. Samtidigt uppstår situationer där krav definieras i en kontext, medan verifierbar information tillhandahålls i en annan. I dag saknas gemensamma principer för hur sådana situationer ska hanteras, vilket innebär att varje integration riskerar att lösas separat.

Uppdraget innebär därför att ta fram principer för hur olika tillitsmodeller kan samverka. Det handlar inte om att införa en generell översättning mellan modeller eller att ersätta befintliga lösningar, utan om att skapa en gemensam grund för hur egenskaper kan tolkas i relation till krav och hur tillit kan etableras mellan olika kontexter. Sveriges dataportal kan bidra genom att synliggöra hur olika lösningar fungerar, men ersätter inte behovet av dessa principer.

Uppdrag 4 – Nationell tillitsgrund i relation till europeiska strukturer

I flera av de analyserade användningsfallen, exempelvis deltagande i europeiska dataområden eller EHDS, behöver svenska aktörer kunna styrka sin identitet och sina egenskaper i ett gränsöverskridande sammanhang.

I dessa scenarier etableras tillit i regel via nationella kontaktpunkter, där medlemsstater litar på varandra. Samtidigt behöver den nationella nivån kunna verifiera aktörer enligt egna krav, vilket skapar ett behov av en sammanhållen nationell tillitsgrund.

I dag saknas en tydlig modell för hur denna nationella tillit kopplas till europeiska strukturer, vilket innebär en risk för att olika domäner utvecklar separata lösningar. Uppdraget innebär därför att definiera hur en gemensam nationell tillitsgrund kan användas i relation till EU. Det omfattar hur svenska aktörer kan styrka identitet och egenskaper på ett sätt som kan accepteras i andra medlemsstater, samt hur information från europeiska aktörer kan tolkas i relation till nationella krav.