TJÄNSTEBESKRIVNING FÖR
SAMBIS FEDERATIONSTJÄNST

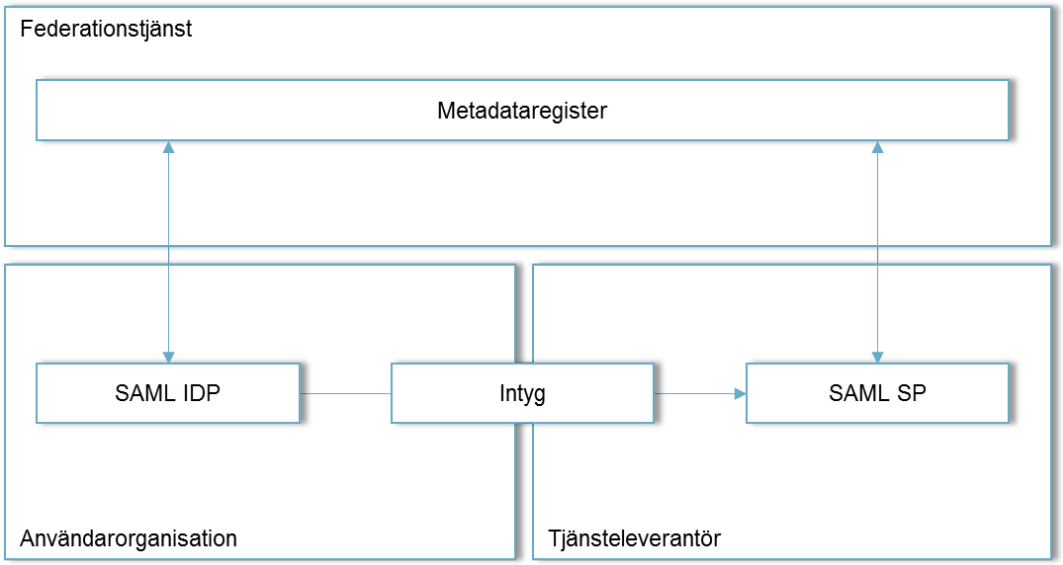
1 Introduktion

1.1 Tjänsten och dess kunder

Sambis Federationstjänst tillhandahåller en sammanhållen teknisk infrastruktur till vilken Sambis Medlemmar kan ansluta system för identifiering och åtkomsträttigheter.

Anslutna organisationer ska uppfylla kraven i Sambis Tillitsramverk och tillämpa gemensamma standarder för åtkomsthantering, vilket underlättar integration och reducerar administration mellan parter.

Den centrala komponenten i Sambis Federationstjänst är federationens aggregerade Metadataregister. Registret innehåller information om anslutna Medlemmar, vilken är kvalitetskontrollerad och verifierad att den kommer från rätt organisation. Informationen används av respektive anslutet system bland annat för att säkerställa att Intyg skickas till eller kommer från rätt part.



Användarorganisation ansvarar för att Användare har giltig Elektronisk identitet och respektive behörighetsstyrande Attribut för att kunna nyttja E-tjänster inom Federationen.

Tjänsten baseras på den tekniska standarden SAMLv2, enligt profilerna eGov2 och saml2int.

Federationstjänsten erbjuds i första hand till Medlem inom Sambi, men vissa tjänster erbjuds till andra intressenter såsom blivande Medlem och Leverantör till Medlem eller blivande Medlem.

1.2 Behov av tjänsten

Federationstjänstens huvudsakliga uppgift är att upprätthålla driften av Sambis gemensamma infrastruktur och de processer som är kopplade till detta.

Visionen för Sambi är att vara en nationell mötesplats för enkel och säker åtkomst till e-tjänster inom hela sektorn. För att möjliggöra visionen krävs en effektiv och säker hantering av Elektroniska identiter och Attribut. Sambi kräver därför att alla Användarorganisationer ansvarar för att deras egna användares identiteter och Attribut är uppdaterade och korrekta. Detta så att de kan användas av de medverkande e-tjänsterna för att fatta beslut om åtkomst.

Sambi kräver även av Tjänsteleverantörerna att de hanterar åtkomsten till sina E-tjänster och de erhållna användaruppgifterna på ett säkert sätt. Detta så att en Användarorganisation som använder en E-tjänst ska kunna känna tillit till att hantering av personuppgifter och patientsäkerheten motsvarar deras krav.

Genom Sambis Metadataregister kan Medlemmar dra nytta av en gemensam källa med verifierad information enligt ett gemensamt regelverk avseende Tillitsramverk och tekniska standarder istället för att upprätta bilaterala överenskommelser med respektive part.

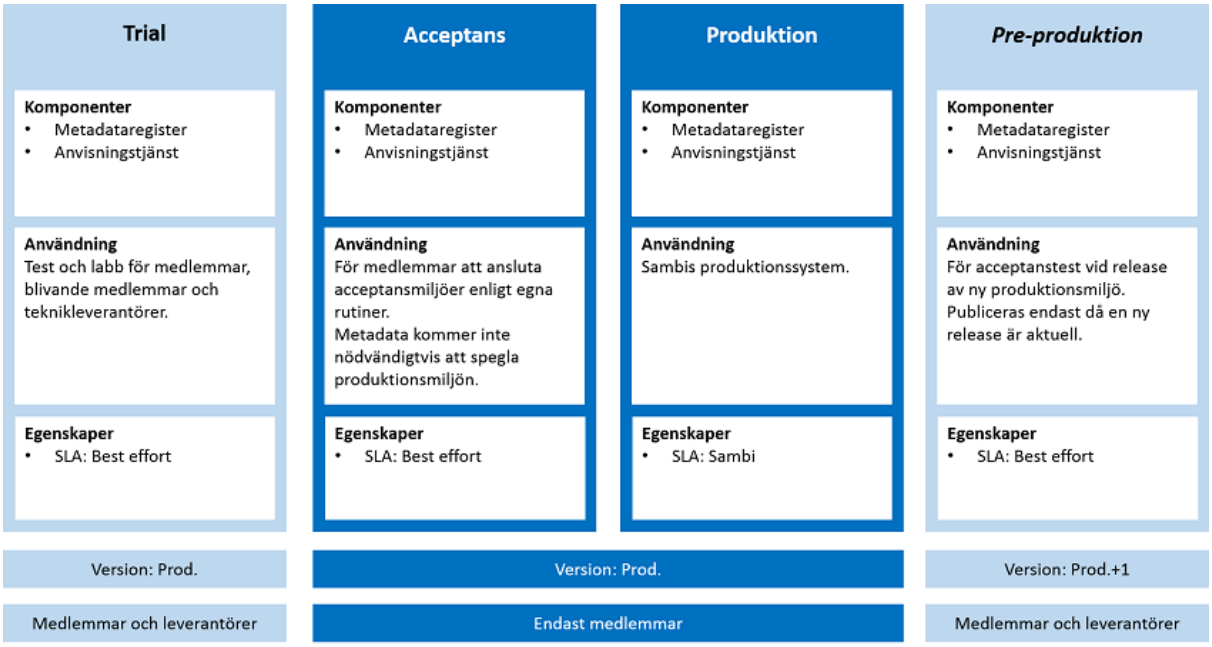
1.3 Relation till Sambis Tillitsgranskningstjänst

Kunderna för Sambis Tillitsgranskningstjänst och Sambis Federationstjänst är till stora delar desamma. Kundkommunikationen mellan de två tjänsterna ska därför vara samordnadgentemot den Sökande.

Produktionen av de två tjänsterna är dock av skild karaktär. Sambis federationstjänst är en IT-tjänst baserad på standarden SAML 2.0 och styrs efter IT-tekniska principer, medan principerna för Sambis Tillitsgranskningstjänst har hämtats från IT-revision och informationssäkerhetsområdet. Stora delar av tjänsternas respektive produktionsprocesser kommer därför drivas separat från varandra.

2 Systemmiljöer

I bilden nedan ges en övergripande beskrivning av de systemmiljöer som tillhandahålls av Sambis federationstjänst. Miljöerna “Acceptans” och “Produktion” är strikt reserverade för Medlemmar i Sambi, medan “Trial” och “Pre-produktion” även tillhandahålls till intressenter i Sambi som inte är Medlemmar.



2.1 Testmiljö (Trial)

Systemmiljö för testning som kan användas av Sökande, Medlemmar och Leverantörer.

2.2 Acceptansmiljö (Acceptans)

Systemmiljö för Medlemmar att genomföra acceptanstester av sina respektive system. Acceptansmiljön utgör ett eget metadataregister, separerat från produktionsmiljön, och håller samma version som produktionsmiljön. Vid vissa typer av uppdateringar av systemmiljöer kan acceptansmiljöns version skilja från produktionsmiljön under en definierad tid, för att underlätta ett säkert versionsbyte av produktionsmiljön.

2.3 Produktionsmiljö (Produktion)

Produktionsmiljön utgör Sambis gemensamma infrastruktur, till vilken Medlemmars produktionssystem ansluts.

2.4 Nästa version Produktion (Pre-produktion)

Vid nya releaser av produktionsmiljön som kan påverka Medlemmars implementationer, ska den kommande versionen tillhandahållas för testning i god tid innan förändringen genomförs i produktionsmiljön. Denna testmiljö tillgängliggörs bara i samband med nya releaser och ska vara tillgänglig för Sökande, Medlemmar och Leverantörer.

3 Systemkomponenter

3.1 Metadataregister

Metadataregistret är den centrala komponenten i en systemmiljö och innehåller ett aggregat av Metadata från samtliga användare som anslutit till systemmiljön. Registret ska signeras med Federationsoperatörens publika nyckel och vara tillgängligt under domänen sambi.se.

3.2 Anvisningstjänst

En unik anvisningstjänst tillhandahålls per systemmiljö, till vilken E-tjänster kan hänvisa Användare för val av Intygsutgivare.

Anvisningstjänsten hanterar användarnas val över tid med syfte att underlätta valsituationen för Användare. För att möjliggöra detta ska en Användares tidigare val av sin Användarorganisations Intygsutgivare framhävas, så att Användaren endast behöver bekräfta sitt tidigare val.

Federationens centrala Anvisningstjänst publiceras på en för Federationen central webbadress (URL).

En E-tjänst ska inte vara beroende av tillgängligheten hos Federationsoperatörens Anvisningstjänst. E-tjänster med höga tillgänglighetskrav ska därför använda en egen anvisningstjänst baserad på Federationens Metadata.

3.3 Validator

Validatorn är en tjänst för Sökande, Medlemmar och Leverantörer där Metadata kan testas innan det skickas in för publicering i aktuellt Metadataregister.

Validatorn ska tydligt ange om Metadata innehåller avvikelser som inte kommer att godkännas för publicering.

Valideringstjänsten är gemensam för samtliga tekniska miljöer.

3.4 Övervakning

Funktioner för övervakning hanteras internt inom federationstjänsten och är i nuläget inte tillgängliga för andra intressenter. Eventuella avvikelser från normal drift rapporteras på Sambis webbplats och beslutade kontaktvägar beroende på avvikelsens art.

4 Metadatahantering

Federationstjänsten tar emot, administrerar, kontrollerar samt publicerar Metadata i Metadataregistret för den aktuella systemmiljön. Hanteringen av Metadata innefattar att:

- kontrollera att den som lämnar Metadata är behörig att göra detta.

- kontrollera att Metadata innehåller information om den aktuella Användarorganisationen, Tjänsteleverantöreren eller Leverantören.
- för de olika systemmiljöerna tillhandahålla en lättanvänd och säker infrastruktur dit behöriga kan lämna sitt Metadata på ett effektivt och säkert sätt.
- tillhandahålla aggregerade och digitalt signerade Metadata på en URL under domänen sambi.se.
- spara loggfiler i 12 månader för att i efterhand kunna spåra förändringar av Metadata-registren i produktionsmiljön.

5 Ändringshantering

Syftet med Federationstjänstens ändringshantering är att ge förutsättningar för väl avvägda beslut om ändring och metod för införande. Processen finns beskriven i sin helhet på Sambis webbplats.

Ändringshanteringen utgår från ett antal fördefinierade bedömningsmodeller för vägledning av beslut om införande och metod för införande. De olika metoderna för införande beskriver notifiering, möjlighet till test, tid för införande och eskaleringsvägar.

Ändringar som inte kan beskrivas enligt de fördefinierade modellerna eskaleras till Sambis Ändringsråd som utgörs av representanter för Medlemmar i Sambi.

Akuta ändringar hanteras av Sambis Ändringsråd för Akut ändring. Rådet finns inte i nuläget och ärendena hanteras tillsvidare av Federationsoperatören.

6 Incidenthantering

Med incident menas här: Alla informationssäkerhetshändelser som hotar riktigheten och tilliten till de Elektroniska dentiteter och Attribut som används i Sambi.

6.1 Incident som inträffar hos Medlemmen

Vid ett problem eller incident hos en Medlem, Användarorganisation eller Tjänsteleverantör, är Medlemmen själv ansvarig för att tillhandhålla support till sina egna Användare. Medlemmarnas driftsorganisationer kan dock vid en incident vända sig till Federationsoperatörens kundtjänst.

För Federationstjänsten finns följande definierat:

- krishanteringsrutiner och krisorganisation för hantering av kris.
- kontaktuppgifter för incidenthantering mellan federationens Medlemmar.
- förmåga att medverka till att hantera incidenter och problem som har att göra med Federationstjänsten eller där felet är av sådan art att Medlemmen behöver tillgång till Federationsoperatörens information.

- rutiner för att verkställa tillfällig avstängning av Medlem i samband med incidenter (dess metadata avlägsnas från metadataregistret). Ett beslut om permanent spärr får dock inte fattas av Federationsoperatören, utan ska fattas av Sambis styrgrupp.

Efter att en incident har inträffat hos en Medlem ska Federationsoperatören ha rätt att begära att Tillitsgranskningstjänsten genomför en granskning hos Medlemmen.

6.2 Incident som inträffar hos Federationsoperatören

Federationstjänsten har etablerade rutiner för incidenthantering i sin egen miljö.

För det fall en incident inträffar hos Federationsoperatören ska Federationsoperatören skyndsamt:

a) informera Medlemmarna om det inträffade,

b) vidta åtgärder för att återställa informationen.

E-hälsomyndigheten beslutar vem som ska granska Federationsoperatören efter att en incident har inträffat.

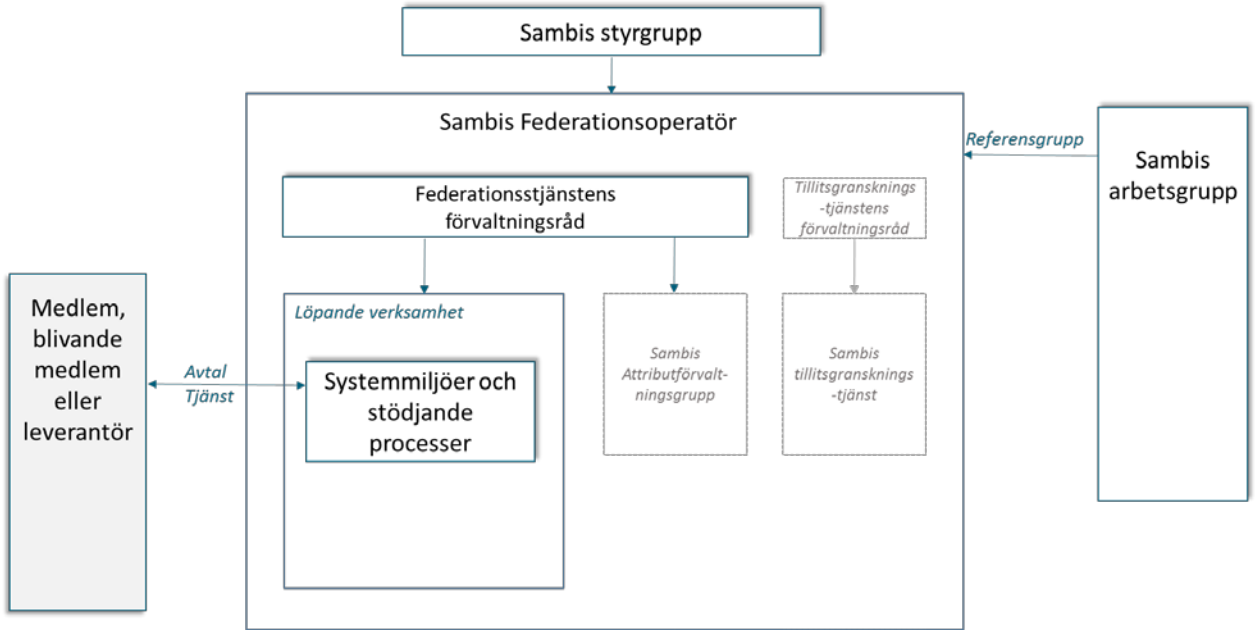
7 Problemhantering

Åtgärdade incidenter med kvarstående rotorsak eller andra typer av problem inom Federationstjänsten hanteras och samordnas av Federationsoperatören. Processen för problemhantering är ännu inte definierad.

8 Organisation

Organisationen för att driva och utveckla Sambis Federationstjänst involverar flera parter. Nedan beskrivs vilka uppgifter följande parter har för tjänsten:

- Sambis styrgrupp
- Sambis arbetsgrupp
- Federationstjänstens förvaltningsråd
- Sambis Attributförvaltningsråd
- Federationsoperatören



8.1 Sambis styrgrupp

Sambis styrgrupp är ansvarig för att fastställa vision och långsiktiga mål för Sambis Federationstjänst, godkänna dess styrande dokument samt följa och utvärdera tjänstens utveckling. Sambis styrgrupp är ansvarig för att utse medlemmarna i Federationstjänstens förvaltningsråd.

8.2 Federationstjänstens förvaltningsråd

Federationstjänsten förvaltningsråd ansvarar för Federationstjänsten och Attributstandardens förvaltningsprocesser och ska bestå av representanter från Användarorganisationerna.

Federationstjänstens förvaltningsråd kan använda sig av flera arbetsgruper som exempelvis ändringsråd eller motsvarande. Idag finns endast ett ändringsråd men förvaltningsråd ska etableras. I väntan på det ska Federationsoperatören fylla dess roll.

8.3 Sambis arbetsgrupp

Sambis arbetsgrupp är en referensgrupp till Sambi som är öppen för alla som vill medverka och bidra till Sambis utveckling. Sambis arbetsgrupp ska även utgöra en referensgrupp för Federationstjänsten.

Sambi arbetsgrupp ska konsulteras i frågor om tjänstens utveckling samt informeras om tjänstens löpande verksamhet.

8.4 Sambis Attributförvaltningsgrupp

Den grupp inom Sambi vars uppgift är att koordinera attributanvändning samt granska och bereda beslutsunderlag för standardisering av Attribut inom Sambi. Federationstjänsten har ett nära samarbete med gruppen för att säkerställa effektiva tekniska lösningar.

8.5 Federationsoperatören

Federationsoperatören ska koordinera arbete mellan Sambis Tillitsgranskningstjänst och:

- Tillitsgranskningstjänstens förvaltningsråd
- Sambis styrgrupp
- Sambis arbetsgrupp
- Sambis Federationstjänst
- Sambis Attributstandard

Federationsoperatören ansvarar för att det finns en aktuell tjänstebeskrivning för Sambis Federationstjänst.

9 Krav

9.1 Allmänna krav

Beskrivningarna i detta dokument följer kraven under kapitel 3 ”Krav på Sambis Federationstjänst” i dokumentet ”Föreskrifter för Sambis Federationsoperatör, version 1.1”.

9.2 Servicenivåer

Definierade servicenivåer avser enbart Produktionsmiljön och processer som är kopplade till denna.

Allmänt	Målsättning
Öppettider	Kontorstid Sverige
Publicering av metadata	Nytt eller uppdaterat metadata publiceras inom en arbetsdag från godkänd validering och motringning.
Systemkomponenter	**Målsättning**
Metadataregister	• 100% korrekt innehåll avseende format och organisation. • 100% tillgänglighet inom angivet intervall för metadatafilens publicerade giltighetstid.

Anvisningstjänst	• Tillgänglighet 99,8% (förannonserade servicefönster tas inte med i beräkning av tillgänglighet)
	• Incident under kontorstid:
	  o Påbörjas inom 30 minuter
	  o Hindertid 3 timmar

	• Incident övrig tid o Påbörjas inom 30 minuter o Hindertid 3 timmar
Validator	• Incident under kontorstid: o Påbörjas inom 30 minuter o Hindertid 4 timmar • Incident övrig tid: o Påbörjas inom ”Best effort” o Hindertid 12:00 följande vardag

9.3 Certifiering

Organisationen för Sambis Federationstjänst är certifierad enligt SS ISO/IEC27001.