Tillitsramverk för pilot Sambiombud begränsad

Dokumentet utgår från hypotes avseende koncept för IdP-centrisk anslutning till Internetstiftelsens federationer. Konceptet beskrivs i Pilot av nytt anslutningskoncept för användarorganisationer i Sambi - Internetstiftelsens Federationer - Federation Wiki.

Tillitsramverk för pilot Begränsad anslutning till Sambi bygger på Sambis tillitsramverk 2.1 Sambi-Bilaga-3-Tillitsramverk-v2.1.pdf

Sambiombud begränsad granskas utifrån detta tillitsramverk.

Anslutningsformen är begränsad till personlig identifierare och organisatorisk tillhörighet.

Detta tillitsramverk för piloten kommer införlivas i befintligt aktuellt tillitsramverk för Sambi.

Ändringslogg

Version	Ändring
Första version	Dokumentet skapat utan versionsnummer
0.2	Lagt till avsnitt ”F”
0.3	A.7C Ändrat ”Organisation” till användares organisatoriska tillhörighet C Formulerat avgränsning av attribut. D.1 lagt till “organisatoriska tillhörighet” D.2 Ändrat tillitsnivå och ändrat hänvisning till Sambi och inte DIGG F.2 tagit bort hela stycket och lagt till nytt. Tagit bort hänvisning till föreskrifter
0.4	Skrivit om inledning. Skillnad mot orginal: inledning olika, E-kravstycket borttaget Lagt till term: Sambiombud begränsad F – tagit bort rubriker. Ändrat medlem till användarorgansation.

INTERNET STIFTELSEN

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 och vara fullt operationell i alla delar som berörs i detta dokument.

Säkerhetsarbete

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

(a) Riskanalys avseende den Funktion som Tillitsdeklarationen avser. 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. Riskanalysen ska genomföras årligen och leda till en förbättringsplan innehållande rekommenderade säkerhetsåtgärder.

(b) Ett ledningssystem för informationssäkerhet (LIS) för Funktionen baserat på ISO/IEC 27001. Säkerhetsåtgärderna ska hantera riskerna enligt riskanalysen för Funktionen.

(c) Genomförd internrevision av införandet och efterlevnaden av ledningssystemet för informationssäkerhet (b). Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs i detta Tillitsramverk ska minst en gång per treårsperiod vara föremål för internrevision, utförd av en till Funktionen oberoende kontrollfunktion.

A.4 Betrodd Part har inrättat en process för incidenthantering i enlighet med de av Federationsoperatören angivna instruktionerna.

Kryptografisk säkerhet

A.5 Betrodd Part ska skydda Funktionen mot obehörig åtkomst.

Ansvar för användning av Underleverantörer

A.6 Betrodd Part som, i delar eller helhet, lägger ut utförande av Funktionen på Underleverantör är, oavsett avtalsform, ansvarig för Underleverantörens uppfyllande av kraven i Tillitsramverket och ska på begäran informera om vilka delar av Funktionen som är utlagda.

Handlingars bevarande

A.7 Betrodd Part ska, i tillämpliga delar, bevara:

(a) avtal,

(b) styrande dokument,

(c) handlingar som rör förändringar av uppgifter hänförliga till Användare, användares organisatoriska tillhörighet 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.8 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.

Informationsplikt

A.9 Betrodd Part ska informera Federationsoperatören vid incidenter, samt vid ändringar av kontaktpersoner och federationsgemensamma metadata.

Krav på Sambiombud begränsad

B. E-legitimationsutfärdare

B.1 E-legitimationsutfärdare ska

(a) vara godkänd av Myndigheten för digital förvaltning (DIGG) i enlighet med Tillitsramverket för Svensk e-legitimation eller

(b) vara anmäld av annat land enligt EU:s eIDAS-förordning.

C. Attribututgivare

Tillåtna attribut är begränsat till användares identitet och organisatoriska tillhörighet.

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 organisatoriska tillhörighet är giltiga.

D.2 Tillitsnivå för autentisering ska anges i identitetsintyget enligt Sambis tillitsnivåer.

D.3 Lämnade Identitetsintyg ska vara giltiga endast så länge som det krävs för att Användaren ska få tillgång till den efterfrågade E-tjänsten.

D.4 Informationen i identitetsintyg ska skyddas mot obehörig åtkomst.

D.5 Identitetsintyg ska utfärdas på ett sådant sätt så att Tjänsteleverantören kan kontrollera att mottagna intyg är äkta.

D.6 Identifierad Användares inloggningssession mot intygsutgivningstjänsten ska tidsbegränsas, varefter en ny identifiering av Användaren ska ske i enlighet med D.1.

F. Övergripande krav på verksamheten

F.1 Sambiombud begränsad ska ha erforderliga försäkringar samt förfoga över tillräckliga

ekonomiska medel för att kunna bedriva verksamheten vidare i minst 1 år

F.2 Sambiombud begränsad ska ha väl dokumenterade rutiner för att säkerställa att anslutna Användarorganisationer har god kontroll av egen personal, inkluderande rutiner för avslut av anställning eller tillhörighet, samt regelbunden, minst kvartalsvis, granskning av register.

Incidenthantering

F.3 Sambiombud begränsad 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 Användarorganisationen i dess arbete att återskapa förtroendet för Användarorganisationens Elektroniska identiteter och Attribut