INTERNET STIFTELSEN

Document	Tillitsramverk för Svenska federationer
Identifier	https://wiki.federationer.internetstiftelsen.se/x/XgGOC
Version	1.0
Last modified	2026-02-11
Pages	16
Status	Fastställd
License	Creative Commons BY-SA 3.0

Tillitsramverk för Svenska federationer

Utgåva 1.

Innehållsförteckning

1. Inledning

Syftet med detta tillitsramverk är att skapa förutsättningar för tillit mellan federationsmedlemmar avseende hantering och förmedling av elektroniska intyg som ligger till grund för åtkomst för användare och tekniska aktörer (såsom API:er, system och maskinella entiteter) på ett integritetsskyddande sätt.

Tillitsramverket specificerar de krav som ska uppfyllas av anslutna medlemmar och andra betrodda parter. Kraven omfattar informationssäkerhet, tekniska- och organisatoriska skyddsåtgärder, intern styrning och kontroll, hantering av identiteter och attribut samt incidenthantering.

Tillitsramverket gäller för samtliga federationsparter som omfattas av en federationspolicy som tillämpar kraven i detta tillitsramverk.

2. Nivåer av tillit

Tillitsramverket definierar fyra nivåer av tillit (T1–T4). Nivåerna syftar till att tillhandahålla en flexibel och anpassningsbar modell för tillit och kan ses som en mognadstrappa, där varje nivå representerar successivt högre krav på förmåga, säkerhet och tillit.

Varje steg i mognadstrappan innebär en ökad grad av ansträngning och uppfyllelse av krav, vilket möjliggör för organisationer att stegvis utveckla sin förmåga att uppnå och upprätthålla tillitsramverkets högsta tillitsnivå.

I denna utgåva av tillitsramverket är tillitsnivå T1 specificerad. Övriga tillitsnivåer (T2–T4) kommer att utvecklas successivt i samverkan med berörda myndigheter och andra samhällsaktörer, inom ramen för utvecklingen av Sveriges digitala infrastruktur för samordnad identitets- och behörighetshantering.

3. Roller och ansvar

3.1 Användarorganisation

Användarorganisationen ansvarar för identifiering och livscykelhantering av sina användare och tekniska aktörer.

Användarorganisationen får, i enlighet med federationens tekniska profil, antingen ställa ut elektroniska intyg eller använda andra godkända autentiseringsmekanismer i syfte att möjliggöra åtkomst till digitala resurser, tjänster och information.

3.2 Tjänsteleverantör

Tjänsteleverantören tillhandahåller digitala resurser, tjänster eller information och som med stöd av federationens tillitsramverk och tillhörande federationspolicy fattar åtkomstbeslut baserade på elektroniska intyg eller andra federationsgodkända auktorisationsmekanismer.

Beroende på federationens tekniska profil kan detta innebära:

a) verifiering och tolkning av elektroniska intyg, eller

b) verifiering av tekniska aktörers identitet genom kryptografiska mekanismer såsom ömsesidig TLS eller motsvarande federationsprofil.

3.3 Federationsoperatör

Federationsoperatören ansvarar för att föra en förteckning över erkända tillitsramverk samt alla betrodda parter som hanteras av federationsoperatören.

Federationsoperatören ansvarar för att federationerna fungerar såväl tekniskt som administrativt. Detta inkluderar att:

a) hålla metadata aktuellt och korrekt,
b) hålla medlemsregistret uppdaterat,
c) efterlevnad av tillitskrav kontrolleras enligt gällande policy för varje federation.

Federationsoperatören ansvarar för att tillhandahålla de gemensamma infrastrukturella federationstjänsterna. Det omfattar bland annat metadatahantering, testmiljöer och testverktyg samt gemensamma specifikationer.

Federationsoperatören förvaltar och utvecklar tillitsramverket samt verkställer de federationspolicyer som utformas i samverkan med de sammanslutningar av organisationer som vill samverka digitalt i federation. Federationsoperatören agerar inom de ramar och avgränsningar som varje policy anger.

Federationsoperatören är mottagare av incidentrapporter och annan information från medlemmar och andra betrodda parter samt ansvarar för att samordna återställande av tillit vid incidenter.

Federationsoperatören ska kommunicera förändringar i ramverket, specifikationer och federationspolicy till alla berörda aktörer på ett tydligt och spårbart sätt.

3.4 Övriga betrodda parter

En federation kan nyttja andra betrodda parter som genomgått tillitsgranskning och godkänts enligt ett särskilt tillitsramverk för en specifik funktion eller ett visst

ansvarsområde. Syftet är att stärka tilliten till en medlem och dess informationssäkerhetsarbete genom erkända tredjepartsgranskningar och certifieringar.

Exempel på sådana betrodda parter är:

- Attributtjänster som hanterar behörighetsstyrande uppgifter (t ex HSA eller motsvarande system som lever upp till kraven för attributhantering).
- E-legitimationsutfärdare som godkänts enligt *Tillitsramverket för Svensk e-legitimation*.
- Utländska e-legitimationsutfärdare som är anmälda enligt EU-förordningen eIDAS och godkända av annat medlemsland.

En sådan betrodd part ska vara tillitsgranskad och godkänd enligt ett etablerat och offentligt tillgängligt tillitsramverk vars syfte och krav motsvarar, eller överstiger, de krav som ställs i detta tillitsramverk. En förteckning över erkända tillitsramverk och godkända betrodda parter förs av federationsoperatören och hålls tillgänglig för samtliga betrodda parter.

Följande tillitsramverk erkänns i nuläget:

- Tillitsramverk för Svenska federationer (detta dokument),
- Tillitsramverket för Svensk e-legitimation (Digg – Myndigheten för digital förvaltning),
- eIDAS-förordningen (EU 910/2014) för gränsöverskridande e-legitimering.

4. Funktioner

Följande funktioner omfattas av detta tillitsramverk och redovisas i tabellen nedan.

Funktion	Beskrivning
Attributhantering	Processer och tekniska lösningar för att administrera (definiera, tilldela, ändra och avlägsna) attribut om sina användare och tekniska aktörer.
Elektronisk identitet	Processen och de tekniska lösningarna för att skapa, hantera, verifiera och avregistrera elektroniska identiteter för användare och tekniska aktörer.
E-tjänst	Digitala tjänst som distribueras genom ett grafiskt användargränssnitt. E-tjänster kan vara utformade för både individer och organisationer och omfattar ett brett spektrum av funktioner.

Funktion	Beskrivning
Intygsutgivning	Processen och de tekniska lösningarna för utgivning och förmedling av elektroniska intyg till betrodda Tjänsteleverantörer.
Klient	Teknisk funktion i exempelvis ett verksamhetssystem eller en applikation, som anropar en server för att få åtkomst till digitala resurser, tjänster eller information.
Server	Tekniskt gränssnitt, exempelvis API eller motsvarande teknisk lösning, som tillhandahåller digitala resurser, tjänster eller information för system-till-system-kommunikation.

5. Förhållande till standarder och regelverk

Detta tillitsramverk är teknikneutralt. Det innebär att kraven inte är skrivna för ett särskilt tekniskt protokoll eller standard (såsom SAML, OIDC, mTLS eller andra), utan gäller oavsett underliggande lösning. Detta möjliggör långsiktig användning, flexibilitet och formar en grund som kan fungera även när tekniska standarder förändras eller byts ut.

Utformning av tillitsramverket är harmoniserad med etablerade standarder och regelverk för att underlätta efterlevnad och interoperabilitet:

- ISO/IEC 27001/27002 för ledningssystem och säkerhetsåtgärder inom informationssäkerhet.
- Tillitsramverk för *Svensk e-legitimation*, särskilt avseende identitetskontroll, tillitsnivåer och intygsutgivning.
- EU-förordningen *eIDAS*, där den är tillämplig på gränsöverskridande e-legitimering i Europa.

Tillitsramverket ska därmed kunna användas både som ett internt styrande ramverk för federationsinfrastrukturens medlemmar och som ett komplement till andra nationella och internationella regelverk.

6. Tillitsramverkets utformning

Tillitsramverket är indelat i ett antal kravområden som tillsammans beskriver de organisatoriska, administrativa och tekniska förutsättningar som krävs för att etablera och upprätthålla tillit i federationsinfrastrukturen.

Kravområdena är strukturerade enligt följande:

K1. **Organisation och styrning**: krav på juridisk person, verksamhetsförmåga, resurser och ansvarsfördelning.
K2. **Informationssäkerhet**: krav på ledningssystem, riskhantering, incidenthantering och säkerhetsåtgärder.
K3. **Internkontroll och revision**: krav på uppföljning av efterlevnad, dokumentation och intern kontrollfunktion.
K4. **Teknisk säkerhet**: krav på spårbarhet, autentisering, kryptering, logghantering och tekniska skyddsåtgärder.
K5. **Identifiering**: krav på fastställande och livscykelhantering av digitala identiteter.
K6. **Attributhantering**: krav på kvalitet, aktualitet, verifiering, spårbarhet och skydd av behörighetsstyrande attribut.
K7. **Intygsutgivning**: krav på processer, kontroller och tekniska mekanismer för att utfärda tillförlitliga identitets- och åtkomstintyg.
K8. **Tolkning och användning av intyg**: krav på hur mottagare verifierar, tolkar och använder intyg i behörighetsstyrning.
K9. **Incidenthantering**: krav på upptäckt, rapportering av incidenter, och åtgärder för återställande av tillit.
K10. **Ansvar för underleverantörer**: krav på avtal, uppföljning och kontroll av utlagda funktioner.
K11. **Informationsplikt**: krav på att föra löpande och korrekt information vidare till federationsoperatören.

Kravområdena är utformade för att vara teknikneutrala och utgör ett gemensamt ramverk för olika samverkanskontexter. En samverkanskontext kan i sin federationspolicy ange hur tillitsramverkets krav tillämpas i praktiken.

7. Tillitskrav

7.1 Organisation och styrning

Nivå	Referens	Krav
T1	**K1.1**	Betrodd part som inte är ett offentligt organ ska drivas som registrerad juridisk person samt teckna och vidmakthålla för verksamheten erforderliga försäkringar.
T1	**K1.2**	Betrodd part ska ha en etablerad verksamhet och vara fullt operationell i alla delar som berörs i detta tillitsramverk.
T1	**K1.3**	Verksamheten ska ha tillräckliga resurser och kompetens för att uppfylla sina åtaganden gentemot federationen.

7.2 Informationssäkerhet

Nivå	Referens	Krav
T1	**K2.1**	Betrodd part ska bedriva ett systematiskt informations-säkerhetsarbete som omfattar de delar av verksamheten som berör federationens funktioner. Arbetet ska omfatta styrning, riskhantering, incidenthantering, kontinuerlig förbättring samt organisatoriska och tekniska säkerhetsåtgärder. Säkerhetsåtgärderna ska anpassas efter identifierade risker, verksamhetens skyddsvärden och gällande lagstiftning. Rekommenderad utgångspunkt är ISO/IEC 27001 som ramverk för ledningssystem samt ISO/IEC 27002 som vägledning för säkerhetsåtgärder.

7.3 Internkontroll och revision

Nivå	Referens	Krav
T1	**K3.1**	Betrodd part ska säkerställa att efterlevnaden av tillitsramverkets krav följs upp genom dokumenterade rutiner för internkontroll.
T1	**K3.2**	Dokumentation som styrker kravuppfyllnad ska bevaras så länge det krävs för uppföljning, dock minst tre år. Material ska kunna tillhandahållas i läsbar form under hela denna tid, såvida inte gallringskrav enligt lag eller annan författning motiverar annat.

7.4 Teknisk säkerhet

Nivå	Referens	Krav
T I	**K4.1**	Kryptografiska nycklar som används av tekniska aktörer, e-tjänster och tekniska lösningar för intygsutgivning ska genereras med kryptografiskt säkra metoder och i enlighet med federationsoperatörens aktuella rekommendationer avseende algoritmer och nyckellängder.
T I	**K4.2**	Kryptografiska nycklar ska hanteras genom dokumenterade rutiner som omfattar lagring, användning, rotation och avveckling av kryptografiskt material. Hanteringen ska säkerställa nycklarnas konfidentialitet, integritet och spårbarhet under hela livscykeln.
T I	**K4.3**	Privata nycklar ska skyddas mot obehörig åtkomst, kopiering, manipulation och förlust genom lämpliga tekniska och organisatoriska skyddsåtgärder.
T I	**K4.4**	Hårdvarubaserat nyckelskydd eller motsvarande säkerhetsnivå bör användas där riskbilden motiverar det.
T I	**K4.5**	Betrodd part ska säkerställa spårbarhet vid all logisk- och fysisk åtkomst till känsliga IT-system och utrymmen (t ex serverrum, nätverksskåp, arkiv för säkerhetskopior och mediavalv). Åtkomst ska: a) vara begränsad till behörig personal genom dokumenterad tillträdeskontroll och regelbunden behörighetsöversyn. b) kunna härledas på individnivå och identifieringen av individen ska ske på ett betryggande och säkert sätt.
T I	**K4.6**	Elektronisk kommunikation som direkt eller indirekt berör känsliga uppgifter ska skyddas mot manipulation och obehörig insyn genom starka kryptografiska metoder.
T I	**K4.7**	Loggar ska förvaras säkert, skyddas mot manipulation och bevaras minst tre år eller enligt gällande lagkrav.

Nivå	Referens	Krav
T1	**K4.8**	Informationsbärande media (inklusive säkerhetskopior, bärbara lagringsenheter och pappersmedia) ska förvaras och hanteras på ett säkert sätt under hela livscykeln.
T1	**K4.9**	Tillträde till skyddade utrymmen ska kontinuerligt övervakas och loggas.
T1	**K4.10**	Tekniska säkerhetsåtgärder ska fortlöpande anpassas till identifierade risker, hotbild och förändringar i omvärlden.

7.5 Identifiering

7.5.1 Identifiering av användare

Nivå	Referens	Krav
T1	**K5.1.1**	Betrodd part ska fastställa användarens digitala identitet innan ett användarkonto eller motsvarande elektronisk identitetshandling utfärdas.
T1	**K5.1.2**	Identifiering ska ske på ett sätt som är spårbart, dokumenterat och tillförlitligt över tid.
T1	**K5.1.3**	Identiteter ska förvaltas under hela livscykeln och avregistreras när relationen till användaren upphör.
T1	**K5.1.4**	Betrodd part kan använda kvalificerade digitala identiteter, såsom svenska e-legitimationer eller erkända e-legitimationer inom ramen för eIDAS-förordningen. E-legitimationens tillitsnivå fastställer nivån för elektronisk identifiering.

Nivå	Referens	Krav
T1	**K5.1.5**	Betrodd part kan själv utfärda digitala identiteter på tre nivåer: **al1**: Minimal eller ingen verifiering av den fysiska identiteten vid utfärdande av digital identitet. Identitetsbeteckningen baseras ofta på interna uppgifter (exempelvis ett användarnamn). Autentisering kan vara svag och lätt att kompromettera. **al2**: Den digitala identiteten är kopplad till en grundidentifiering, exempelvis genom skol- eller HR-system (användarnamn kopplat till personnummer). Identifiering kan ske vid inskrivning eller anställning. Det finns inget krav på kontinuerlig verifiering. Identifieringen kan inkludera stark autentisering. **al3**: Identiteten är verifierad mot en betrodd identitetshandling eller e-legitimation. Rutiner för identifiering, registrering och underhåll är väldefinierade, dokumenterade och spårbara. Flerfaktorsautentisering krävs och autentiseringslösningen ska ge spårbarhet på systemnivå.
T1	**K5.1.6**	Betrodd part ska tillämpa flerfaktorautentisering där kraven i tillitsramverket förutsätter det, exempelvis vid identitetsutfärdande i egen regi på nivå al3. Godkänd flerfaktorsautentisering ska kombinera minst två av följande faktorkategorier: a) Kunskap, det vill säga något användaren vet (t ex lösenord eller PIN). b) Ägande, det vill säga något användaren har (t ex elektronisk säkerhetsnyckel, autentiseringsapp, smartkort). c) Inneboende egenskaper, det vill säga något användaren är (t ex biometri). Användning av kod i SMS eller e-postmeddelande är inte godkänd autentiseringsfaktor.

7.5.2 Identifiering av tekniska aktörer

Nivå	Referens	Krav
T I	**K5.2.1**	Tekniska aktörer ska tilldelas en entydigt identifierbar digital identitet som ska: a) vara unik inom federationen, b) kunna kopplas till en ansvarig betrodd part, c) omfattas av dokumenterad livscykelhantering, d) avregistreras eller spärras skyndsamt när den inte längre används eller när ansvarsförhållandet upphör.
T I	**K5.2.2**	Autentisering av tekniska aktörer ska ske med kryptografiskt starka metoder baserade på asymmetriska nycklar eller motsvarande säkerhetsmekanismer, i enlighet med de tekniska profiler och specifikationer som federationsoperatören fastställer.

7.6 Attributhantering

Nivå	Referens	Krav
T I	**K6.1**	Attribut som tillhandahålls ska vara korrekta, aktuella och verifierade mot en tillförlitlig källa.
T I	**K6.2**	Registrering och uppdatering av attribut, både i ursprungskällor och i temporära mellanlager, ska dokumenteras och vara spårbar med avseende tidpunkt, innehåll och ansvarig person eller process.
T I	**K6.3**	Attribut ska endast användas för de syften som är definierade i federationen och ska skyddas mot obehörig åtkomst och otillbörlig spridning.
T I	**K6.4**	Avregistrering eller borttagning av attribut ska ske skyndsamt när relationen till användaren upphör eller uppgiften inte längre är relevant.

7.7 Intygsutgivning

Nivå	Referens	Krav
T1	**K7.1**	Betrodd part ska säkerställa att tjänsten för intygsutgivning har god tillgänglighet och att intygsutgivning föregås av en tillförlitlig identifiering i enlighet med bestämmelserna i avsnitt *7.5 Identifiering*.
T1	**K7.2**	Intyg ska endast utfärdas om användarens identitet är fastställd och den elektroniska identitetshandlingen är giltig. Identitetens tillitsnivå bör anges i identitetsintyget. Fastställande av tillitsnivån ska ske i enlighet med bestämmelserna i avsnitt *7.5 Identifiering*.
T1	**K7.3**	Attribut i intyget ska vara korrekta, aktuella och motsvara vad som framgår av källsystem.
T1	**K7.4**	Utgivet intyg ska vara giltigt endast under den tid som krävs för att säkerställa åtkomst för användaren eller systemet till den aktuella digitala tjänsten (t ex e-tjänst, API).
T1	**K7.5**	Utgivaren ska skydda intyg mot manipulation och obehörig åtkomst samt möjliggöra för mottagande tjänsteleverantör att verifiera intygets äkthet och integritet.
T1	**K7.6**	Utgivaren bör med hänsyn till riskerna för missbruk av intygstjänsten, begränsa den tidsperiod inom vilken flera på varandra följande intyg kan ställas ut för en viss innehavare innan denne på nytt ska identifieras.
T1	**K7.7**	Intygsutgivning ska ske i enlighet med de tekniska och organisatoriska specifikationer som fastställs av federationsoperatören.

7.8 Tolkning och användning av intyg

Nivå	Referens	Krav
T1	**K8.1**	Mottagare av intyg ska endast tolka och använda intyg i enlighet med de tekniska och organisatoriska specifikationer som fastställs av federationsoperatören.
T1	**K8.2**	Mottagare av intyg ska säkerställa att mottaget intyg är äkta, oförändrat och utfärdat av en betrodd part inom federationen.

Nivå	Referens	Krav
T1	**K8.3**	Attribut och uppgifter i intyget får endast användas för behörighetsstyrning och åtkomstbeslut till den aktuella tjänsten.
T1	**K8.4**	Användarens identitet och information i intyget ska skyddas mot obehörig åtkomst och får inte användas för andra ändamål som är definierade inom federationen.

7.9 Incidenthantering

Nivå	Referens	Krav
T1	**K9.1**	Betrodd part ska ha en dokumenterad process för att upptäcka, rapportera, hantera och följa upp incidenter som påverkar federationens tillit, tillgänglighet eller informationssäkerhet.
T1	**K9.2**	Incidenthantering ska inkludera rutiner för att snabbt begränsa skada, återställa normal drift och vid behov kommunicera med berörda parter.
T1	**K9.3**	Betrodd part ska informera federationsoperatören om incidenter som kan påverka federationens tillit eller andra medlemmars verksamhet. Rapportering ska ske skyndsamt enligt federationsoperatörens instruktioner.
T1	**K9.4**	Slutsatser och lärdomar från incidenter ska dokumenteras och användas för att förbättra säkerhetsarbetet.

7.10 Ansvar för underleverantörer

Nivå	Referens	Krav
T1	**K10.1**	Betrodd part som helt eller delvis lägger ut en funktion på underleverantör ansvarar fortfarande fullt ut för att tillitsramverkets krav uppfylls.
T1	**K10.2**	Betrodd part ska ha dokumenterade avtal med underleverantörer som säkerställer att dessa följer relevanta krav i tillitsramverket.
T1	**K10.3**	Betrodd part ska på begäran kunna redovisa vilka delar av en funktion som utförs av underleverantör och vilka kontroller som finns på plats.

7.11 Informationsplikt

Nivå	Referens	Krav
TI	**KII.I**	Betrodd part ska informera federationsoperatören vid förändringar som påverkar federationens funktion eller tillit. Detta omfattar exempelvis ändringar av kontaktpersoner, tekniska konfigurationer, federationsmetadata eller annan information av betydelse för digital samverkan inom federationen.

8. Revisionshistorik

Version	Datum	Kommentar
1.0	2026-03-02	Utgåva 1.