TJÄNSTEBESKRIVNING FÖR
SAMBIS TILLITSGRANSKNINGSTJÄNST

1 Introduktion 3
1.1 Tjänsten och dess kunder 3
1.2 Behov av tjänsten 3
1.2.1 Ansvar för Leverantörer 4
1.2.2 Utveckling av behovet 4
1.3 Relation till Sambis Federationsoperatörstjänst 4
2 Granskning av Sökandes självdeklarationer 5
2.1 Initial kontra återkommande Tillitsgranskning 5
2.2 Tillitsgranskningens omfattning 5
2.3 Arbetsmoment 6
2.3.1 Uppstart 6
2.3.2 Avtal 7
2.3.3 Förberedelser 7
2.3.4 Tillitsgranskning 7
2.3.5 Beslut 8
2.4 Hantering vid ändringar av Tillitsramverket 8
3 Kontroll av efterlevnad 8
4 Information 9
4.1 Sambis webbplats 9
4.2 Sambi Tillitsdeklarationskurs 9
4.3 Konsultation 9
5 Organisation 10
5.1.1 Sambis styrgrupp 10
5.1.2 Tillitsgranskningstjänstens förvaltningsråd 10
5.1.3 Sambis arbetsgrupp 11
5.1.4 Tillitsadministratören 11
5.1.5 Granskare 11
5.1.6 Federationsoperatören 12
6 Krav 12
6.1 Allmänna krav 12
6.2 Servicenivåer 13
6.2.1 Granskning av Sökandes Tillitsdeklarationer 13
6.3 Säkerhetskrav på tjänsten 14
6.4 Övervakning av tjänsten 15
6.4.1 Certifiering 15

1 Introduktion

1.1 Tjänsten och dess kunder

Den part vars verksamhet ska Tillitsgranskas benämns Sökande. Sökande kan vara en befintlig Användarorganisation eller Tjänsteleverantör i Sambi, en Användarorganisation eller Tjänsteleverantör som avser att söka medlemskap i Sambi eller en Leverantör till någon av dessa. Sambis Tillitsgranskningstjänst ska granska de Sökandes Tillitsdeklarationer gentemot de uppställda kraven i Sambis Tillitsramverk.

Inom Sambi ska Tillitsgranskningar göras för att säkerställa att nya Sökande och redan befintliga Medlemmar uppfyller kraven i Sambis Tillitsramverk. Både nya Sökande och befintliga Medlemmar ska upprätta en Tillitsdeklaration som beskriver hur denna uppfyller Tillitsramverket.

Utöver att göra granskningar ska Tillitsgranskningstjänsten även bistå Sökanden med information och rådgivning för att underlätta dennes arbete med att utveckla och dokumentera sitt säkerhetsarbete så att det uppfyller Sambis krav.

Sambis Tillitsgranskning ska erbjuda följande deltjänster:

1. Granskning av Sökandes Tillitsdeklaration.
2. Kontroll av efterlevnad hos Sökande.
3. Information till Sökande om hur denne kan utveckla och dokumentera sitt säkerhetsarbete för att uppfylla Sambis krav.

Styrande för samtliga tjänster är Sambis Tillitsramverk. Tjänsternas utformning beskrivs närmare var för sig i kommande kapitel.

1.2 Behov av tjänsten

Det primära målet för Tillitsgranskningstjänsten är att bidra till att Sambi är en Federation med hög säkerhet och stor tillit till Användarnas Identiteter och Attribut.

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.

Den direkta nyttan med Sambis Tillitsgranskningstjänst för nya Användarorganisationer och Tjänsteleverantörer är att kunna bli medlem och dra nytta av federationen Sambi. För befintliga Användarorganisationer och Tjänsteleverantörer kräver Sambi en återkommande granskning vart tredje år.

1.2.1 Ansvar för Leverantörer

Om en Användarorganisation eller Tjänsteleverantör anlitar en Leverantör för hela eller delar av sin hantering av Elektroniska identiteter och Attribut, är denna likväl ansvarig för Leverantören, så som om denna själv utfört arbetet. Användarorganisation och Tjänsteleverantör ska därför redogöra för Sambis Tillitsgranskningstjänst hur deras Leverantörer uppfyller kraven i Sambis Tillitsramverk.

För att underlätta Användarorganisationers och Tjänsteleverantörers arbete med att Tillitsdeklarera kan en Leverantör själv välja att bli granskad av Sambi. Därefter kan en Användarorganisation eller Tjänsteleverantör referera till Leverantörens godkända Tillitsgranskning.

För en Leverantör är därför en genomförd Tillitsgranskning en konkurrensfördel, då den underlättar Tillitsgranskningen för deras kunder.

1.2.2 Utveckling av behovet

Behovet av Sambis Tillitsgranskningstjänst förväntas växa i takt med Sambi. Vid ett väl utbyggt Sambi kan Tillitsgranskningstjänsten kunna behöva klara av att hantera ett hundratal granskningar per år.

Det är även troligt att det successivt kommer önskemål på att utveckla kravställningen i Sambis Tillitsramverk, vilket kan påverka omfattningen och utformningen av Tillitsgranskningstjänsten. Inte minst kan ett ökat internationellt samarbete kring vård- och omsorgstjänster, så som EU:s eIDAS (Electronic Identification and Trust Services), förväntas få en påvarkan på Sambis Tillitsramverk och Tillitsgranskningstjänst.

1.3 Relation till Sambis Federationsoperatörstjänst

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

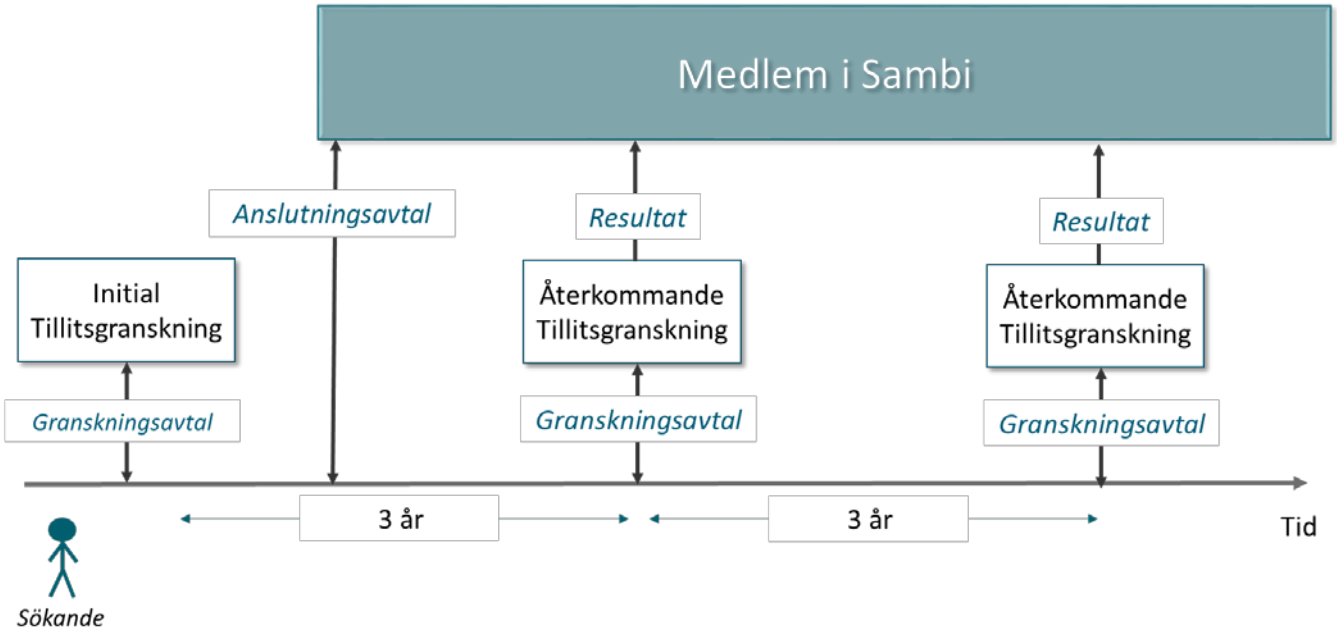
Produktionen av de två tjänsterna är dock av skild karaktär. Sambis Federationstjänst är en IT-tjänst baserad på standarden SAML 2.0 och styrs efter IT-tekniska principer, medan principerna för Sambis Tillitsgranskningstjänst har hämtats från IT-revision och informationssäkerhetsområdet. Stora delar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

2 Granskning av Sökandes självdeklarationer

2.1 Initial kontra återkommande Tillitsgranskning

Granskning av Sökandes Tillitsdeklarationer görs av både nya Sökande som saknar en tidigare godkänd Tillitsgransking, vilket här kallas för en initial granskning, och av Sökande med en tidigare godkänd Tillitsgransking men som behöver förnyas, vilket här kallas för återkommande granskning. En granskning kan även vara aktuell för Sökande som önskar utöka eller förändra omfattningen av en tidigare Tillitsgranskning.

För båda initial och återkommande granskning ska Sökande ingå ett Tillitsgranskningsavtal med Federationsoperatören avseende utförande av Tillitsgranskningstjänsten.



2.2 Tillitsgranskningens omfattning

Tjänsten omfattar att adminstrera och granska de Sökandes Tillitsdeklarationer. Granskningen ska kontrollera att den Sökande uppfyller de krav som Tillitsramverket ställer.

För samtliga Sökande granskas: den Sökandes verksamhet, säkerhetsarbete, ansvar för Leverantörer, hantering av handlingar och tillhandahållande av information.

För Användarorganisation och deras Leverantörer granskas dessutom en eller flera av de tre funktionerna:

- E-legitimationsutfärdare (funktion som utfärdar E-legitimationer till Användare).
- Attribututgivare (funktion som tillhandahåller Attribut för en Användare baserat på en Användares Elektroniska identitet).

- Identitetsintygsutgivare (funktion som utfärdar Identitetsintyg baserat på användares Elektroniska identitet och Attribut avsedda för Tjänsteleverantörs E-tjänst).

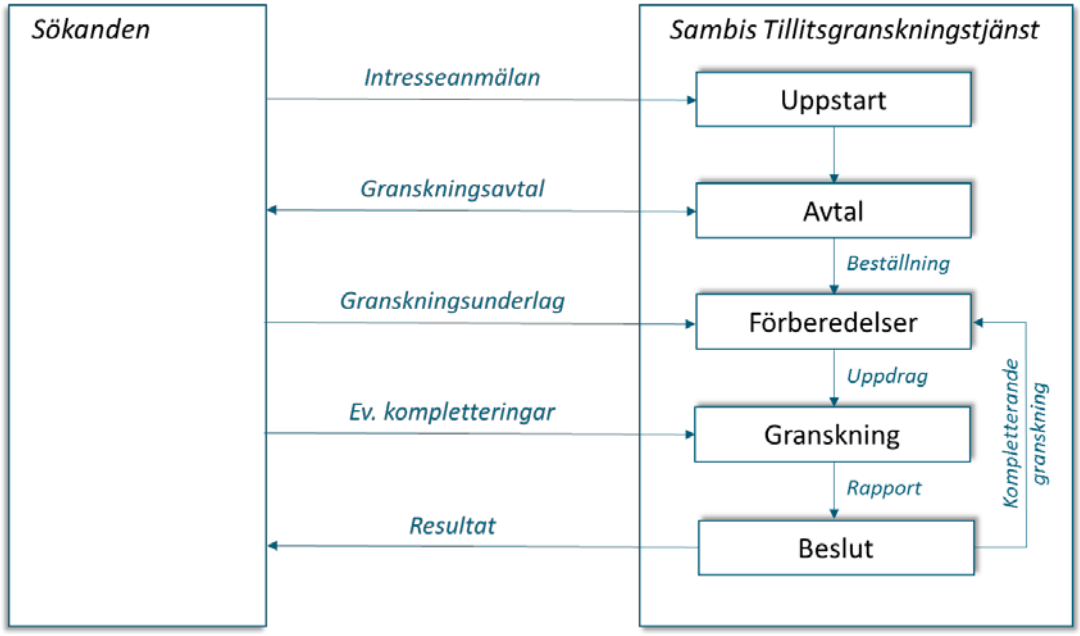
Tjänsteleverantörer och deras Leverantörer granskas efter hur de uppfyller specifika krav för Tjänsteleverantörer.

Tjänsten ska tillhandahålla malldokumentet ”Tillitsdeklaration” för Sökande på vilken denna ska utföra sin Tillitsdeklaration. I detta dokument ska även en vägledning ges för hur Sökanden ska göra sin Tillitsdeklaration.

Tjänsten ska även tillhandahålla dokumentet ”Granskningsinstruktion och checklista för Tillitsdeklaration” som är en checklista för Granskarna och beskriver hur de ska genomföra granskningen.

2.3 Arbetsmoment

En granskning av en Sökandes Tillitsdeklaration består av flera arbetsmoment. Tillitsadministratören är den administrativa part underställd Federationsoperatören som ansvarar för handläggningen av Tillitsdeklarationer och kommunikationen med de Sökande. I figuren nedan anges de olika arbetsmomenten samt det informationsutbyte som ska ske mellan Sökanden och Tillitsadministratören.



2.3.1 Uppstart

Vid en initial granskning ska arbetet inledas med att Sökande sänder in en intresseanmälan, varefter Tillitsadministratören ska påbörja sin planering av granskningsuppdraget.

Inför en återkommande granskning ska Sambis Tillitsgranskningstjänst skicka ut en påminnelse till Medlemmen eller Leverantören senast fyra (4) månader före utgångsdatumet för godkännandet. Arbetsmomenten och hanteringen för en återkommande granskning skiljer sig därefter inte från en initial granskning.

Arbetet i denna etapp omfattar att:

- Förse Sökanden med information om granskningen och upplysa om möjligheten att gå Sambis tillitsdeklarationskurs.
- För det fall intresse finns för ett möte ska ett sådant erbjudas, antingen fysiskt eller på distans.
- Klargöra vad Tillitsgranskningen avser:
  - För en Användarorganisation eller dess Leverantörer kan granskningen avse en eller flera av deras funktioner för att vara Identitetsintygsutgivare, Attribututgivare eller E-legitimationsutfärdare.
  - För en Tjänsteleverantör kan granskningen avse en eller flera tjänster.

När etappen är avslutad förväntas Sökanden ha en god bild av vad deras arbete omfattar, vilka krav som ställs på dem, ha en övergripande plan för sitt arbete och ha avsatta resurser för det.

2.3.2 Avtal

Syftet med detta arbetsmoment är att formalisera granskningsuppdraget i ett påskrivet avtal avseende Tillitsgranskningen mellan Sökanden och Sambis Tillitsgranskningstjänst. I samband med att det signerade avtalet returneras till Sökanden faktureras också Sökanden granskningsavgiften.

När avtalet har upprättats ska den Sökande instrueras att skicka in sin Tillitsdeklaration för granskning.

2.3.3 Förberedelser

Under detta arbetsmoment görs följande förberedelser för granskningen av Tillitsadministratören:

- Kontrollera att Sökanden har lämnat en Fullständig tillitsdeklaration.
- Vid behov begära att den Sökande kompletterar sitt material.
- Utse Granskare. Val av Granskare ska göras utifrån en rotationsprincip i kombination med hänsyn till eventuella jävrisker och Granskarens tillgänglighet.

När en Fullständig tillitsdeklaration har inkommit ska den utsedda Granskaren ges uppdraget att genomföra granskningen.

2.3.4 Tillitsgranskning

Under detta arbetsmoment utförs arbetet av en Granskare i enlighet med instruktionerna i dokumentet ”Granskningsinstruktion och checklista för Tillitsdeklaration”.

Vid behov av förtydliganden eller kompletterande information sänder Granskaren en begäran till Tillitsadministratören, som i sin tur begär in uppgifterna från Sökanden.

Förutom den ifyllda checklistan ska Granskaren sammanfatta granskningsresultatet i en rapport tillsammans med en rekommendation på beslut. Rapporten skickas till Tillitsadministratören.

2.3.5 Beslut

I denna etapp sammanställs ett beslut av Federationsoperatören baserat på rapporten från Tillitsgranskningen. Beslutet kan vara av tre typer:

- Godkänd.
- Godkänd med krav på komplettering eller förbehåll. Det ska då anges för vilken del en kompletterande granskning ska göras eller vad förbehållet avser.
- Ej godkänd.

Granskningsresultatet och eventuella krav på kompletterande Tillitsgranskning meddelas Sökanden. Om inte Sökanden önskar annorlunda, ska alla godkända granskningsresultat publiceras på Sambis webbplats. Ej godkända resultat ska inte publiceras på Sambis webbplats.

För det fall Sökanden inte är nöjd med granskningsresultatet och önskar överklaga resultatet ska överklagandet administreras via Tillitsadministratören som hänskjuter frågan till Sambis styrgrupp.

2.4 Hantering vid ändringar av Tillitsramverket

Den Sökande ska göra sin Tillitsdeklaration med det Tillitsramverk och Tillitsdeklarationsmall som gällde vid tidpunkten då Tillitsgranskningsavtalet slöts. Om Tillitsramverket och/eller Tillitsdeklarationsmallen ändras därefter kan dock den Sökande själv välja att i stället göra sin Tillitsdeklaration enligt det nya Tillitsramverket och/eller Tillitsdeklarationsmallen.

Om inte en Fullständig tillitsdeklaration har inkommit inom den maximala tidsram[1] som anges för tjänsten på Sambis webbplats, måste dock en ny ansökan göras. Den nya Tillitsdeklarationen ska då göras med det då gällande Tillitsramverket och Tillitsdeklarationsmallen.

3 Kontroll av efterlevnad

Sambis Tillitsgranskningstjänst har rätt att utan speciellt skäl genomföra stickprovskontroller om Medlemmen följer Anslutningsavtalet, dock maximalt en gång per år och Medlem.

Kontroll av efterlevnad ska även göras om Medlem eller Federationsoperatören har goda skäl att misstänka att en Medlem eller dess Leverantör inte följer Anslutningsavtalet.

Vid dessa tillfällen ska Sambis Tillitsgranskningstjänst tillse att representant från Sambis Tillitsgranskningstjänst genomför kontroll hos Medlemmen för att undersöka om Medlemmen följer Anslutningsavtalet. En kontroll av efterlevnaden ska föregås av ett skriftligt meddelande till Medlem med angivande av åberopade skäl senast 14 dagar innan granskningen ska ske.

Motiveringen för denna kontroll är att:

- Bibehålla en hög tillit till Medlemmarnas hantering av Elektroniska identiteter och Attribut.
- Få en bättre helhetsbild av hur Elektroniska identiteter och Attribut hanteras.
- Kunna utvärdera hur effektiv Sambis Tillitsgranskningstjänst är.

[1] Se https://www.sambi.se/tillit/tidsramar/, den maximala tiden var per den 2016-03-30 12 månader

Kontrollen av efterlevnaden ska genomföras med hänsyn till Medlemmens behov av sekretess och Sambis Tillitsgranskningstjänst svarar för att erforderliga avtal om sekretess träffas med de som ska utföra kontrollen.

Denna tjänst planeras att införas när Sambis styrgrupp så beslutar (preliminärt under 2017 eller tidigare ifall behov uppstår).

4 Information

4.1 Sambis webbplats

All publik information om Tillitsgranskningstjänsten ska tillhandahållas under fliken Tillit, se https://www.sambi.se/tillit/, på Sambis webbplats.

4.2 Sambi Tillitsdeklarationskurs

Sambi Tillitsdeklarationskurs utgör en viktig informationskälla för de som önskar en förståelse för Sambis Tillitsramverk och hur en Tillitsdeklaration ska genomföras. Information om och anmälan till kursen ska finnas på Sambis webbplats.

4.3 Konsultation

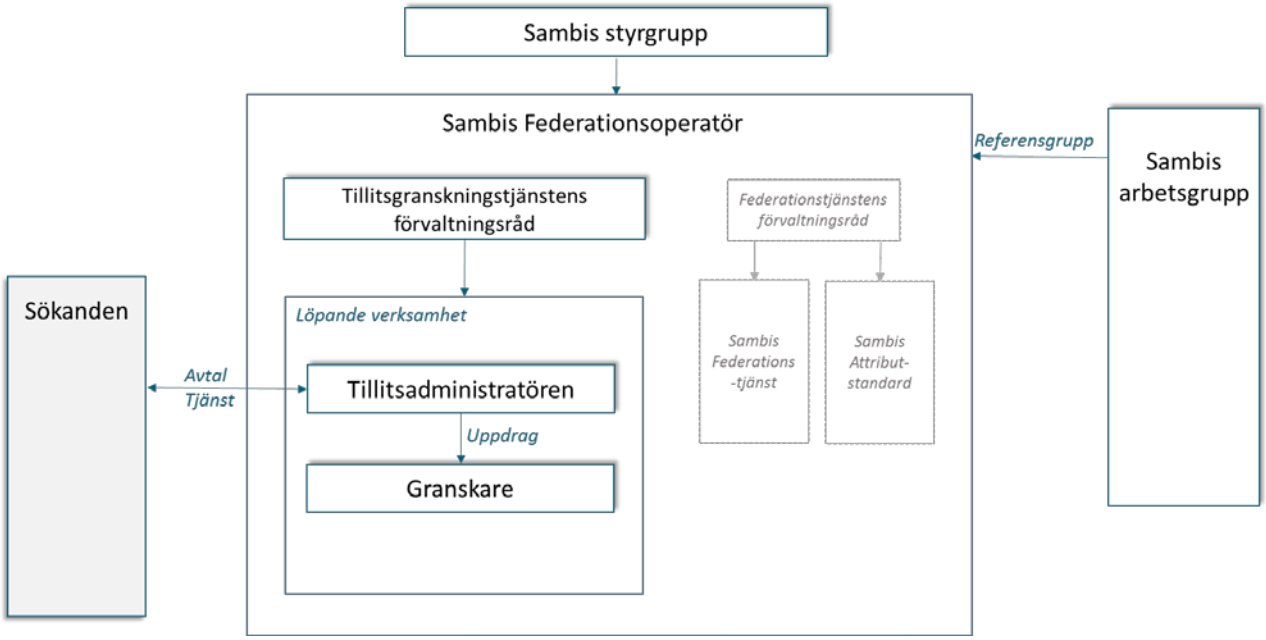
Information till Sökande om hur denne kan utveckla och dokumentera sitt säkerhetsarbete för att uppfylla Sambis krav ska tillhandahållas om önskemål finns.

Ett uppstartsmöte ska ingå utan extra kostnad i tjänsten. Därefter kan Sökanden komma att debiteras.

5 Organisation

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

- Sambis styrgrupp
- Sambis arbetsgrupp
- Tillitsgranskningstjänstens förvaltningsråd
- Tillitsadministratören
- Granskare
- Federationsoperatören



5.1.1 Sambis styrgrupp

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

5.1.2 Tillitsgranskningstjänstens förvaltningsråd

Tillitsgranskningstjänstens förvaltningsråd ska bestå av representanter från Användarorganisationerna.

Det ansvarar för att utarbeta visioner och långsiktiga mål för Sambis Tillitsgranskningstjänst, utarbeta dess styrande dokument, att för den löpande verksamheten fatta beslut i policyfrågor samt följa och utvärdera tjänstens utveckling. Rådets arbete ska rapporteras till Sambis styrgrupp.

Tillitsgranskningstjänstens förvaltningsråd finns för närvarande inte, men ska etableras. I väntan på det ska Federationsoperatören fylla dess roll.

5.1.3 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 Tillitsgranskningstjänsten.

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

5.1.4 Tillitsadministratören

Tillitsadministratören ska utföra tjänstens löpande arbete och utgöra den part med vilken den Sökande tecknar avtal om Tillitsgranskning.

Idag innehar IIS denna roll och tjänstens löpande arbete utförs av en intern administrativ arbetsgrupp. Dess arbete omfattar bland annat att:

- Hantera den löpande kommunikationen med Sökanden.
- Hantera intresseanmälan och Tillitsgranskningsavtal.
- Ansvara för att utse de Granskare som ska granska de Sökandes Tillitsdeklarationer.
- Förvalta de tekniska system som används för Sökandens Tillitsdeklarationer och granskningsresultat.
- Ansvara för tjänstens Tillitsgranskningsavtal och avtal med Sambis Granskare.

Så länge IIS innehar rollen som Tillitsadministratör ska arbetet bedrivas enligt IIS principer för tjänstehantering. Detta innebär att tjänsten leds av en Tjänsteägare som ansvarar inför IIS VD och ledningsgrupp och i detta fall även för Tillitsgranskningstjänstens förvaltningsråd. I ansvaret ingår bland annat att:

- Ta fram en tjänstebeskrivning för tjänsten (detta dokument).
- Ta fram och årligen uppdatera en tjänsteplan vilket sker i samband med budgetarbetet.
- Månadsvis rapportera status för tjänsten.
- Agera systemägare för tjänstens IT-system och/eller utse systemägare/systemförvaltare samt ajourföra listan över ”IT–system”.
- Vid större förändringar ansvara för att IIS tjänsteprocess följs genom att: ta fram en tjänsteförstudie, ansvara för eventuell konceptutveckling och dess resultat samt ansvara för införandet av tjänsten.
- Ansvara för tjänstens löpande arbete, så att den drivs och utvecklas optimalt enligt beslutad tjänsteplan.

5.1.5 Granskare

Granskarna är de som utför Tillitsgranskningarna av Sökandes Tillitsdeklarationer i enlighet med Tilllitsgranskningstjänstens föreskrifter och instruktioner. De utgörs idag av externa konsulter som avropas för att genomföra granskningsuppdragen.

Granskare ska uppfylla kraven i dokumentet ”Instruktioner för Sambis Granskare”. Innan en Granskare engageras ska ett ramavtal tecknas, vilket finns i dokumentet ”Ramavtal - Konsulttjänster för Tillitsgranskning”. Inför varje nytt granskningsuppdrag ska ett avrop tecknas med Granskaren. För detta används dokumentet Uppdragsbekräftelsemall.

5.1.6 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 Tillitsgranskningstjänst.

6 Krav

6.1 Allmänna krav

För att Tillitsgranskningstjänsten ska motsvara Medlemmarnas och intressenternas förväntningar ska tjänsten uppfylla följande generella krav:

- Tillitsgranskningarna ska hålla en hög och jämn kvalité. Detta innebär att en granskning ska vara korrekt och förutsägbar (det vill säga att de som lever upp till kraven ska bli godkända och de som inte gör det ska inte bli godkända).
- Tillitsgranskningsunderlagen och resultaten ska hanteras som konfidentiell information och den granskade ska känna förtroende för hanteringen.
- Återkopplingen av granskningsresultatet till den Sökande ska ske skyndsamt.
- Administrationen av Tillitsgranskningarna ska vara effektiv att genomföra för Sambis Tillitsgranskningstjänst.
- Det ska vara möjligt för en Sökande med en god informationssäkerhet att bli godkänd med en rimlig arbetsinsats.
- Den Sökande ska kunna få lämplig vägledning för att göra sin ansökan och vid behov utveckla sitt informationssäkerhetsarbete så att Sambis krav på tillit kan uppnås.
- Tillitsgranskningstjänsten ska kunna hantera den volym som Sambi kräver för hela vård- och omsorgssektorn.
- Tillitsgranskningstjänsten ska ska vidta åtgärder för att öka förståelsen och acceptansen för Sambis Tillitsgranskning inom sektorn.

6.2 Servicenivåer

Allmänt	Målsättning
Öppettider	Kontorstid Sverige

6.2.1 Granskning av Sökandes Tillitsdeklarationer

Allmänt	Målsättning
Period för att tillitsdeklarera	Efter Tillitsgranskningsavtalet har slutits ska Sökanden skicka in sin Tillitsdeklaration. Tiden från det att Tillitsgranskningsavtalet har slutits till att en Fullständig Tillitsdeklaration har inkommit får inte överskrida 12 månader.
Servicenivå för arbetsmoment	**Målsättning**
Uppstart	Sökande ska besvaras inom fem (5) arbetsdagar.
Avtal	Sökande ska besvaras inom fem (5) arbetsdagar.
Förberedelser	Federationsoperatören ska återkomma med besked inom 10 arbetsdagar till Sökande om dess insända Tillitsdeklaration är komplett och Tillitsgranskning kan påbörjas eller om kompletteringar krävs.
Tillitsgranskning	Efter att en Fullständig tillitsdeklaration inkommit till Federationsoperatören ska ett granskningsresultat ges till Sökande inom 30 arbetsdagar. Under Tillitsgranskningen kan ytterligare begäran om komplettering av Tillitsdeklarationen krävas. En sådan komplettering ska inkomma från den Sökande inom fem (5) arbetsdagar. Vid behov kan Tillitsadministratören förlänga tiden för komplettering. Om en eller flera kompletteringar krävs under tillitsgranskningen kan tillitsgranskningsperioden komma att utökas och ett granskningsresultat delges senare än inom 30 arbetsdagar.
Beslut	Beslut ska meddelas den Sökande senast fem (5) arbetsdagar efter granskningsrapporten har erhållits.

6.3 Säkerhetskrav på tjänsten

Tillitsgranskningen innebär att Granskaren får del av information om Sökanden eller Medlemmen som är konfidentiell och i vissa fall också sekretessbelagd enligt lag. Tjänsten ska därför kunna hantera tillitsgranskningsunderlag enligt IIS regler för sekretess vilket innebär att:

- Granskare och Tillitsadministratörens personal ska vara bunden av ett sekretessavtal som omfattar Tillitsgranskningar i Sambi. Sekretessen ska även innefatta namnet på organisationer som ska eller har granskats.
- Granskaren ska ha vidtagit grundläggande försiktighetsåtgärder för skydd mot skadlig kod i sin miljö.
- Information som erhållits i samband med Tillitsgranskningen ska inte ges till utomstående eller nyttjas annat än i samband med Tillitsgranskningen. Detta gäller även efter Tillitsgranskningens slutförande.
- All elektronisk överföring av information ska vara krypterad och alla dokument aktuella för en Tillitsgranskning mottas av Granskaren via Sambis system för dokumenttransport. Allt underlag ska hanteras som konfidentiellt.
- All dokumentation ska förvaras på en separat krypterad partition på datorn som endast tillgängliggörs vid utförandet av tillitsgranskningsarbetet. När partitionen inte behövs ska den avmonteras. Partitionens krypteringsnyckel ska skyddas genom användning av ett starkt lösenord som måste anges varje gång den ska tillgängliggöras.
- Informationen får lagras på flyttbart media under förutsättning att det flyttbara mediet är märkt på ett sådant sätt att det inte kan förväxlas och att informationen som lagras på mediet krypteras i dess helhet på motsvarande sätt som vid hårddiskkryptering. Samt att nyckelmaterialet för krypteringen hålls skilt från mediet och i övrigt skyddas på samma sätt som vid hårddiskkryptering.
- Förlust av lagringsmedia, fast installerad och flyttbar, ska vid upptäckt utan dröjsmål anmälas till Tillitsadministratören.
- Under Tillitsgranskningsperioden ska den del av Granskarens miljö som används för att lagra information om Tillitsgranskningen vara krypterad och undantagen från alla typer av backuprutiner och automatiskt säkerhetskopiering så att endast de avsedda mottagarna kan ta del av uppgifterna.
- Granskningar får endast utföras i skyddade (icke-offentliga) miljöer och konversationer och annan kommunikation ska ske på ett säkert sätt. Endast i undantagsfall bör något underlag tillhörande en Tillitsgranskning skrivas ut på papper. Underlaget får aldrig exponeras för någon annan än Granskaren och måste förstöras (tuggas eller brännas) efter användning.
- Informationen får inte faxas och vid försändning med extern post ska typen rekommenderat brev användas.
- Raderingsprogram ska finnas installerat hos Granskaren och användas för all dokumentation som hör till Tillitsgranskningen efter att en Tillitsgranskning är avslutad.

6.4 Övervakning av tjänsten

Tjänsten ska övervakas löpande av IIS ledningsgrupp och Sambis styrgrupp. När Tillitsgranskningstjänstens förvaltningsråd har etablerats kan detta ta över ansvar för den löpande övervakningen av tjänsten.

Sambis arbetsgrupp utgör en referensgrupp för tjänsten.

6.4.1 Certifiering

Federationsoperatören IIS har ett certifierat Ledningssystem för informationssäkerhet (LIS) enligt SS ISO/IEC27001:2013. Detta omfattar även Tillitsgranskningstjänsten.

Förslag har väckts om att certifiera Sambis Tillitsgranskningstjänst gentemot “ISO/IEC 27007:2011 Guidelines for information security management systems auditing”. ISO-standarden ger vägledning om hantering av ett revisionsprogram för ledningssystem för informationssäkerhet (LIS) omfattande utförandet av Tillitsgranskningar och kompetens hos revisorer. I detta fall skulle i så fall en certifiering ske av Tillitsgranskningstjänsten gentemot Sambis Tillitsramverk och tjänstens processer. Inga sådana planer finns dock, men kan undersökas om intresse framkommer.