BILAGA 3 – Tillitsramverk

Version: 2.02

Innehåll

Inledning

Bakgrund

Detta dokument är federationen Sambis gemensamma Tillitsramverk. Det specificerar de säkerhetskrav som ställs på Sambis Medlemmar och Sambiombud. Syftet med Tillitsramverket och det säkerhetsarbete som bedrivs inom ramen för Sambi är att Medlemmarna ska kunna lita på varandras elektroniska identiteter och behörighetsstyrande attribut samt att den personliga integriteten skyddas. Tjänsteleverantörer ska kunna ha tillit till Identitetsintyg utställda av en Användarorganisation och Användarorganisationer ska kunna ha tillit till Tjänsteleverantörernas hantering av personuppgifter.

Alla Medlemmar i Sambi måste ha upprättat en Tillitsdeklaration, det vill säga en självdeklaration som beskriver hur de uppfyller Tillitsramverket, samt ha genomgått en Tillitsgranskning med godkänt resultat innan de tillåts att bli Medlemmar i Sambi. Innan ett Sambiombud tillåts erbjuda sina tjänster till Användarorganisationer, måste de ha upprättat en Tillitsdeklaration och genomgått en Tillitsgranskning med godkänt resultat. Både Medlemmar och Sambiombud ska därefter bedriva ett löpande säkerhetsarbete för att fortsatt uppfylla Tillitsramverkets krav.

Sambis Tillitsgranskningstjänst ansvarar för att granska Sökandens Tillitsdeklaration, kontroll av efterlevnad gentemot Tillitsramverket samt att informera Sökande om hur de kan utveckla och dokumentera sitt säkerhetsarbete för att leva upp till Tillitramverkets krav.

Förutom Användarorganisationer, Tjänsteleverantörer och Sambiombud är Tillitsramverket även tillämpligt för deras Underleverantörer, vilka kan välja att låta sig granskas enligt detta Tillitsramverk.

Kravställning

Tillitsramverkets krav är uppdelade i sex avsnitt vilka är tillämpliga för Användarorganisationer, Tjänsteleverantörer, Sambiombud och Underleverantörer enligt tabellen nedan.

Kapitel i Tillitsramverket	Generella krav	E-legitimations-utfärdare	Attributs-utgivare	Idenitets-intygs-utgivare	Tjänste-leverantör	Sambi-ombud
Användar-organisation	Skall krav	Skall Krav	Skall Krav	Skall Krav	-	-
Tjänste-leverantör	Skall Krav	-	-	-	Skall krav	-
Sambiombud	Skall Krav	Skall Krav	Skall Krav	Skall Krav	-	Skall Krav
Under-leverantör	Skall Krav	Valbar	Valbar	Valbar	Valbar	-

Definitioner

En Användarorganisation, Tjänsteleverantör, Sambiombud eller Underleverantör som innehar en av Sambi aktuell och godkänd Tillitsgranskning benäms i detta dokument **Betrodd part**. Andra termer av speciell betydelse för Tillitsramverket finns definierade i Bilaga 1 – Definitioner.

A. Generella krav

Övergripande krav på verksamheten

A.1 Betrodd Part som inte är ett offentligt organ ska drivas som registrerad juridisk person samt teckna och vidmakthålla för verksamheten erforderliga försäkringar.

A.2 Betrodd Part ska ha en etablerad verksamhet, vara fullt operationell i alla delar som berörs i detta dokument.

Säkerhetsarbete

A.3 Betrodd Part ska för den funktion som medlemskapet avser ha infört ett strukturerat säkerhetsarbete anpassat efter risker och säkerhetsbehov, bestående av:

(a) En **riskanalys** avseende funktionen. Denna ska ta hänsyn till skyddsvärde, befintliga skyddsåtgärder och legala krav. Riskanalysen ska omfatta analys av hot och sårbarheter, samt sannolikhet och konsekvens (skada) på Användare, den egna organisationen, andra Medlemmar och Federationsoperatören.
(b) Ett **ledningssystem för informationssäkerhet** för funktionen baserat på ISO/IEC 27001 eller motsvarande. Säkerhetsåtgärderna ska hantera riskerna enligt riskanalysen för funktionen.
(c) Genomförd **internrevision** av införandet och efterlevnaden av säkerhetsregelverket för funktionen.

Riskanalys och internrevision ska genomföras årligen och leda till en förbättringsplan innehållande rekommenderade säkerhetsåtgärder.

A.4 Betrodd Part ska tillhandahålla dokumentation över genomförd riskanalys, ledningssystemet för informationssäkerhet samt genomförd internrevision av efterlevnaden och införandet av säkerhetsregelverket, inklusive aktuell förbättringsplan, avseende funktionen.

A.5 Medlem ska inrätta en process för incidenthantering som innefattar vidarerapportering till Federationsoperatören i enlighet med de av Federationsoperatören angivna instruktionerna.

Granskning och uppföljning

A.6 Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs på Betrodd Part ska under en treårsperiod vara föremål för internrevision, utförd av oberoende kontrollfunktion.

Sambi granskningsgrupp ska genomföra en Tillitsgranskning vid ansökan och därefter minst vart tredje år enligt bilaga 4 av Sambis Anslutningsavtal. Ett Sambiombud ska granskas årligen enligt Bilaga 5 av Sambiombudsavtalet.

Kryptografisk säkerhet

A.7 Betrodd Part ska skydda kryptografiskt nyckelmaterial, omfattande minst signeringsnycklar för:

a) metadata
b) identitetsintyg
c) kommunikation

Krav på nyckelhantering ges i Bilaga 2, Tekniska krav.

Ansvar för användning av Underleverantörer

A.8 Betrodd part som lägger ut utförande av funktion på Underleverantör är som huvudman ansvarig för Underleverantörens uppfyllande av kraven i Tillitsramverket, oavsett avtalsform, och ska redogöra för hur Underleverantören uppfyller kraven så som om det vore utfört av den Betrodde Parten själv. I denna redogörelse ska Betrodd Part bl.a. redovisa:

(a) hur Underleverantören uppfyller kraven i Tillitsramverket.
(b) vilka funktioner och kritiska processer som har lagts ut på Underleverantör och hur Betrodd Part säkerställer att Underleverantörens uppfyller kraven för dessa.
(c) de avtal som definierar vilka funktioner som har lagts ut, hur kraven uppfylls av Underleverantören samt hur uppföljningen utförs.

Handlingars bevarande

A.9 Betrodd Part ska, i tillämpliga delar, bevara:

(a) avtal,
(b) styrande dokument,
(c) handlingar som rör förändringar av uppgifter hänförliga till Användare, Attribut och Metadata, och
(d) övrig dokumentation som stöder efterlevnaden av de krav som ställs på denne, och som visar att de säkerhetskritiska processerna och kontrollerna fungerar.

A.10 Tiden för bevarande ska inte understiga tre år och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritets-synpunkt och har stöd i lag eller annan författning.

Information

A.11 Betrodd Part ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av funktionen till Användare, Tjänsteleverantörer och andra som kan komma att förlita sig på denne.

A.12 Betrodd Part ska till Federationsoperatören tillhandahålla en Tillitsdeklaration som beskriver hur Betrodd Part uppfyller Tillitsramverket. Dokumentet ska följa av Federationsoperatören angivet format. Till denna ska bifogas efterfrågade dokument enligt detta tillitsramverk.

A.13 Betrodd Part ska på begäran av Federationsoperatören lämna uppgifter om hur verksamheten ägs och styrs.

A.14 Betrodd Part ska på ett tydligt sätt informera sina Användare och Federationsoperatören om villkor för funktionen vid nyteckning eller ändring av funktionen. Betrodd Part ska informera Federationsoperatören även vid ändringar av kontaktpersoner, federationsgemensamma metadata och attribut.

A.15 En Betrodd Part som upphör med sin verksamhet ska informera berörda Användare, Betrodda Parter och Federationsoperatören. Den Betrodda Parten ska hålla arkiverat material tillgängligt i enlighet med A.10 och A.11.

B. E-legitimationsutfärdare

B.1 E-legitimationsutfärdare ska vara godkänd av E-legitimationsnämnden som Utfärdare av Svensk e-legitimation på tillitsnivå 3 i enlighet med E-legitimationsnämndens tillitsramverk.

C. Attribututgivare

C.1 Informationsinnehållet i Attribut ska vara korrekt, aktuellt samt verifierat mot ursprungskällan.

C.2 Förändringar av informationsinnehållet i Attribut ska gå att spåra avseende tidpunkt för förändring och vem som utfört förändringen.

D. Identitetsintygsutgivare

D.1 Betrodd Part som tillhandahåller tjänst för utgivning av Identitetsintyg ska se till att denna tjänst har god tillgänglighet och att utlämnande av Identitetsintyg föregås av en tillförlitlig kontroll av att den angivna Användarens Elektroniska identitet och Attribut är giltiga.

D.2 Lämnade Identitetsintyg ska vara giltiga endast så länge som det krävs för att Användaren ska få tillgång till den efterfrågade E-tjänsten.

D.3 Identitetsintyg ska skyddas så att informationen endast är läsbar för den mottagande Tjänsteleverantören och att denne kan kontrollera att mottagna intyg är äkta.

D.4 Identifierade Användares anslutningar mot intygsutgivningstjänsten ska tidsbegränsas, varefter en ny identifiering av Användaren ska ske i enlighet med D.1.

E. Tjänsteleverantör

E.1 Tjänsteleverantör ska ha en dokumenterad rutin för att publicera aktuella Attribut och Tillitsnivåer som används för Tjänstens behörighetskontroll.

E.2 Tjänsteleverantör ska skydda Användares identitet och tillhörande Attribut.

E.3 Tjänsteleverantör ska informera Användare om informationen sprids eller används på annat sätt än för behörighetsstyrning.

F. Sambiombud

Övergripande krav på verksamheten

F.1 Sambiombud ska ha förmåga att bära risken för skadeståndsskyldighet samt förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst 1 år.

Tillitsgranskning av anslutna Användarorganisationer

F.2 Sambiombudet ska ha väl dokumenterade rutiner för att säkerställa att anslutna Användarorganisationer uppfyller Tillitsramverket, samt att aktuella Tillitsdeklarationer finns för samtliga Användarorganisationer. Dessa rutiner skall minst omfatta kraven i ”Bilaga 5, Föreskrifter för Sambiombud”, till Sambiombudsavtalet. Sambiombudet ska kunna visa att dessa rutiner tillämpas och efterlevs.

Hänsyn ska tas till att Användarorganisationen utnyttjar Sambiombudets tjänster för E-legitimationsutfärdande, attributhantering och intygsutgivning och därmed följande minskning av de återstående riskerna för Användarorganisationen.

Om Användarorganisationen för sin kravuppfyllnad använder ytterligare riktlinjer utfärdade av Sambiombudet skall denne säkerställa att dessa följs och uppfylls.

Incidenthantering

F.3 Sambiombudet ska ha väl dokumenterade rutiner för hantering av incidenter i den egna verksamheten och hos sina Användarorganisationer. Dessa ska minst omfatta att:

- informera Federationsoperatören om det inträffade,
- vidta åtgärder för att återställa förtroende, och
- bistå Medlemmen i dess arbete att återskapa förtroendet för Elektroniska identiteter och Attribut i Sambi.

Revisionshistorik			
Version	**Datum**	**Författare**	**Kommentar**
1.0	2013-09-23	Staffan Hagnell	Första utgåva
1.1	2014-11-04	Staffan Hagnell	Ändringar enligt arbetsgruppens förslag
1.2	2014-11-26	Staffan Hagnell	Sista stycket under ”Allmänt” tillagt
1.3	2015-09-17	Staffan Hagnell	Ändringar enligt remissammanställningen och styrgruppens beslut
2.0	2017-10-06	Staffan Hagnell	Revidering av Tillitsramverket inför införandet av Sambiombud och synpunkter inkomna från remissen 2017-08-17.
2.01	2017-10-10	Staffan Hagnell	Ändera Funktion till funktion, då detta inte är en definerad term.
2.0.2	2018-04-04	Staffan Hagnell	Förtydliganden efter den första granskningen av ett Sambiombud. Ändra texten ”tjänst och dess funktioner” till ”funktioner”