Tillämpning IAM: e-legitimering och e-underskrift baserat på referensarkitektur

Arkitekturen för SITHS anpassas till
Ineras referensarkitektur inom IAM-området

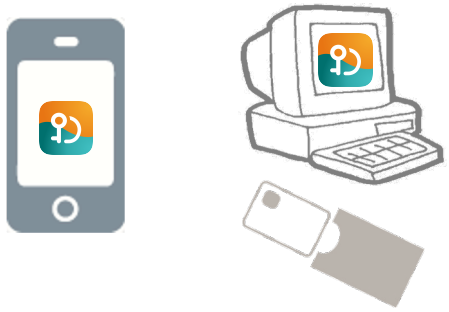
Nya möjligheter för ***mobil autentisering*** *och*
avancerad elektronisk underskrift

Per Mützell Lösningsarkitekt, sektion Arkitektur, Inera

inera

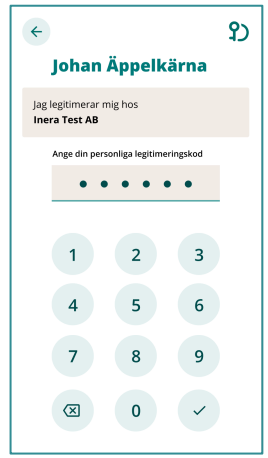
Nya förmågor inom SITHS & Säkerhetstjänster

- **Mobilt SITHS eID** som komplement till SITHS eID på kort.
  Utfärdande av Mobilt SITHS eID via självservicefunktion.



- **Elektronisk underskrift som tjänst**

- **Enhetlig användarupplevelse** och **minskat teknikberoende** vid inloggning och underskrift med SITHS eID-app

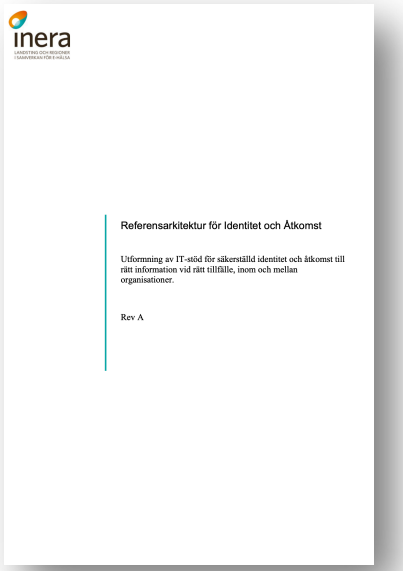


Följsamhet till samverkansarkitekturer inom IAM-området

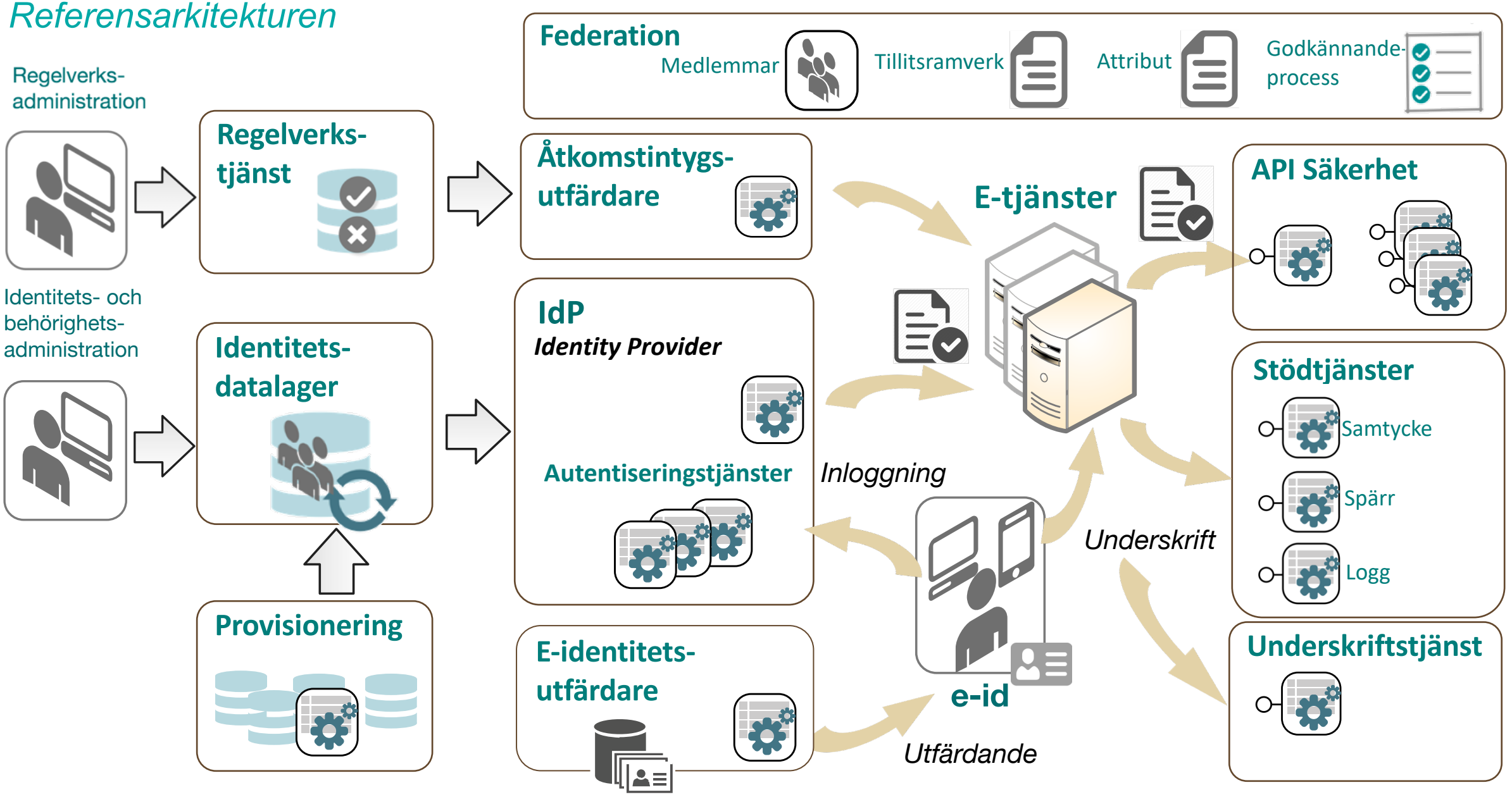
Arkitekturen för SITHS eID och Inera Säkerhetstjänster har utformats utifrån

- *Referensarkitektur för **Identitet och åtkomst (IAM)***
- *Referensarkitektur för **Elektronisk underskrift och stämpel***

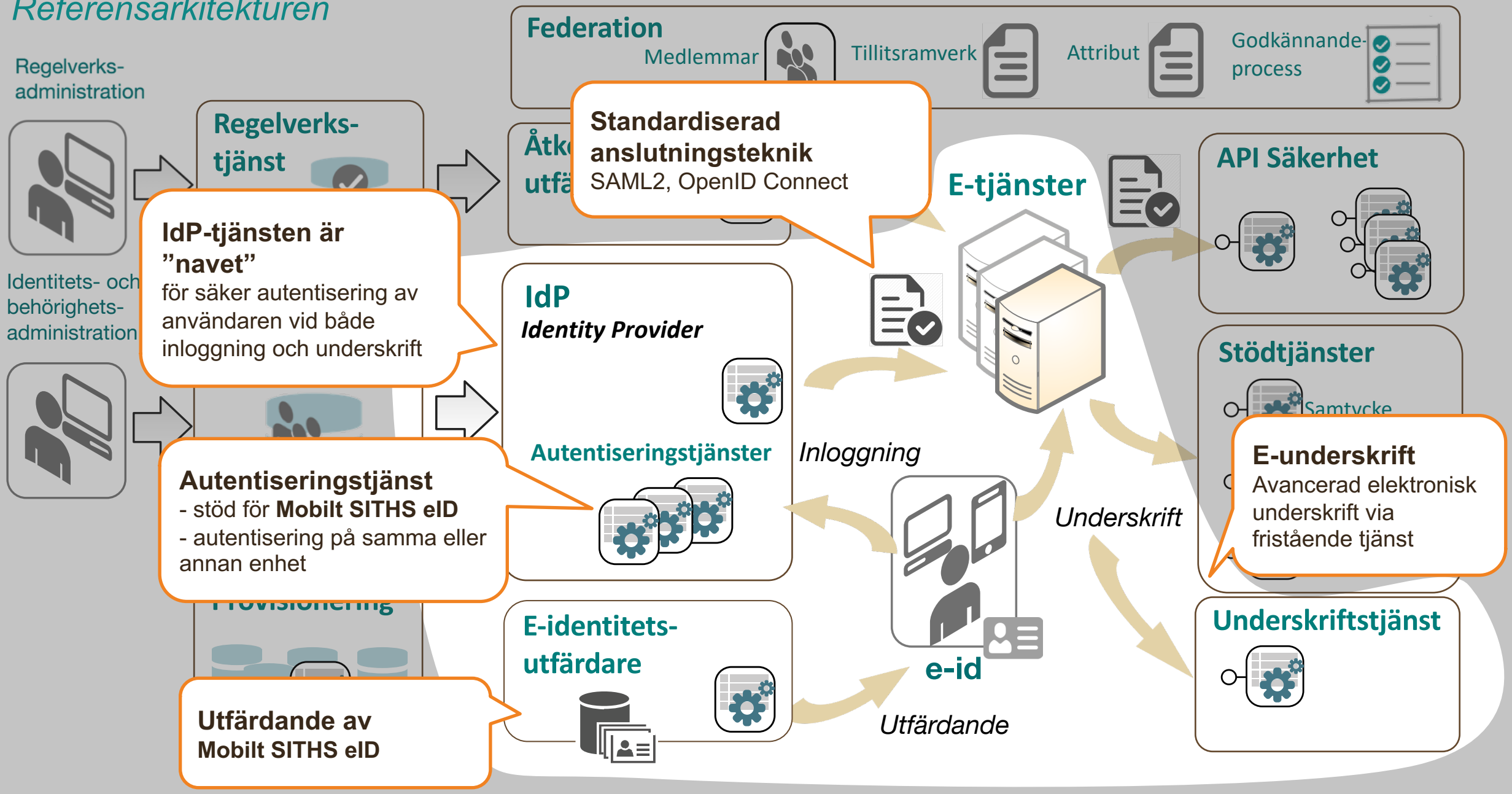
Källa: https://rivta.se



Referensarkitekturen



Referensarkitekturen

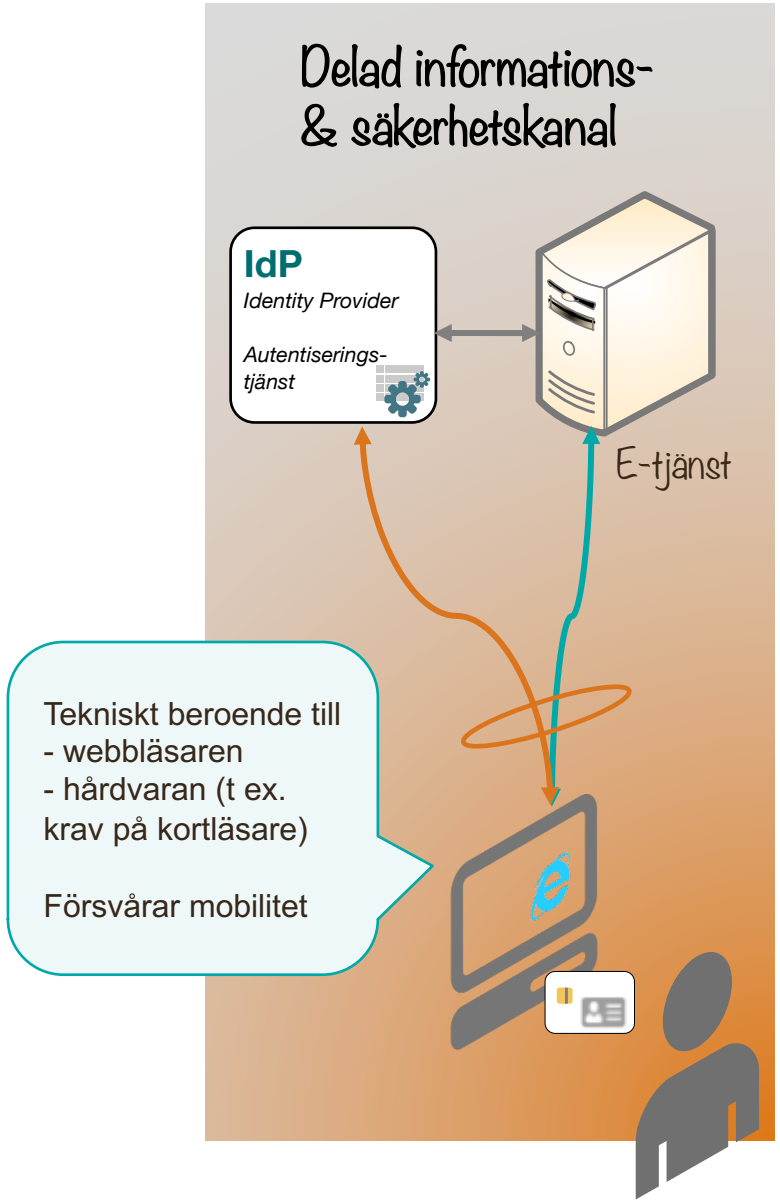


E-legitimering
enligt referensarkitekturen

Tillämpat med SITHS eID, mobilt och stationärt

Från delad till separat säkerhetskanal för autentisering

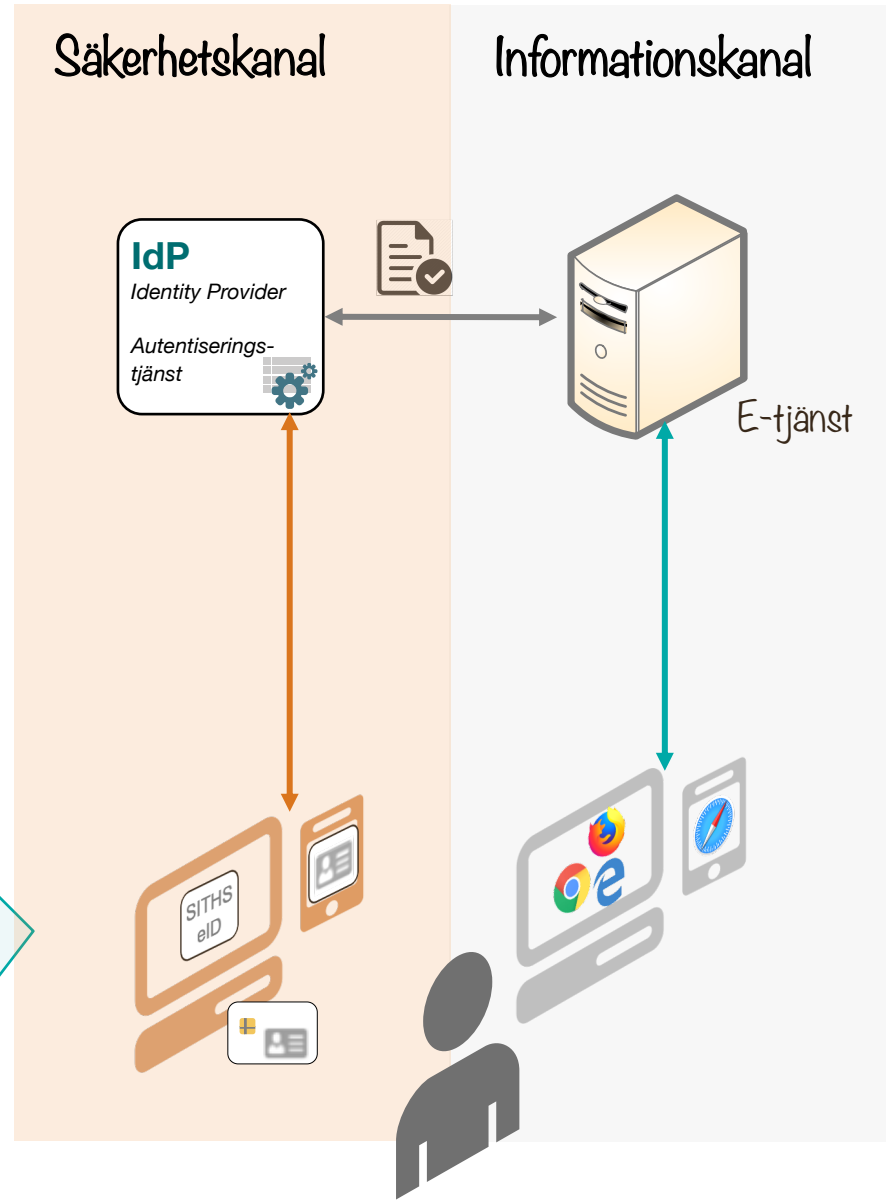
Ökad flexibilitet & mobilitet - minskat teknikberoende



Separat säkerhetskanal med säkerhetsapp *”Out-of-band” (OOB)*

Både för autentisering och underskrift

- ✓ Använd **samma eller olika enheter**
- ✓ **Delade arbetsverktyg,** men **personliga e-id**
- ✓ **Minskat hårdvaruberoende,** stöd för ”nedlåst” utrustning
- ✓ **Öppna för andra e-id-bärare** och **mobilitet**

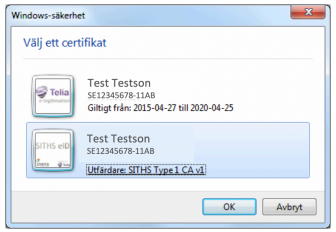


Vad vi vill komma ifrån…

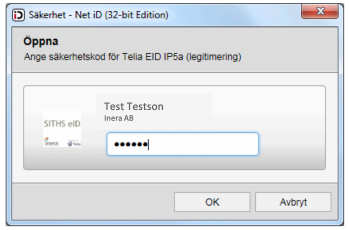
Exempel: inloggning med smart kort via webbläsaren (delad informations- och säkerhetskanal)

Olika användarupplevelse för olika webbläsare, versioner & plattformar **Komplext**!

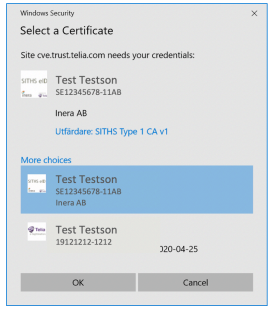
Internet Explorer 11



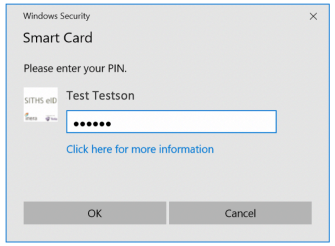
+

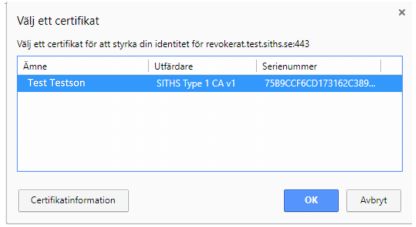


Microsoft Edge

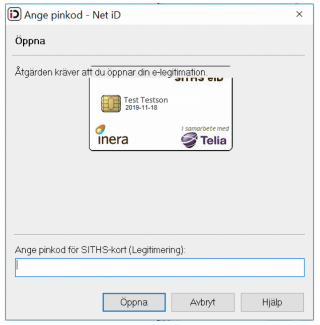


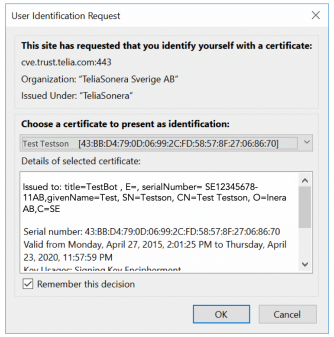
+



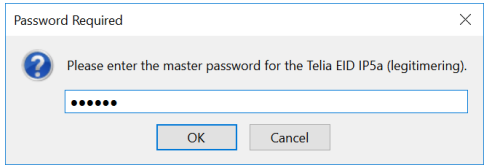


+

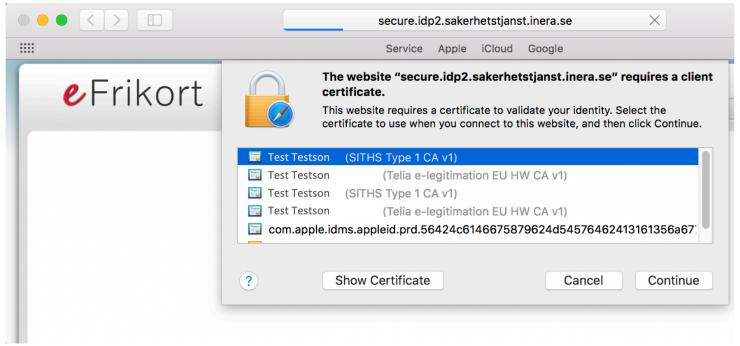




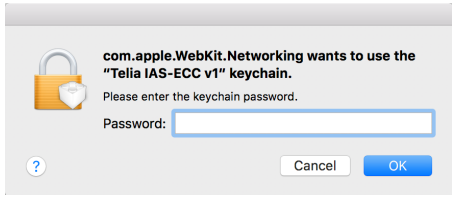
+



Google Chrome



+



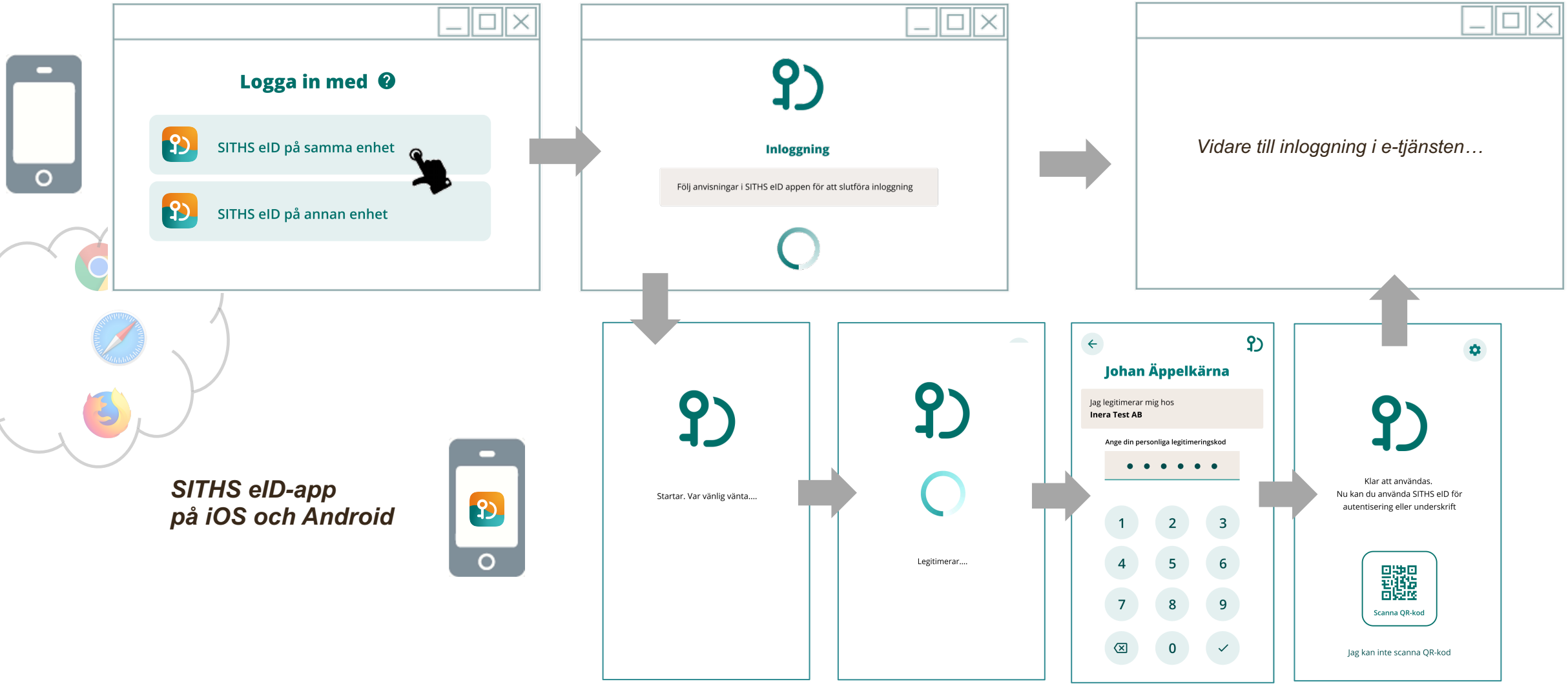
Mozilla Firefox

Mobil inloggning

på samma enhet

Princip: Enhetlig användarupplevelse

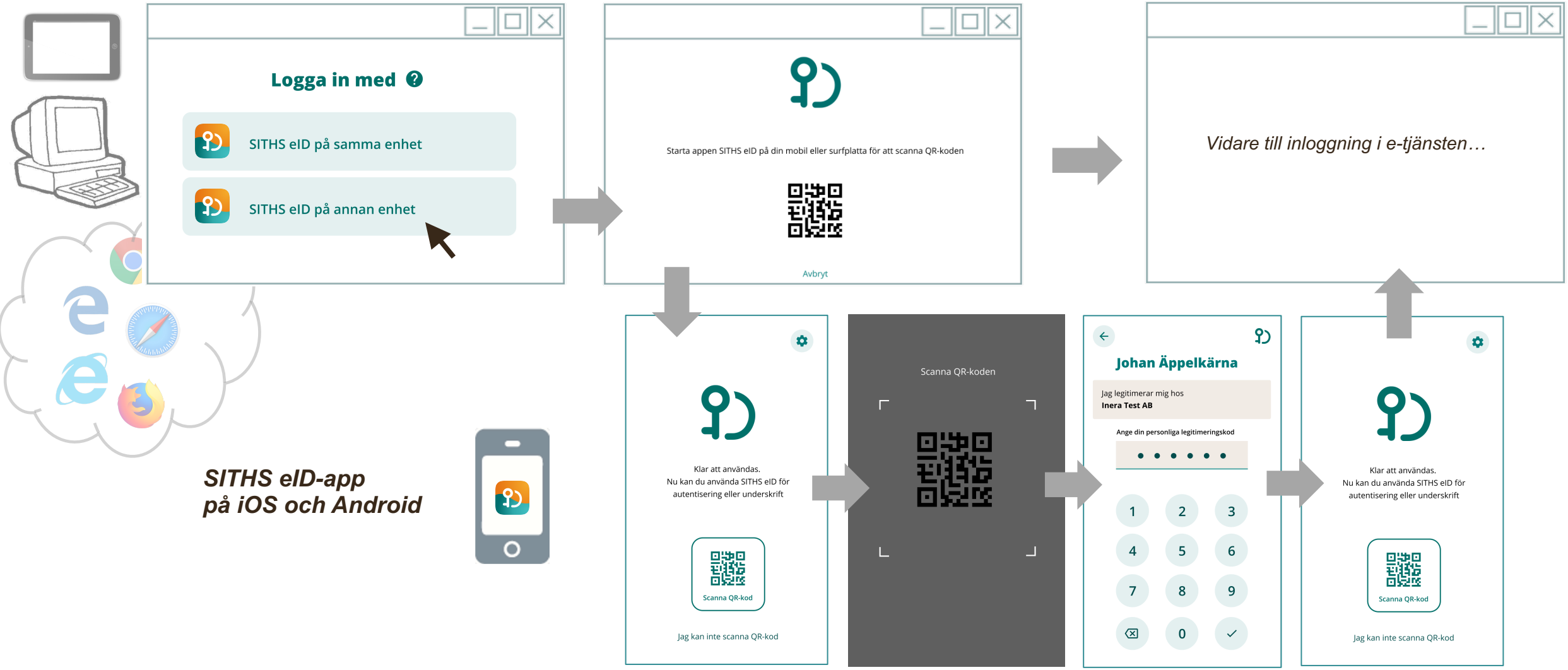
på såväl mobil/surfplatta som dator och olika webbläsare



SITHS eID-app på iOS och Android

Mobil inloggning

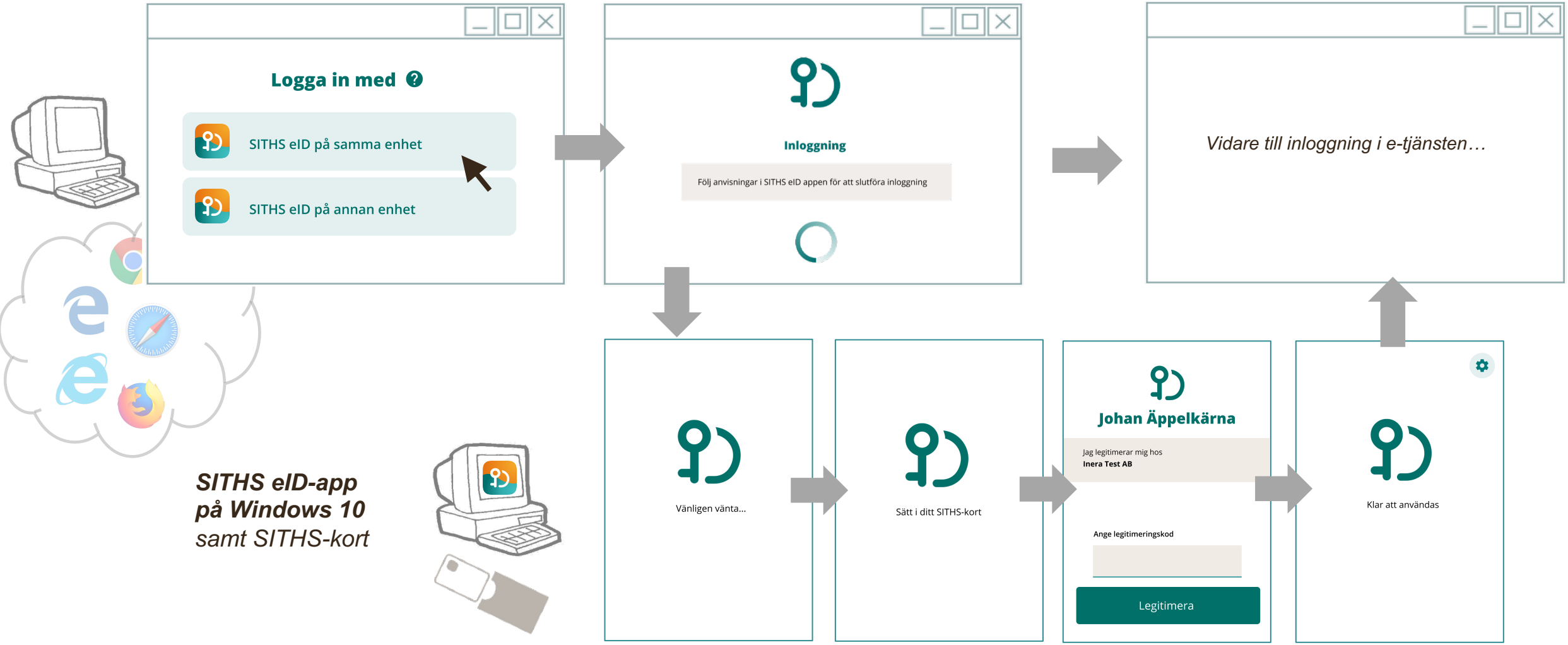
på annan enhet



SITHS eID-app
på iOS och Android

Inloggning med smart kort på dator

på samma enhet



SITHS eID-app på Windows 10
samt SITHS-kort

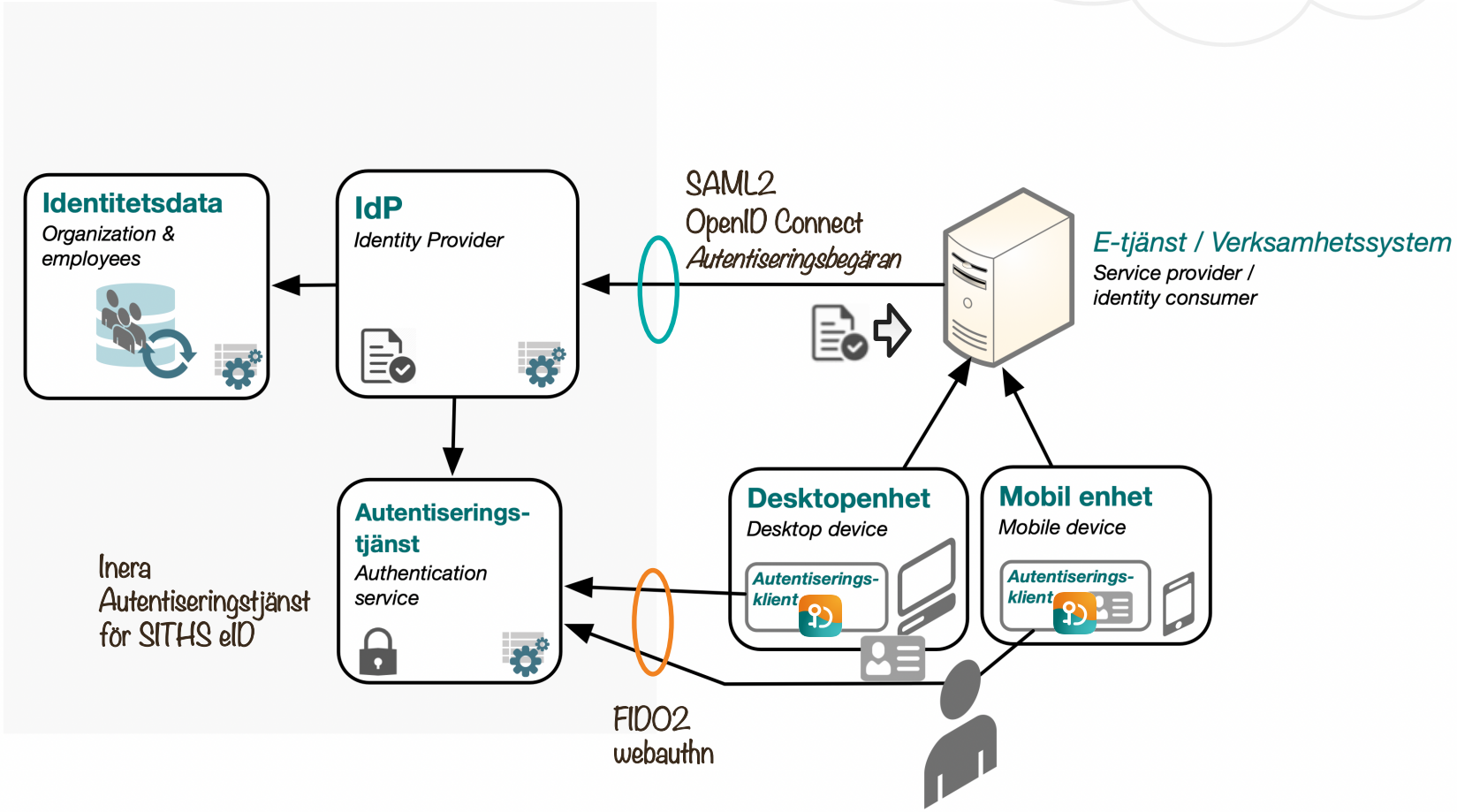
E-legitimering

Arkitekturell översikt & standarder

E-legitimering

Översiktlig arkitektur

Baserad på standarder och nationell profilering



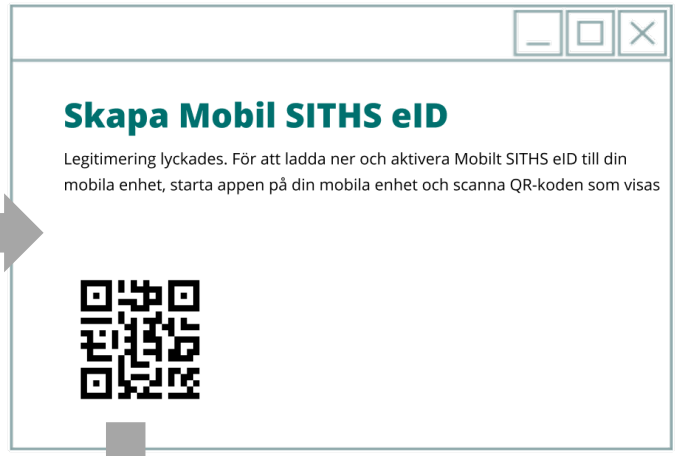
Utfärdande av Mobilt SITHS eID

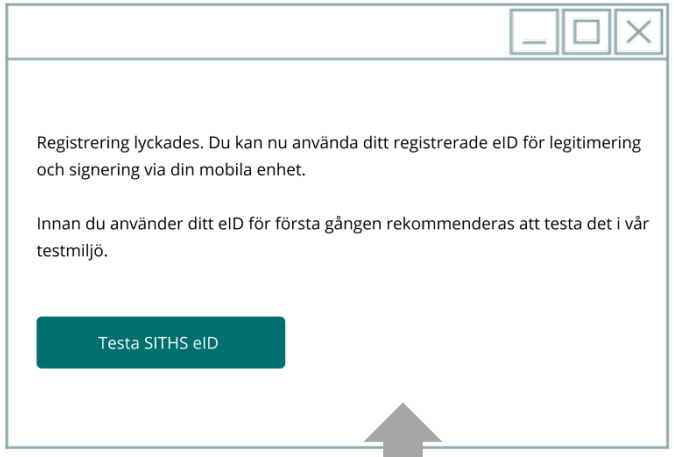
Självservice

med id-växling från SITHS-kort (LoA3)

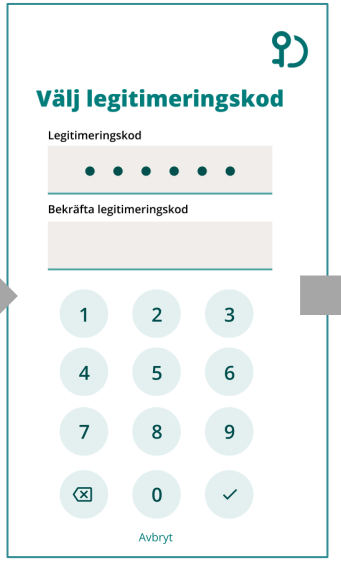
Utfärdande av Mobilt SITHS eID - via självservice

Win 10





iOS/iPadOS och Android

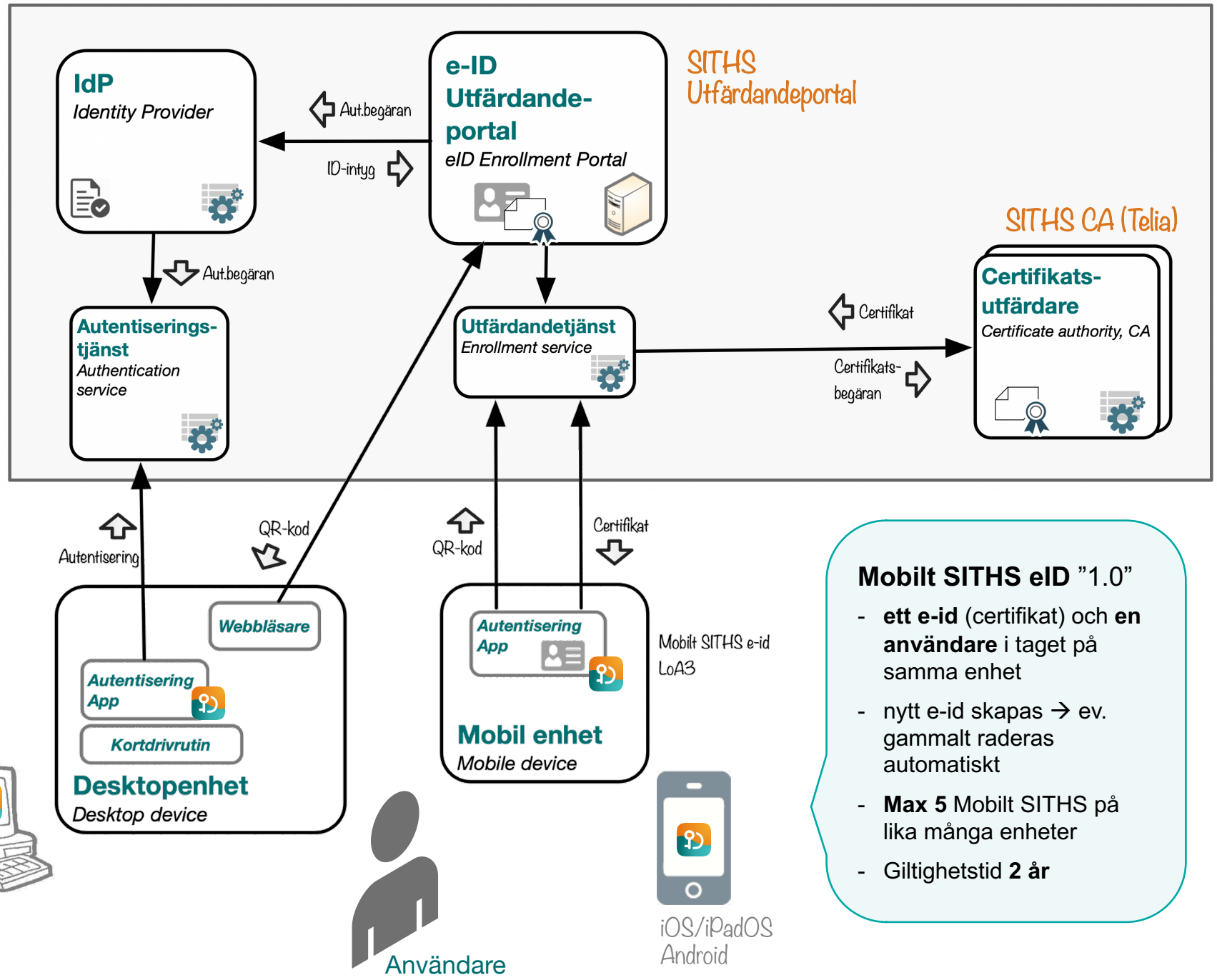


Utfärdande av Mobilt SITHS eID via självservice

Id-växling
från SITHS eID (LoA3)
till Mobilt SITHS eID (LoA3)

För granskning enligt Svensk e-legitimation tillitsnivå 3

LoA = Level of Assurance = tillitsnivå



Mobilt SITHS eID ”1.0”

- **ett e-id** (certifikat) och **en användare** i taget på samma enhet
- nytt e-id skapas → ev. gammalt raderas automatiskt
- **Max 5** Mobilt SITHS på lika många enheter
- Giltighetstid **2 år**

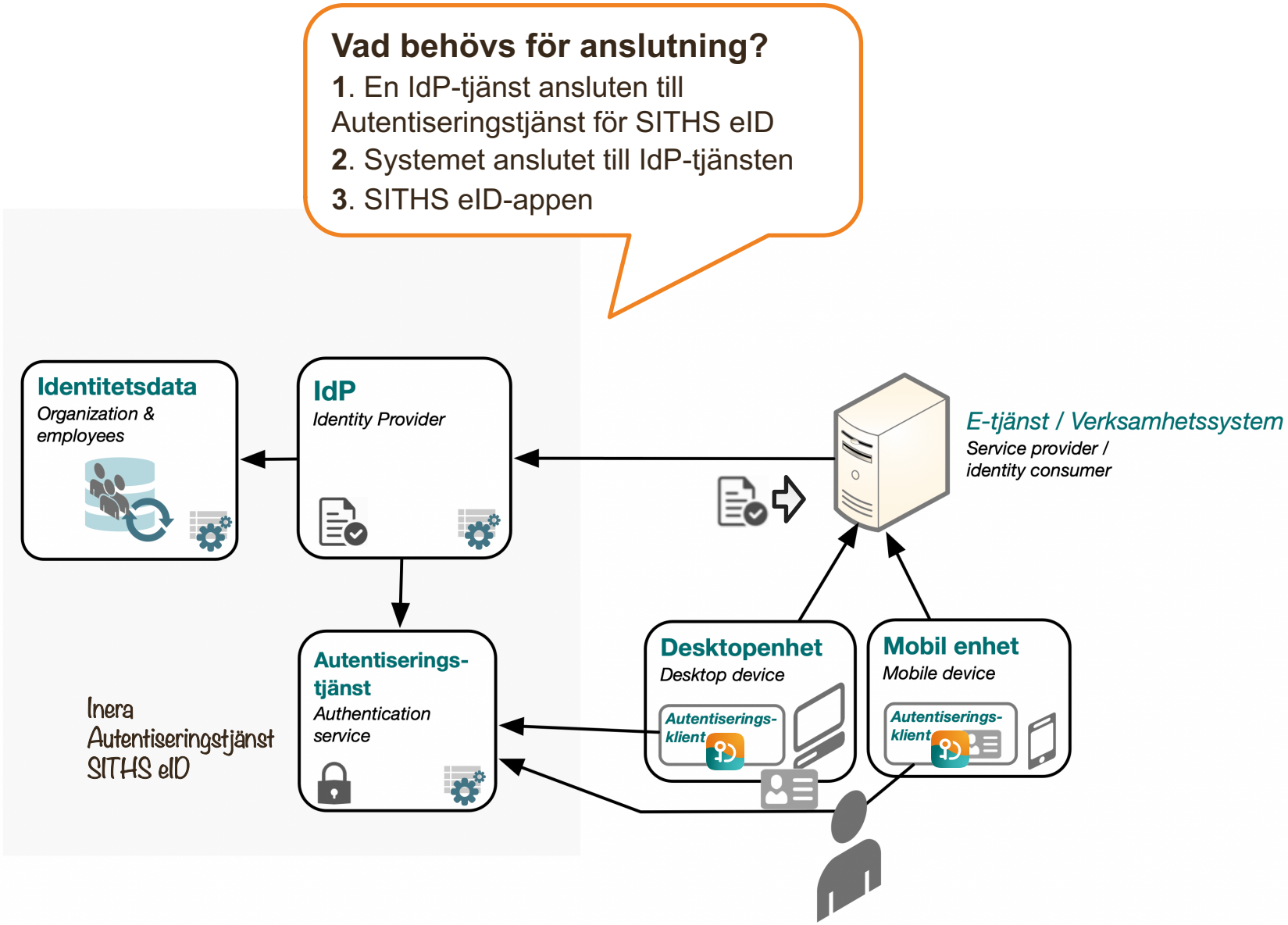
Hur komma igång med de nya metoderna för e-legitimering inklusive Mobilt SITHS?

Anslutningsmönster – från start jan-2021

Tillämpningar - Pilotprojekt

E-legitimering

Översiktlig arkitektur



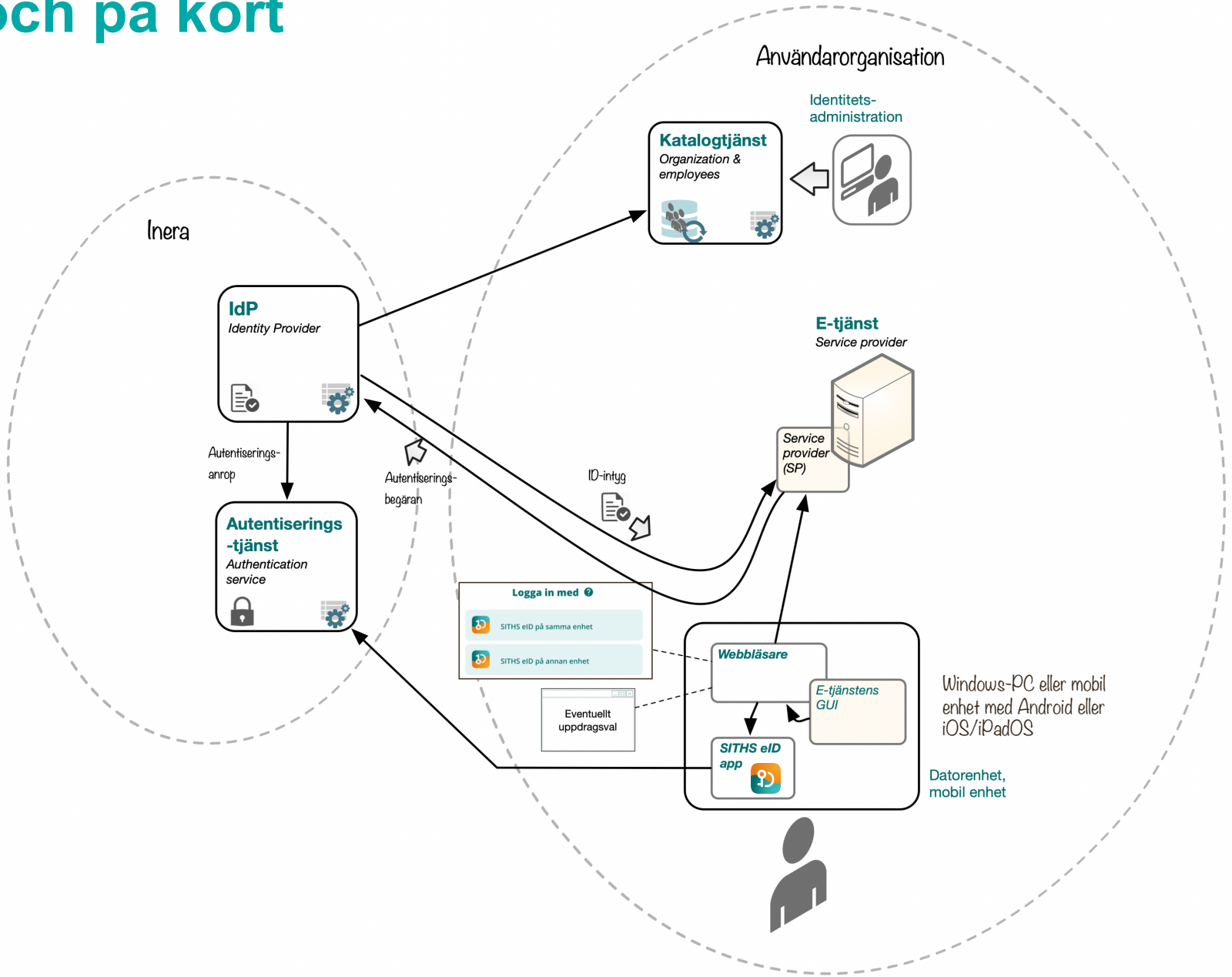
SITHS eID - Mobilt och på kort

Anslutningsmönster

Lokalt system till Ineras IdP

- ✓ Nyttjar färdig funktionalitet i Inera IdP (SaaS)
- ✓ Standardiserad anslutning

- ➢ Mindre utrymme för lokal anpassning / funktionalitet



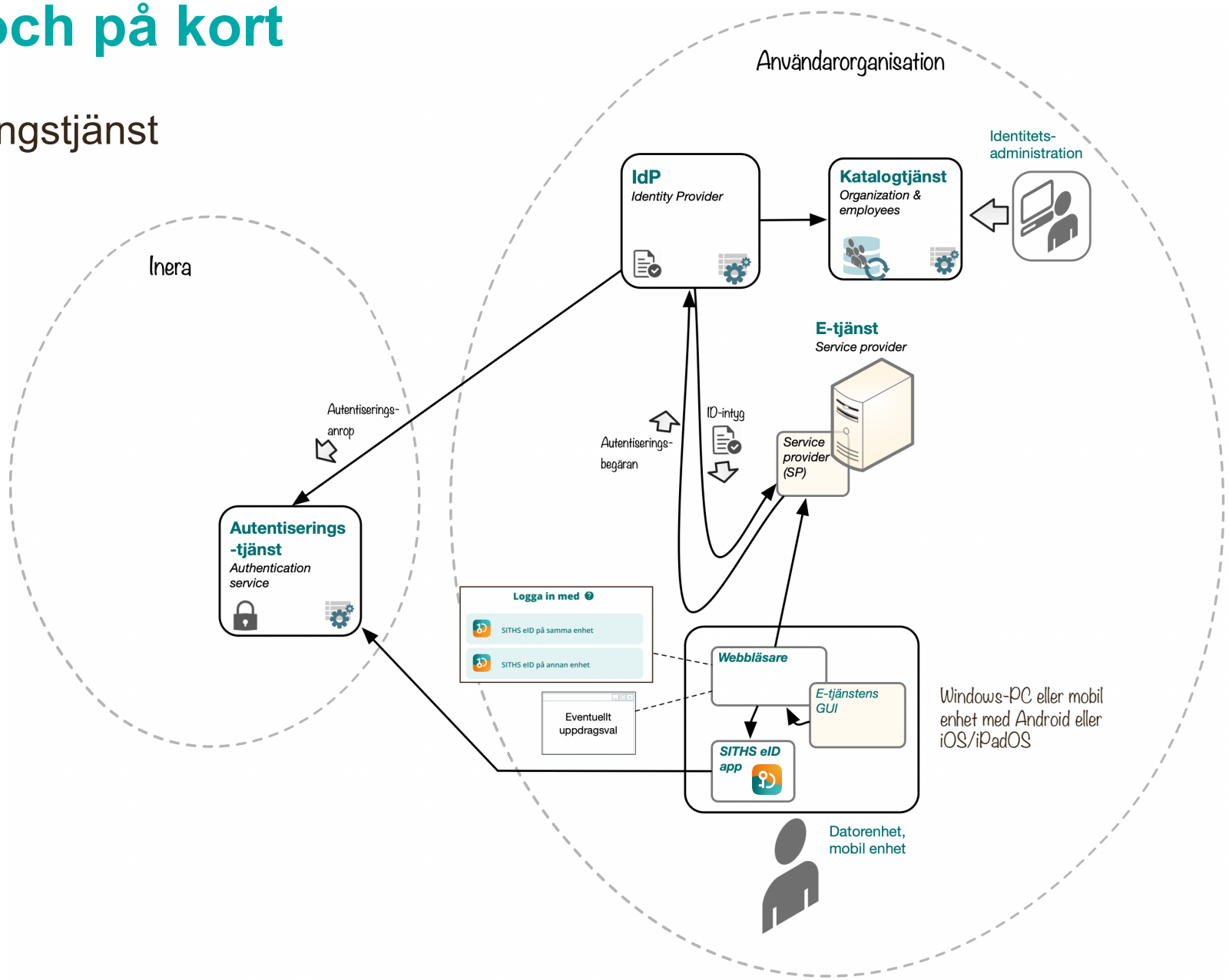
SITHS eID - Mobilt och på kort

Anslutningsmönster

Lokal IdP till Inera Autentiseringstjänst

- ✓ Sammanhållen användarupplevelse, SSO, om fler tjänster är anslutna lokalt
- ✓ Full kontroll över funktionalitet lokalt

- ➢ Måste implementera IdP-funktionalitet och integrera Lokal IdP mot autentiserings-API



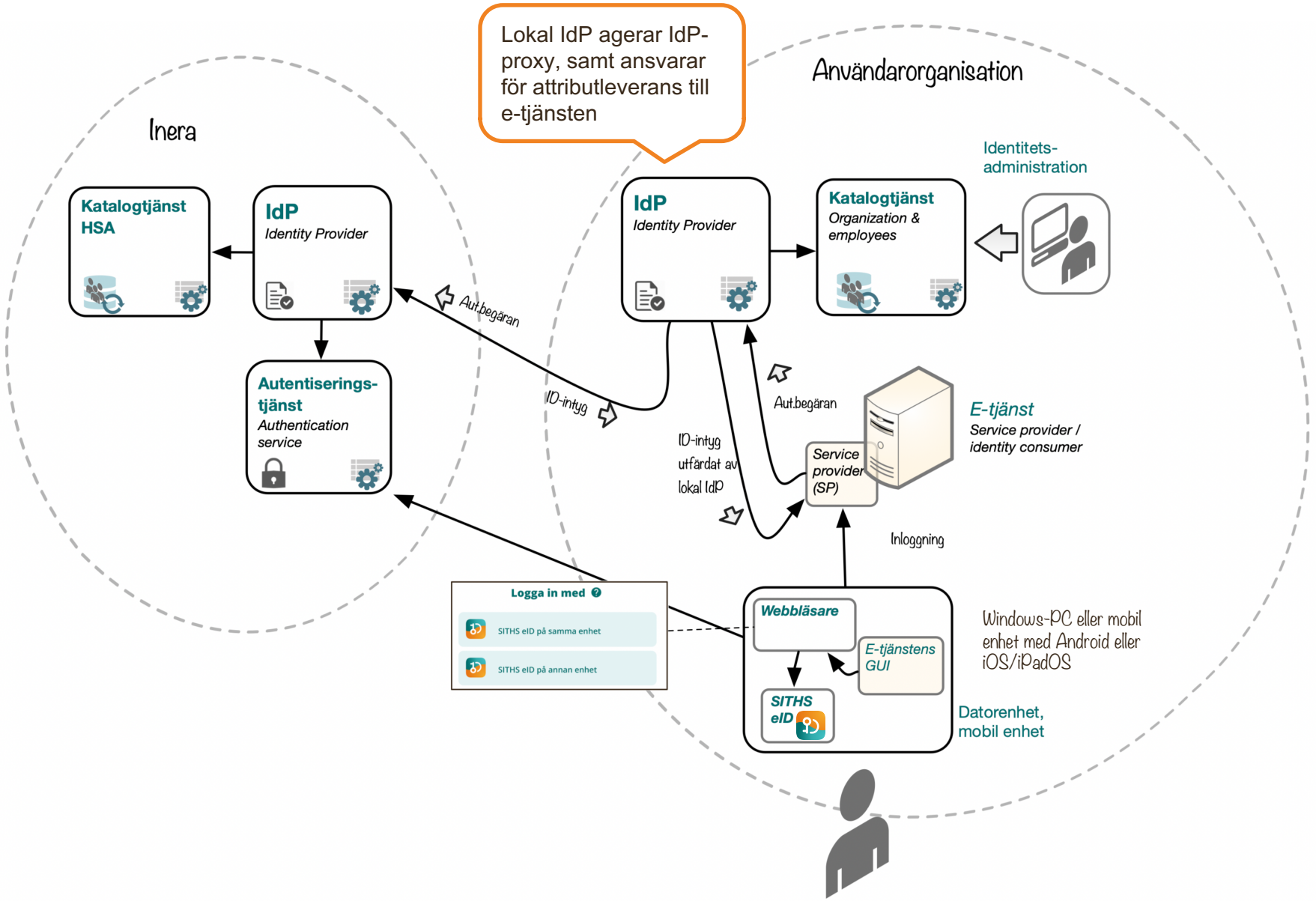
SITHS eID - Mobilt och på kort

Anslutningsmönster

Lokal IdP till Ineras IdP

- ✓ Möjlighet till SSO, om fler tjänster är anslutna lokalt
- ✓ Nyttjar färdig funktionalitet i Inera IdP
- ✓ Standardiserad anslutning – tänkbart enklare livscykelhantering

- ➢ Lokal IdP måste klara att agera proxy-IdP

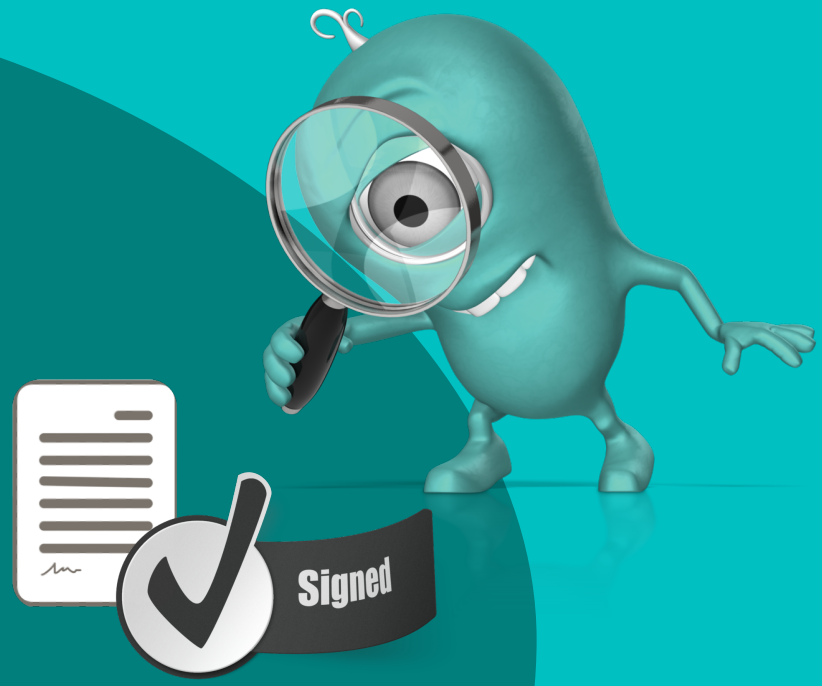


Mobilt SITHS eID

Tillämpningar – Aktuella piloter

- Region Kronoberg:
  Mobilt SITHS – Mobil Journal (Cosmic Nova) på plattor
- Region Skåne:
  Mobilt SITHS – Mobil Bedside-tillämpning (Medanets) för sjuksköterskor
- Region Västmanland:
  Mobilt SITHS – Mobil Journal (Cosmic Nova) på plattor
- Göteborgs stad:
  Mobilt SITHS – Utveckling mobila tjänster inom bl.a. vård och omsorg
- Region Östergötland:
  Mobilt SITHS – Teknisk verifiering

E-underskrift
enligt referensarkitekturen



Tillämpning med SITHS eID, mobilt och stationärt, samt
Inera Underskriftstjänst

Centrala begrepp

- **Digital signatur**

  ”*Information i elektronisk form som är kryptografiskt kopplad till ett annat elektroniskt material, i syfte att säkerställa det elektroniska materialets dataintegritet och ursprung*”

- **Elektronisk underskrift**

  Digital signatur – underskrivet av en fysisk person

- **Elektronisk stämpel**

  Digital signatur – där en juridisk person (typiskt organisation) står bakom signaturen

Starkt kopplad och i efterhand verifierbar signatur samt skydd mot förvanskning

Fysisk person undertecknar ett dokument

Organisation stämplar ett dokument

eIDAS-förordningen:

”*avancerad elektronisk underskrift och stämpel”*

I vilka fall behövs en digital signatur?

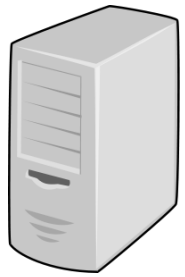
Jämför…

Extra verifiering av användaren (autentisering)

Digital signatur

Kan göras verifierbar inom ***samma IT-system***

Dokumentet kan ändras utan att bryta ”signeringen”



Dokumentet kan **inte** ändras utan att bryta signaturen

Löst kopplad information om vem som signerat och när

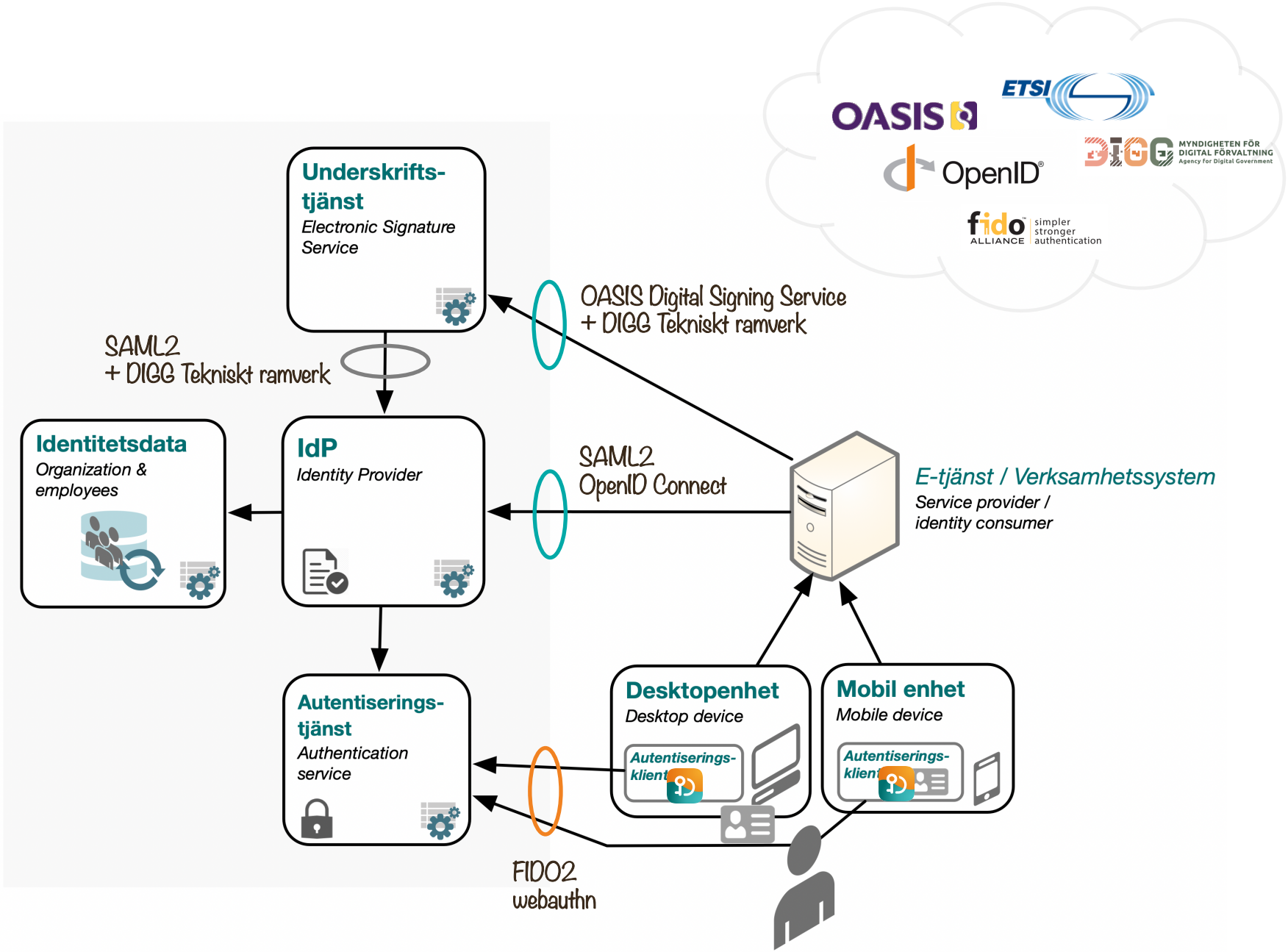
Starkt kopplad information om vem som signerat och när.

Verifierbar även hos ***andra parter med andra IT-system***

E-underskrift

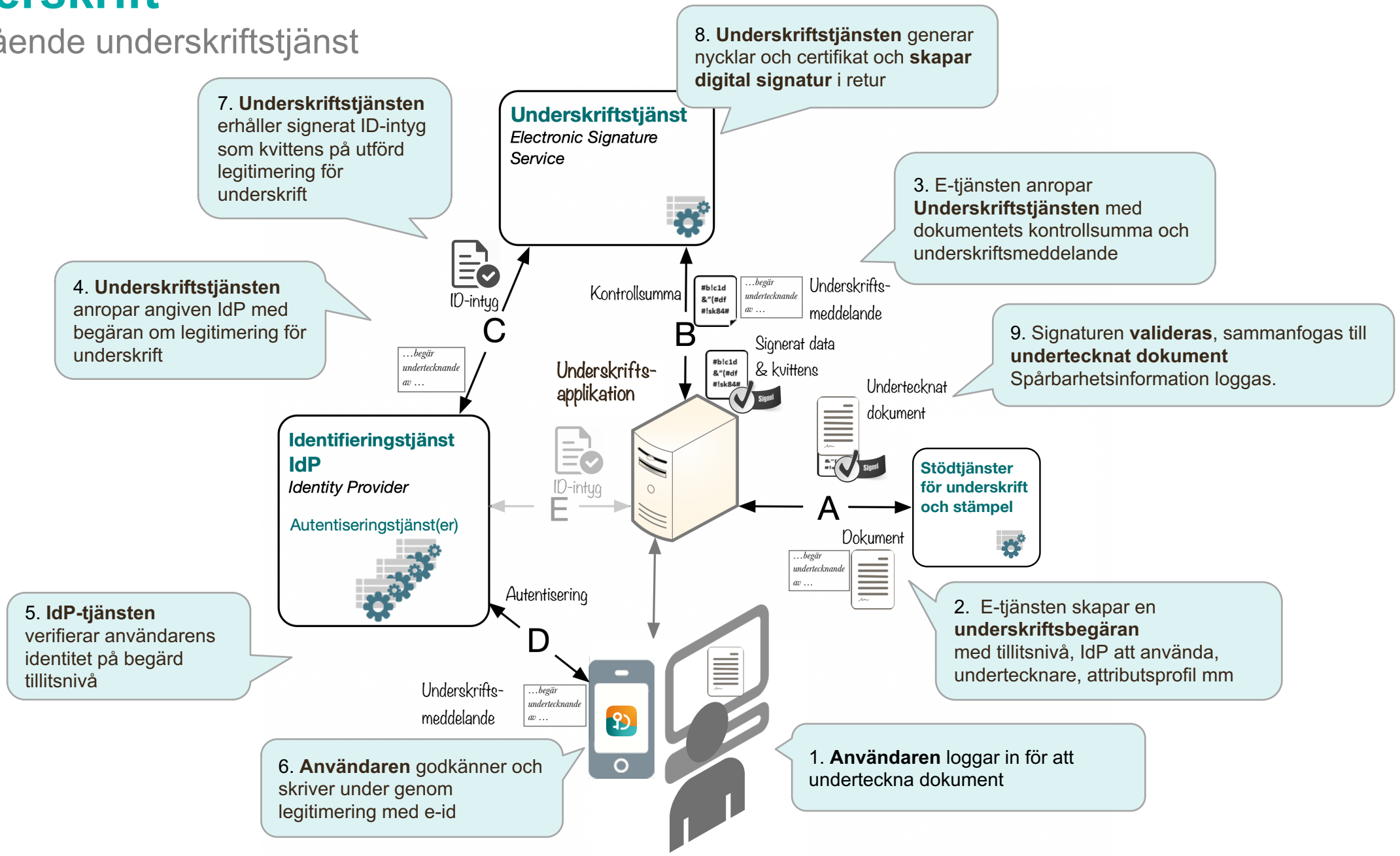
Översiktlig arkitektur
Baserad på standard och nationell profilering

- ✓ **Avancerad elektronisk underskrift** [eIDAS] som **fristående tjänst**
- ✓ Följer **DIGG Tekniskt ramverk**, baserad på ETSI/OASIS standarder
- ✓ Nyttjar IdP-tjänsten för **e-legitimering för underskrift**



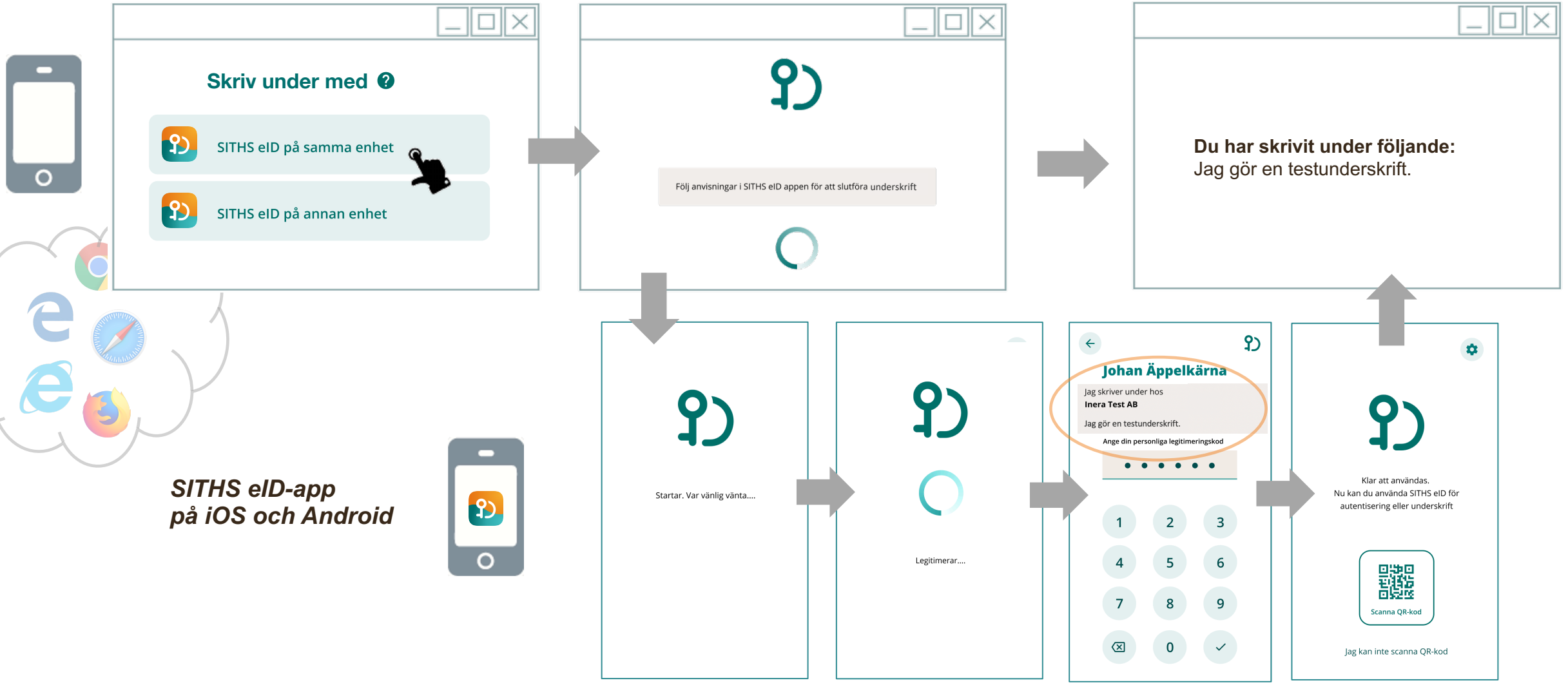
E-underskrift

med fristående underskriftstjänst



Mobil underskrift

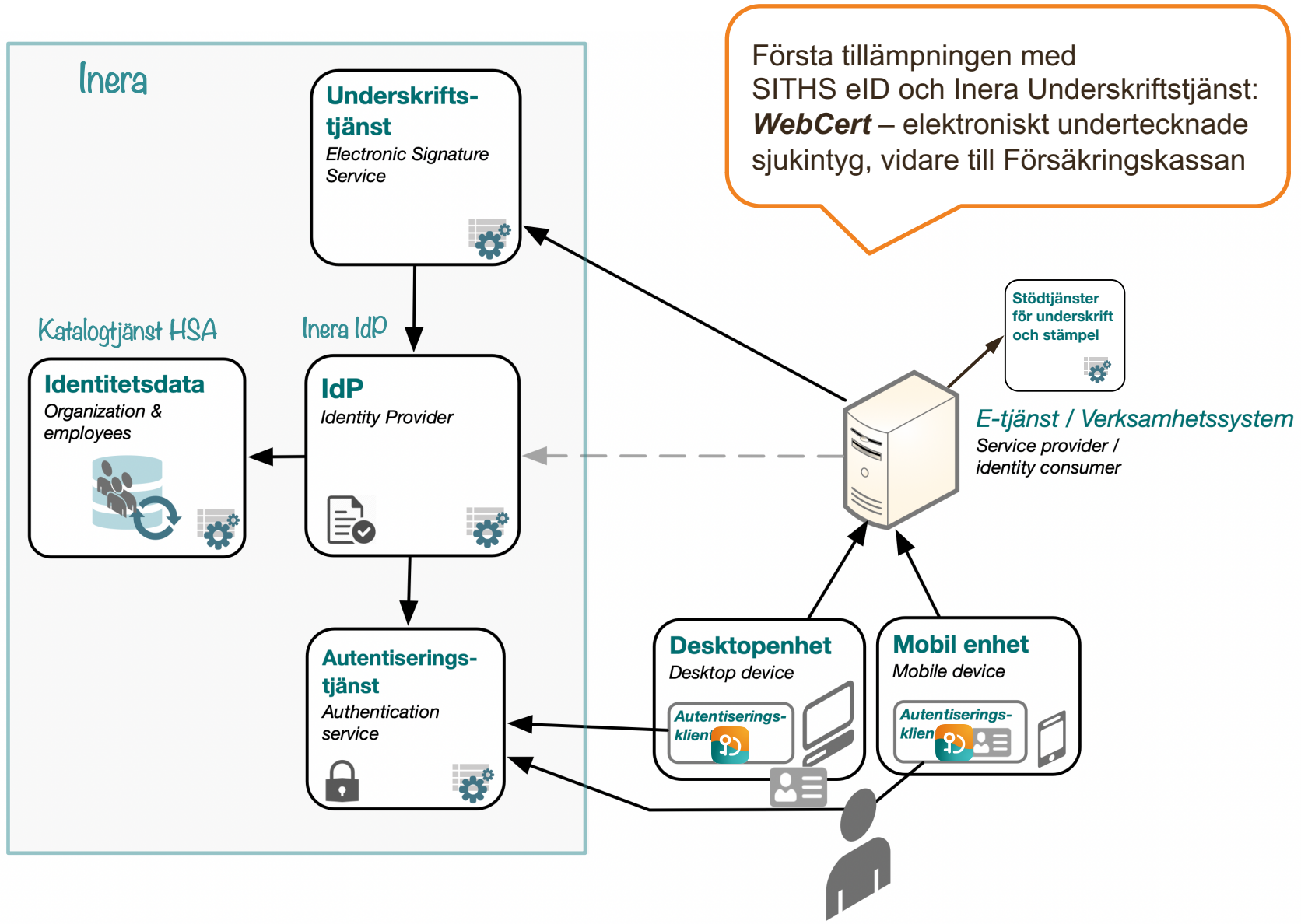
på samma enhet



SITHS eID-app
på iOS och Android

E-underskrift

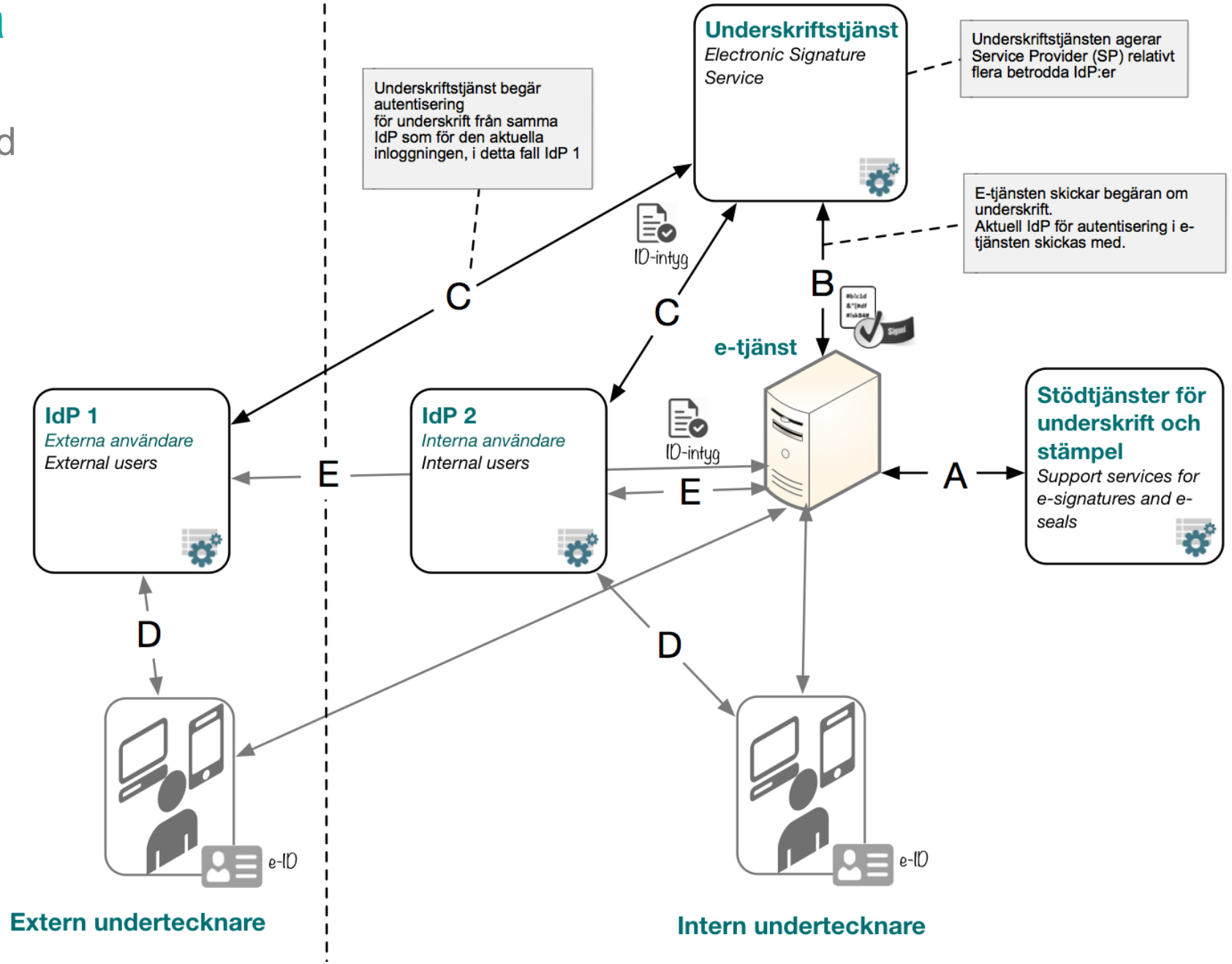
Anslutning till Ineras Underskriftstjänst



Externa och interna undertecknare

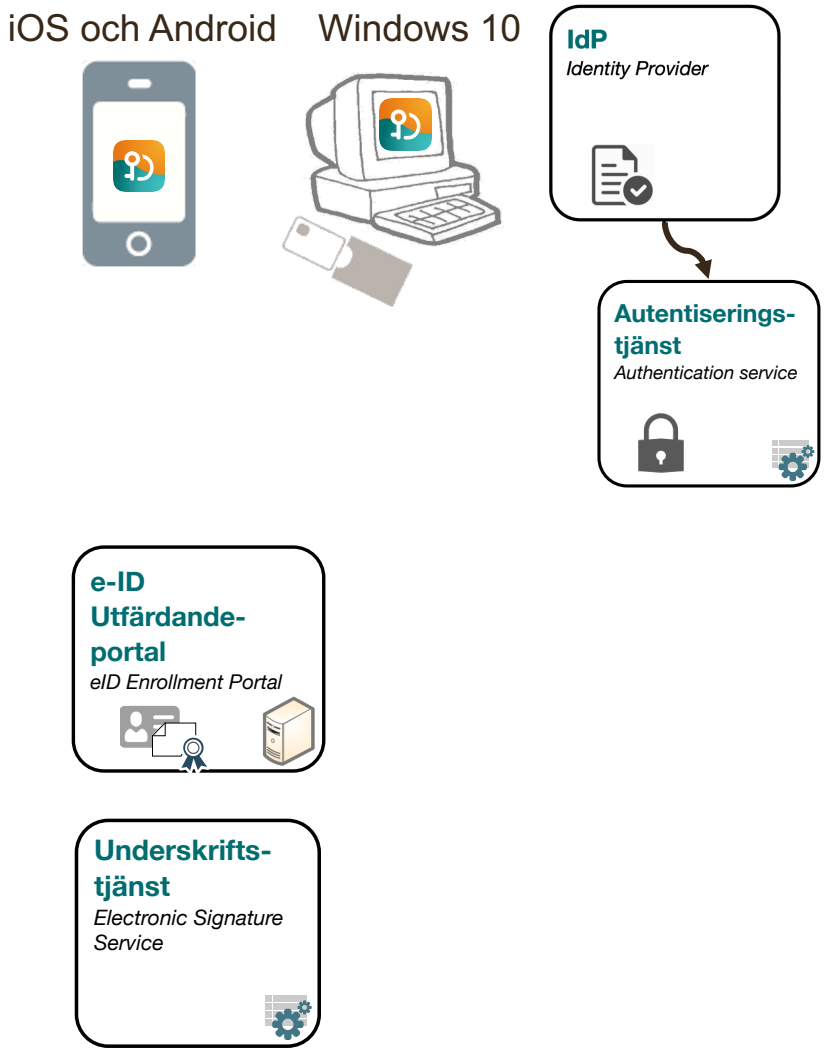
- via federativ samverkan med flera IdP:er

Exempel:
Interna användare hanteras av kommunens interna IdP, medan externa användare = privatpersoner hanteras av IdP för svensk e-legitimation



Sammanfattning

- **Mobilt SITHS eID**
  - Verksamhetspiloter i teststadie
  - Lanseras jan-2021
  - Anslutning via IdP-tjänst enligt referensarkitektur, flera anslutningsmönster
  - SITHS eID-appar för e-legitimering och e-underskrift
- **Utfärdandeportal** för Mobilt SITHS eID
  - Självservice, kräver SITHS eID–kort på tillitsnivå 3
  - Inväntar godkännande för tillitsnivå 3
- **Inera Underskriftstjänst**
  - Underskrift som tjänst för behov av avancerad elektronisk underskrift enligt eIDAS



inera