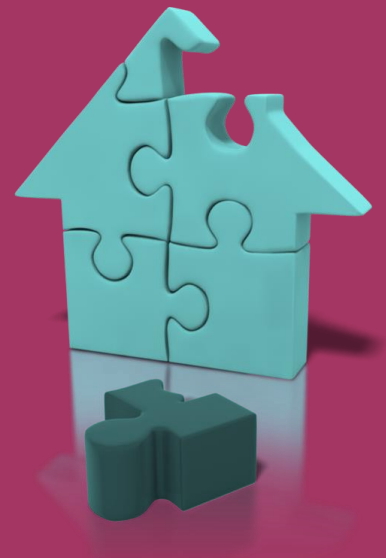
Referensarkitektur för Identitet och åtkomst (IAM)

Stöd till utformning av IT-stöd för säkerställd identitet och åtkomst till rätt information vid rätt tillfälle



Introduktion

www.inera.se

inera
Ett företag inom SKR

Referensarkitektur för Identitet och åtkomst (IAM)

Bakgrund och syfte

identitets- och åtkomsthantering *(Identity and Access Management, IAM)*
område som hanterar användares digitala identiteter och behörighetsstyrande egenskaper, åtkomst till information i IT-system och regelverken som styr åtkomsten

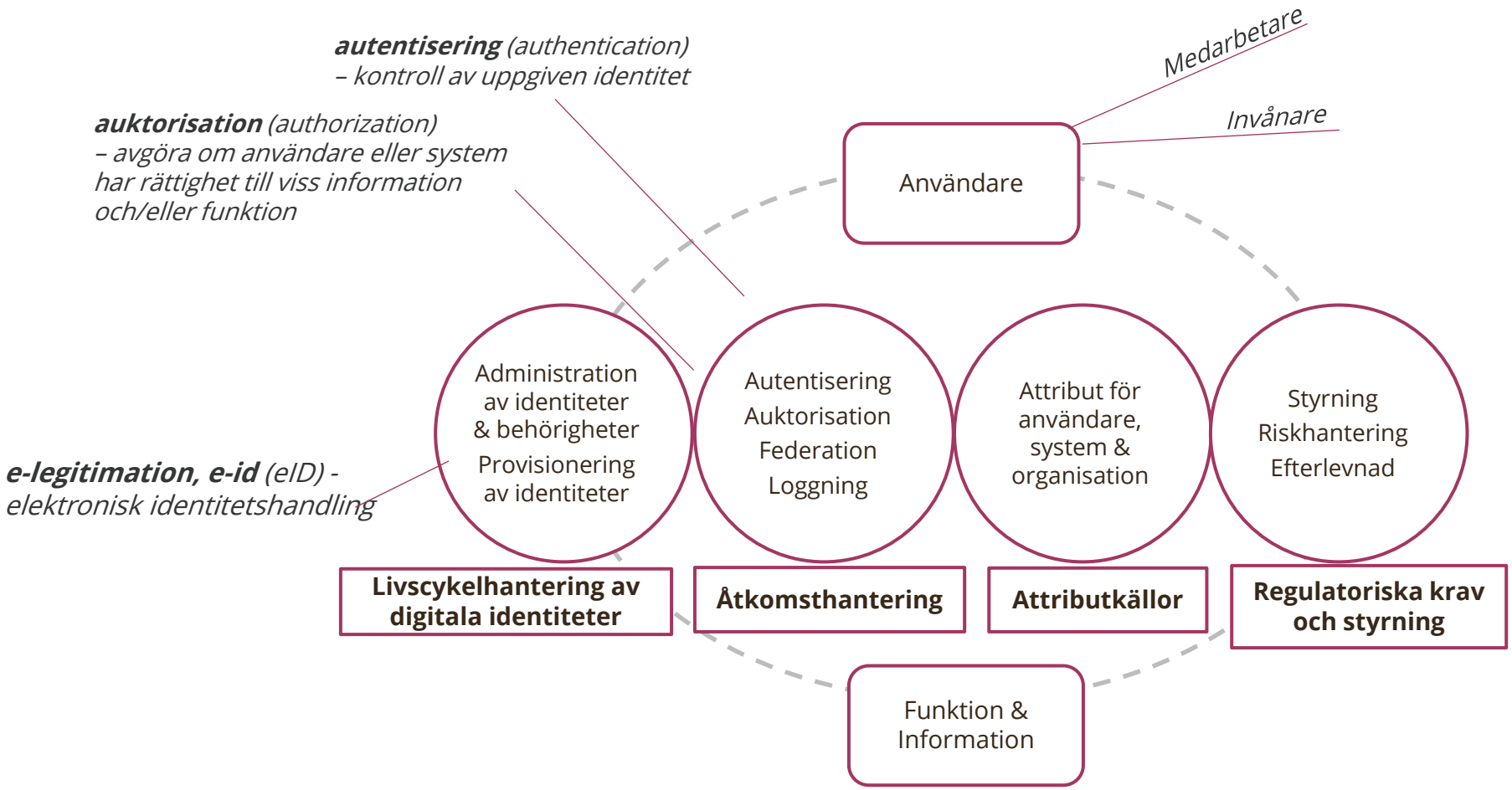
Referensarkitekturen ska
inom området identitet och åtkomst fungera som

- **Vägledning** – tillhandahålla styrande principer, gemensamma krav, normerande termer och begrepp, arkitekturella mönster och en sammanhållen referensmodell för förmågor och tillhörande tjänster
- **Referensunderlag och kravställning** vid anskaffning och vidareutveckling av IT-infrastruktur och verksamhetssystem

Referensarkitekturen kan tillämpas såväl inom **den egna organisationen** som vid **samverkan med andra organisationer** såsom regionala eller nationella digitala tjänster och infrastruktur

inera

Området Identitet och åtkomst (IAM)



Referensarkitektur för Identitet och åtkomst (IAM)

Drivkrafter - verksamhetsbehov

Single sign-on till flera system

Ett e-id för alla mina inloggningar

Enkel, enhetlig och säker tillgång
till digital information

Kan vi införa ny säkerhetsteknik utan att anpassa alla våra system?

Nya inloggnings-metoder
kunna införa ny teknik

Kan vi använda den senaste mobila tekniken?

Mobilt arbetssätt
som klarar säkerhetskrav

Kan vi se och ändra behörigheten i ETT samlat gränssnitt?

Hur förse våra medarbetare med tillförlitliga e-id för elektronisk legitimering?

Kvalitetssäkring
av digitala identiteter och egenskaper

Kan vi ha enhetliga och plattformsneutrala IAM-infrastrukturtjänster för alla våra digitala tjänster?

Standardisering
öka förvaltningsbarhet, minska teknisk inlåsning och kostnader

Hur kan vi tillhandahålla säker API-åtkomst till våra samarbetsorganisationer?

Samverka över organisationsgränser
utan att säkerheten blir hindrande

inera

Vilka problem löser referensarkitekturen?

Olika varianter av inloggning & behörighet per system och applikation - frustrerande för användaren!

Direktintegrationer med säkerhetslösningar skapar inlåsning i gammal teknik

Komplicerat och kostsamt att realisera säkerhet, singelinloggning osv.

Dålig förvaltningsbarhet, svårt att förändra systemen

inera

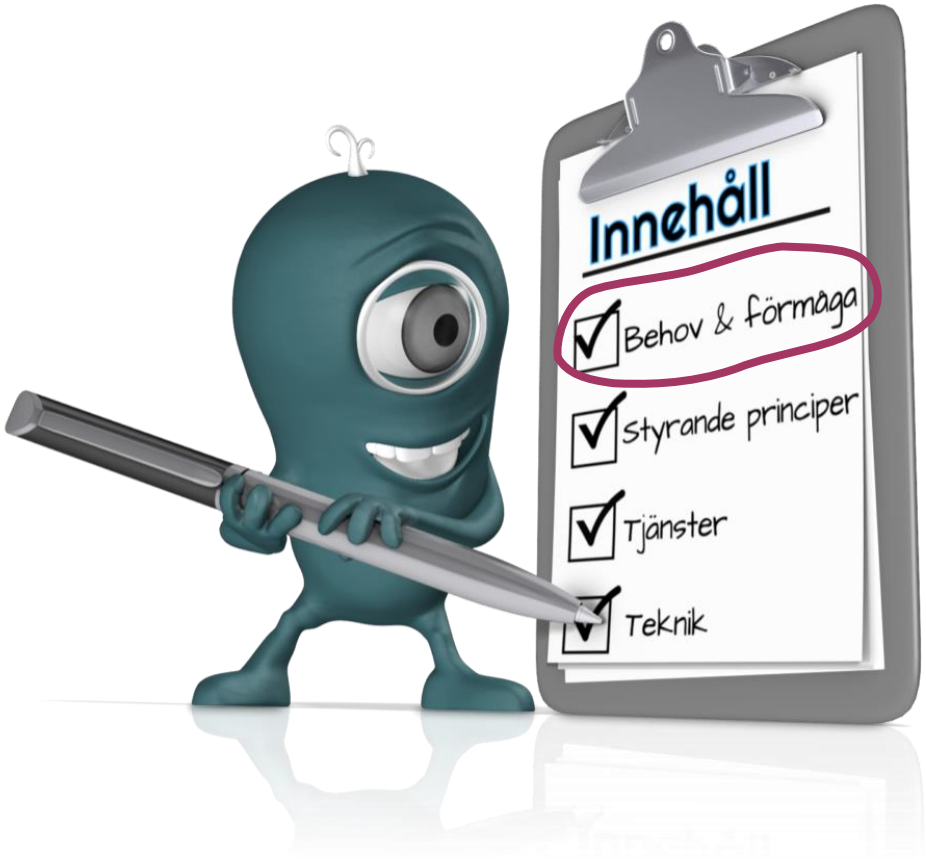
En smartare och mer skalbar arkitektur

- ✓ Samla säkerhetstekniken i en i grunden **plattformsoberoende infrastruktur** för IAM och integrera systemen med **standardprotokoll** för långsiktighet i förvaltning
- ✓ **Möjliggör ny teknik** i infrastrukturen: flerfaktorsautentisering, mobila bärare, biometri
- ✓ **Konsolidera identitetsdata** för underlättad kvalitetssäkring för tilldelning av e-id och behörigheter

inera

Referensarkitektur Identitet och åtkomst

Användningsfall och förmågor



identifiering och **autentisering** av användare

singelinloggning (SSO)

möjliggör sammanhållen **identitets- och behörighetsadministration**

autentisering och auktorisation av system för säker system-system-kommunikation inom och mellan organisationer

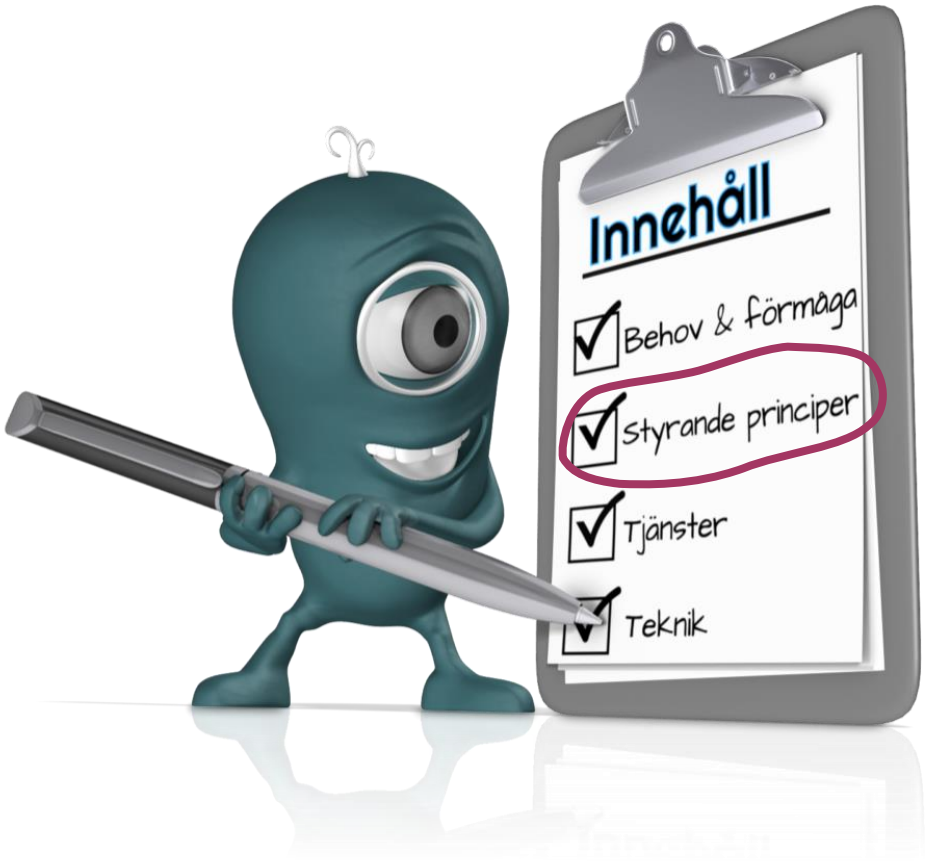
säker och behörig **API-åtkomst**

säker federativ samverkan med andra parter

inera

Referensarkitektur Identitet och åtkomst

Styrande priciper, ett urval



e-tjänsterna respektive IT-infrastrukturen för identitet och åtkomst separeras genom **standardiserade gränssnitt**

plattformsneutral IT-infrastruktur

inloggning sker i **tjänst för e-legitimering**

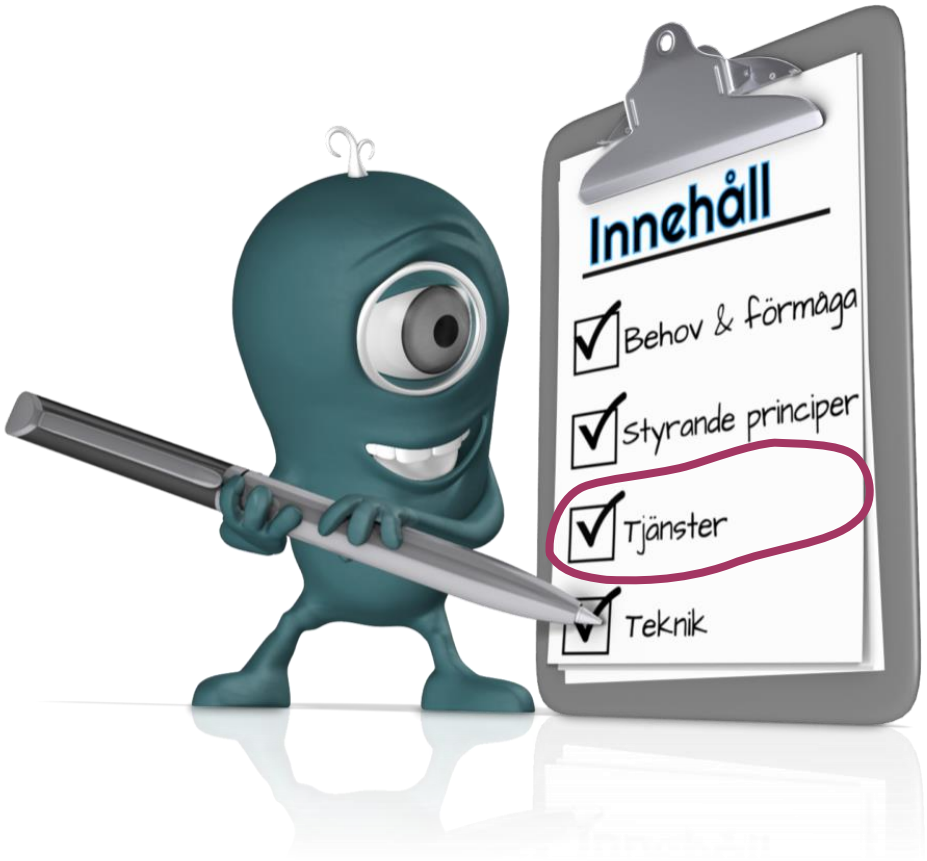
identitets- och åtkomstintyg utfärdas som grund för inloggning och behörighet

tillit till andra organisationers IT-lösningar för identitet och åtkomst skapas via öppna **gemensamma tillitsramverk**

inera

Referensarkitektur Identitet och åtkomst

Tjänstevyn



gemensam **referensmodell** med samverkande tjänster

arkitekturella mönster och krav

inera

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare Klient
User
User agent

e-id

Utfärdande

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister | Metadatatjänst | Tillitsramverk | Attribut | Godkännandeprocess

Regelverks-administration

Regelverkstjänst

Legitimeringstjänsten är ”navet”

Ställer ut digitala identitetsintyg
Tillhandahåller Single Sign-On

Standardisera tekniken
SAML2, OpenID Connect, OAuth2, SCIM

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Flexibilitet & utbyggbarhet

Lägg till stöd för autentiseringsteknik i infrastrukturen efter verksamhetsbehov

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

E-legitimering

Användare Klient
User
User agent

e-id

E-legitimationsutfärdare
eID issuer

Utfärdande

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator
Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Åtkomstintygstjänst
Token service

Åtkomstintyg

E-tjänster
Verksamhetssystem
Service provider / identity consumer

API Säkerhetstjänst
API Gateway
Integrationstjänster, API:er

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Identitetsintyg

Åtkomstintyg

Användare
Klient
User
User agent

e-id

Stödtjänster för åtkomst
Support services for access control

Provisioneringstjänst
Provisioning service

Konsolidera & kvalitetssäkra
identitets- och behörighetshanteringen

Provisionera (överför) identitetsdata till e-tjänster vid behov

Utfärdande

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator
Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Åtkomstintygstjänst
Token service

Åtkomstintyg

E-tjänster
Verksamhetssystem
Service provider / identity consumer

API Säkerhetstjänst
API Gateway
Integrationstjänster, API:er

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Identitetsintyg

Åtkomstintyg

Autentiseringstjänst(er)
Authentication services

E-legitimering

Användare
Klient
User
User agent

e-id

Stödtjänster för åtkomst
Support services for access control

Elektroniska identitetshandlingar, e-id
Jämförbarhet via **tillitsnivåer**

E-legitimationsutfärdare
eID issuer

Utfärdande

Möjliggör olika bärare
för e-id för att anpassa till verksamhetsbehov
- smart kort, mobilt, ...

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister | Metadatatjänst | Tillitsramverk | Attribut | Godkännandeprocess

Åtkomstintyg
OAuth2 standard

Regelverks-administration

Regelverkstjänst
Authorization rules service

Åtkomstintygstjänst
Token service

Åtkomstintyg

E-tjänster
Verksamhetssystem
Service provider / identity consumer

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Identitetsintyg

Åtkomstintyg

Autentiseringstjänst(er)
Authentication services

E-legitimering

Användare
Klient
User
User agent

e-id

Säker API-åtkomst,
baserat på åtkomstintyg
Exempel "*Smart On FHIR*"

Provisioneringstjänst
Provisioning service

E-legitimationsutfärdare
eID issuer

Utfärdande

Ref… Id…

Federera identitet och behörighetsgrundande attribut mellan organisationer via identitetsintyg och betrodda tjänster

Federation
Federationsoperatör
Federation operator

Medlemsregister

Metadatatjänst

Tillitsramverk

Attribut

Godkännandeprocess

Rege… admi…

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-legitimering

Utfärdande

Åtkomstintyg

Användare
Klient
User
User agent

e-id

Gemensam syn på tillit till säkerhetsteknik och säkerhetsrutiner

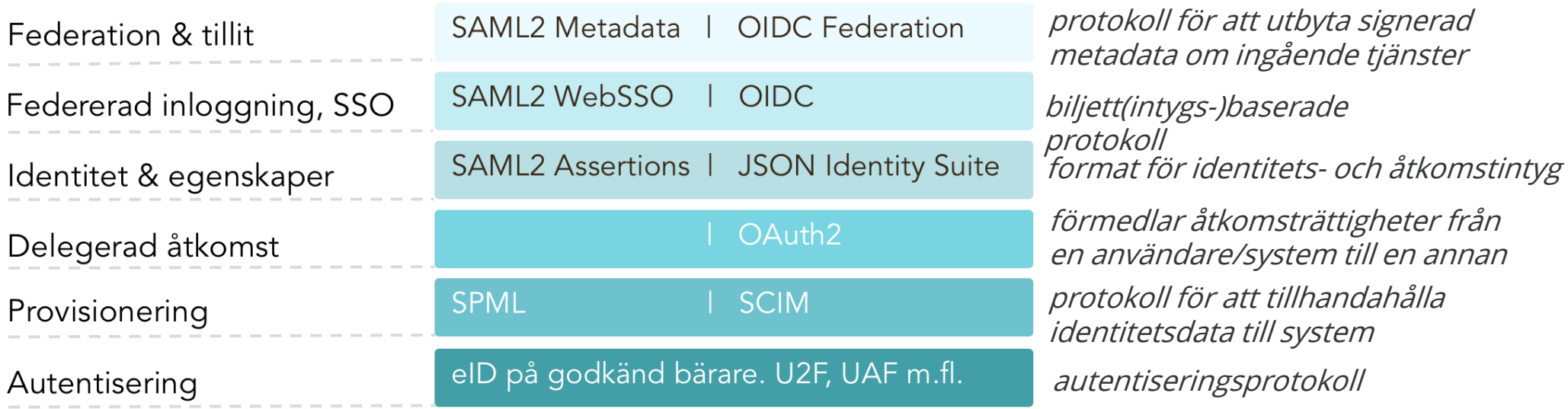
Gemensamma definitioner för identitet och behörighet

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur för Identitet och åtkomst (IAM)

Förmågor och tekniska protokoll



Tack!

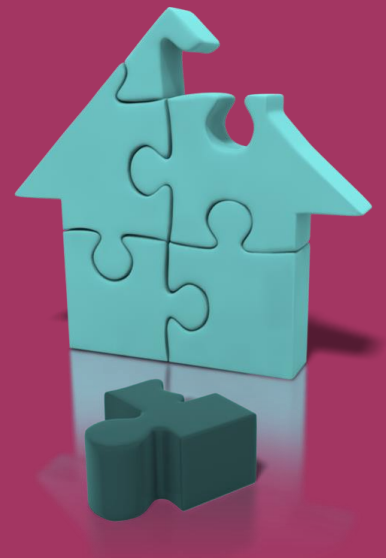
Mer information om Referensarkitektur för Identitet och åtkomst (IAM) på
www.inera.se

www.rivta.se

inera
Ett företag inom SKR

Referensarkitektur för Identitet och åtkomst (IAM)

Vad är nytt i Revision B?



www.inera.se

inera
Ett företag inom SKR

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare Klient
User
User agent

e-id

Utfärdande

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister

Metadatatjänst

Tillitsramverk

Attribut

Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Utfärdande

Åtkomstintyg

Identitetsintyg

E-tjänster
Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare
Klient
User
User agent

e-id

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

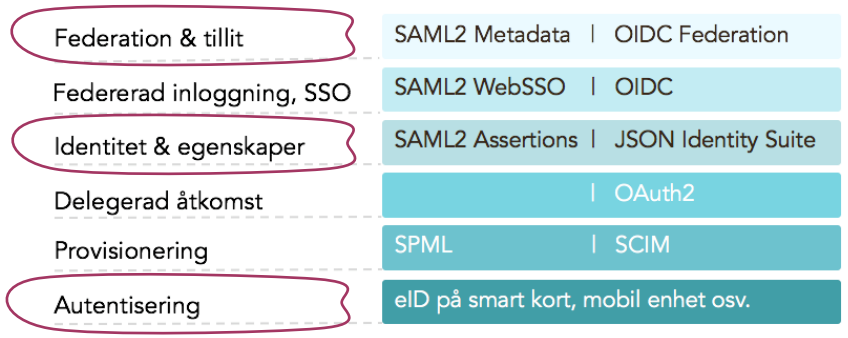
Stödtjänster för åtkomst
Support services for access control

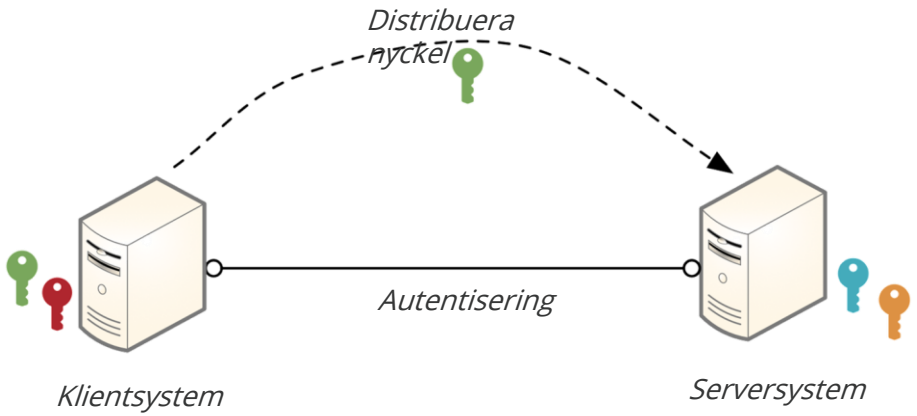
Referensarkitektur för Identitet och åtkomst (IAM)

Vad är nytt i revision B?

Fokus: System-till-system

- **Autentisering av system**
  - **Principer för att etablera tillit** till system
    - **Registering av system**, grundläggande krav och principer, asymmetriska nycklar
    - **Certifikatsutfärdare** och **federation** för systemtillit
      - Öppen PKI
      - Sluten PKI
      - Publik nyckel-registrering
    - **Organisationstillit**
  - Rekommenderade **autentiseringsprotokoll**





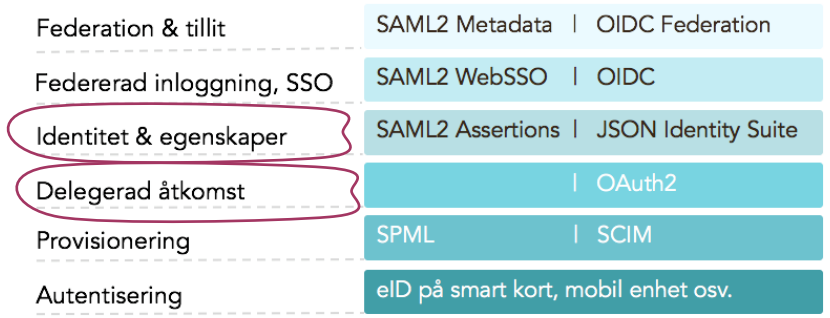
inera

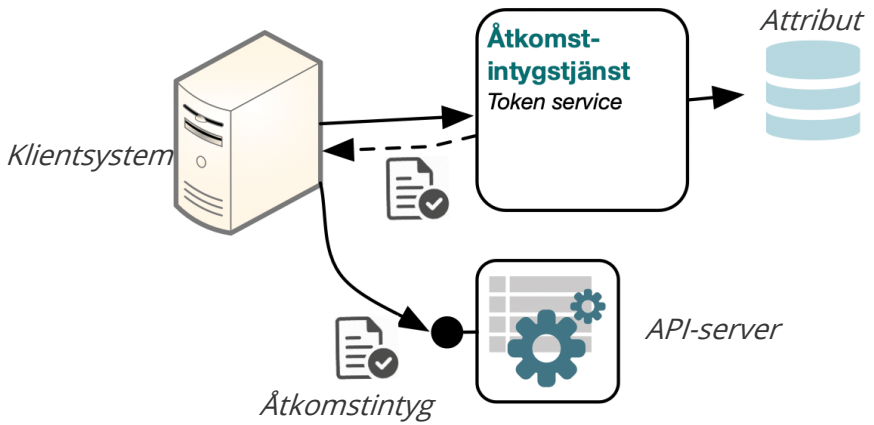
Referensarkitektur för Identitet och åtkomst (IAM)

Vad är nytt i revision B?

Fokus: System-till-system

- **Auktorisation av system**
  - **Interaktionsmönster** för system-till-system-kommunikation (API-klient → API-server)
  - Konsolidera auktorisationen till **Åtkomstintygstjänst** för ökad skalbarhet
  - **Systemegenskaper (attribut)** som underlag för skalbar auktorisation
  - Åtkomstintyg med **innehavsbevis** - *Proof-of-Possession* för ökad säkerhet
  - **Sammansatta tjänster** och auktorisation – **delegering** av systemets rättigheter





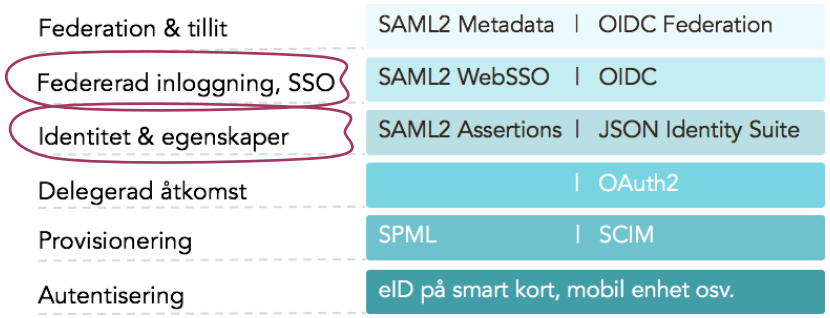
inera

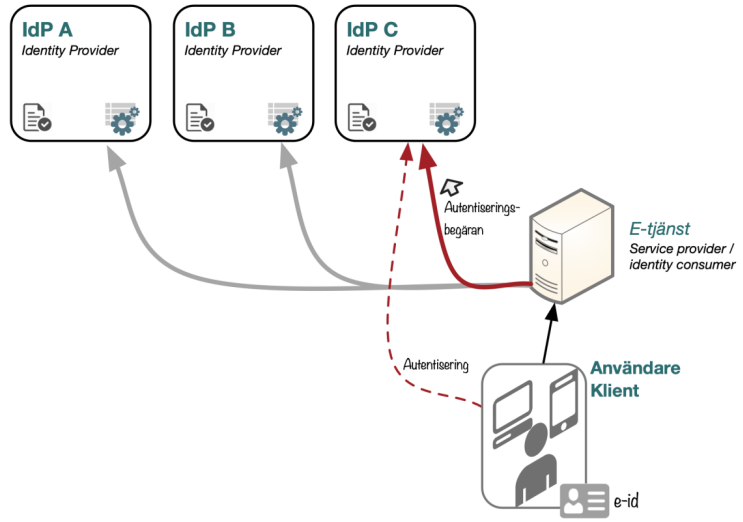
Referensarkitektur för Identitet och åtkomst (IAM)

Vad är nytt i revision B?

Fokus: Användare – inloggning & legitimering

- **Legitimeringstjänst** (IdP)
  - Samverkan vid **flera legitimeringstjänster**
    - Mönstret **IdP-proxy** för anslutning av fler IdP:er
    - Principer för **val av IdP**
  - Principer för **tillhandahållande av användarattribut**
  - Principer för **leverans av ID-intyg** - oombedda ID-intyg avrådes (s.k. IdP-initierad inloggning)
  - **Mer om SSO** – avsluta SSO-session, tvingande autentisering
  - OpenID Connect - Tagit bort stöd för flödena *Implicit* och *Hybride*





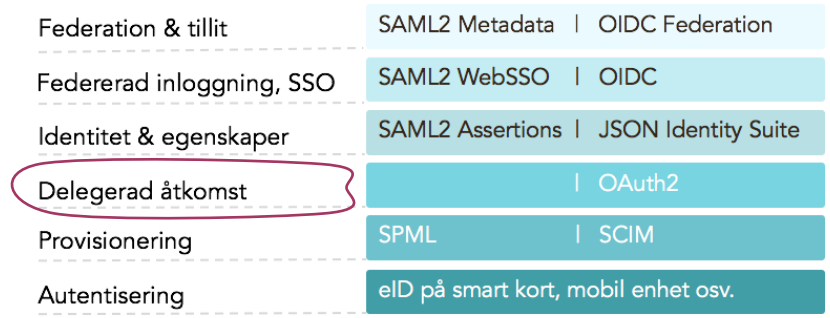
inera

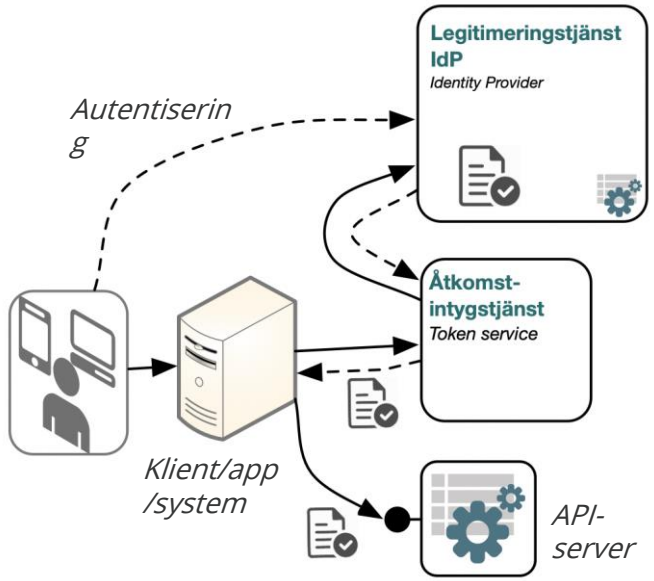
Referensarkitektur för Identitet och åtkomst (IAM)

Vad är nytt i revision B?

Fokus: Användare – åtkomst

- **Delegerad åtkomst från användare**
  - Användaren auktoriserar en app eller ett system (delegerar) att läsa/skriva till ett API
  - Olika interaktionsmönster, t.ex. delegering via förnyad användarautentisering i en IdP
  - Åtkomst till egen data via ett aktivt medgivande
  - Åtkomst över organisationsgränser





inera

Tack!

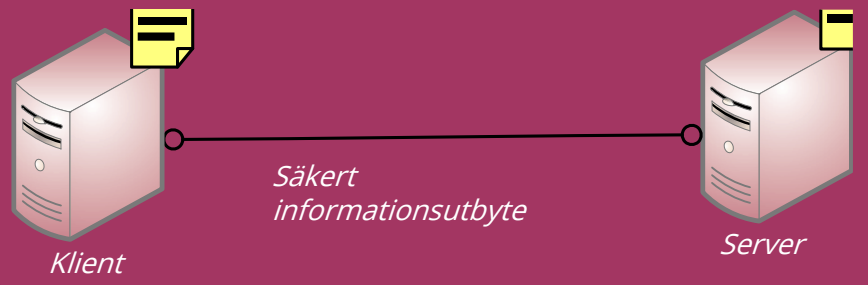
Mer information om Referensarkitektur för Identitet och åtkomst (IAM) på
www.inera.se

www.rivta.se

inera
Ett företag inom SKR

Referensarkitektur för Identitet och åtkomst (IAM)

Autentisering och auktorisation av system



www.inera.se

inera
Ett företag inom SKR

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare Klient
User
User agent

e-id

Utfärdande

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator
Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

E-legitimering

Användare Klient
User
User agent

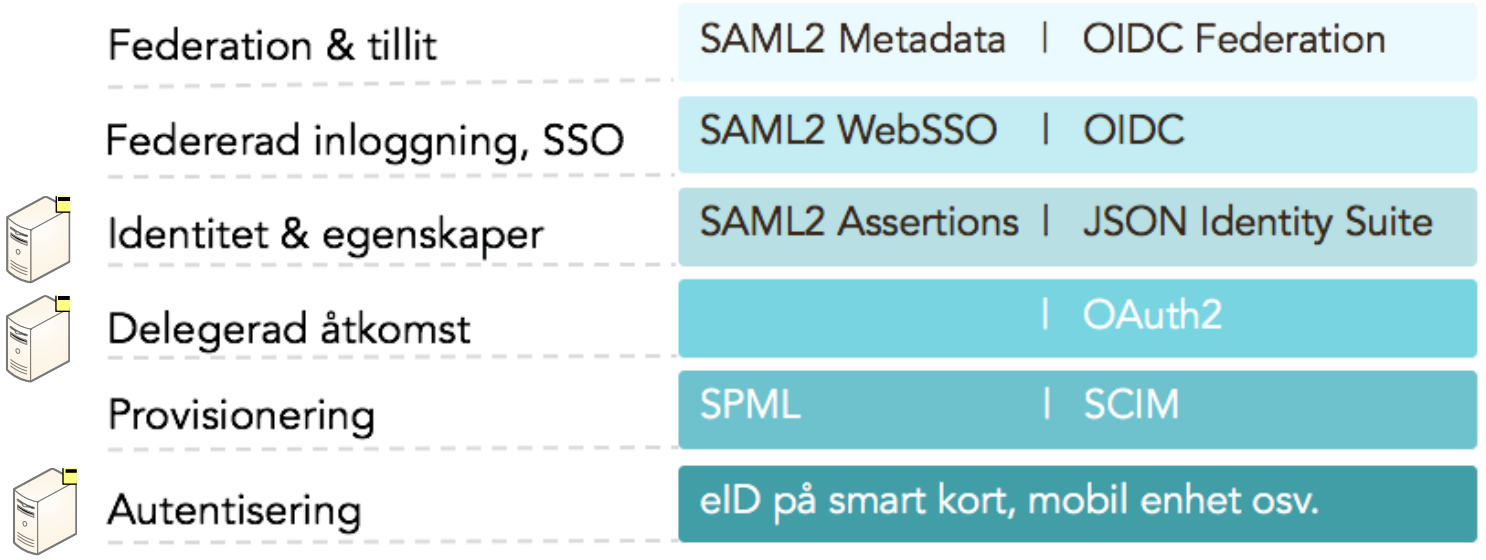
e-id

Utfärdande

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur för Identitet och åtkomst (IAM)

Autentisering och auktorisation av system



autentisering– kontroll av uppgiven identitet

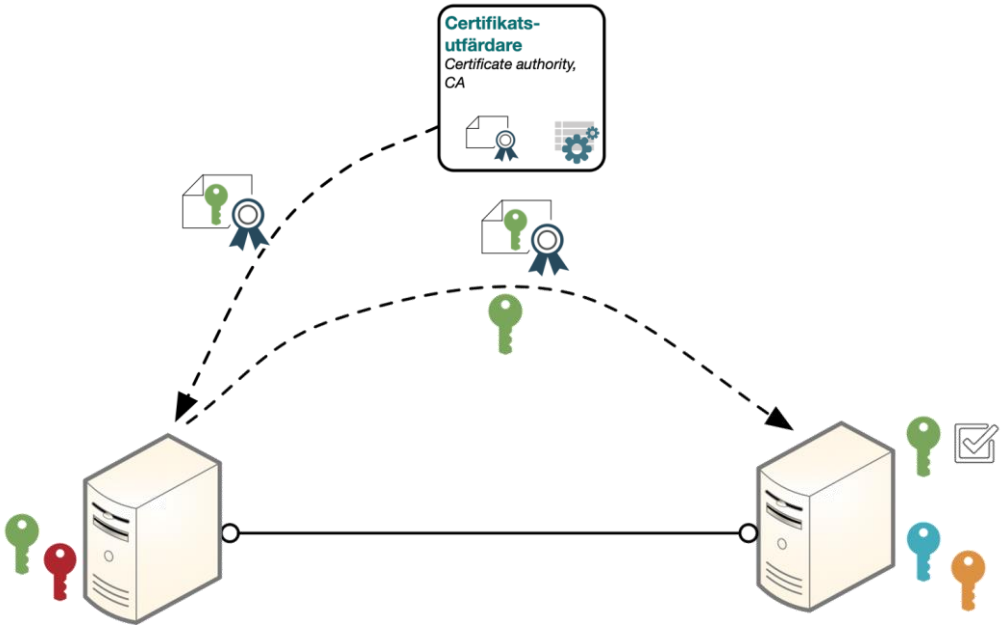
auktorisation *- avgöra om en aktör (användare eller system) har rättighet till viss information och/eller funktion*

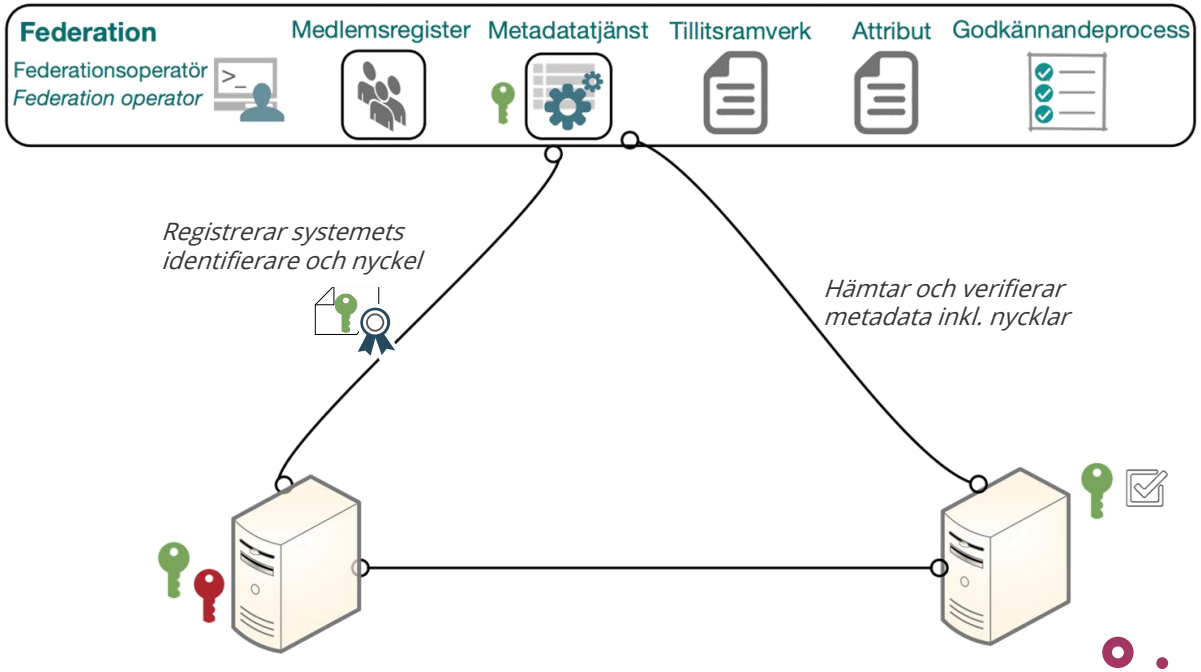
inera

Registrering av systemidentiteter

Etablera tillit till system

- Krav: ett system ska kunna hålla ett asymmetriskt **nyckelpar** (privat/publik)
  → möjliggör god skalbarhet, stöd för standardiserad säkerhetsteknik samt hög tillitsnivå
- Använd **unika systemidentifierare**, rekommenderat i form av URL:er
- Registrera **bilateralt** eller via **federation**, ev. med stöd av certifikatsutfärdare (CA)





inera

Registrering av systemidentiteter

Principer för att etablera tillit

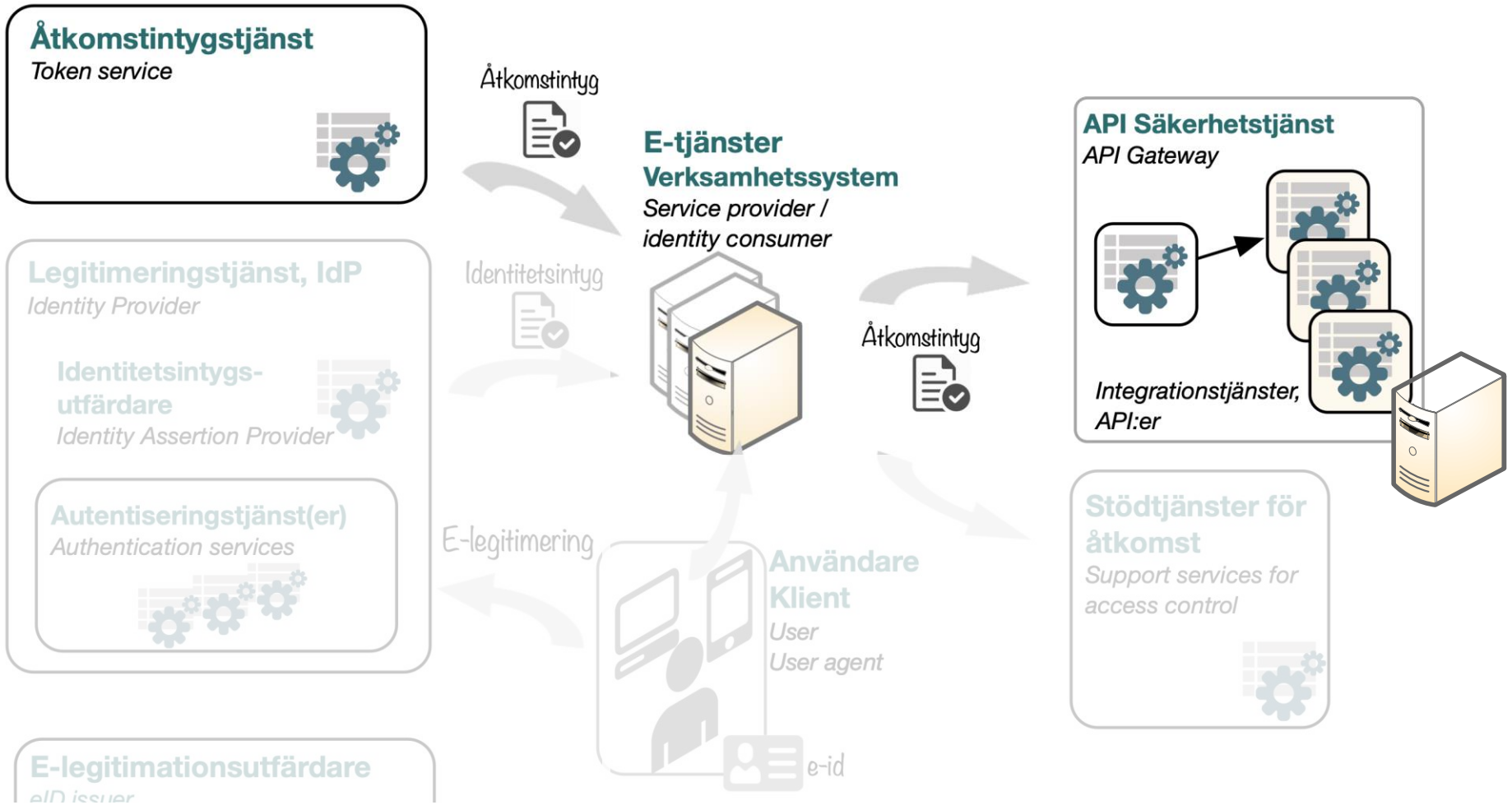
- **Öppen PKI**
  - Certifikat från flera publika utfärdare; komplext att hantera godkännandeprocessen
  - Kombineras oftast med att registrera en unik del av certifikatet, ett attribut, den publika nyckeln eller hela certifikatet (s.k. *pinning*) för att öka säkerheten
  - Kräver spärrkontroller samt certifikatutbyte innan det blir ogiltigt, förutom nyckelutbyte vid behov
- **Sluten PKI**
  - Certifikat från en dedikerad utfärdare för respektive form av datautbyte
  - Kräver spärrkontroller samt certifikatutbyte innan det blir ogiltigt, förutom nyckelutbyte vid behov
  - Kan leda till många olika certifikat för ett och samma system om deltagande i flera slutna PKI:er
- **Publik nyckel-registrering** - *rekommenderas*
  - Mycket god skalbarhet och kontroll över registreringsprocessen - från bilateralt till stora federationer
  - Nyckeln kan med fördel levereras i ett självsignerat certifikat
  - Nyckelutbyte vid behov

Stöd i standarder:
OASIS SAML 2.0 Metadata Interoperability Profile
OpenID Connect Federation 1.0

inera

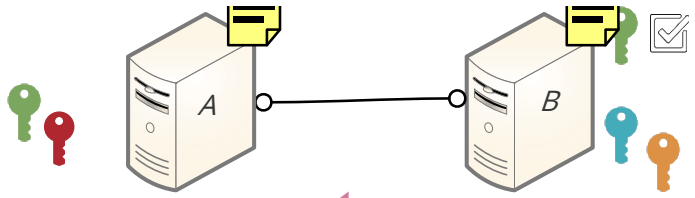
System-system-kommunikation

enligt Referensarkitektur IAM



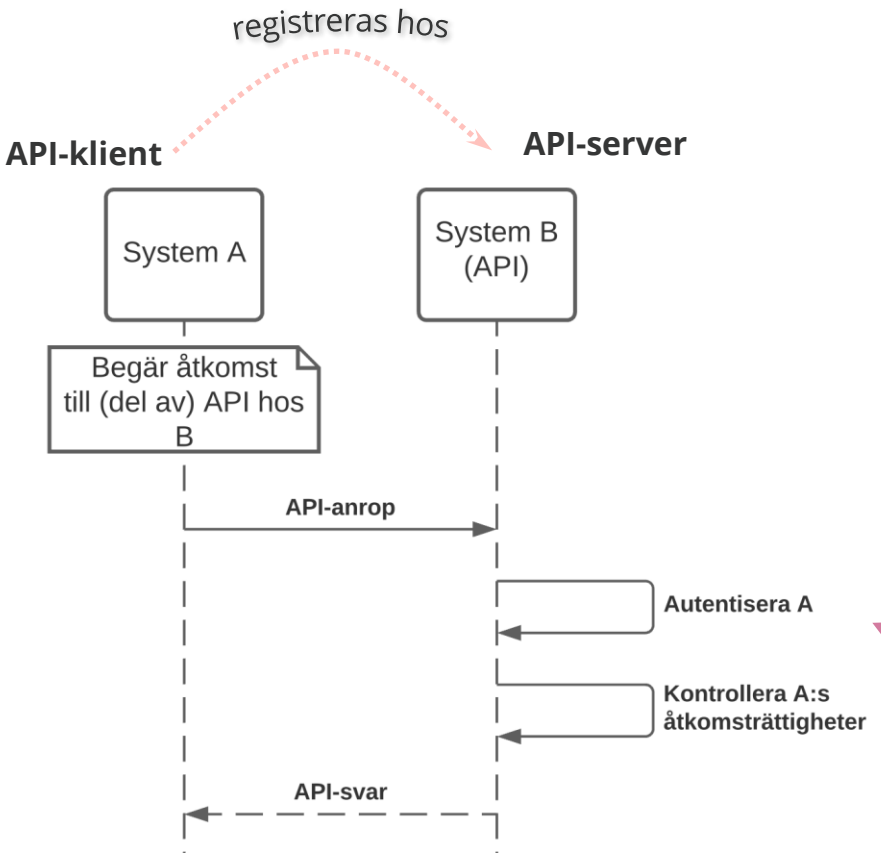
System-system-kommunikation

Grundläggande interaktionsmönster



Rekommenderade autentiseringsprotokoll:

- *mutual TLS*
- *private_key_jwt*



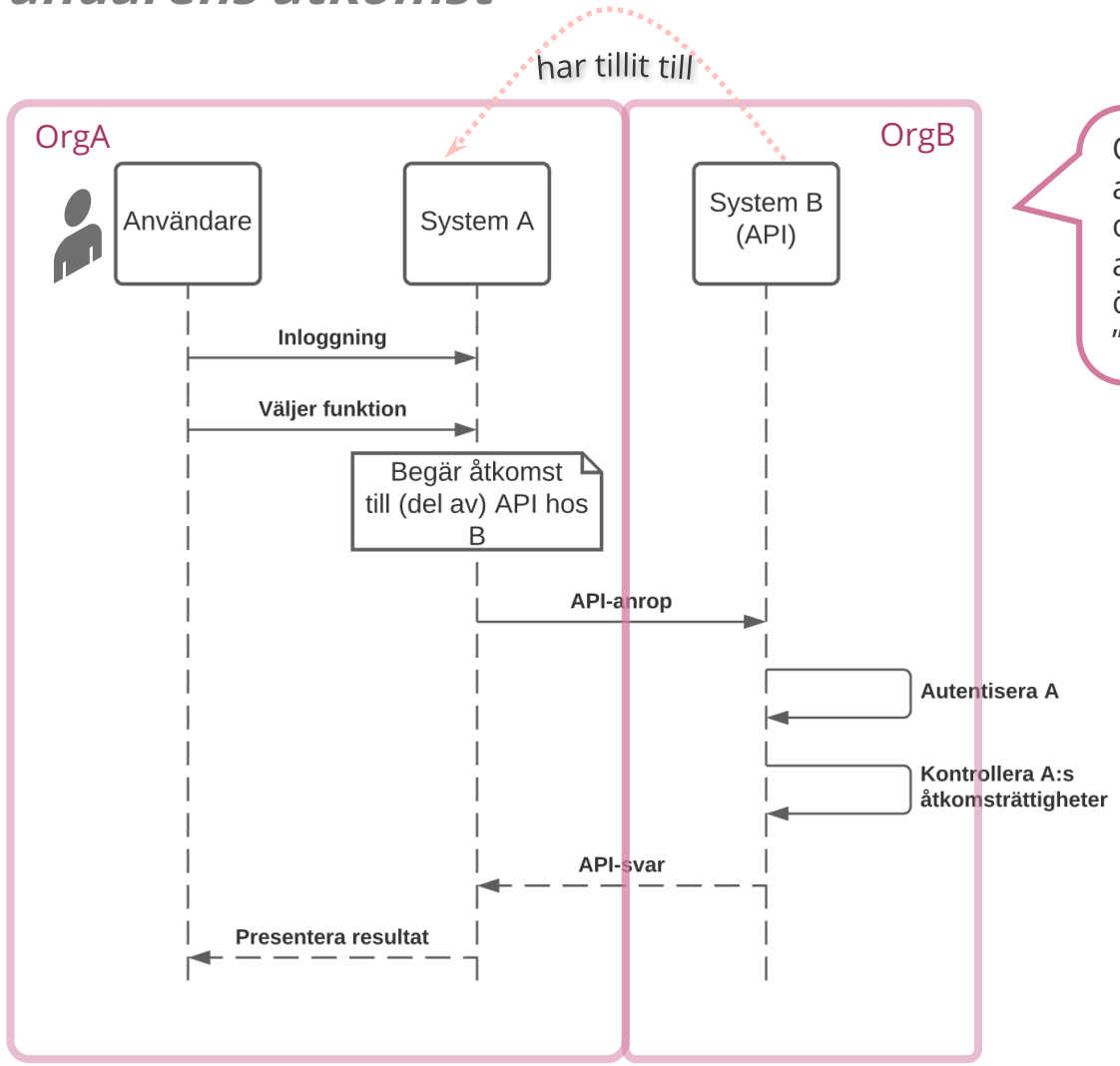
Autentisering och auktorisation av systemet vid varje anrop (t.ex med vitlistning av system)

Enkel integration men kan vara utmanande att skala upp till många system

inera

System-system-kommunikation

Organisationstillit för användarens åtkomst



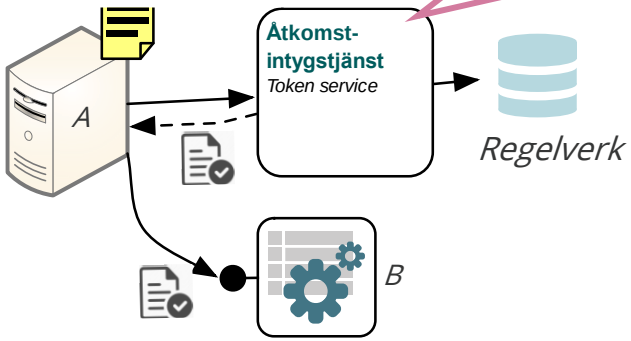
Organisation B litar på att A ansvarar för att autentisering och åtkomstkontroll av användare hanteras utifrån överenskomna krav, "*organisationstillit*"

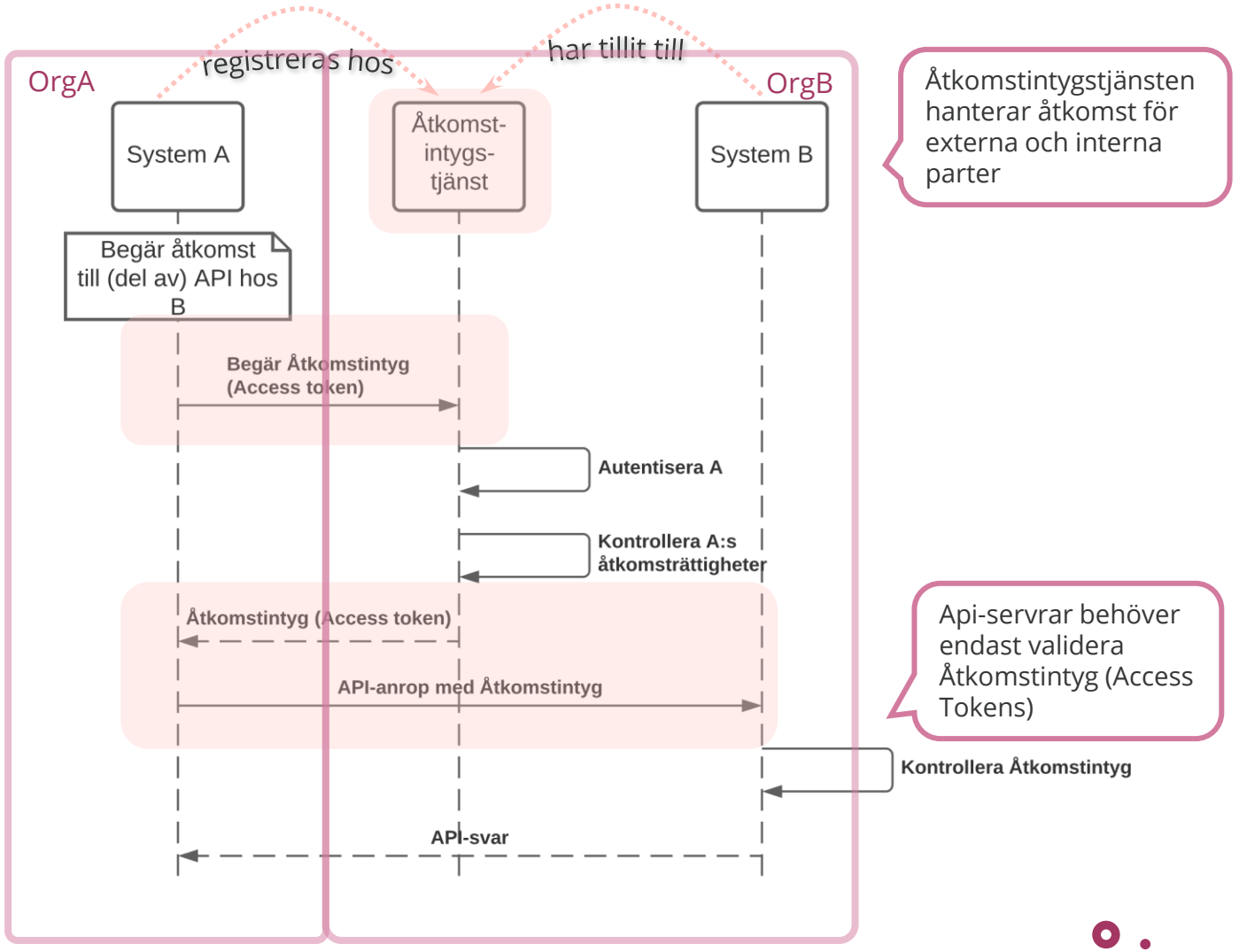
inera

System-system-kommunikation

Konsolidera åtkomsthanteringen med åtkomstintygstjänst

OAuth 2.0 RFC6749 Client Credentials Flow



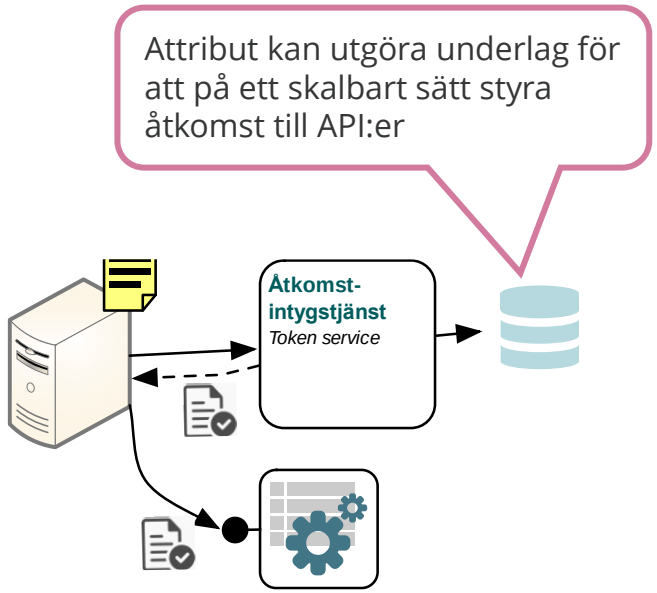


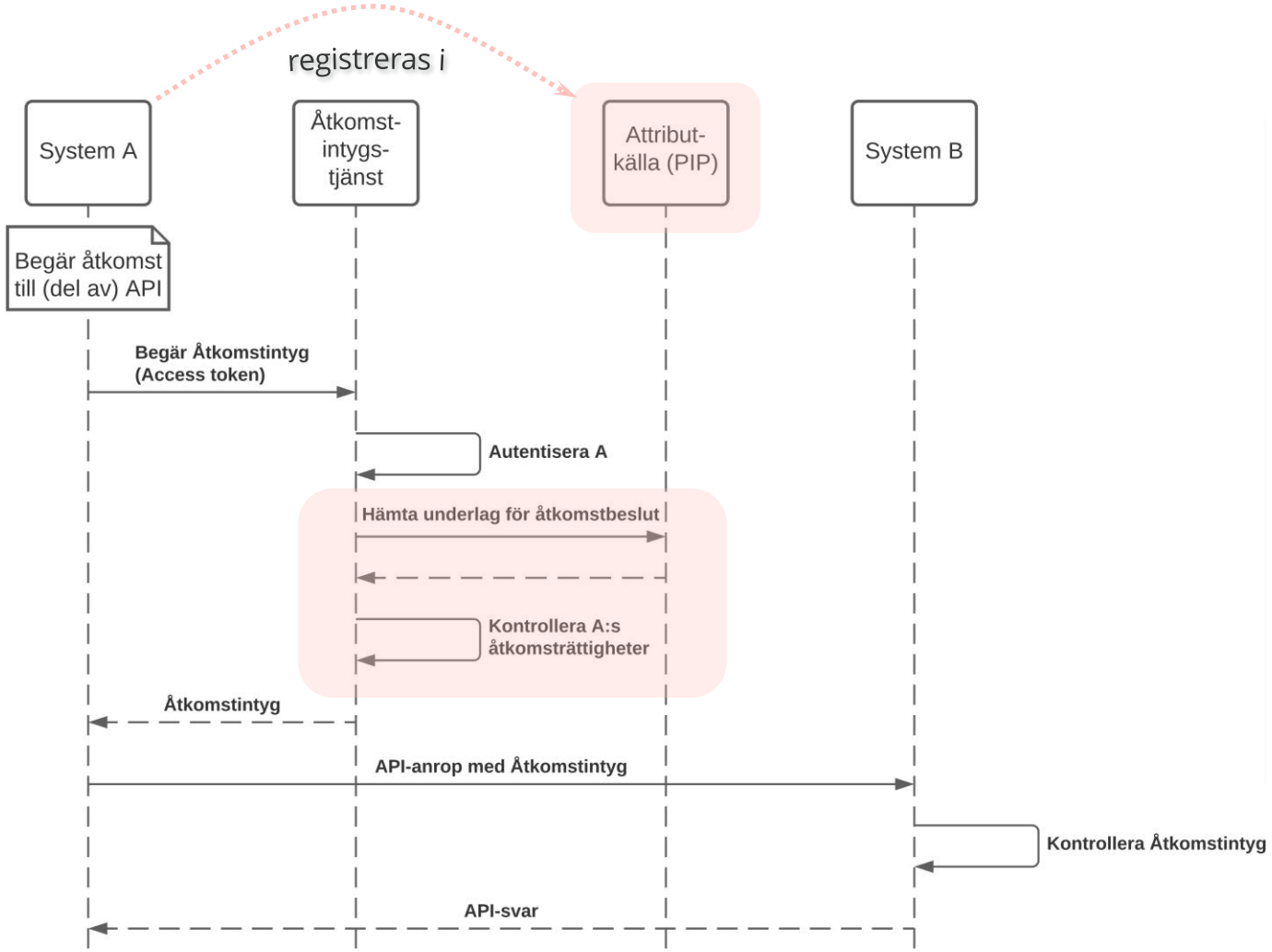
Åtkomstintygstjänsten hanterar åtkomst för externa och interna parter

Api-servrar behöver endast validera Åtkomstintyg (Access Tokens)

Hantera egenskaper för system

Ökad skalbarhet med attribut som underlag för åtkomstbeslut



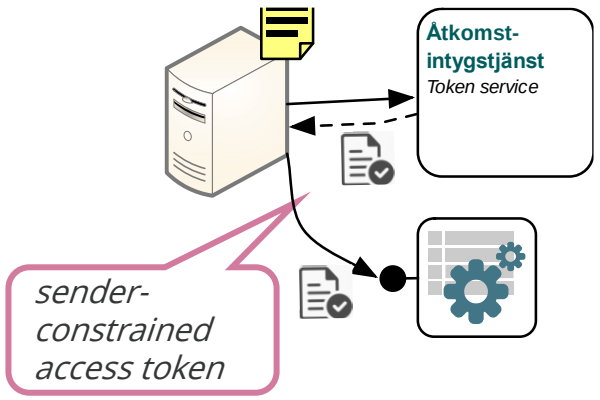


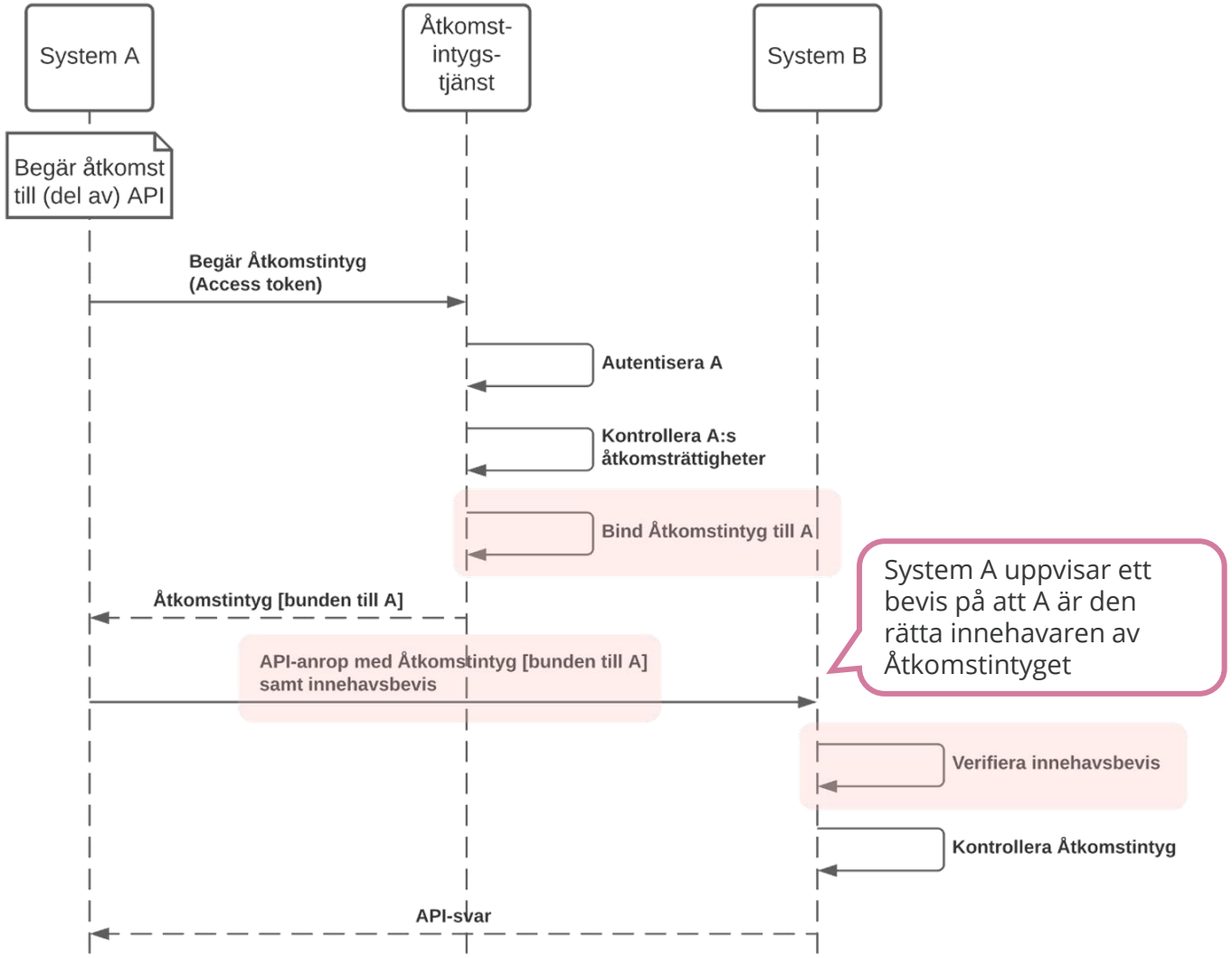
Bevisa innehav av åtkomstintyg

Proof-of-Possession (PoP)

Förstärkt skydd av åtkomstintygen mot återuppspelningsattacker

Rekommenderas vid höga krav på säkerhet





Innehavsbevis

Rekommenderat protokoll för ”Proof-of-Possession” för säkrare åtkomstintyg

- *OAuth 2.0 DPoP ”Demonstrating Proof-of-Possession at the Application Layer”*
  - Bygger på **publik/privat nyckel** och **signering av ett bevis**
  - Fungerar både ***confidential clients*** och ***public clients***
    - Kan t.ex. använda säkert utrymme i en mobiltelefon för nyckeln
  - **Oberoende av transportprotokollet**
    - End2end mellan API-klient och API-server på applikationsnivån
    - Kräver inte en relativt kostsam upprepning av mutual TLS i alla led.
      En mTLS-kedja bryts i lastbalanserare framför API-server, vilket kräver produktspecifika lösningar
  - Stödjer **olika autentiseringstekniker**
  - Kan **införas successivt**
    - Möjliggör i infrastrukturen för IAM först, kräv innehavsbevis efter behov

confidential clients *– applikationen har en serversida som kan förvara en nyckel säkert*

public clients *– app som enbart körs ute på användarens enhet (t.ex en SPA)*

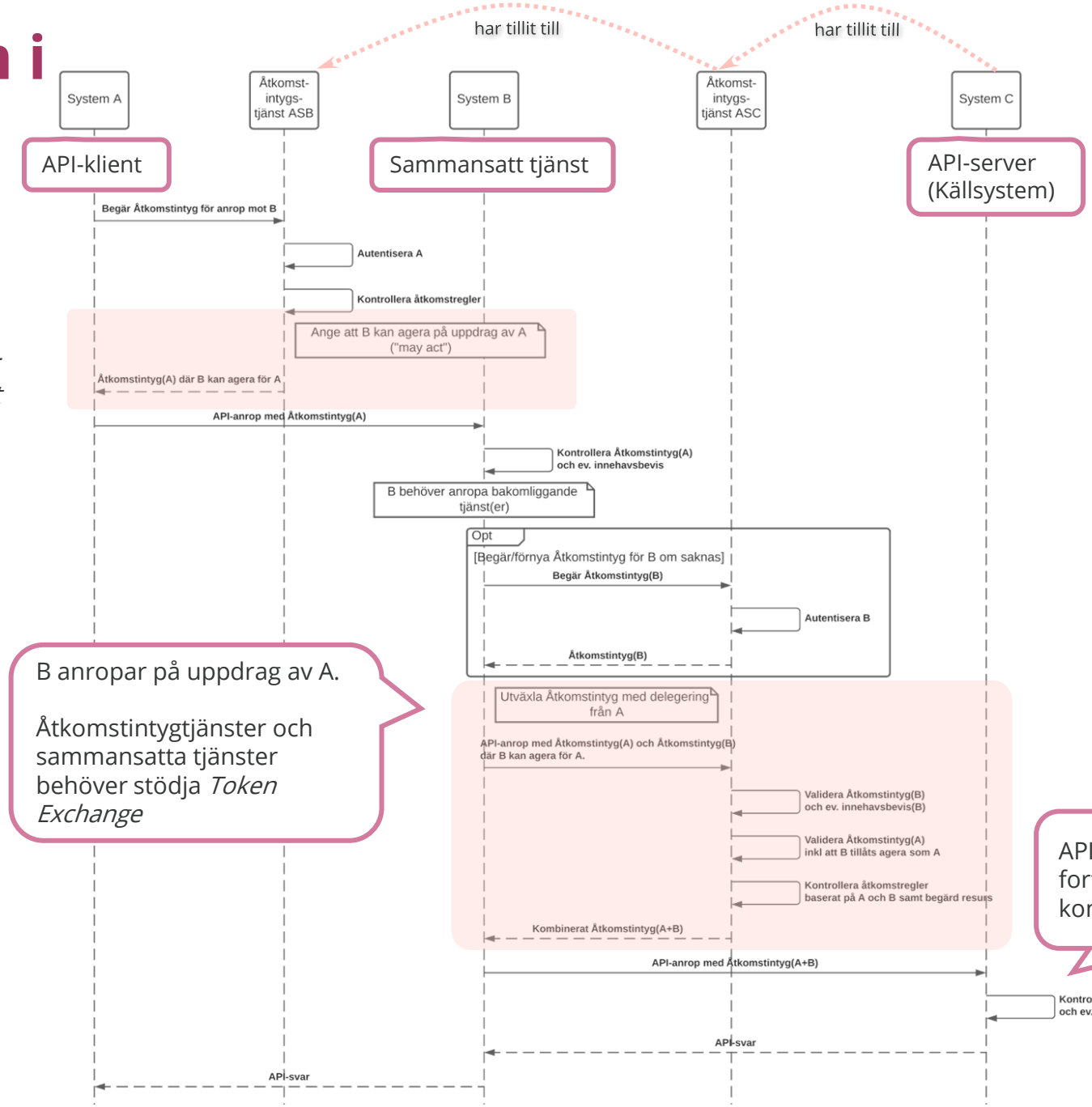
inera

System-till-system i flera led

Autentisering och auktorisation för **sammansatta tjänster** med hjälp av delegering

Sammansatt tjänst - API som i sin tur hämtar data från andra API:er och sammanställer ett svar

RFC8693 Token Exchange



Referensarkitektur Identitet och åtkomst

Autentisering och auktorisation av system

Regelverks-administration

Identitets- och behörighets-administration

Regelverkstjänst
Authorization rules service

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Federation
Federationsoperatör
Federation operator

Medlemsregister | Metadatatjänst | Tillitsramverk | Attribut | Godkännandeprocess

Principer för hur **etablera tillit** till och mellan system, registrering och nyckelhantering

Olika mönster för **säker system-system-kommunikation**

Åtkomstintygstjänst
Token service

Åtkomstintyg

Konsolidera åtkomsthanteringen med Åtkomstintygstjänst

Ökad skalbarhet med **attribut** för system

Legitimeri
Identity Provi

Identitet utfärdare
Identity As

Autentiseringstjänst(er)
Authentication services

E-tjänster
Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

E-legitimering

An
Kli
Use
Use

e-id

Säker API-åtkomst med **åtkomstintyg**

Stärkt säkerhet med **innehavsbevis**

Säkra API-anrop i flera led för sammansatta tjänster

E-legitimationsutfärdare
eID issuer

Utfärdande

Tack!

Mer information om Referensarkitektur för Identitet och åtkomst (IAM) på
www.inera.se

www.rivta.se

inera
Ett företag inom SKR

Referensarkitektur för Identitet och åtkomst (IAM)

Autentisering och auktorisation av användare

www.inera.se

inera
Ett företag inom SKR

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare Klient
User
User agent

e-id

Utfärdande

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister

Metadatatjänst

Tillitsramverk

Attribut

Godkännandeprocess

Regelverks-
administration

Regelverkstjänst
Authorization rules service

Identitets- och
behörighets-
administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster
Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare
Klient
User
User agent

e-id

Utfärdande

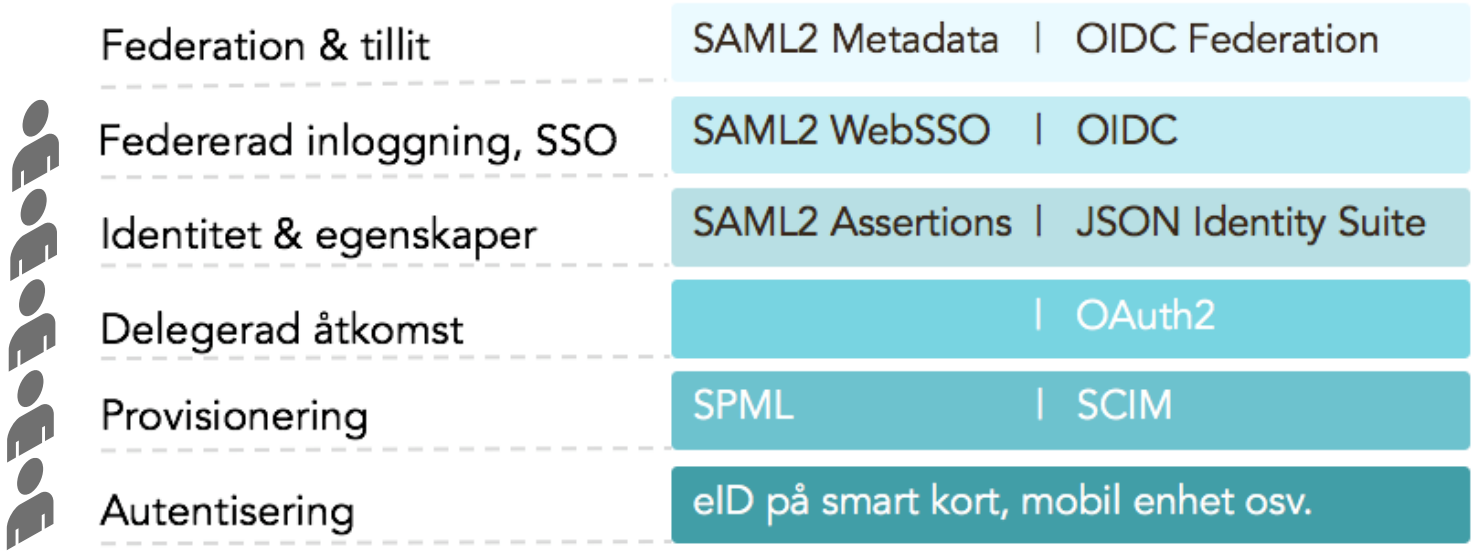
API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur för Identitet och åtkomst (IAM)

Autentisering och auktorisation av användare



autentisering– kontroll av uppgiven identitet

auktorisation *- avgöra om en aktör (användare eller system) har rättighet till viss information och/eller funktion*

e-legitimation, e-id *– elektronisk id-handling*

inera

Autentisering av användare

Legitimeringstjänst, autentiseringstjänst och identitetsdata

inera

Autentisiering av användare

Grundläggande principer

- En användare kan t.ex vara en **medarbetare** i en verksamhet eller en **invånare** i Sverige
- En autentisering omfattar kontroll av en eller flera oberoende **autentiseringsfaktorer**
  ”något man har”, ”något man vet”, ”något man är” (biometri).
- Tillitsramverket för kvalitetsmärket Svensk e-legitimation definierar de **tillitsnivåer** som kan och bör användas för att bedöma styrkan i autentiseringen, exempel:
  - **Tillitsnivå 2**: krav på tvåfaktorsautentisering och viss tillit till identiteten, t.ex. genom att en kod skickas i kodkuvert till sökandens folkbokföringsadress
  - **Tillitsnivå 3**: krav på tvåfaktorsautentisering, och identiteten verifieras på likvärdigt sätt som vid utgivning av en fullgod svensk legitimationshandling

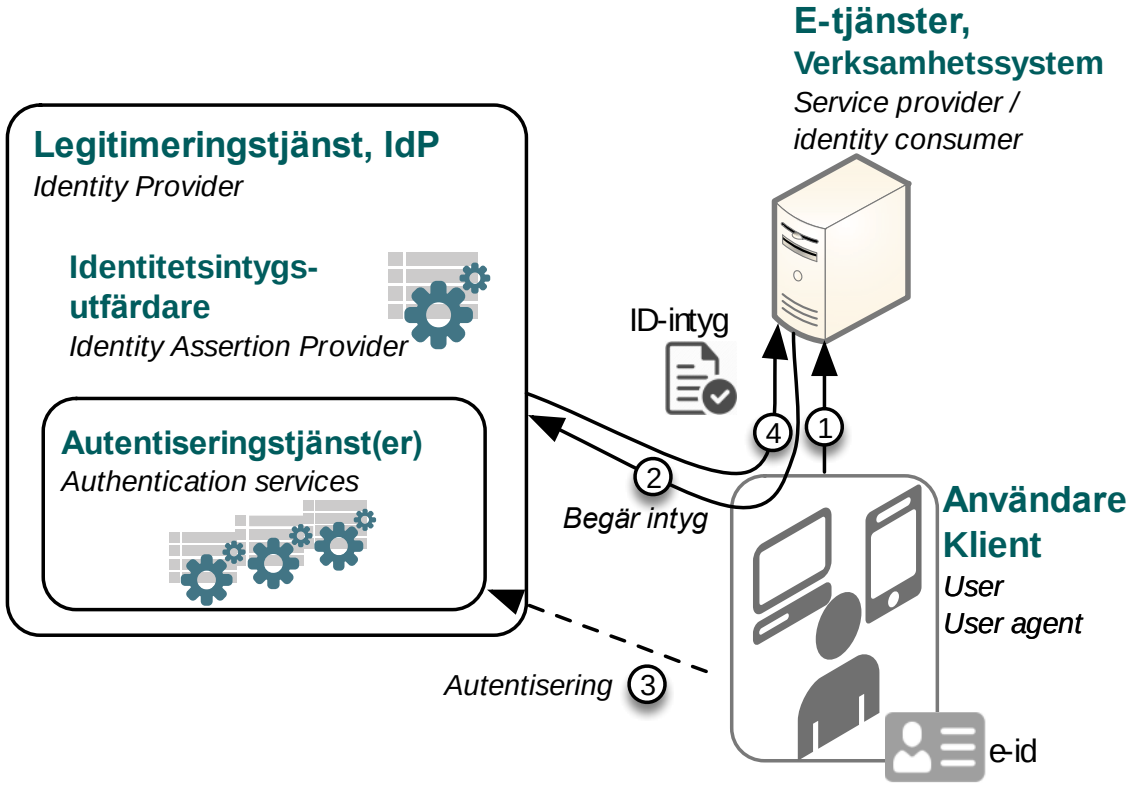
Exempel på tvåfaktorautentisering: ditt fingeravtryck SAMT innehav av en skyddad e-legitimation på en personlig mobil enhet

inera

Legitimeringstjänst (IdP)

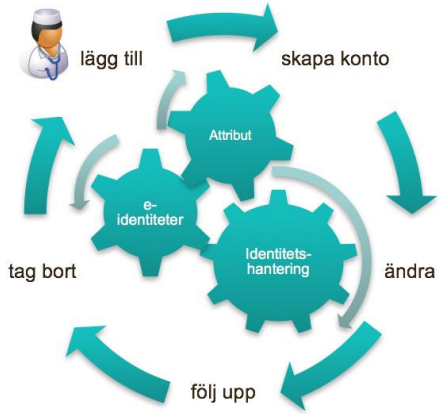
”Navet” i IT-infrastrukturen för identitet- och åtkomst

- Legitimeringstjänsten **identifierar och autentiserar användaren** på begäran av e-tjänsten
- E-tjänsten kan kräva att autentiseringen möter en viss **tillitsnivå**
- Legitimeringstjänsten utfärdar **identitetsintyg** vid godkänd autentisering
- E-tjänsten ansvarar för **utloggning** ur e-tjänsten
- Möjlighet till **singelinloggning** (SSO)
- **Standardprotokoll** för integration med e-tjänster
  - SAML2
  - OpenID Connect

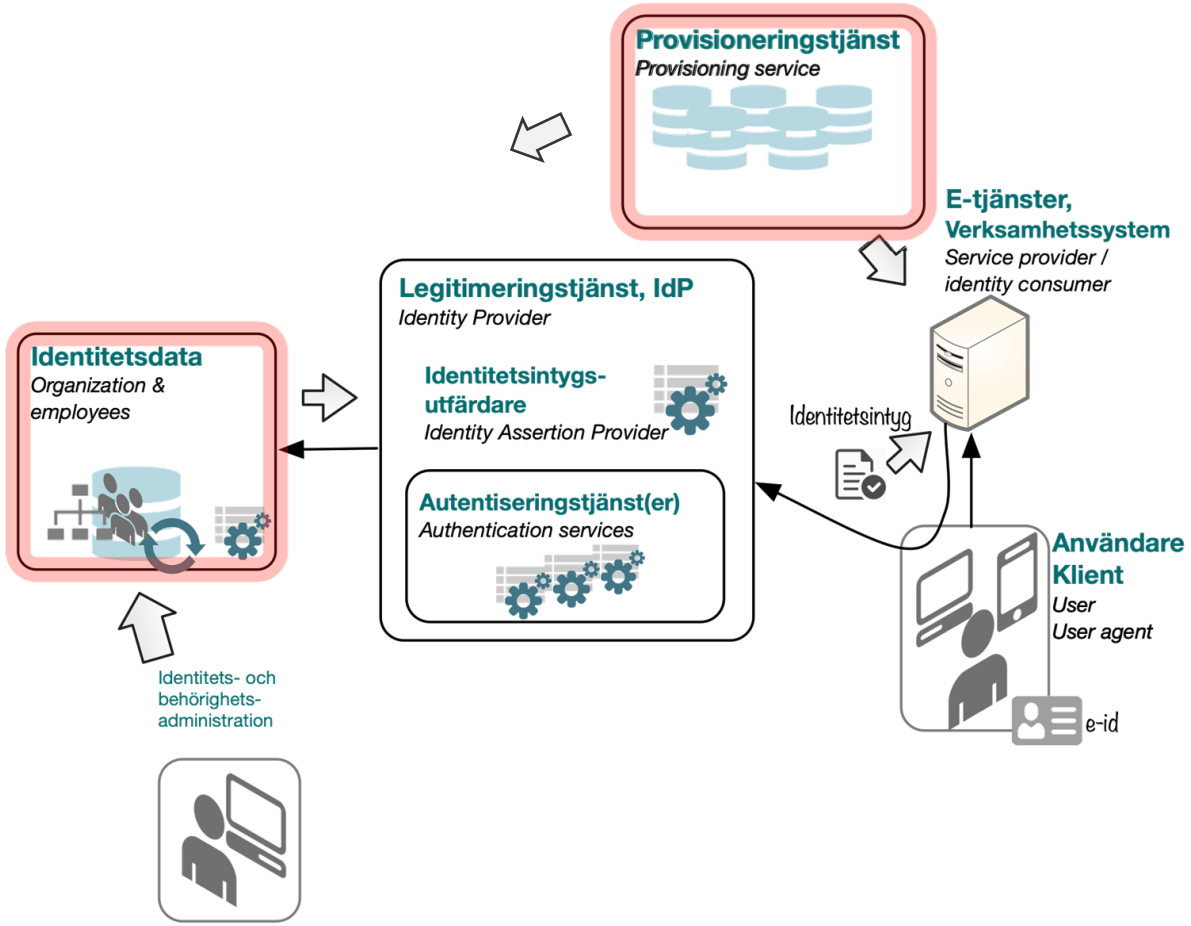


Identitetsdatalager och provisionering *Livscykelhantering och kvalitetssäkring av identitetsdata*

- Identitetsintyg – signerade egenskaper/attribut ifrån **identitetsdatalager** (attributkälla)
  - Personliga (*personnummer, namn*)
  - Anställningsrelaterade (*tjänste-id, organisation*)
  - Uppdragsrelaterade (*uppdrag för organisation*)
- **Provisionering** av identitetsdata
  - från flera källsystem till identitetsdatalagret
  - till e-tjänsten för att skapa användarkonton



Livscykelhantering och kvalitetssäkring av data



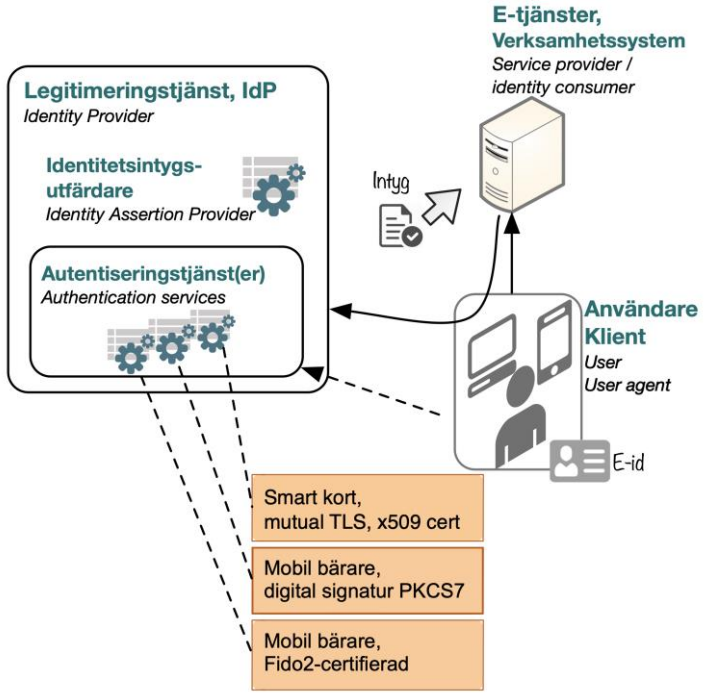
inera

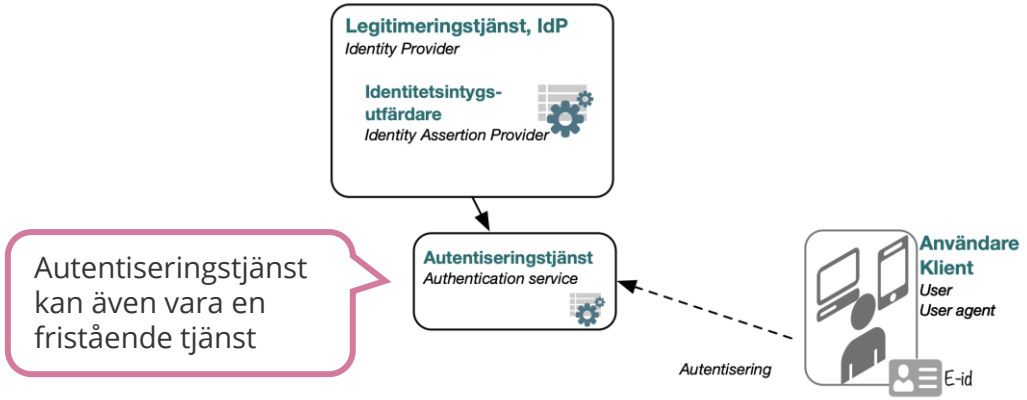
Legitimeringstjänst (IdP)

Autentisieringstjänsterna ger stöd för olika tekn

- Legitimeringstjänsten kan tillhandahålla flera autentiseringsmetoder och för det nyttja olika autentiseringstjänster och teknik

  → Ny autentiseringsteknik kan införas i verksamheten **utan att ändra integrationen** med e-tjänsterna



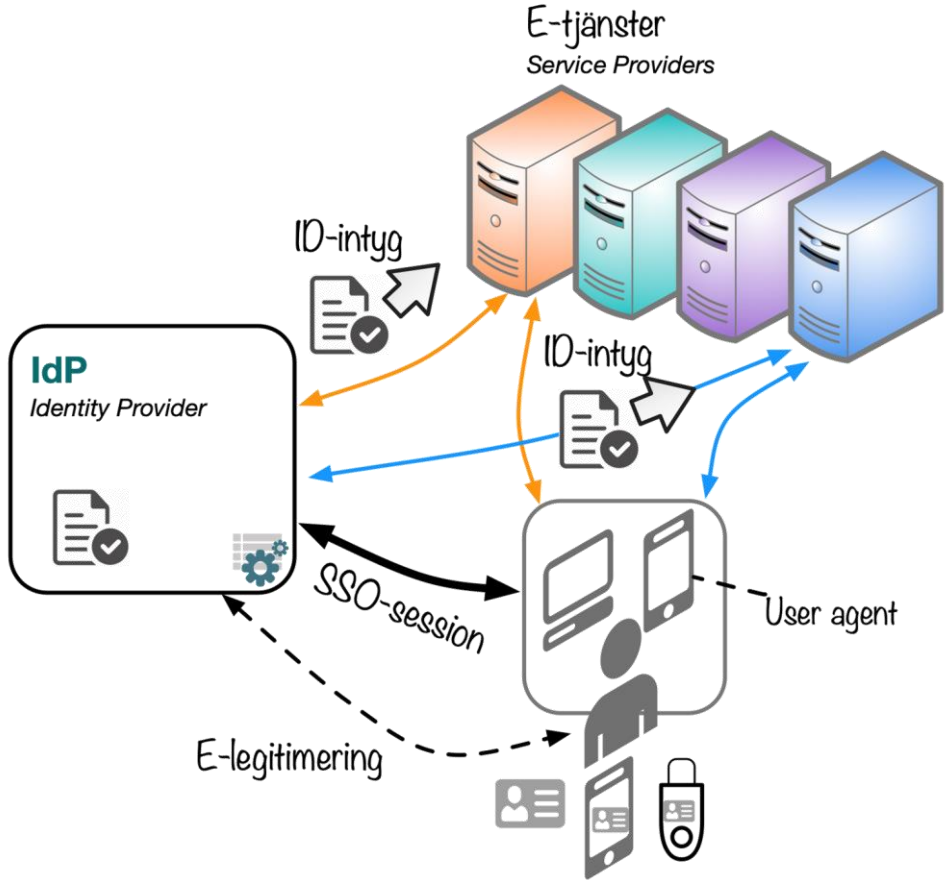


inera

Legitimeringstjänst (IdP)

Singelinloggning (SSO) styrs via IdP och e-tjänsten själv

- IdP etablerar en **SSO-session** mot användarens klient efter godkänd autentisering
- Om giltig SSO-session finns med användarens klient kan nytt identitetsintyg utfärdas utan ny autentisering av användaren
- Hur länge SSO-sessionen gäller sätts i IdP utifrån verksamhetskrav
- Användaren - via e-tjänsten - kan närsomhelst avsluta SSO-sessionen
- E-tjänsten kan välja **tvingande e-legitimering** (forced authentication) för att inte nyttja SSO om behov finns



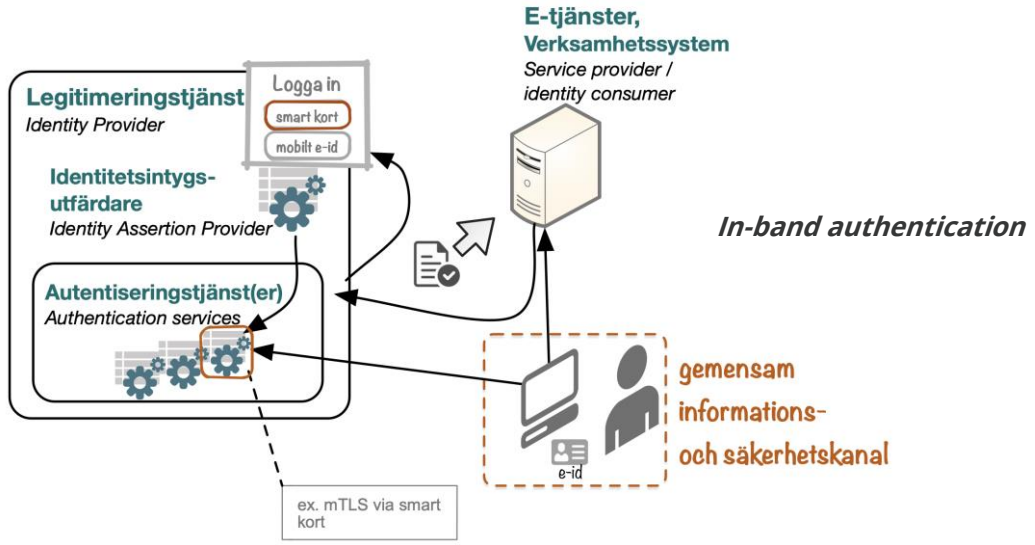
Legitimeringstjänst (IdP)

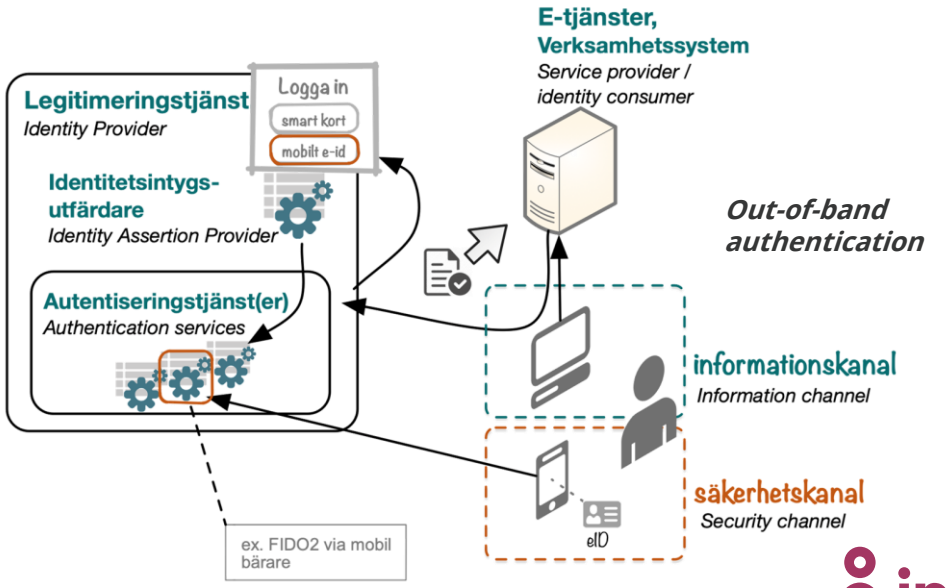
Autentisering in-band och out-of-band

Styrande princip:

Autentisering ska (vid behov) kunna ske i separat säkerhetskanal skild ifrån informationskanalen, även kallad ***out-of-band authentication***

→ lös koppling mellan klienten, e-tjänsten och autentiseringslösningen (e-leg)
→ möjliggör autentisering mot utrustning/system som saknar möjlighet att ansluta extra hårdvara osv.
→ underlättar mobilitet
→ möjliggör att använda e-leg på nya typer av bärare



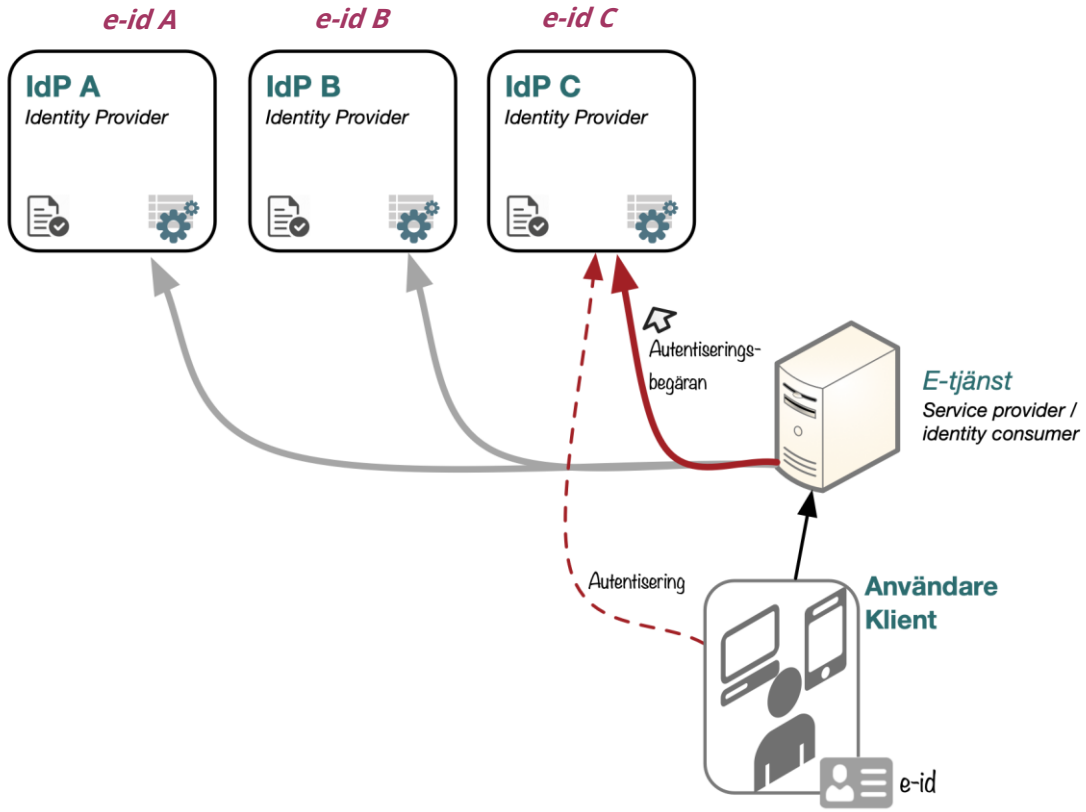


inera

Legitimeringstjänst (IdP)

Att använda flera IdP:er från en och samma e-tjänst

- En e-tjänst kan få stöd för inloggning med flera olika typer av e-legitimationer som hanteras av olika IdP:er
- I federativa sammanhang kan e-tjänst erbjuda inloggning via respektive organisations egna IdP

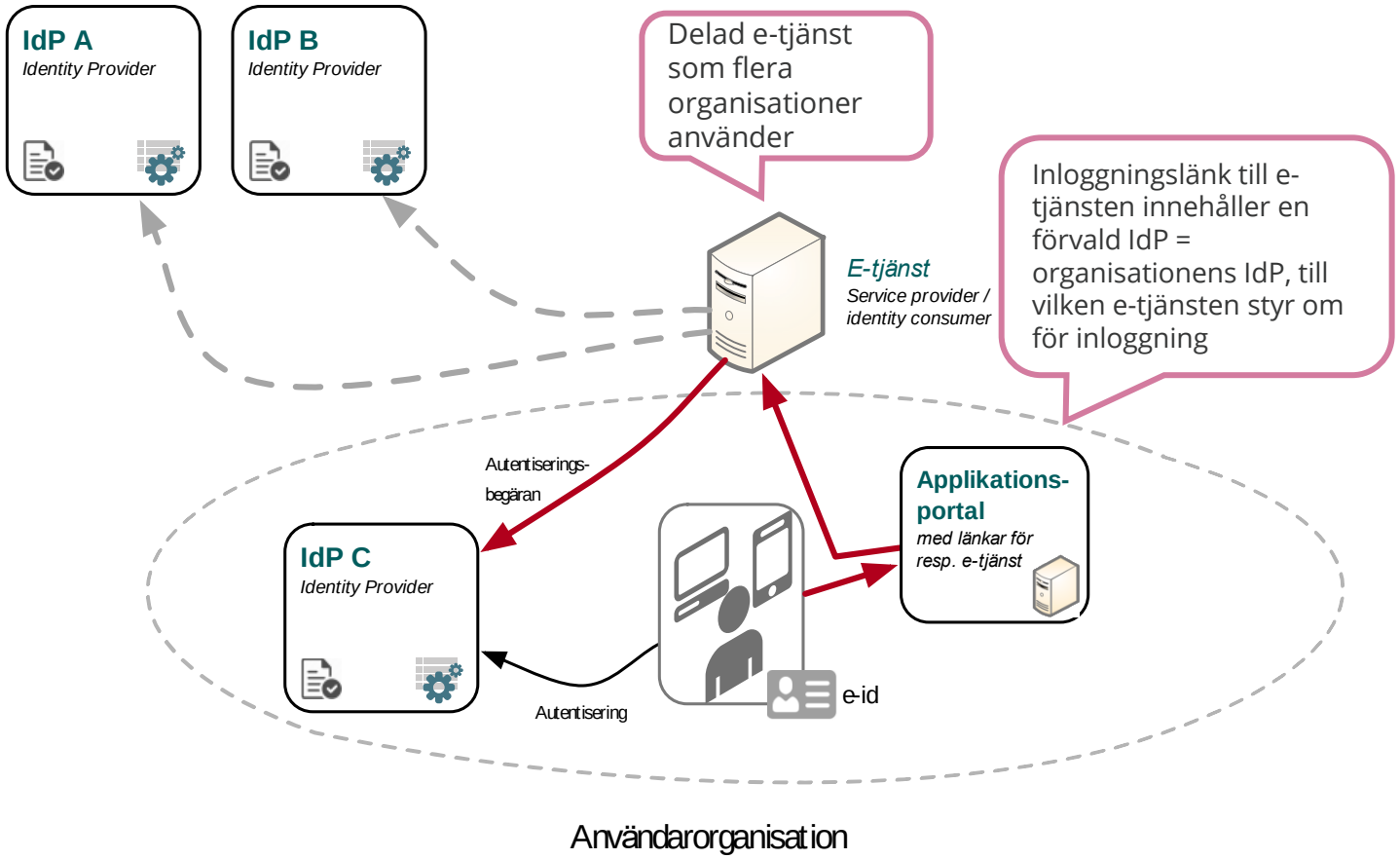


Legitimeringstjänst (IdP)

Hur väljs IdP i det aktuella fallet?

Referensarkitekturen pekar ut mönster man kan använda för val av IdP:

1. E-tjänsten **implementerar val av IdP** och presenterar valet för användaren
2. E-tjänsten nyttjar en **Anvisningstjänst** som realiserar en gemensam funktion för att välja IdP
3. Organisationen ger användarna **inloggningslänkar** till e-tjänsten med **förvald IdP** = organisationens egna legitimeringstjänst

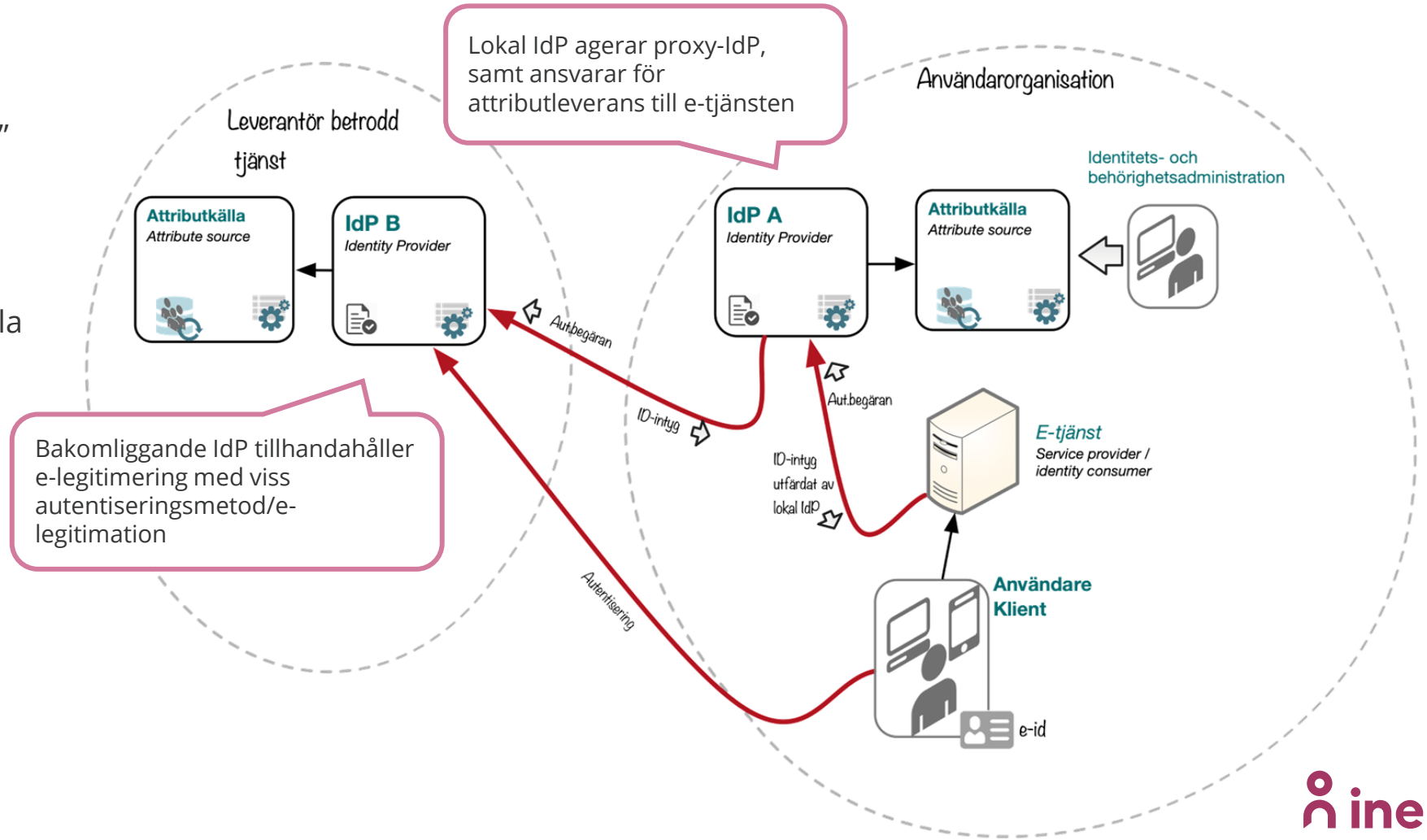


Legitimeringstjänst (IdP)

Mönstret proxy-IdP för att ansluta ytterligare IdP:er

Ge tillgång till fler IdP:er bakom den lokala IdP-tjänsten som agerar ”proxy”

Den lokala IdP-tjänsten kan tillhandahålla lokala autentiseringsmetoder, hålla ihop användarupplevelsen och ge möjlighet till SSO

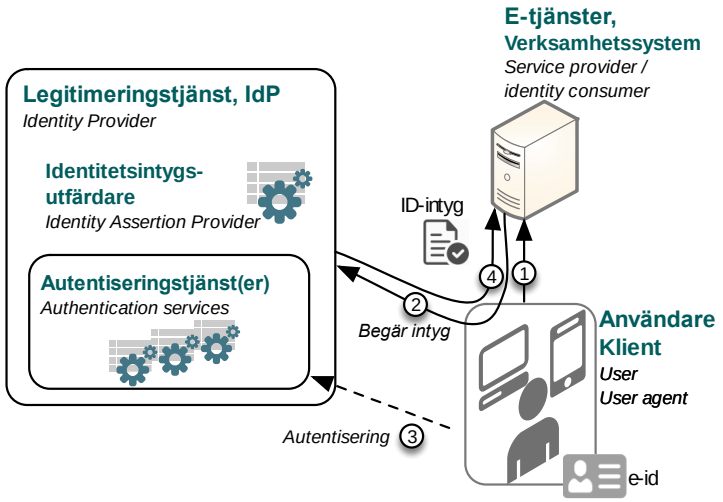


Legitimeringstjänst (IdP)

Utfärdande och förmedling av identitetsintyg

ombedda intyg (solicited assertions) – ***bör användas***

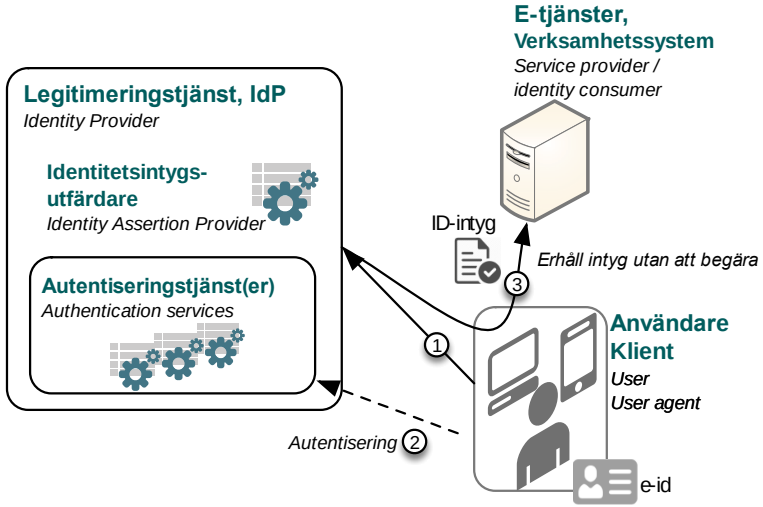
Användaren väljer att logga in i e-tjänst (1).
E-tjänsten (*Service Provider, SP*) skickar en **autentiseringsbegäran** till IdP (2) och anger vilka attribut som den behöver, och får efter autentiseringen (3) ett ID-intyg i retur (4)



oombedda intyg (unsolicited assertions)

Användaren använder en anpassad länk (1) som först går till önskad IdP, och efter autentiseringen (2) styrs användaren vidare till e-tjänsten (3). E-tjänsten får ett ID-intyg **utan** föregående begäran

Stödjer inte djuplänkning, försvårar uppgiftsminimering, brister i standardisering och stödet i tekniska ramverk



inera

Auktorisation av användare

Styra och kontrollera användarens rättigheter för åtkomst till information och resurser

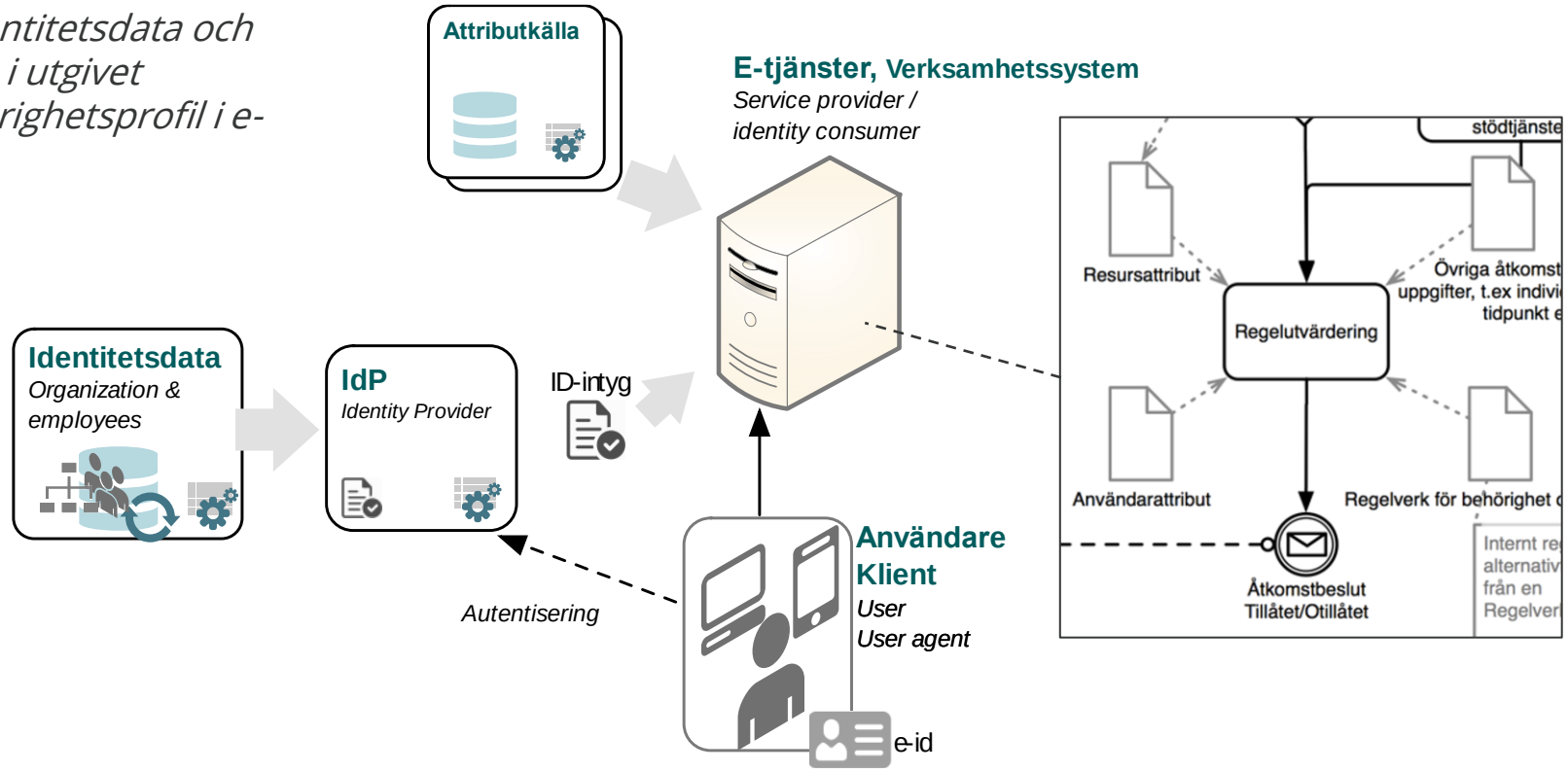
inera

Användares åtkomst till resurser

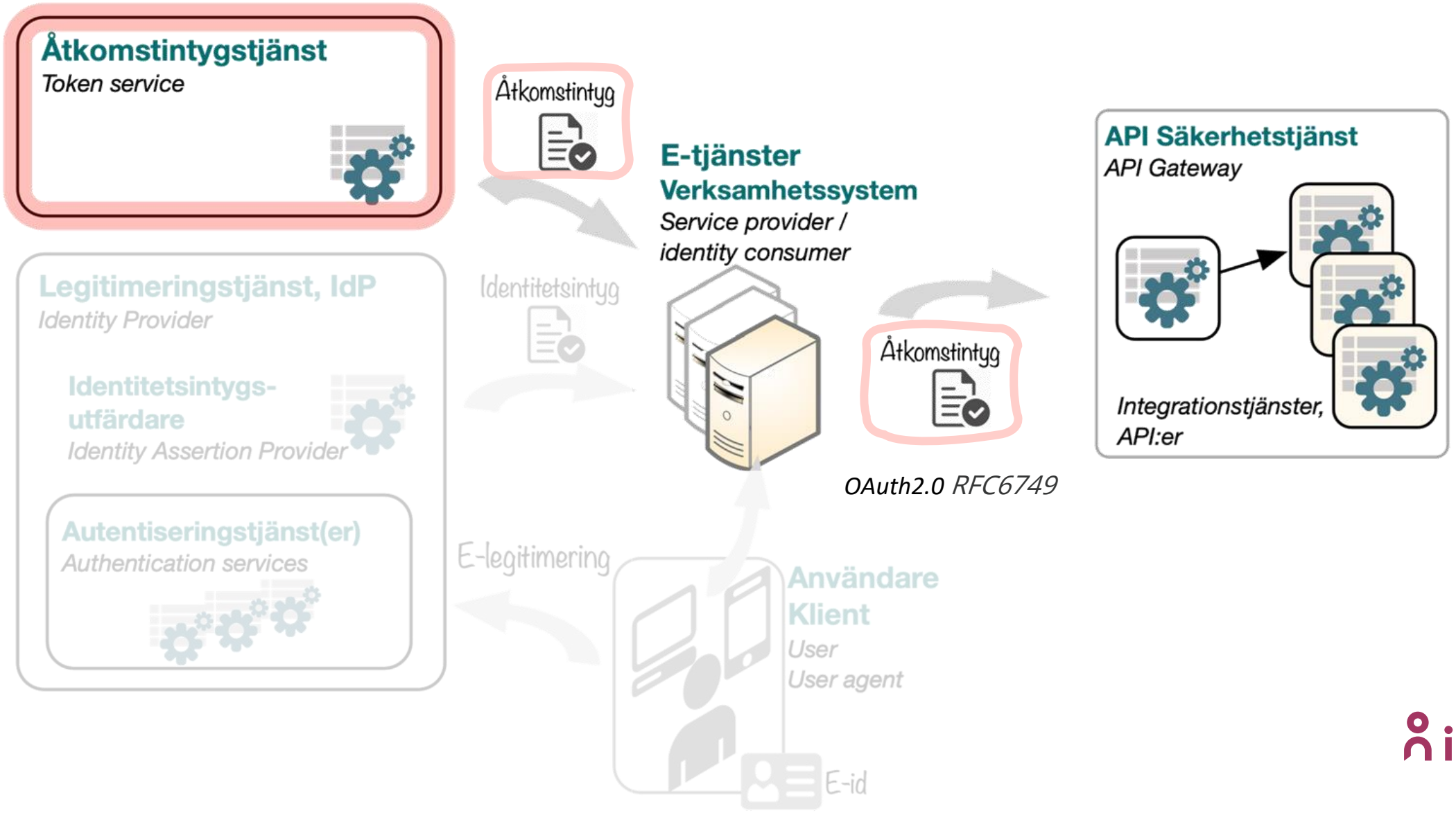
Styrande princip

”e-tjänster använder federerade identitetsdata och behörighetsgrundande information i utgivet identitetsintyg som bas för en behörighetsprofil i e-tjänsten…”

- E-tjänsten (verksamhetssystemet) ansvarar för att implementera åtkomstkontrollen
- Identitetsdata och ev. behörighetsgrundande information i ID-intyget utgör grund för en behörighetsprofil
- E-tjänsten kompletterar efter behov med andra uppgifter för att avgöra användarens rättigheter
- Möjliggör attributsbaserad behörighetsstyrning

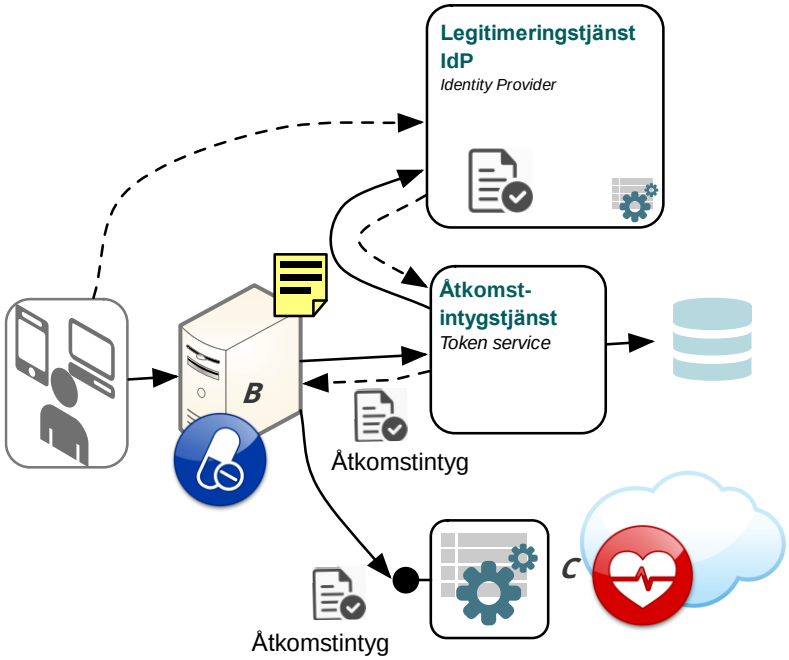


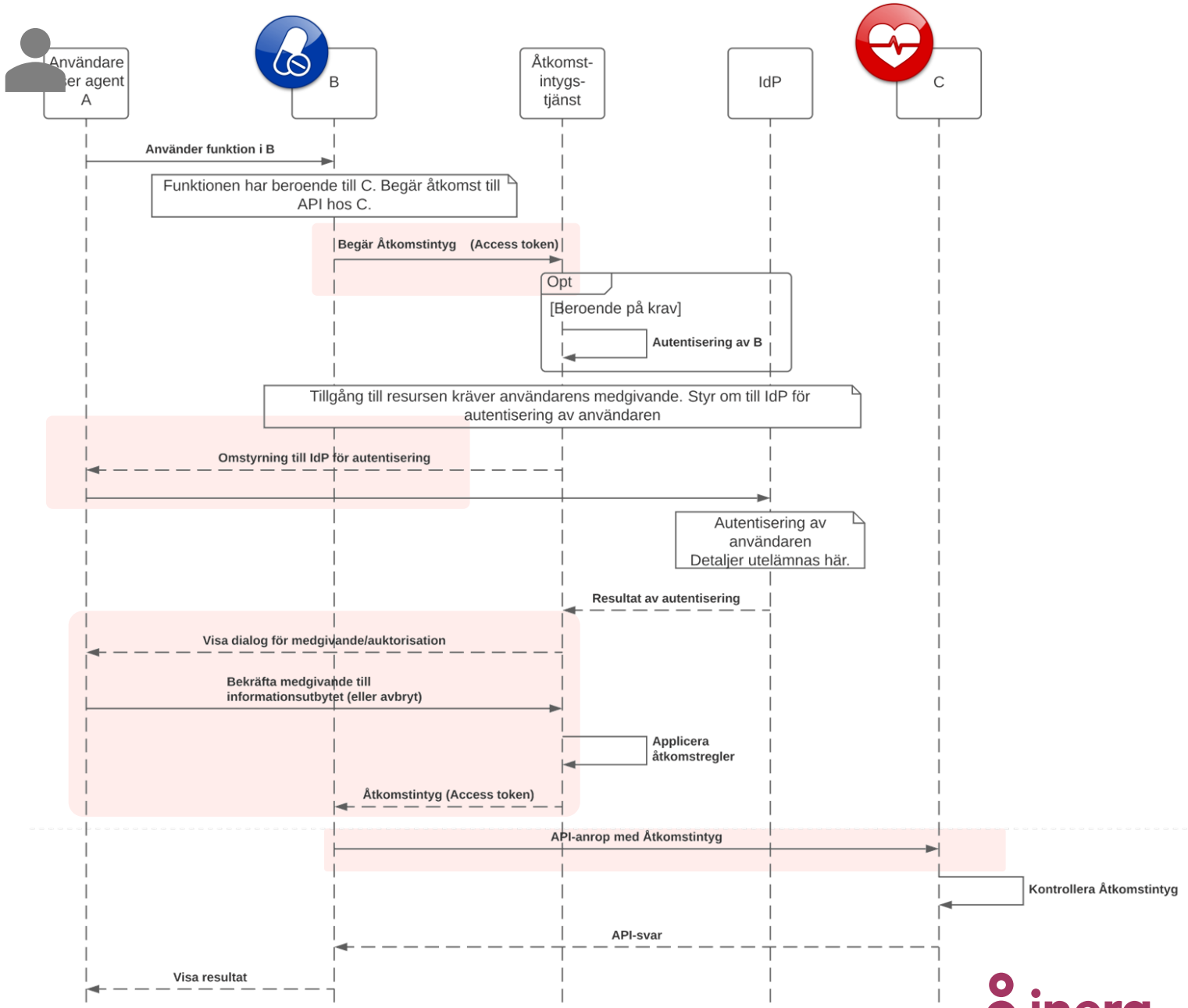
Åtkomstintyg för effektiv och säker API-åtkomst



API-åtkomst: Delegering av användarens rättigheter till en ”app”

Användaren (A) auktoriserar en app (B) att hämta/publicera data hos API (C)



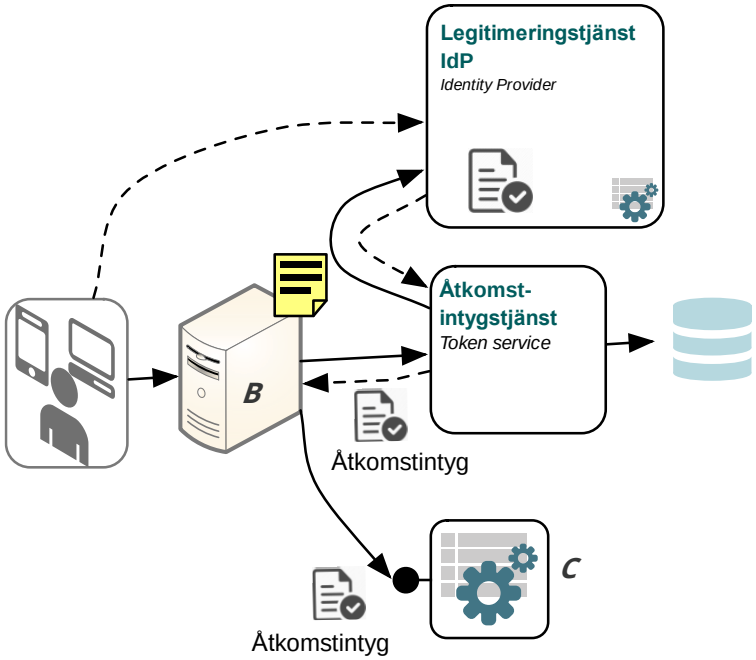


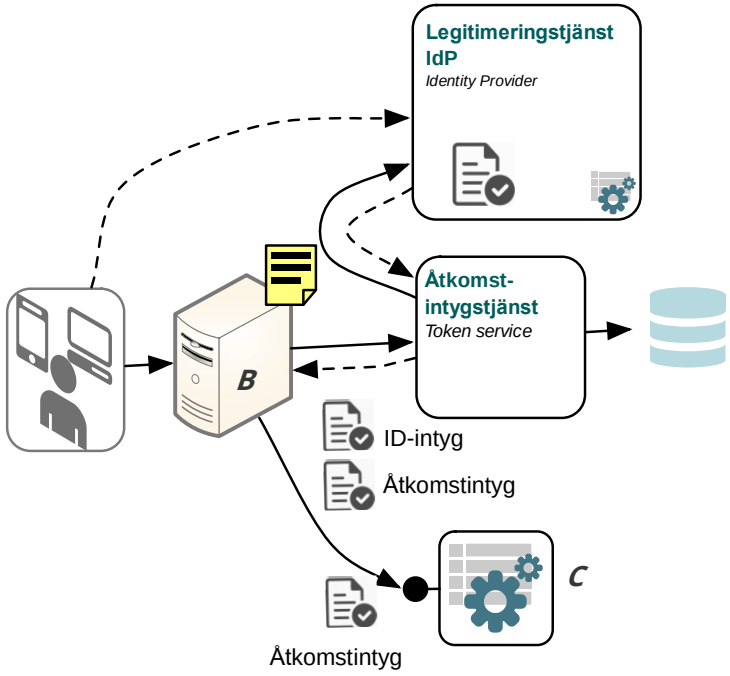
OAuth2.0 RFC6749

inera

API-åtkomst: Delegering av användarens rättigheter till en ”app”

Det går även att utfärda åtkomstintyg + identitetsintyg direkt i samband med inloggningen till e-tjänsten/appen:





Kombinera med åtkomstintyg för appen B, så att rättigheten också beror på vilken app som används (RFC8693 Token Exchange)

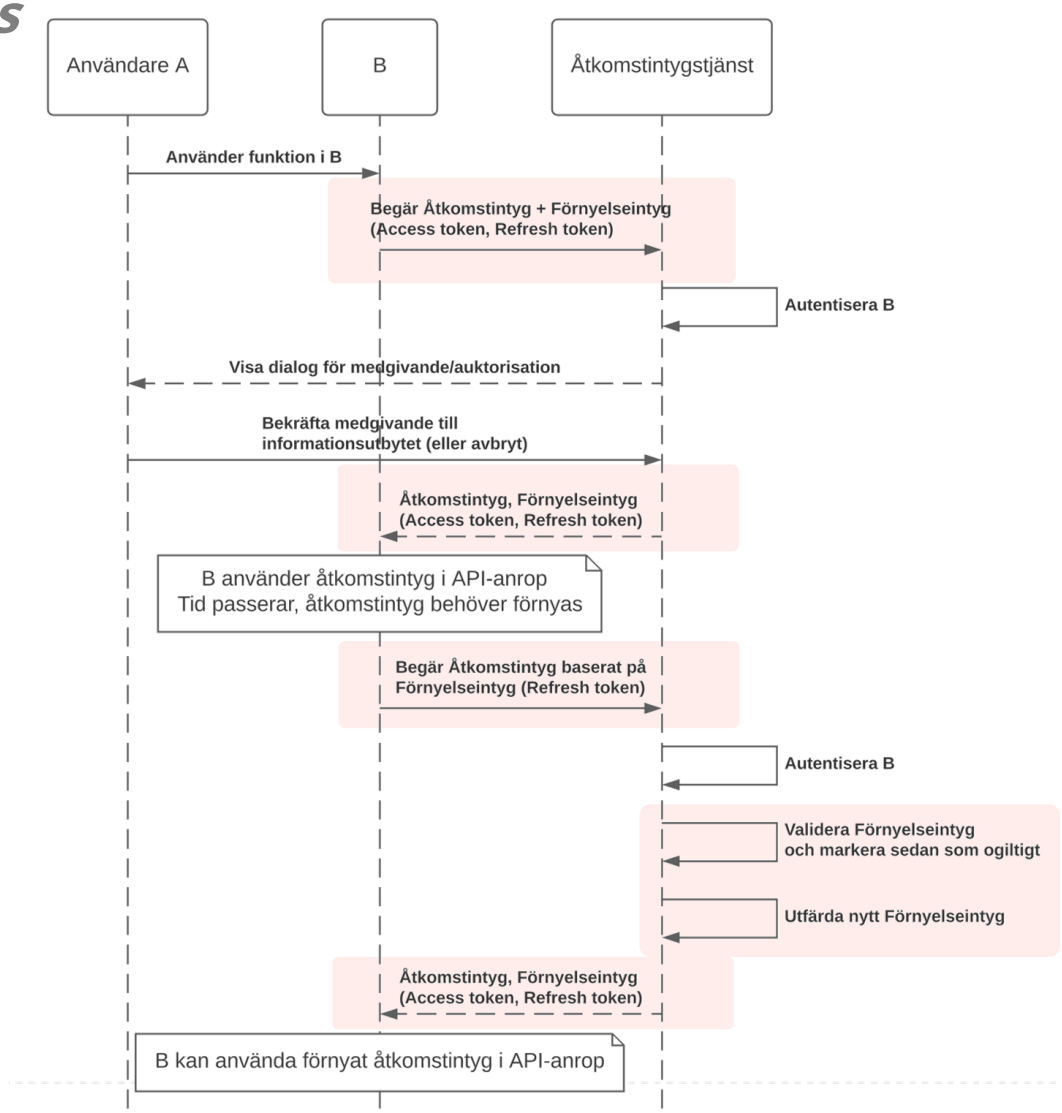
Förnya åtkomstintyget

utan att användaren behöver autentiseras igen

Förnyelseintyg (*Refresh tokens*)

Förläng en auktorisation genom att förnya åtkomstintyget
– användaren behöver inte lika ofta återautentiseras (legitimera sig)

Förnyelseintyg är engångs med begränsad giltighetstid.
Överförs endast över autentiserad och krypterad kommunikation mellan samma klient och den betrodda Åtkomstintygstjänsten.

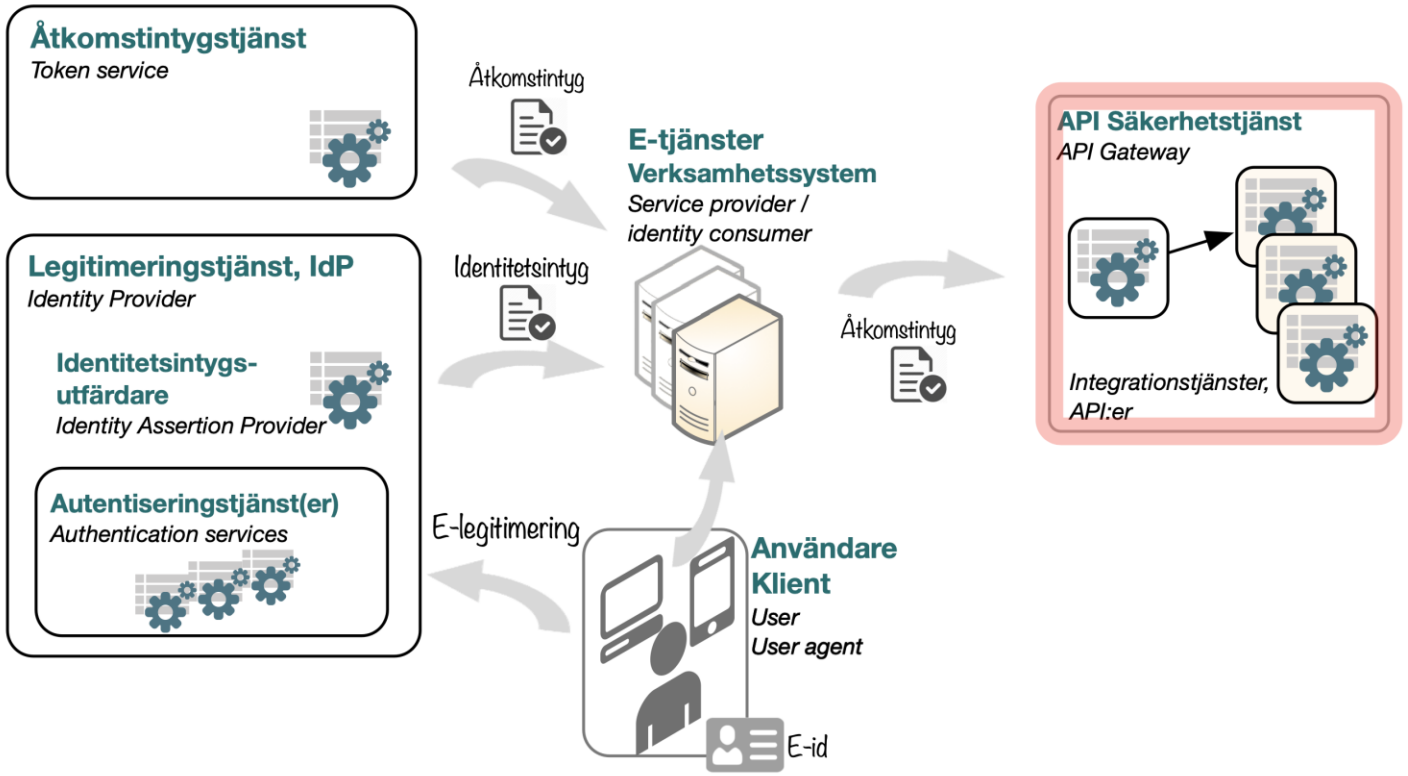


API Säkerhetstjänst (API Gateway)

konsolidera säkerhetslagret för alla API-servrar

API Säkerhetstjänst kan ansvara för

- **autentisering** av anropande system
- hantera **åtkomstintyget**, giltighet och omfattning
- ev. **mellanlagra** resultat för effektiv återanvändning



API Säkerhetstjänst agerar gemensamt säkerhetslager för skydd av flera integrationstjänster (API:er)

inera

Referensarkitektur Identitet och åtkomst

Autentisering och auktorisation av användare

Federation
Federationsoperatör
Federation operator
Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

E-tjänsten ansvarar för **åtkomstkontroll**
Möjlighet till **attributbaserad** behörighetsstyrning

Användar-administration

IdP är ”navet” för identifiering och autentisering för användare, utfärdar identitetsintyg och möjligör SSO

Flera anslutningsmönster

Åtkomstintygstjänst
Token service

Åtkomstintyg

E-tjänster
Verksamhetssystem
Service provider / identity consumer

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Identitetsintyg

Åtkomstintyg

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Livscykelhantering och kvalitetssäkring av **identitetsdata**

E-legitimering

Användare
Klient
User
User agent

e-id

Säker API-åtkomst med åtkomstintyg.
Ge appar rättigheter för att hämta/skriva användarens data

Konsolidera kontrollen med Åtkomstintygstjänst och API Gateway

Provisioneringstjänst
Provisioning service

Inför **autentiseringsteknik** med minimal påverkan på systemintegrationer
”Out-of-band” och ”in-band”

E-leg
eID issu

Utfärdande

Tack!

Mer information om Referensarkitektur för Identitet och åtkomst (IAM) på
www.inera.se

www.rivta.se

inera
Ett företag inom SKR

Referensarkitektur för Identitet och åtkomst (IAM)

Federation

federation (federation) *– överenskommelse mellan parter där man inom federationen har gemensamma regler och att parterna litar på varandra att upprätthålla dessa regler. Inom identitets- och åtkomsthantering avses oftast en* ***identitets- och behörighetsfederation***

www.inera.se

inera
Ett företag inom SKR

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare Klient
User
User agent

e-id

Utfärdande

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Refe
Ider

Federera identitet och behörighetsgrundande attribut **mellan organisationer** (medlemmar) via identitetsintyg från betrodda tjänster

Skala upp samverkan till **många parter och tjänster**

Federation
Federationsoperatör
Federation operator

Medlemsregister

Metadatatjänst

Tillitsramverk

Attribut

Godkännandeprocess

Gemensam metadata – digitalt signerad information (publika nycklar mm) om anslutna tjänster som kan hämtas av alla parter

Gemensam syn på tillit till autentiserings-lösningar och säkerhetsrutiner via **tillitsramverk** och process för godkännande

Gemensamma definitioner för identitet och tillhörande attribut

Regelver
administ

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla

Åtkomstintygstjänst
Token service

intyg

Legitim
Identity

Identitet utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

E-legitimering

Användare
Klient
User
User agent

e-id

E-legitimationsutfärdare
eID issuer

Utfärdande

Styrande princip

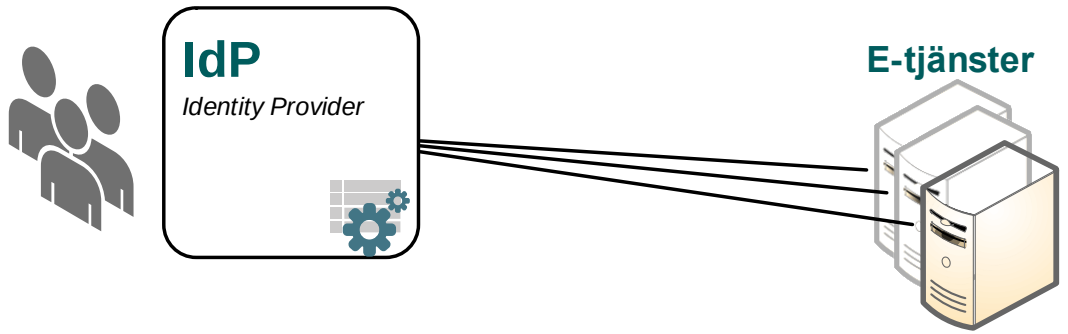
Samverkan över organisationsgränser sker genom federation, exempelvis via identitetsfederation

Tillit till andra organisationers IT-lösningar för identitet och åtkomst skapas via öppna gemensamma regelverk, s.k. tillitsramverk

Federation

Grundidé

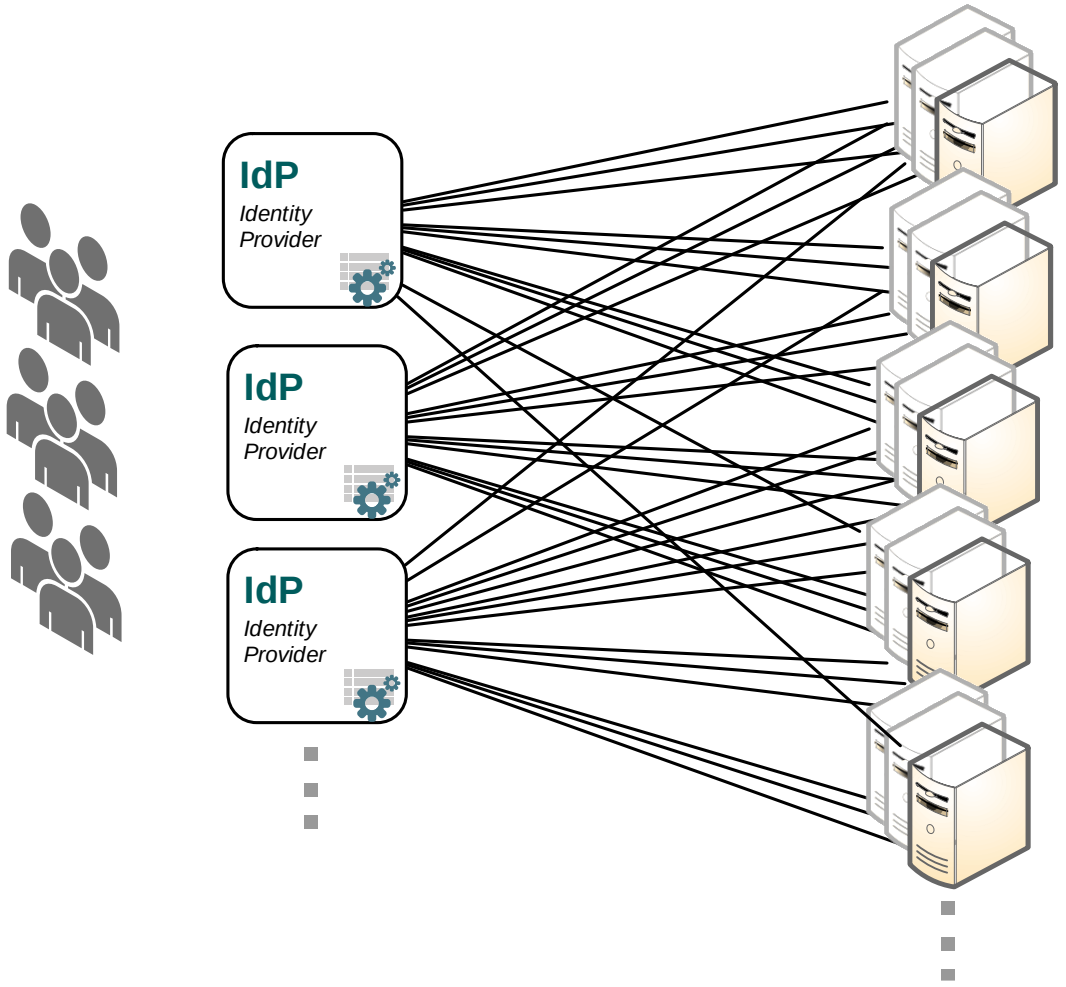
Enkelt att etablera tilliten mellan tjänsterna med få parter och tjänster…



Federation

Grundidé

Mer utmanande om det ska fungera i helt ekosystem…

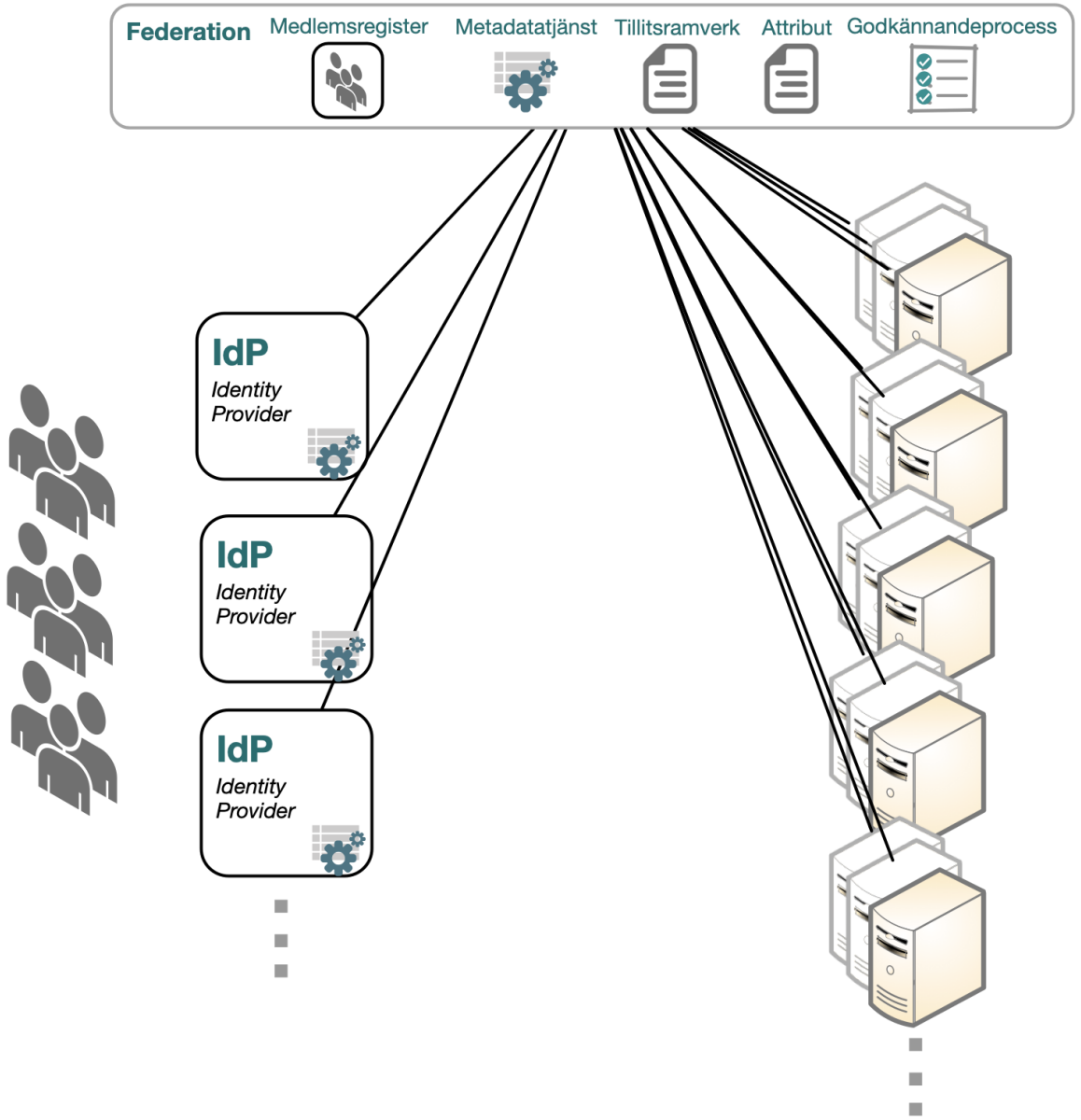


inera

Federation

Grundidé

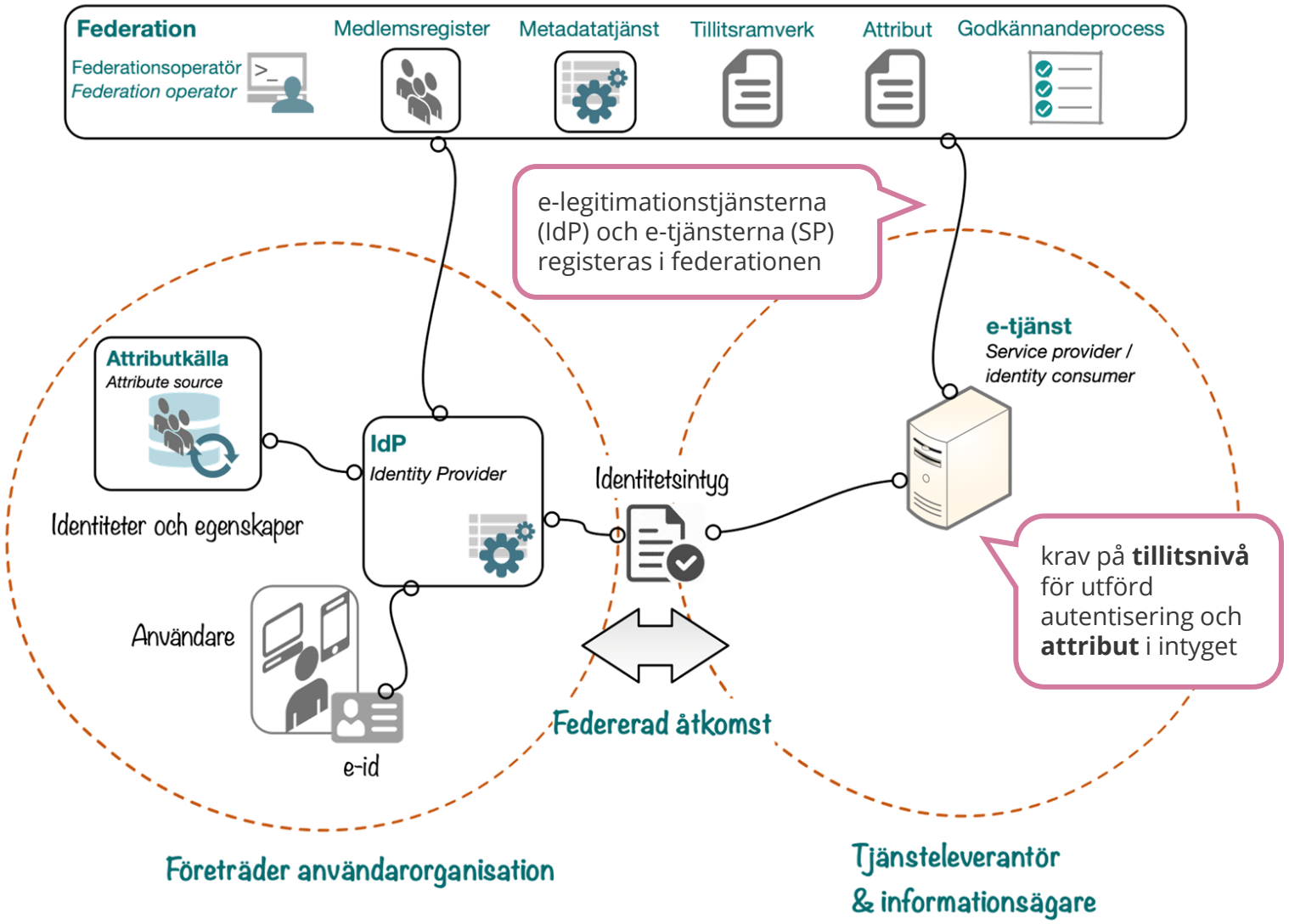
Med **federationen som tillitsnav** ansluts varje part och tjänst **en gång**



inera

Identitets- och behörighetsfederationer

Mönster och mekanism



Identitets- och behörighetsfederationer

Några nyttoeffekter

Varje part kan hantera sina medarbetare (på/avanställning, egenskaper osv)
– **minskar administrationen** och **underlättar att dela e-tjänster**

Organisationen kan använda sin **ordinarie IT-infrastruktur** för inloggning och identifiering

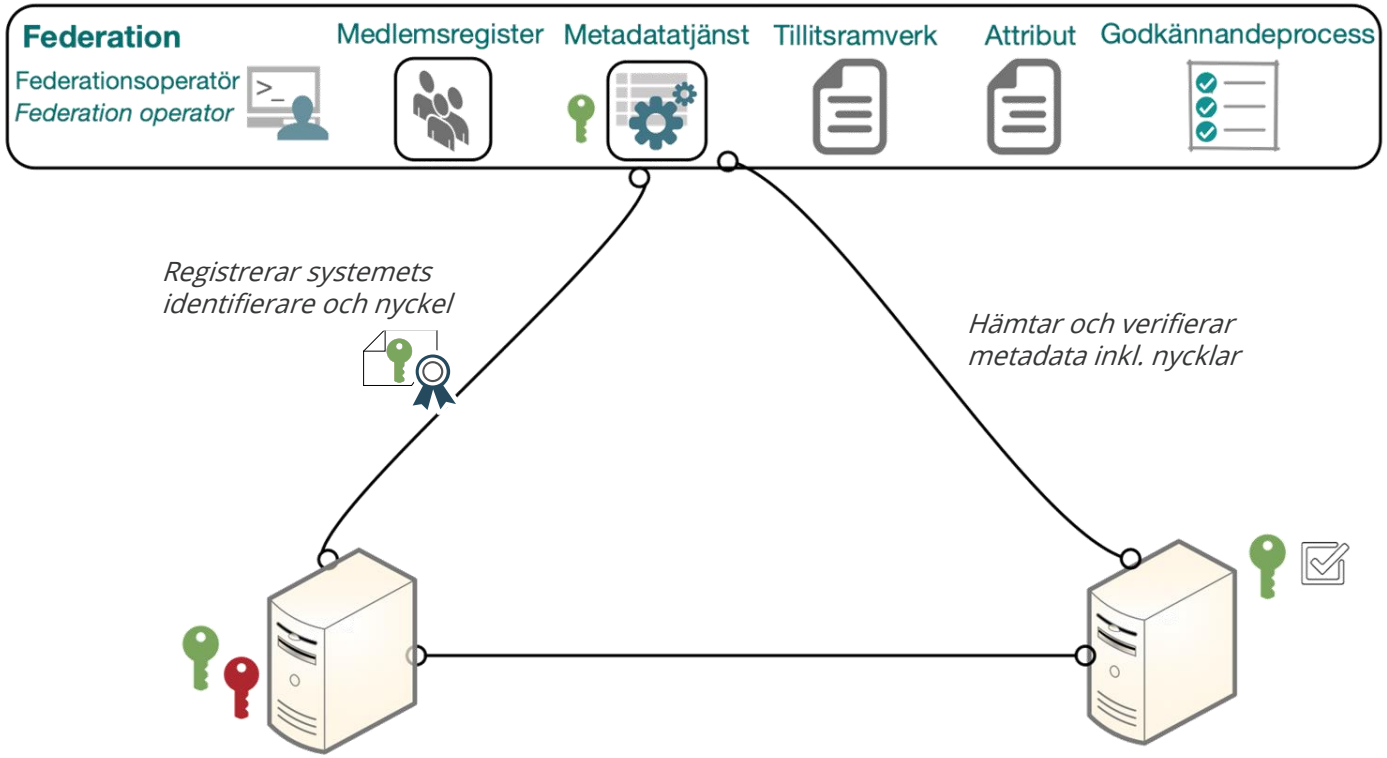
Behöver inte ”uppfinna” eget **ramverk och processer** för att godkänna säkerhetslösningar och andra parter att kommunicera med – använd nationella tillitsramverk!

Federationen och dess metadata underlättar **nyckelutbyten och etablering av tillit** till alla ingående tjänster
- nyttan ökar med många parter och tjänster

Tillitsramverk för kvalitetsmärket Svensk e-legitimation

Federation för systemåtkomst

Federativ säkerhet för säker system-system-kommunikation (api-åtkomst)

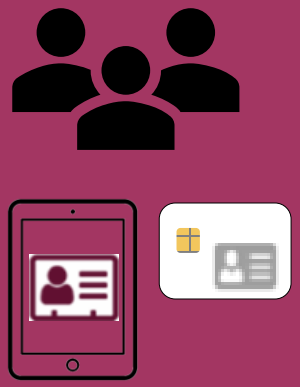


Tack!

Mer information om Referensarkitektur för Identitet och åtkomst (IAM) på
www.inera.se

www.rivta.se

inera
Ett företag inom SKR



Referensarkitektur för Identitet och åtkomst (IAM)

E-legitimationsutfärdare

Utfärdande av e-legitimation (e-id)
- person erhåller en e-legitimation för att använda som hens elektroniska identitetshandling i kommunikationen med digitala system

- *I tjänsten*
- *Privat*

www.inera.se

inera
Ett företag inom SKR

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Provisioneringstjänst
Provisioning service

Åtkomstintygstjänst
Token service

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

E-legitimationsutfärdare
eID issuer

Åtkomstintyg

Identitetsintyg

E-tjänster Verksamhetssystem
Service provider / identity consumer

Åtkomstintyg

E-legitimering

Användare Klient
User
User agent

e-id

Utfärdande

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Stödtjänster för åtkomst
Support services for access control

Referensarkitektur Identitet och åtkomst

Federation
Federationsoperatör
Federation operator

Medlemsregister | Metadatatjänst | Tillitsramverk | Attribut | Godkännandeprocess

Regelverks-administration

Regelverkstjänst
Authorization rules service

Åtkomstintygstjänst
Token service

Åtkomstintyg

E-tjänster
Verksamhetssystem

API Säkerhetstjänst
API Gateway

Integrationstjänster, API:er

Identitets- och behörighets-administration

Identitetsdatalager, attributkälla
Attribute source

Legitimeringstjänst, IdP
Identity Provider

Identitetsintygs-utfärdare
Identity Assertion Provider

Autentiseringstjänst(er)
Authentication services

Tillitsnivån för e-legitimeringen beror på **säkerhetsnivån i utfärdandeprocessen** och **skyddet för e-legitimationen** på dess bärare

E-legitimering

Användare
Klient
User
User agent

e-id

Stödtjänster för åtkomst
Support services for access control

Utfärdande av e-legitimation som uppfyller **nationellt erkända krav - tillitsnivåer**

E-legitimationsutfärdare
eID issuer

Utfärdande

E-legitimationsutfärdare

Tillitsnivå för utfärdade e-legitimationer

Krav att uppfylla för att en e-legitimation ska uppnå viss **tillitsnivå**:
Tillitsramverk för Svensk e-legitimation

- Nivå 2 (LoA2) – Viss tillit
- Nivå 3 (LoA3) – Hög tillit
- Nivå 4 (LoA4) – Mycket hög tillit

Exempel:

Kod som skickats i kodkuvert till folkbokföringsadressen

Engångslösenord från dosa eller mobiltelefon

Motsvara fullgod id-handling, fysiskt eller på distans

E-id i skyddad app i en smarttelefon

Fullgod id-handling, fysiskt besök enbart

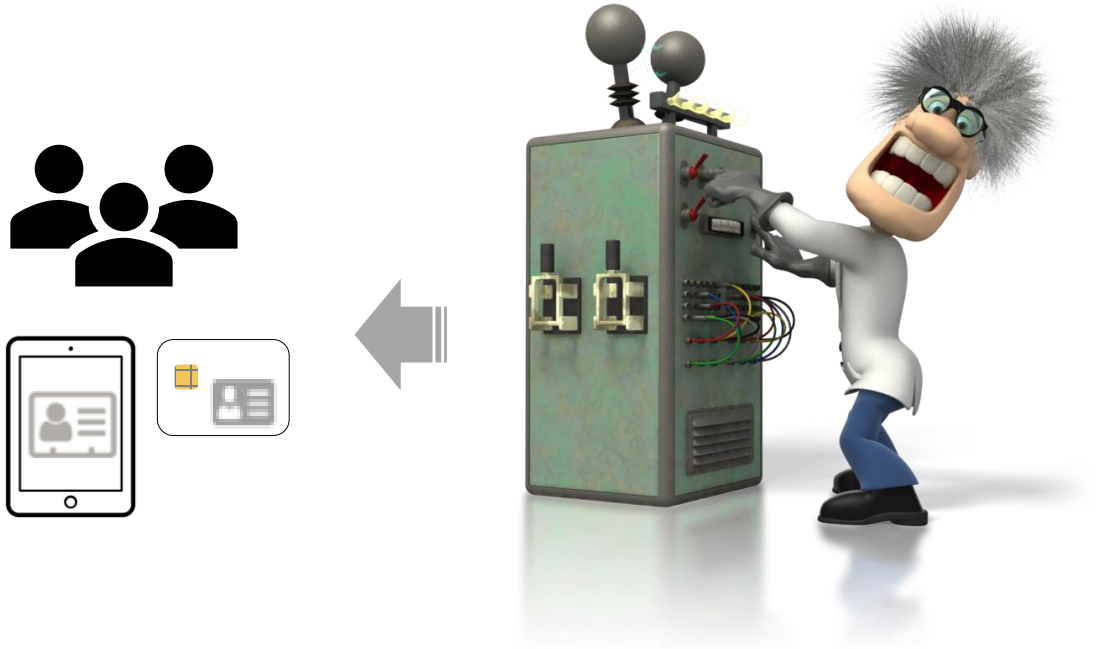
E-id skyddas i ett särskilt chip

inera

E-legitimationsutfärdare

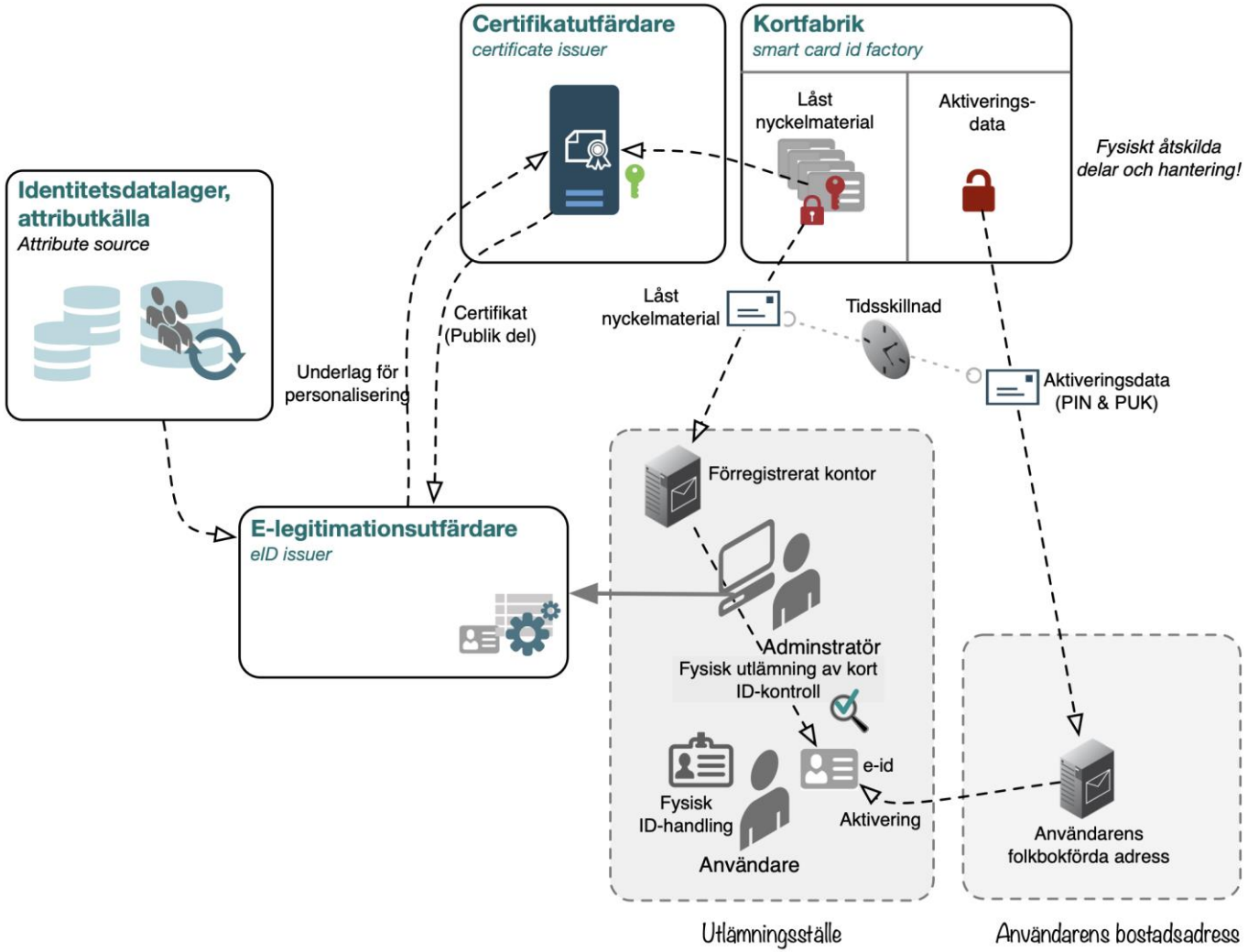
Principer för utfärdande av e-legitimationer

- Administrativ process
- Självservice
- Självservice med ”ärvd legitimering”



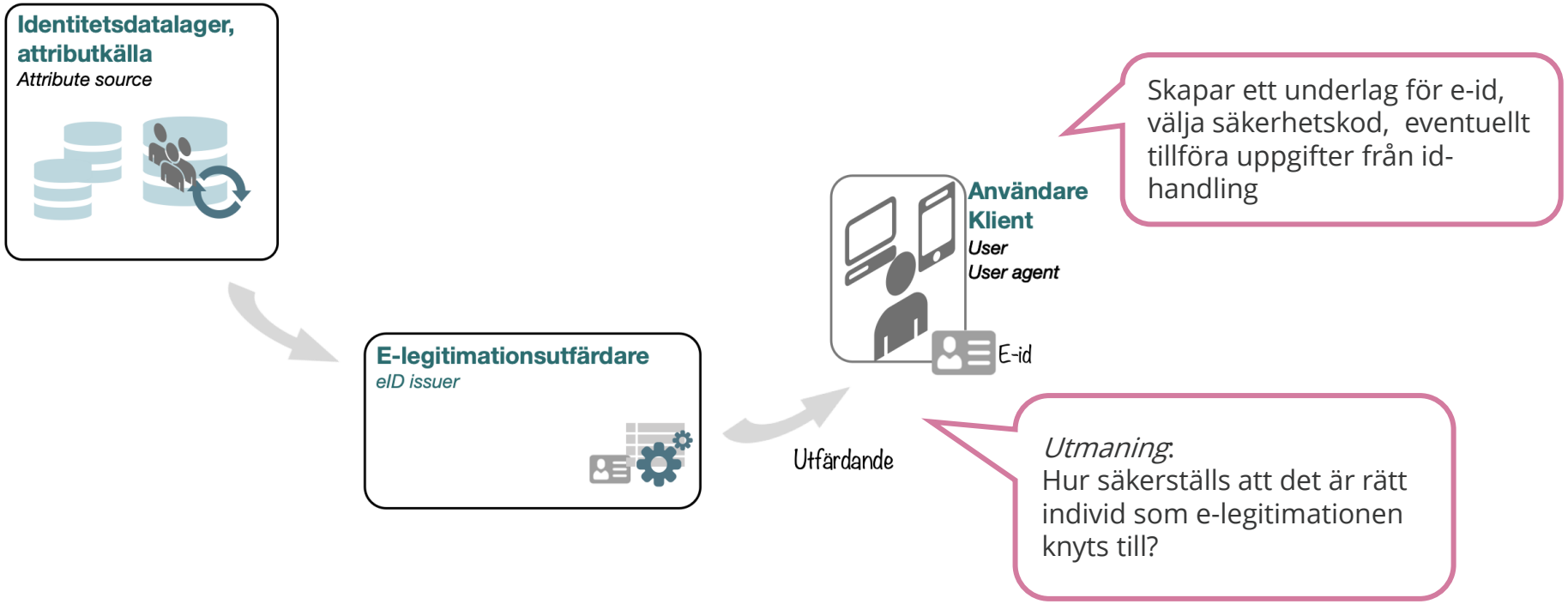
E-legitimationsutfärdare

Utfärdande av e-legitimation med administrativ process



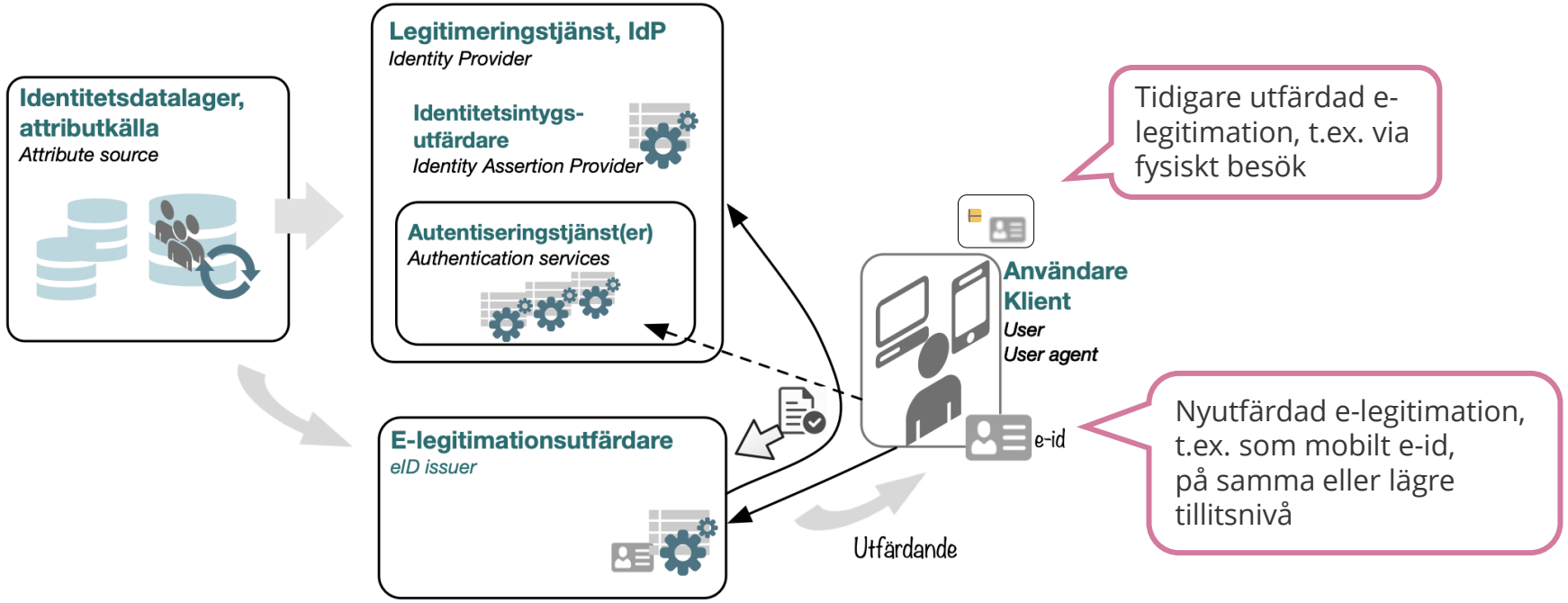
E-legitimationsutfärdare

Utfärdande av e-legitimation via självservice



E-legitimationsutfärdare

Utfärdande av e-legitimation via självservice med ärvd legitimering



Tack!

Mer information om Referensarkitektur för Identitet och åtkomst (IAM) på
www.inera.se

www.rivta.se

inera
Ett företag inom SKR