Sambi
Samverkan
för säkrare
e-hälsa

Sambis tillitsarbete

Staffan Hagnell, Internetstiftelsen

Bakgrund Sambi

2012 ***Ett samarbete mellan eHälsomyndigheten, Inera och Internetstiftelsen***

- Skapa tillit till elektroniska identiteter som används över organisationsgränserna
- Underlätta för informationsägare att fullgöra sina skyldigheter

2015 ***Produktion***

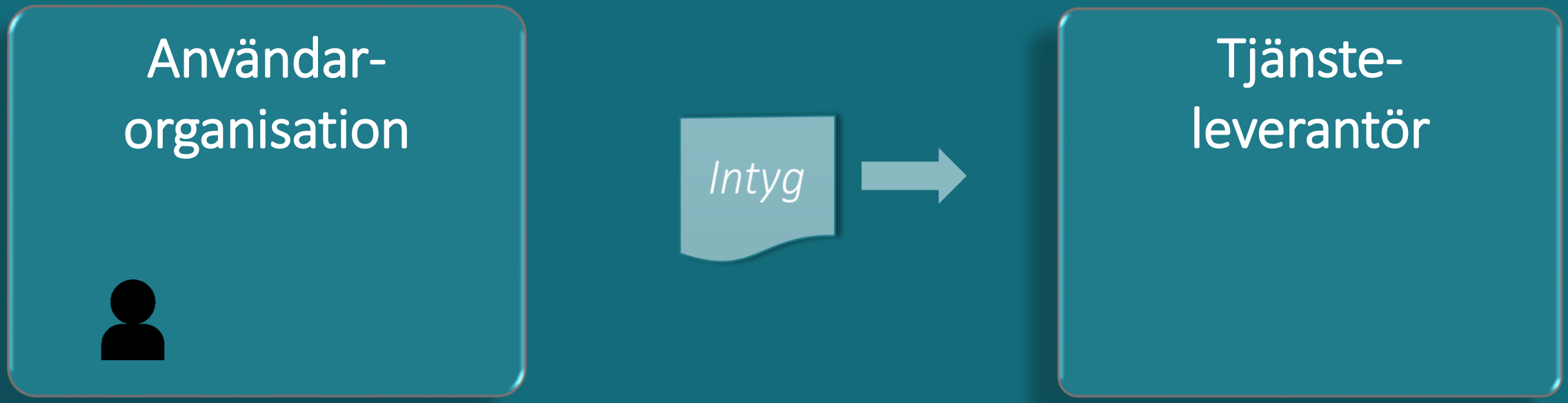
- Teknisk federation
- Tillitsgranskningstjänst

Nu **eHälsomyndighetens nya åtkomstlösning**

Förstudierapporten 2012

- Skapa tillit till elektroniska identiteter som används över organisationsgränserna
- Underlätta för informationsägare att fullgöra sina skyldigheter

Tillit i Sambi



Tjänsteleverantören ska kunna lita på att

- Användaren representerar Användarorganisationen och har den angivna rollen.

Användarorganisationen ska kunna lita på att

- Tjänstens behörighetssystem och att inloggningsuppgifterna skyddas

Tillitsgranskningar

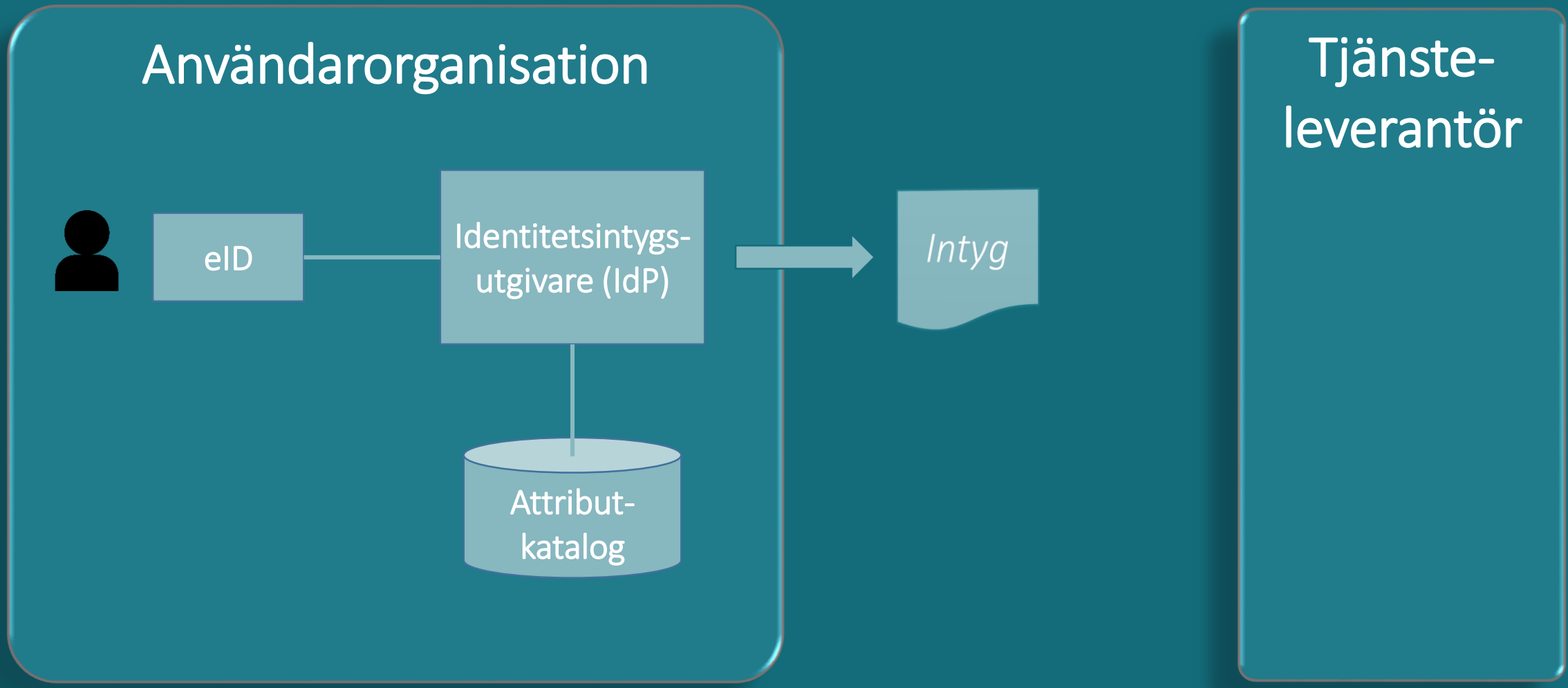
Användar-
organisation

Tjänste-
leverantör

Sambiombud

Under-
leverantör

Tillit till en Användarorganisation?



Krav på en Användarorganisation

Generella krav

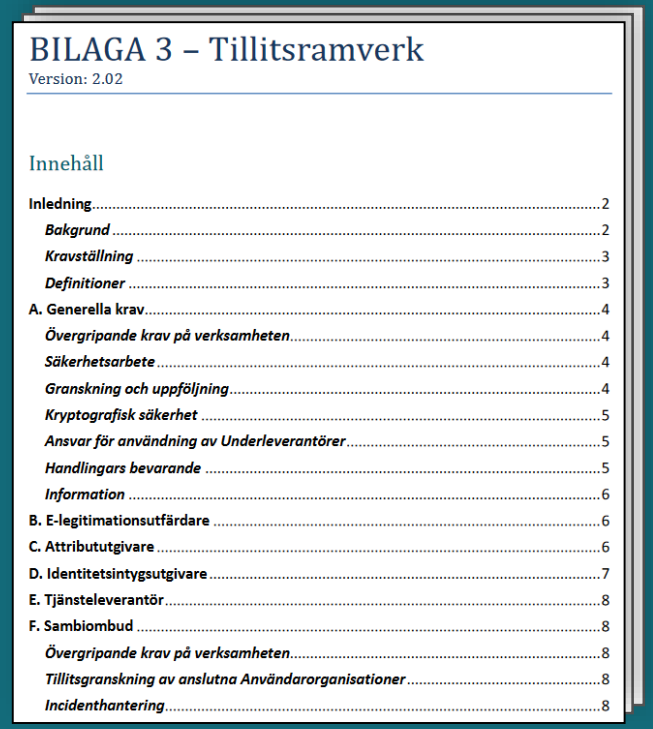
Krav på säkerhetsarbete

Funktioner

E-legitimation

Attribututgivare

Identitetsintygsutgivare



BILAGA 3 – Tillitsramverk

Version: 2.02

Innehåll

Inledning ... 2
Bakgrund ... 2
Kravställning ... 3
Definitioner ... 3
A. Generella krav ... 4
Övergripande krav på verksamheten ... 4
Säkerhetsarbete ... 4
Granskning och uppföljning ... 4
Kryptografisk säkerhet ... 5
Ansvar för användning av Underleverantörer ... 5
Handlingars bevarande ... 5
Information ... 6
B. E-legitimationsutfärdare ... 6
C. Attribututgivare ... 6
D. Identitetsintygsutgivare ... 7
E. Tjänsteleverantör ... 8
F. Sambiombud ... 8
Övergripande krav på verksamheten ... 8
Tillitsgranskning av anslutna Användarorganisationer ... 8
Incidenthantering ... 8

Utmaningen!

Ledningssystem för informationssäkerhet

*Sambis krav på ett **strukturerat säkerhetsarbete** begränsar sig dock till vad SAMBI omfattar, dvs identitets- och behörighetshantering*

Tillitsramverkets krav 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.

Målsättning

- Ökad säkerhet, men med en rimlig arbetsinsats och kostnad

Tillvägagångssätt:

Effektivisera genom att återanvända gjort arbete

Underleverantör (2015)

Användarorganisationens ansvar

Krav på säkerhetsarbete

Underleverantör

E-legitimation

Underleverantör

Attribututgivare

Underleverantör

Identitetsintygs-utgivare

Sambiombud (2017/18)

Användarorganisationens ansvar

Krav på säkerhetsarbete

Sambiombud

Bistå i säkerhetsarbetet

E-legitimation

Attribututgivare

Identitetsintygs-utgivare

”Grupper” 2019?

Krav

1. En rätt att juridiskt företräda Användarorganisationsenheterna
2. Ett sammanhållet säkerhetsarbete för alla Användarorganisationsenheter
3. En förmåga att agera för Användarorganisationsenheterna vid en incident.

Externa juridiska personer

Fortsättning

- Vidareutveckla användningen av Sambiombud och ”grupper”
- Behåll Tillitsramverk på en hög nivå, men komplettera med mer detaljerade checklistor och information
- Harmonisering av säkerhetskrav mellan olika tillämpningsområden för att undvika dubbelarbete