BILAGA 3 – Tillitsramverk

Version: 2.1

Innehåll

Inledning

Syftet med detta tillitsramverk är att skapa tillit mellan medlemmar avseende användares elektroniska identiteter och behörighetsstyrande attribut, samt att skydda användares personliga integritet. Tillitsramverket specificerar de säkerhetskrav som ställs på medlemmar och andra betrodda parter.

Tillitsramverkets begrepp finns definierade i Bilaga 1 – Definitioner.

Läs tillitsramverket så här

Tillitsramverkets krav är uppdelade i sex avsnitt. Avsnitten (kolumnerna) är tillämpliga för rollerna (raderna) enligt tabellen nedan.

		Användar-organisation	Användar-organisation	Användar-organisation		
	A. Generella krav	B. E-legitimations-utfärdare	C. Attributs-utgivare	D. Identitets-intygs-utgivare	E. Tjänste-leverantör	F. 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	-

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, 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.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 användarorganisationer

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

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 Tillitsnivå ska anges i identitetsintyget. Hur Tillitsnivå anges och tolkas ska följa specifikation från Myndigheten för digital förvaltning (DIGG).

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.

Krav på övriga roller

E. Tjänsteleverantör

E.1 Tjänsteleverantör ska ha en dokumenterad rutin för publicering av 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 Sambiombudet ska ha erforderliga försäkringar samt förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten vidare 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 aktuella Tillitsdeklarationer för samtliga Användarorganisationer. Dessa rutiner ska minst omfatta kraven i ”Bilaga 5, Föreskrifter för Sambiombud”, till Sambiombudsavtalet. Sambiombudet ska kunna visa att dessa rutiner tillämpas och efterlevs.

Om Användarorganisationen för sin kravuppfyllnad använder ytterligare riktlinjer utfärdade av Sambiombudet ska 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 Medlemmens Elektroniska identiteter och Attribut.

Revisionshistorik

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	Ändrade Funktion till funktion, då detta inte är en definierad 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”
2.1	2018-11-28	Eva Sartorius	Förenklat texter. Ändrat ”funktion” till ”Funktion” efter tillägg i bilaga Definitioner. Ändrat skrivning om e-legitimationsutfärdare (B.1). Lagt till punkt om att DIGG är normerande för tillitsnivåer (D.2). Skrivmässigt delat upp punkten om skydd mot obehörig åtkomst och åtgärder för äkthet i två (D.4 och D.5).