

VI ♥ INTERNET



INTERNET ♥ STIFTELSEN

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.



Sambis anslutningsprocess

2021-10-06 | Robert Rhudin Sundin | Internetstiftelsen

Anslutningsprocess

Så här blir din organisation medlem i Sambi

Det finns två vägar att bli medlem:

1. med stöd av [Sambiombud](#)
2. på egen hand

Att bli medlem *på egen hand* innebär tre steg:

1. Skriva [avtal om tillitsgranskning](#)
2. Genomgå [tillitsgranskning](#)
3. Skriva [anslutningsavtal](#) om medlemskap i Sambi

<https://www.sambi.se/medlem-i-sambi/bli-medlem-i-sambi/>

Anslutningsprocess

Godkänd
tillitsgranskning

- Avtal om tillitsgranskning
- Tillitsdeklaration
- Granskning
- Beslut

Bli medlem i
Sambi

- Avtal om medlemskap

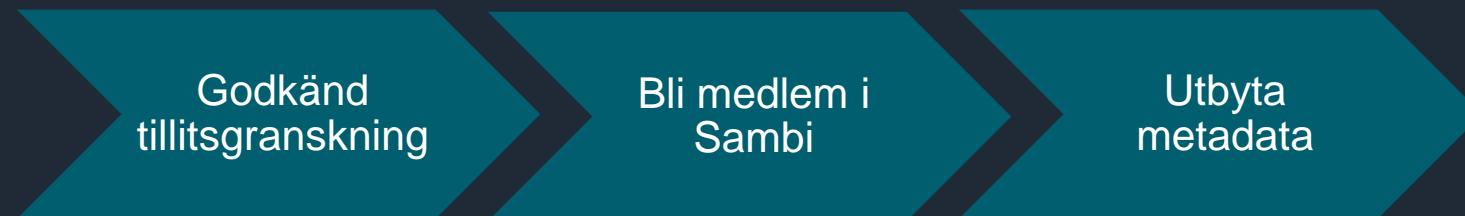
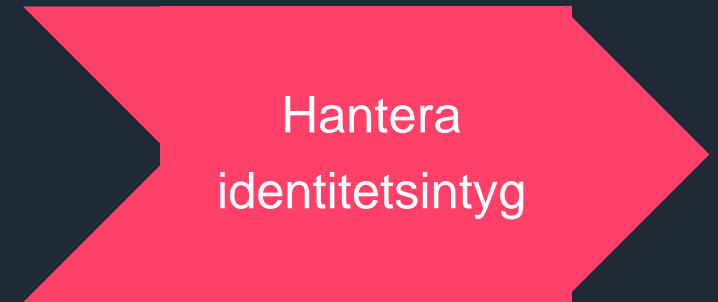
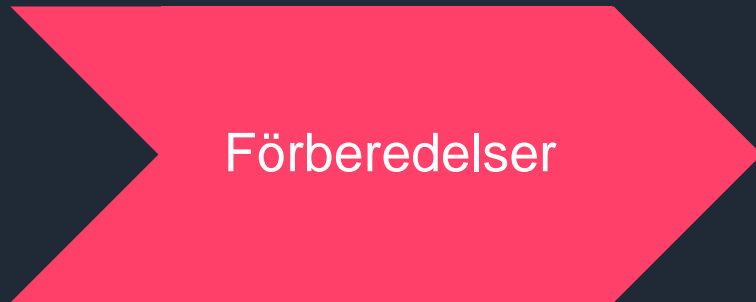
Utbyta
metadata

- Ansluta IdP/SP

Förberedelser och integrationer

- Teknik
- Ledningssystem för informationssäkerhet

- Integrationer



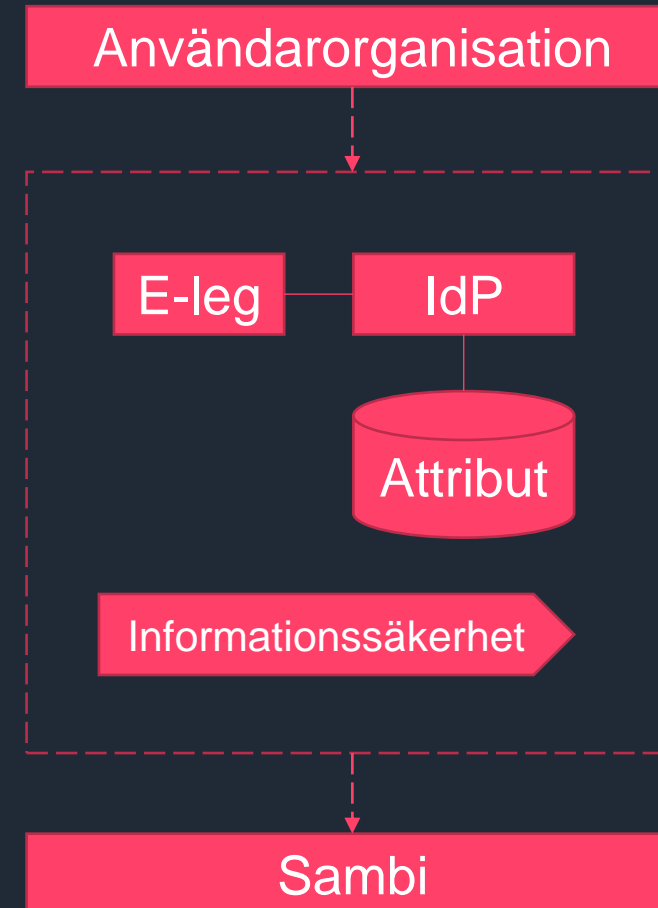
Alternativ för anslutning till Sambi

Anslutning	Användarorganisation	Tjänsteleverantör
Direktanslutning i egen regi	✓	✓
<i>Direktanslutning med betrodd part</i>	✓	(✓)
Via Sambiombud	✓	✗
Via Gruppföreträdare*	(✓)	✗

**Alternativet gruppföreträdare gäller enbart "små" organisationer*

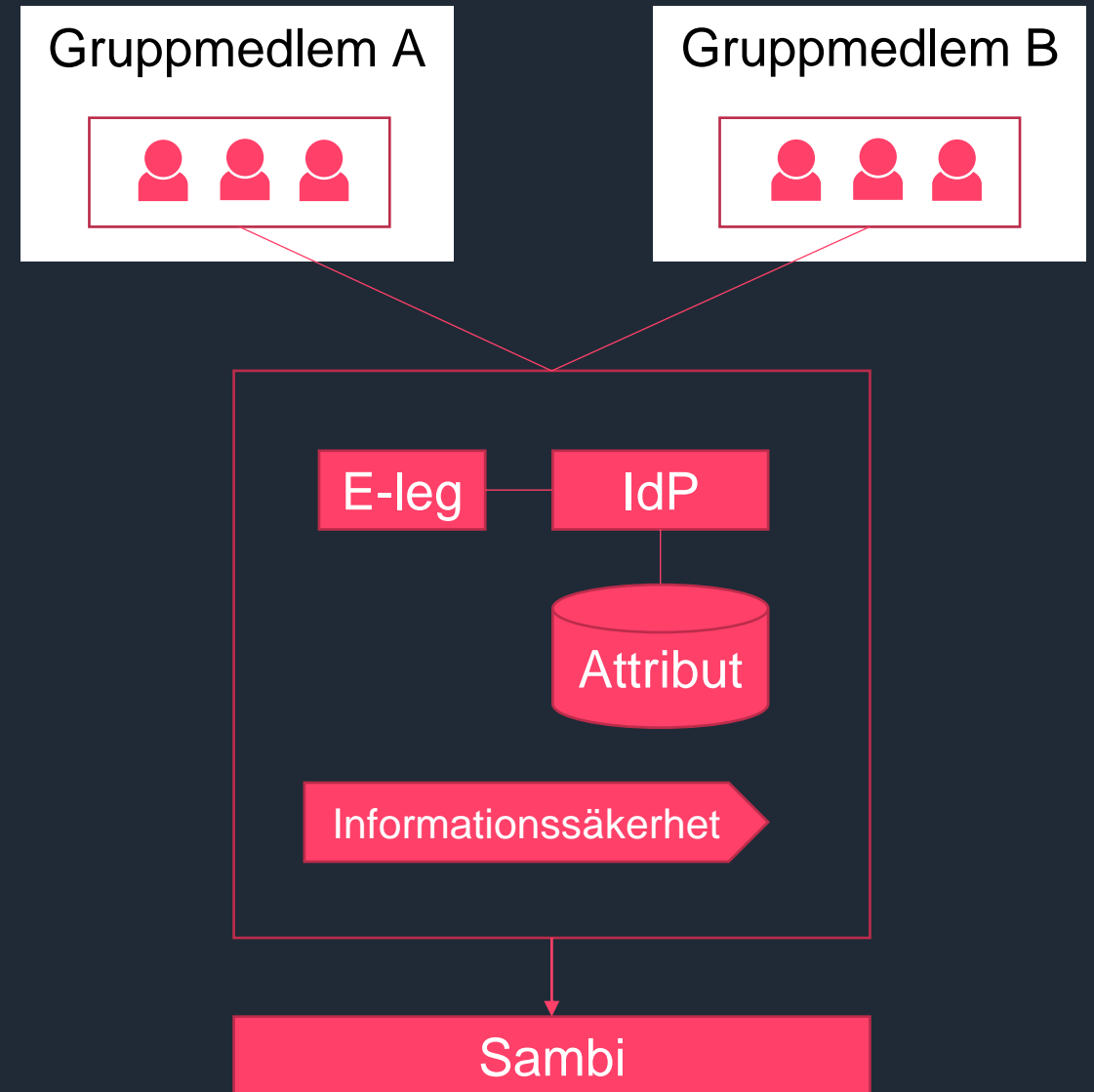
Sambiombud

- Sambiombudet ombesörjer anslutningen till federationen för medlemmar som väljer ombudslösningen
- Merparten av riskerna inom avgränsningen för Sambi faller ut på ombudet, vilket innebär att det LIS som behöver beskrivas av medlemmen blir relativt litet
- Hela hanteringen sker via ombudet



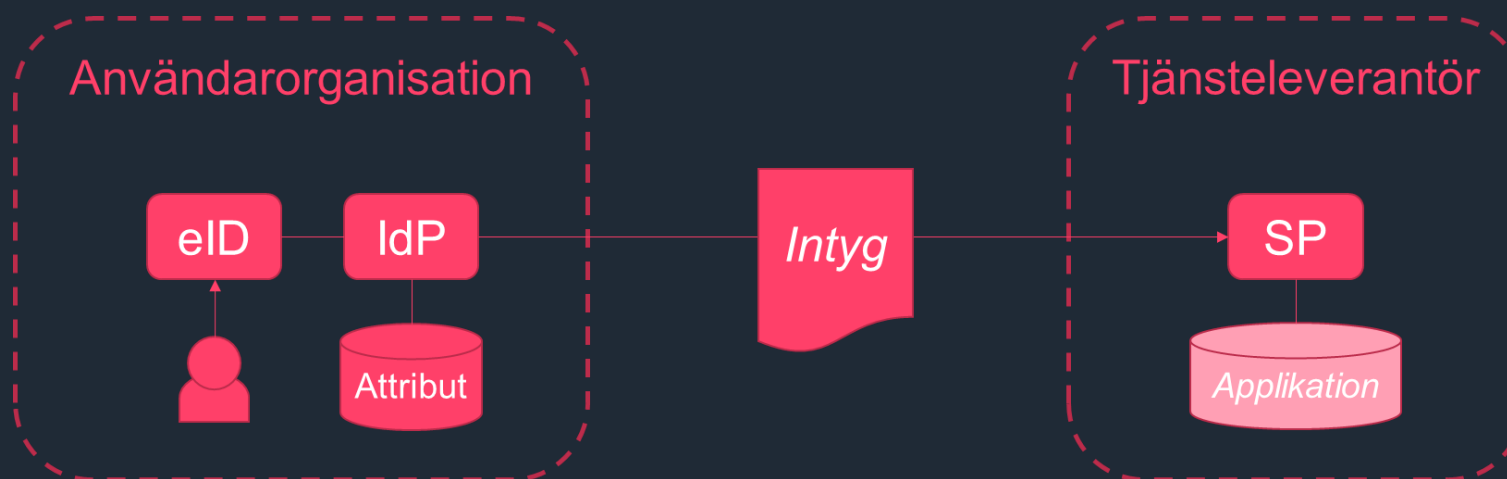
Gruppföreträdare

- Gruppföreträdaren ansluter som medlem till Sambi och tar ansvar för LIS till personal hos Gruppmedlem
- Gruppmedlemmen behöver inget LIS utan Gruppföreträdaren upprättar rutiner för personal hos Gruppmedlemmen
- Hela hanteringen sker via Gruppföreträdaren



Alternativens påverkan på LIS (AO)

Anslutning - användarorganisation	LIS	IdP	Attribututgivare	E-legitimationsutf.
Direktanslutning i egen regi*	Ja	Ja	Ja	Ja
Via Sambiombud	Begränsat	Sambiombud	Sambiombud	Sambiombud
Via Gruppföreträdare	Gruppföreträdare	Gruppföreträdare	Gruppföreträdare	Gruppföreträdare



Ledningssystemets omfattning (1/2)

Sambis tillitsramverk omfattar enbart de funktioner som nyttjas för identitets- och behörighetsstyrning inom ramen för Sambi

Tillitsgranskning

Funktion (2/2)

- från Sambis tillitsdeklarationsmall

Roller som ska granskas

Markera er roll eller era roller som denna Tillitsdeklaration avser.

Användarorganisation; deklarerar för avsnitt A, B, C och D

Underleverantör till Användarorganisation; deklarerar för avsnitt A och därefter avsnitt B, C eller D beroende på vad som levereras

Tjänsteleverantör; deklarerar för avsnitt A och E

Underleverantör till Tjänsteleverantör; deklarerar för avsnitt A och E

Sambiombud; deklarerar för avsnitt A, B, C, D och F

Gruppföreträdare; deklarerar för avsnitt A, B, C, D och E samt skickar med en bilaga om hur Bilaga 5 – Föreskrifter för Gruppföreträdare uppfylls.

Funktion (1/2)

- från Sambis tillitsramverk

A. Generella krav	3
Övergripande krav på verksamheten	3
Säkerhetsarbete	3
Kryptografisk säkerhet	3
Ansvar för användning av Underleverantörer	3
Handlingars bevarande	4
Informationsplikt	4
B. E-legitimationsutfärdare	4
C. Attribututgivare	4
D. Identitetsintygsutgivare	4
E. Tjänsteleverantör	5
F. Sambibud	5

Grunden i Sambis tillitsramverk

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

- (a) **Risikanalys 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.**

Ansvar för hela tillitskedjan

- Använder man underleverantörer för hela, eller delar av, den granskade funktionen så måste man redogöra för hur säkerheten upprätthålls hos leverantören.
- En leverantör kan vara "Betrodd part" i Sambi och har då godkänts vid granskning av en specifik tjänst/funktion.

Sammanfattning

Anslutning	Användarorganisation	Tjänsteleverantör
Direktanslutning i egen regi	✓	✓
Direktanslutning med betrodd part	✓	✓
Via Sambiombud	✓	✗
Via Gruppföreträdare*	(✓)	✗



Sammanfattning - användarorganisation

Anslutning - användarorganisation	LIS	IdP	Attribututgivare	E-legitimationsutf.
Direktanslutning i egen regi*	Ja	Ja	Ja	Ja
Via Sambiombud	Begränsat	Sambiombud	Sambiombud	Sambiombud
Via Gruppföreträdare	Gruppföreträdare	Gruppföreträdare	Gruppföreträdare	Gruppföreträdare

**Viss förenkling av LIS vid användande av betrodd part som underleverantör*



Priser

Antal anställda i Användarorganisation	Medlemsavgift (kr/år)
XS, upp till 99 anställda	5 000
Liten, mellan 100 och 500 anställda	10 000
Medel, mellan 501 och 1 000 anställda	20 000
Stor, mellan 1001 och 5 000 anställda	40 000
XL, över 5000 anställda	50 000

Sambiombud	Medlemsavgift och granskning
Per medlem	Enligt ombudets priser

Gruppföreträdare	Medlemsavgift (kr/år och gruppmedlem)
Per gruppmedlem	500

Tjänsteleverantör	Medlemsavgift (kr/år)
Medlemsavgift	10 000

Tillitsgranskning	Granskningsavgift (per granskning)
Per granskning	40 000

VI  INTERNET

Tack!

sambi.se
info@sambi.se

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

INTERNET 
STIFTELSEN