BILAGA 5 - Föreskrifter för Sambiombud

Version: 1.0.2

Innehåll

1 Inledning

1.1 Om detta dokument

I detta dokument anges de krav som ställs på Sambiombud. Kraven är uppdelade i följande kapitel:

Sambiombudets tekniska tjänst - Krav på de tekniska tjänster som ett Sambiombud erbjuder Användarorganisationer.

Tillitsgranskning av Sambiombud - Krav på den initiala och den årliga återkommande granskningen av Sambiombud.

Tillitsgranskning av Användarorganisation - Krav på det stöd Sambiombudet ska ge åt Användarorganisationer vid tillitsgranskning mot Federationsoperatören.

Administration av kontaktuppgifter - Krav på att inkomma med aktuella kontaktuppgifter för Sambiombud och dess Användarorganisationer.

Medlemsadministration av Användarorganisationer - Krav på hantering vid ansökan om medlemskap i Sambi, hantering av avtal och Metadata.

Incidenthantering - Krav på hantering av incident hos Sambiombudet eller dess Användarorganisationer.

1.2 Samverkan

I Sambi finns flera parter som ett Sambiombud ska samverka med. Dessa är Användarorganisationer, Tillitsgranskningstjänsten, Federationsoperatören och Sambis styrgrupp. Ansvarsfördelningen mellan dessa parter beskrivs översiktligt i tabellen nedan. Med behjälplig avses att parten har en skyldighet att vid behov bistå den ansvariga parten att fullgöra sitt ansvar.

Uppgift	Användar-organisation	Sambiombud	Federations-operatör	Tillitsgransk-ningstjänst	Sambis styrgrupp
Upprätta tillitsdeklaration	Ansvarig	Behjälplig			
Vid initial tillitsgranskning, kontrollera och leverera en Fullständig tillitsdeklaration för Användarorganisationen till Sambis Tillitsgranskningstjänst.	Behjälplig	Ansvarig			
Vid återkommande tillitsgranskning, kontrollera och leverera en fullständig Tillitsdeklaration för Användarorganisationen till Sambis Tillitsgranskningstjänst.	Behjälplig	Ansvarig			
Granska och godkänna tillitsgranskningen		Behjälplig		Ansvarig	
Kontroll av efterlevnad av Tillitsramverket	Behjälplig	Ansvarig		Ansvarig	
Ansöka om Medlemskap i Sambi	Ansvarig	Behjälplig			
Delge och säkerställa att Anslutningsavtalet för Medlemskap i Sambi blir levererat och undertecknat av Användarorganisationen som önskar bli Medlem i Sambi via Sambiombudet.		Ansvarig	Behjälplig		
Lagra aktiva och arkivera avslutade Anslutningsavtal för Medlemskap i Sambi för Användarorganisationer anslutna via Sambiombudet.	Behjälpliga	Ansvarig			

Uppgift	Användar-organisation	Sambiombud	Federations-operatör	Tillitsgransk-ningstjänst	Sambis styrgrupp
Besluta om Medlemskap		Behjälplig	Ansvarig	Behjälplig	
Hantering av incident hos Användarorganisation	Ansvarig	Behjälplig	Behjälplig		
Hantering av incident hos Sambiombud		Ansvarig	Behjälplig		
Publicering, Uppdatering och Borttagning av Metadata		Behjälplig	Ansvarig		
Förse Federationsoperatören med vid var tid korrekt Metadata för Användarorganisationer	Behjälplig	Ansvarig			
Tillfällig avstängning av metadata		Behjälplig	Ansvarig		
Beslut om permanent avstängning			Behjälplig		Ansvarig
Tillhandahålla aktuella kontaktuppgifter för Användarorganisationen till Sambiombudet	Ansvarig	Behjälplig			
Tillhandahålla aktuella kontaktuppgifter för Användarorganisationen till Federationsoperatören		Ansvarig	Behjälplig		
Hålla register över medlemmar		Behjälplig	Ansvarig		
Granskning av Sambiombud				Ansvarig	
Godkännande av Sambiombud			Ansvarig		

2 Sambiombudets tekniska tjänst

Sambiombudets roll är att förenkla anslutning till Sambi för Användarorganisationer genom att erbjuda nödvändiga tjänster för identitets- och åtkomsthantering.

Sambiombudet ska bistå Användarorganisationen med att uppfylla kraven i Sambis Tillitsramverk och utföra den administration som Sambi kräver. Ett Sambiombud ska själv eller via leverantörer även kunna leverera följande funktioner som en paketlösning till sina Användarorganisationer, för de som så önskar:

- E-legitimationsutfärdare
- Attributsutgivare
- Identitetsintygsutgivare

Utöver det ska Sambiombudet erbjuda lösningar och tjänster för uppföljning av informationssäkerhet, incidenthantering, rapportering samt övervakning för Sambi.

3 Tillitsgranskning av Sambiombud

3.1 Initial granskning

Innan Sambiombudet är tillåten att erbjuda sina tjänster åt Användarorganisationer, ska Sambiombudet själv ha genomgått en initial Tillitsgranskning av Sambiombud med ett godkänt resultat. Den initiala Tillitsgranskningen omfattar det blivande Sambiombudets hela Tillitsdeklaration, förutom granskning av Sambiombudets kommande tillämpning av rutiner för hantering av Användarorganisationer anslutna via Sambiombudet.

Efter det att ett Sambiombudsavtal har upprättats med Federationsoperatören och verksamheten har kommit i gång, ska en slutgranskning ske av Sambiombudet. Den ska omfatta granskning av Sambiombudets tillämpning av rutiner för hantering av dess Användarorganisationer, samt eventuella krav på kompletteringar från den initiala Tillitsgranskningen. Slutgranskningen ska genomföras även som ett på platsbesök hos Sambiombudet.

3.2 Årlig återkommande tillitsgranskning

Då Sambiombudet har stor betydelse för tilliten inom federationen, ska ett Sambiombud årligen granskas av Sambis Tillitsgranskningstjänst.

3.3 Omfattning

Ett Sambiombud ska tillitsgranskas mot krav A, B, C, D och F i Sambiombudsavtalets Bilaga 3 – Tillitsramverket, samt de krav som ställs i denna bilaga på Sambiombud.

3.4 Tillkommande tjänster

Om ny tjänst tillkommer ska en ny tillitsgranskning genomföras. Granskningen ska då begränsas till att endast omfatta den aktuella tjänsten.

3.5 Förändring av tillitsgranskad tjänst

Sambiombudet ska utan dröjsmål meddela Sambis Tillitsgranskningstjänst eventuella förändringar i de delar av sin verksamhet som omfattas av Tillitsgranskningen eller andra förändringar som kan påverka Tillitsdeklarationen och/eller sin förmåga att uppfylla Tillitsramverket. Sambis Tillitsgranskningstjänst har, vid meddelande om förändring, rätt att revidera hela eller vissa delar av Tillitsgranskningen om detta bedöms vara nödvändigt eller lämpligt för att säkerställa att Sambiombudet följer Tillitsramverket.

3.6 Kontroll av efterlevnad

Målsättningen för Kontroll av efterlevnad är att:

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

Sambis Tillitsgranskningstjänst har rätt att utföra Kontroll av efterlevnad hos Sambiombudet:

- Om Sambiombud, Medlem, Underleverantör eller Federationsoperatören har skäl att misstänka att ett Sambiombud eller dess Underleverantörer inte följer Tillitsramverket och dess föreskrifter.
- Om en incident har inträffat i enlighet med punkt 7 nedan.
- För att med stickprov undersöka hur Sambiombudet eller dess Underleverantörer följer Tillitsramverket och dess föreskrifter.

Vid Kontroll av efterlevnad genomför en representant från Sambis Tillitsgranskningstjänst kontrollen hos Sambiombudet och dess Underleverantörer. Sambiombudet ska under Kontrollen av efterlevnad vara Sambis Tillitsgranskningstjänst behjälplig och inkomma med de detaljer och uppgifter som behövs.

Kontroll av efterlevnad ska föregås av ett skriftligt meddelande från Federationsoperatören till Sambiombudet med angivande av åberopade skäl senast 14 dagar innan granskningen ska ske. Om Kontroll av efterlevnad ska genomföras hos Sambiombudets Underleverantörer ska meddelandet sändas från Federationsoperatören via Sambiombudet till Underleverantören. Kontrollen av efterlevnad ska genomföras med hänsyn till behov av sekretess och Sambis Tillitsgranskningstjänst svarar för att erforderliga avtal om sekretess träffas med de som ska utföra kontrollen.

4 Tillitsgranskning av Användarorganisation

De krav som ställs på en Användarorganisation ansluten via ett Sambiombud ska vara de samma som för direktanslutning till Sambi.

4.1 Upprättandet av Användarorganisationers Tillitsdeklaration

Sambiombudet ska vara sina Användarorganisationer behjälpliga i deras arbete med att ta fram en Fullständiga tillitsdeklaration för Sambis tillitsgranskning genom att:

- tillhandahålla information och rådgivning för att underlätta deras arbete med att utveckla och dokumentera deras informationssäkerhetsarbete och för att uppfylla Tillitsramverket.
- assistera dem med att sammanställa ett komplett underlag för Sambis tillitsgranskning.
- Sambiombudet ska utan dröjsmål meddela Sambis Tillitsgranskningstjänst eventuella förändringar i de delar av Användarorganisationens verksamhet som omfattas av Tillitsgranskningen, eller andra förändringar som kan påverka Tillitsdeklarationen och/eller Användarorganisationens förmåga att uppfylla Tillitsramverket. Sambis Tillitsgranskningstjänst har, vid meddelande om förändring, rätt att revidera hela eller vissa delar av Tillitsgranskningen om detta bedöms vara nödvändigt eller lämpligt för att säkerställa att Användarorganisationen följer Tillitsramverket.

4.2 Leverans av Fullständig tillitsdeklaration

Sambiombudet är ansvarig att sända in en Fullständig tillitsdeklaration för Användar-organisationer anslutna via dem. Både för den initiala tillitsgranskningen och den vid återkommande tillitsgranskningar vart tredje år.

4.3 Konfidentialitet

Tillitsgranskningsunderlagen och granskningsresultatet ska hanteras som konfidentiell information av Sambiombudet och Sökanden ska kunna känna förtroende för hanteringen.

Tillitsgranskningen innebär att Sambiombudet får del av information om Sökanden som är konfidentiell och i vissa fall också sekretessbelagd enligt lag. Sambiombudet förbinder sig att inte för utomstående röja konfidentiell eller sekretessbelagd information som erhållits i samband med Tillitsgranskningen och inte heller nyttja sådan information annat än i samband med Tillitsgranskningen.

Sambiombudet äger dock rätt att lämna ut Tillitsdeklaration och övrig för Tillitsgranskningen nödvändig information och dokumentation till Sambis Tillitsgranskningstjänst för att genomföra eller administrera Tillitsgranskningen eller för att på annat sätt kunna leva upp till Sambiombudsavtalet.

Sekretessåtagandet gäller inte för sådan information som Sambiombudet kan visa blivit känd på annat sätt än genom Tillitsgranskningen eller som är allmänt känd eller när Sambiombudet enligt lag är skyldig att lämna ut handlingar eller uppgifter.

4.4 Kontaktperson vid tillitsgranskning av Användarorganisationer

Sambiombudet ska vara Användarorganisationens kontaktperson gentemot Sambis Tillitsgranskningstjänst. Detta gäller både för den initiala och de återkommande granskningarna. I detta ansvar ingår att Sambiombudet:

- säkerställer att begärda uppgifter inkommer inom angivna tidsramar.
- är behjälplig med att hantera eventuella kompletteringar som begärs in under deras Användarorganisationers granskningsprocess.

4.5 Kontroll av efterlevnad

Målsättningen för Kontroll av efterlevnad av Användarorganisation ansluten via ett Sambiombud är att:

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

Sambiombudet ska på eget och på Federationsoperatörens initiativ och instruktioner utföra Kontroll av efterlevnad hos dess Användarorganisationer:

- Om Sambiombud, Medlem, Underleverantör eller Federationsoperatören har skäl att misstänka att Användarorganisationen ansluten via ett Sambiombud inte följer Tillitsramverket och dess föreskrifter.
- Om en incident har inträffat hos Användarorganisationen i enlighet med avsnitt 7 nedan.
- För att med stickprov undersöka hur Användarorganisationer följer Tillitsramverket och dess föreskrifter.

Sambis Tillitsgranskningstjänst har rätt att vid behov genomföra Kontroll av efterlevnad hos Användarorganisationen. I dessa fall behöver inte Sambiombudet själv genomföra Kontroll av efterlevnad utan ska vara behjälplig att inkomma med de detaljer och uppgifter som behövs.

Kontroll av efterlevnad genomförs antingen av Sambiombudets representant eller, för det fall Sambis Tillitsgranskningstjänst genomför kontrollen, av en representant från Sambis Tillitsgranskningstjänst.

Kontroll av efterlevnad ska föregås av ett skriftligt meddelande från Sambiombudet med angivande av åberopade skäl senast 14 dagar innan granskningen ska ske. Kontrollen av efterlevnad ska genomföras med hänsyn till behov av sekretess och Sambiombudet, eller vid behov Sambis Tillitsgranskningstjänst, svarar för att erforderliga avtal om sekretess träffas med de som ska utföra kontrollen.

5 Administration av kontaktuppgifter

5.1 Sambiombudets kontaktuppgifter

Sambiombudet ska:

- vid var tid tillhandahålla aktuella av Federationsoperatören begärda kontaktuppgifter för Sambiombudet till Federationsoperatören.
- Sambiombudet är skyldig att omgående meddela Federationsoperatören eventuella förändringar av dessa uppgifter.

5.2 Användarorganisationers kontaktuppgifter

Sambiombudet ska vara Federationsoperatören behjälplig att vid var tid hålla ett aktuellt och uppdaterat medlemsregister för Användarorganisationer anslutna via ombudet. Detta säkerställs genom att Sambiombudet ska:

- ta in och till Federationsoperatören tillhandahålla aktuella, korrekta och valida av Federationsoperatörens begärda kontaktuppgifter för Sambiombudets anslutna Användarorganisationer.
- hålla en uppdaterad förteckning över kontaktuppgifter innehållande namn, e-postadresser, telefonnummer och postadresser samt annan relevant information om Sambiombudets Användarorganisationers kontaktpersoner. Sambiombudet är skyldig att omgående meddela Federationsoperatören eventuella förändringar av dessa kontaktuppgifter.
- föra ett register över sina Användarorganisationer. Så snart en Användarorganisation blivit godkänd, om den lämnar ombudet, eller om godkännande har löpt ut eller dragit in, ska registrets uppdateras omgående.
- tillhandahålla sitt register till Federationsoperatören enligt vid var tid gällande instruktioner, detta för att Federationsoperatören ska kunna hålla ett samlat och uppdaterat register över Sambis samtliga Medlemmar.

6 Medlemsadministration av Användarorganisationer

Sambiombudet ansvarar för stora delar av sina anslutna Användarorganisationernas medlemsadministration i Sambi. Däribland att kontrollera att aktuella kontaktuppgifter upprätthålls, informationsspridning, incidenthantering och att tillse att en aktuell Tillitsgranskning finns för Användarorganisationer. Följande ska gälla för alla Användarorganisationer anslutna via Sambiombudet.

6.1 Vid ansökan om medlemskap

För de Användarorganisationer som önskar bli medlemmar i Sambis, ska Sambiombudet:

- kontrollera att Användarorganisationen är behörig att bli medlem i Sambi
- vara behjälplig Federationsoperatören genom att tilldela Användarorganisationen relevanta avtal och förbindelser för att ingå medlemskap.

6.2 Signering och hantering av Anslutningsavtal

Sambiombudet ska bistå Användarorganisationen med att teckna ett Anslutningsavtal för de Användarorganisationer som önskar ansluta via Sambiombudet.

Sambiombudet är ansvarig för att dess Användarorganisationer har undertecknat anslutningsavtalet till Sambi, samt att undertecknandet har gjorts av firmatecknare eller av person med motsvarande behörighet.

6.3 Lagring och arkivering av Anslutningsavtal

Aktiva Anslutningsavtal till Sambi ska bibehållas och lagras. Sambiombudet ska på begäran kunna visa upp det signerade anslutningsavtalet för Federationsoperatören.

Sambiombudet ska arkivera avslutade Anslutningsavtal till Sambi för Användarorganisationer anslutna via ombudet i 10 år.

6.4 Ändring av Sambis Anslutningsavtal

Om ändring sker av Sambis Anslutningsavtal eller dess bilagor, speciellt Tillitsramverket, ska Sambiombudet meddela Användarorganisationen via e-post senast 30 dagar innan ändringen träder i kraft. Meddelandet ska innehålla information om konsekvenserna för Användarorganisationen och åtgärder som måste vidtas.

6.5 Hantering av Metadata

Sambiombudet ska meddela och Federationsoperatören tillhandahålla Metadata när behov föreligger av att lägga till, ändra eller ta bort Metadata.

6.5.1 Publicering av Metadata

Sambiombudet ska förse Federationsoperatören med Metadata för respektive Användarorganisation anslutna till Sambi via Sambiombudet för publicering. Varje Användarorganisation ska representeras av en unik entitet i Metadata.

Sambiombudet ska kontrollera att Användarorganisation som ansluts via Sambiombudet har en godkänd tillitsgranskning, samt undertecknat Anslutningsavtalet till Sambi innan Metadata laddas upp till Federationsoperatören.

6.5.2 Uppdatering av Metadata

Metadata ska vid var tid vara aktuellt och uppdaterat. Det är Sambiombudets ansvar att säkerställa att det Metadata som sänds in till Federationsoperatören för publicering är korrekt och vid behov förse Federationsoperatören med nytt Metadata.

6.5.3 Borttagning av Metadata

Sambiombudet ska meddela Federationsoperatören när Metadata ska tas bort då Användarorganisation inte längre är Medlem i Sambi.

6.5.4 Spärrning av Metadata

Sambiombudet ska vara behjälplig Federationsoperatören vid spärrning av metadata för deras Användarorganisationer.

7 Incidenthantering

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

Oavsett om incidenten inträffar hos Sambiombudet eller dess Användarorganisationer ska Sambiombudet skyndsamt:

a) informera Federationsoperatören om det inträffade,
b) vidta åtgärder för att återställa förtroende, och
c) bistå Medlemmen i dess arbete att återskapa förtroendet för identiteter och attribut i Sambi.

I det fall en incident inträffar är Sambiombudet införstådd med att Användarorganisationen ansluten via Sambiombudet kan få en varning av Federationsoperatören. Om Federationsoperatören därutöver finner det nödvändigt, är Sambiombudet införstådd med att Användarorganisationens medverkan i Sambi tillfälligt kan spärras (dess metadata avlägsnas från metadataregistret). Federationsoperatören äger rätt att efter beslut av styrgruppen permanent spärra Användarorganisationen.

För det fall en incident inträffar ska Sambiombudet eller vid behov Sambis Tillitsgranskningstjänst ha rätt att genomföra en Kontroll av efterlevnad enligt reglering i avsnitt 3.6 och 4.5.

7.1 Incidenthantering hos Sambiombudet

Ett Sambiombudet ska ha:

a) Färdiga krishanteringsrutiner och krisorganisation,
b) Giltiga kontaktuppgifter för incidenthantering
c) Förmåga att informera incidenter och problem ut mot sina anslutna Användarorganisationer

7.2 Incidenthantering av Sambiombudsansluten Användarorganisation

Sambiombudet ska ha:

a) Giltiga kontaktuppgifter för incidenthantering för sina Användarorganisationer
b) Förmåga att medverka till att hantera incidenter och problem som har att göra med sina Användarorganisationer, och
c) Rutiner för att vara behjälplig Federationsoperatören vid en tillfällig spärr av Metadata för Användarorganisation i samband med incidenter.

8 Revisionshistorik

Revisionshistorik			
Ver	**Datum**	**Författare**	**Kommentar**
1.0	2017-10-06	Staffan Hagnell	Ny bilagan framtagen inför införandet av Sambiombud.
1.0.1	2018-04-04	Staffan Hagnell	Förtydligande av kp 3.1 – Initial granskning.
1.0.2	2018-11-28	Eva Sartorius	Förtydligande om att Samibombudets paketdelar är valfria för Användarorganisationen