

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

*Arkitekturen för SITHS anpassas till
Ineras referensarkitektur inom IAM-området*

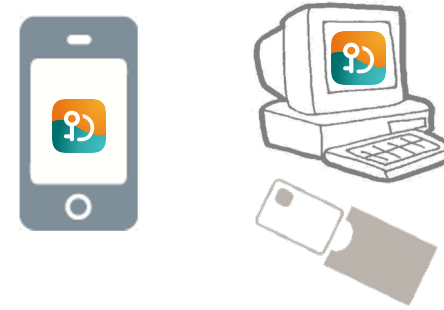
*Nya möjligheter för **mobil autentisering** och
avancerad elektronisk underskrift*

Per Mützell Lösningssarkitekt, sektion Arkitektur, 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

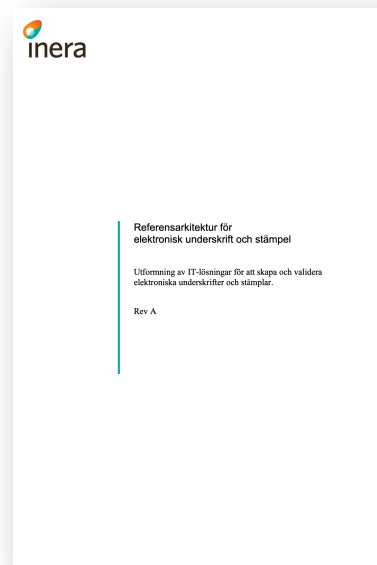
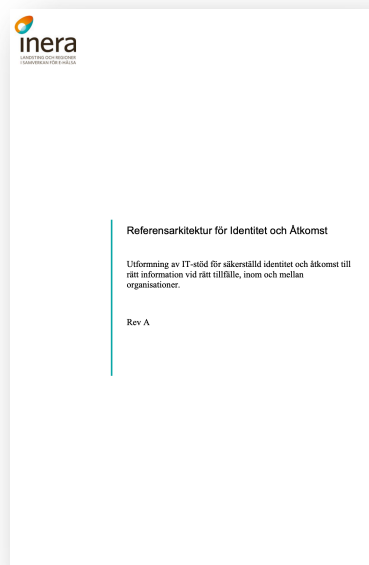
A screenshot of the SITHS eID app interface. The screen shows a back arrow, a user icon, and the name 'Johan Äppelkärna'. Below this, it says 'Jag legitimerar mig hos Inera Test AB'. There is a field for 'Ange din personliga legitimeringskod' with a masked input field containing six dots. At the bottom, there is a numeric keypad with buttons for 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, and a checkmark button.

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

Regelverks-
administration



Regelverks-
tjänst



Identitets- och
behörighets-
administration



Identitets-
datalager



Provisionering



Federation

Medlemmar



Tillitsramverk



Attribut



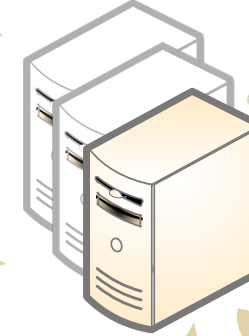
Godkännande-
process



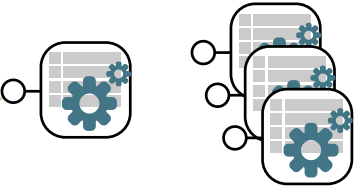
Åtkomstintygs-
utfärdare



E-tjänster



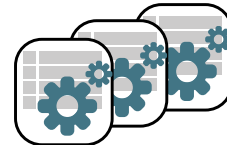
API Säkerhet



IdP
Identity Provider



Autentiseringstjänster

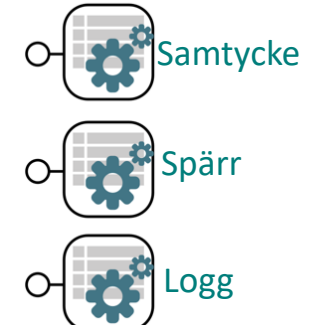


Inloggning



Underskrift

Stödtjänster



E-identitets-
utfärdare

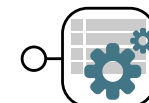


e-id



Utfärdande

Underskriftstjänst



Referensarkitekturen

Regelverks-
administration



Regelverks-
tjänst

Identitets- och
behörighets-
administration



**IdP-tjänsten är
"navet"**

för säker autentisering av
användaren vid både
inloggning och underskrift

Autentiseringstjänst

- stöd för **Mobilt SITHS eID**
- autentisering på samma eller
annan enhet

**Utfärdande av
Mobilt SITHS eID**

Federation

Medlemmar



Tillitsramverk



Attribut



Godkännande-
process

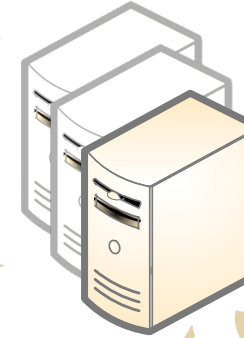


**Standardiserad
anslutningsteknik**

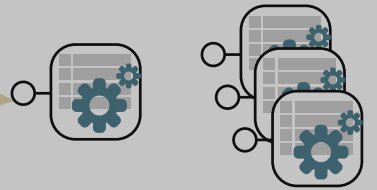
SAML2, OpenID Connect

Åtkomst-
utfärdare

E-tjänster



API Säkerhet



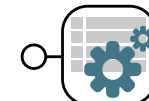
Stödtjänster



E-underskrift

Avancerad elektronisk
underskrift via
fristående tjänst

Underskriftstjänst

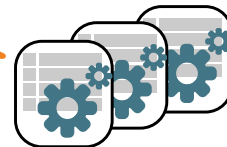


IdP

Identity Provider



Autentiseringstjänster



Inloggning

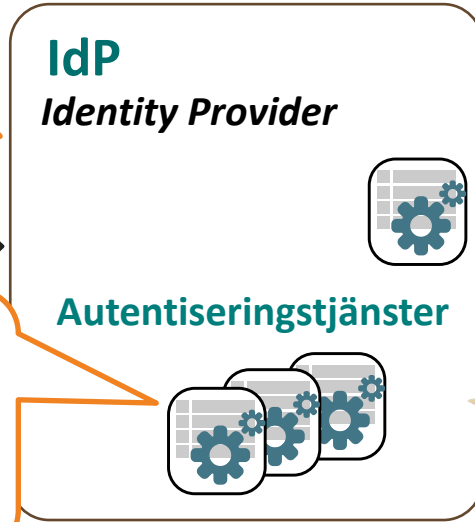
Underskrift

**E-identitets-
utfärdare**



e-id

Utfärdande



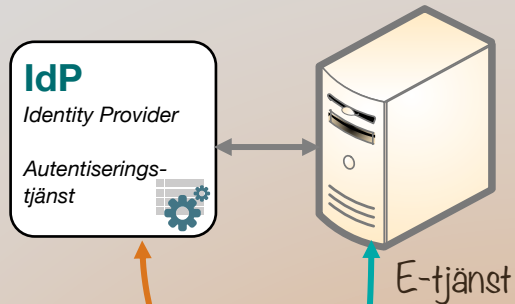
*E-legitimering
enligt referensarkitekturen*

Tillämpat med SITHS eID, mobilt och stationärt

Från delad till separat säkerhetskanal för autentisering

Ökad flexibilitet & mobilitet - minskat teknikberoende

Delad informations- & säkerhetskanal

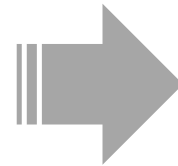


Tekniskt beroende till
- webbläsaren
- hårdvaran (t ex.
krav på kortläsare)

Försvårar mobilitet

Separat
säkerhetskanal med
säkerhetsapp
"Out-of-band" (OOB)

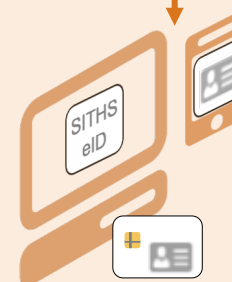
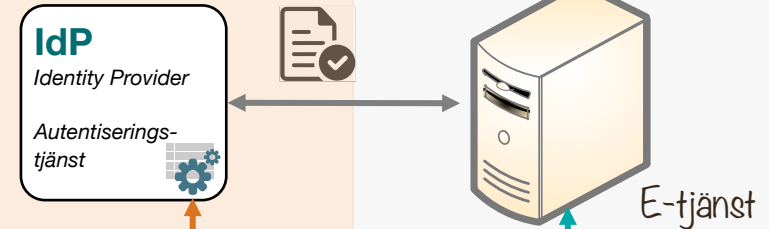
Både för
autentisering och
underskrift



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

Säkerhetskanal

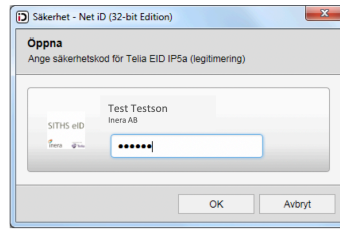
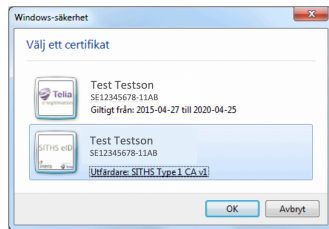
Informationskanal



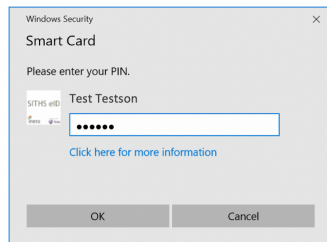
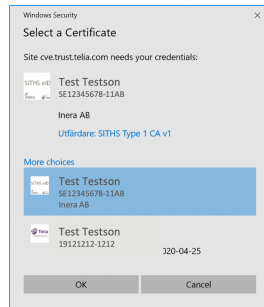
Vad vi vill komma ifrån...

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

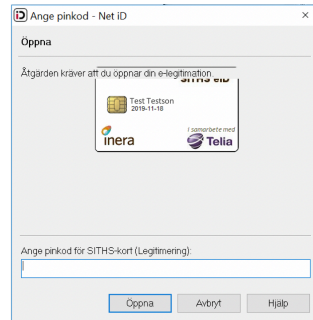
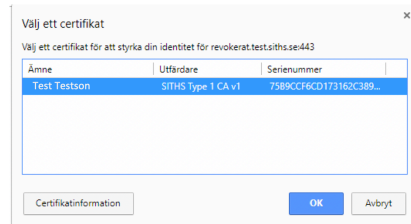
Olika användarupplevelse för olika webbläsare, versioner & plattformar
Komplex!



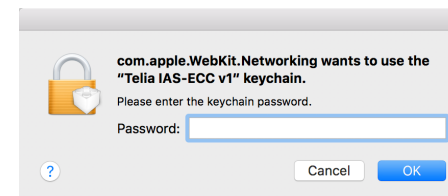
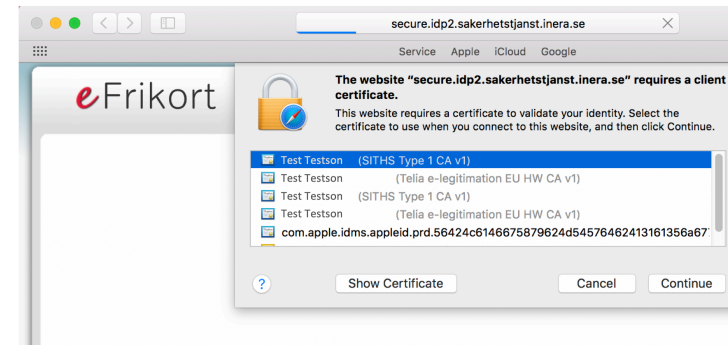
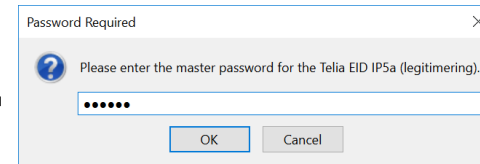
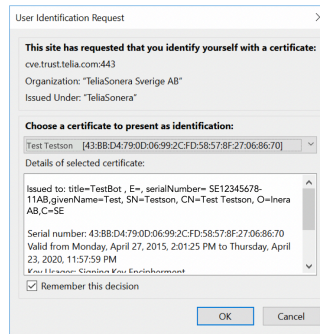
Internet Explorer 11



Microsoft Edge



Google Chrome

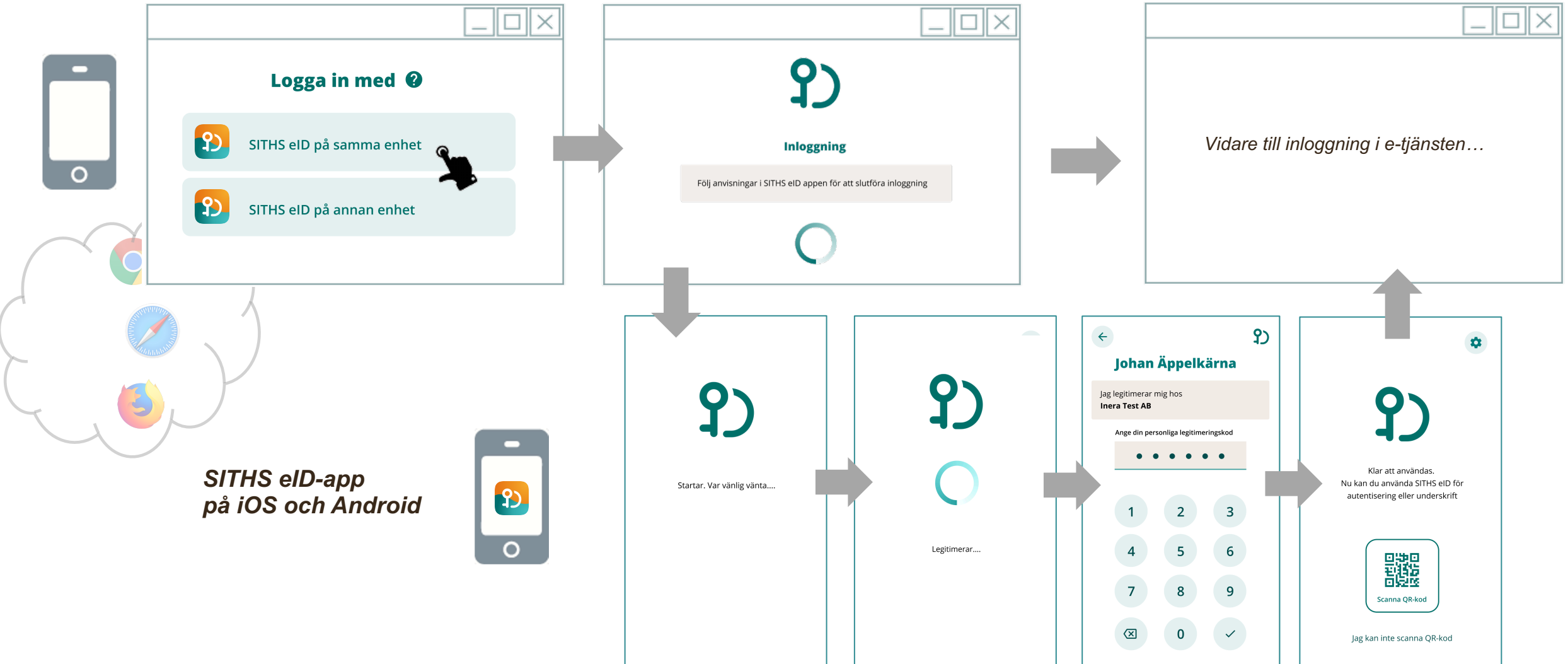


Mozilla Firefox

Mobil inloggning

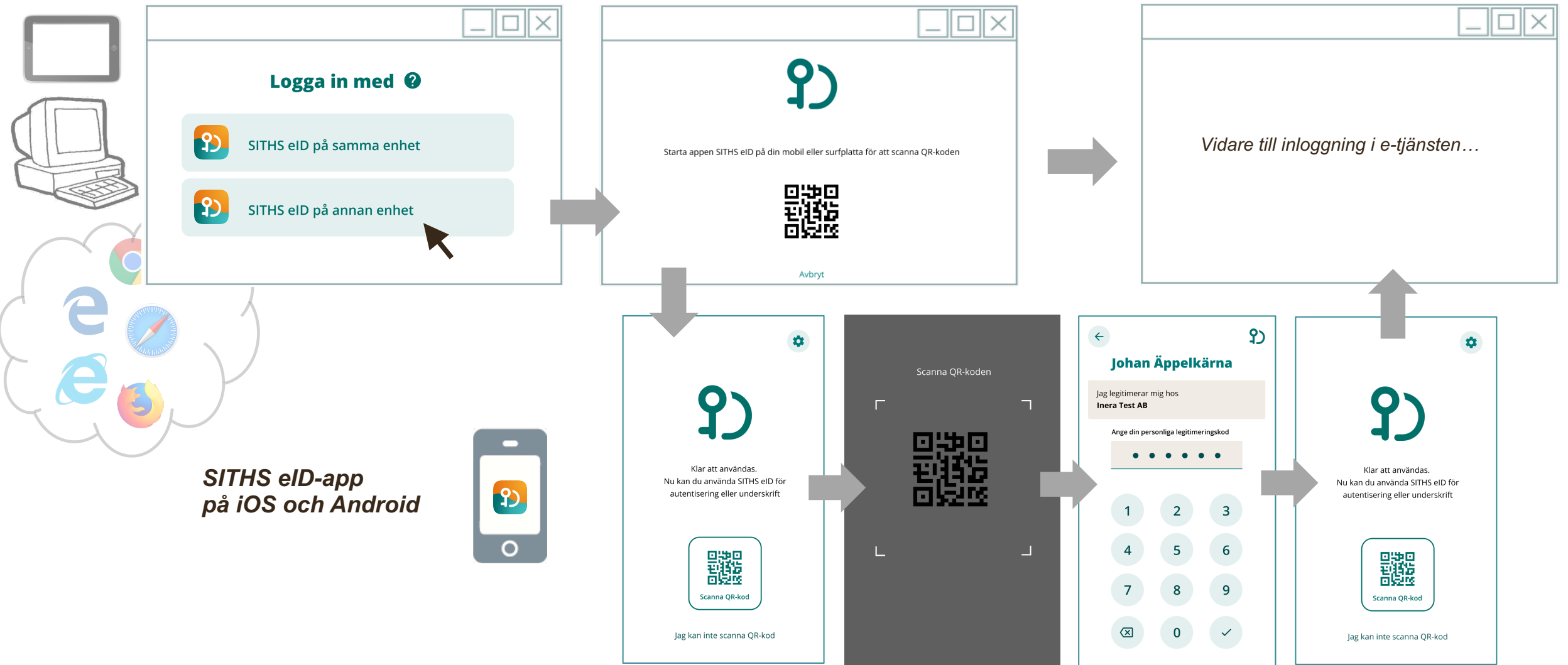
på samma enhet

Princip: Enhetlig användarupplevelse
på såväl mobil/surfplatta som dator och olika webbläsare



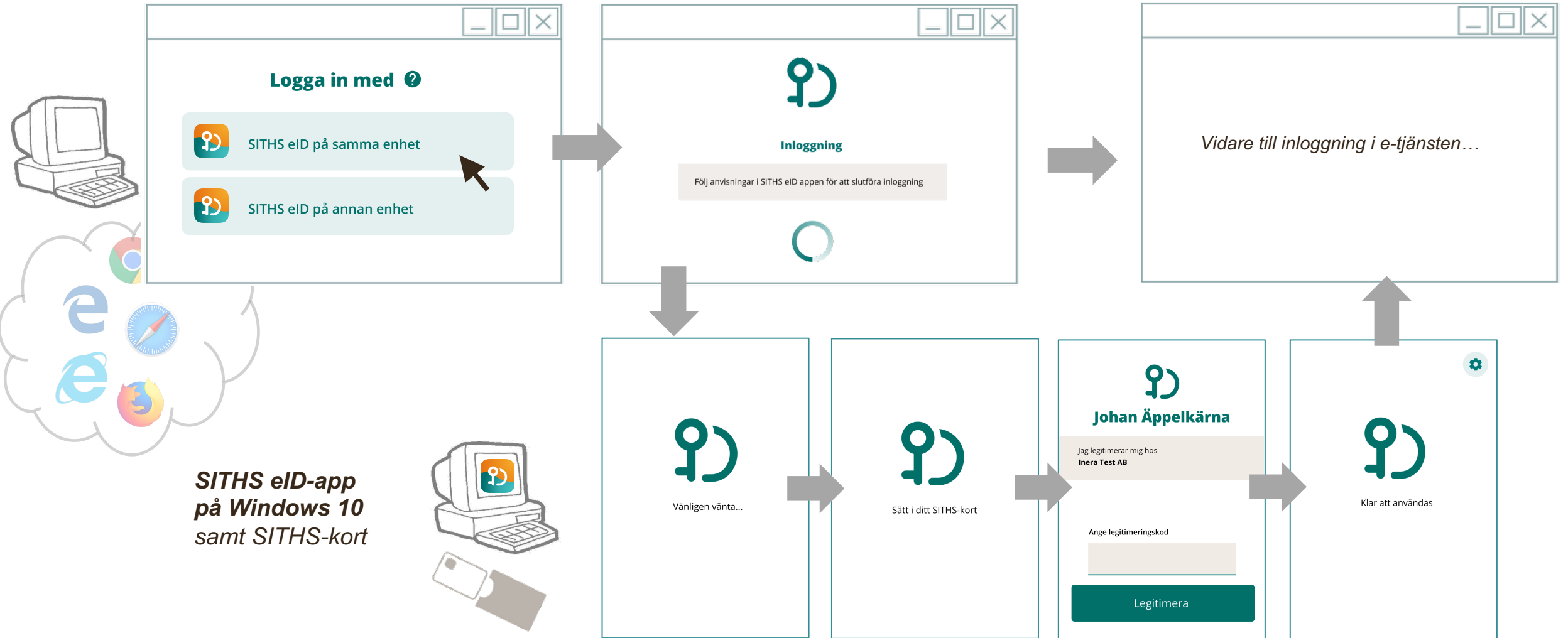
Mobil inloggning

på annan enhet



Inloggning med smart kort på dator

på samma enhet

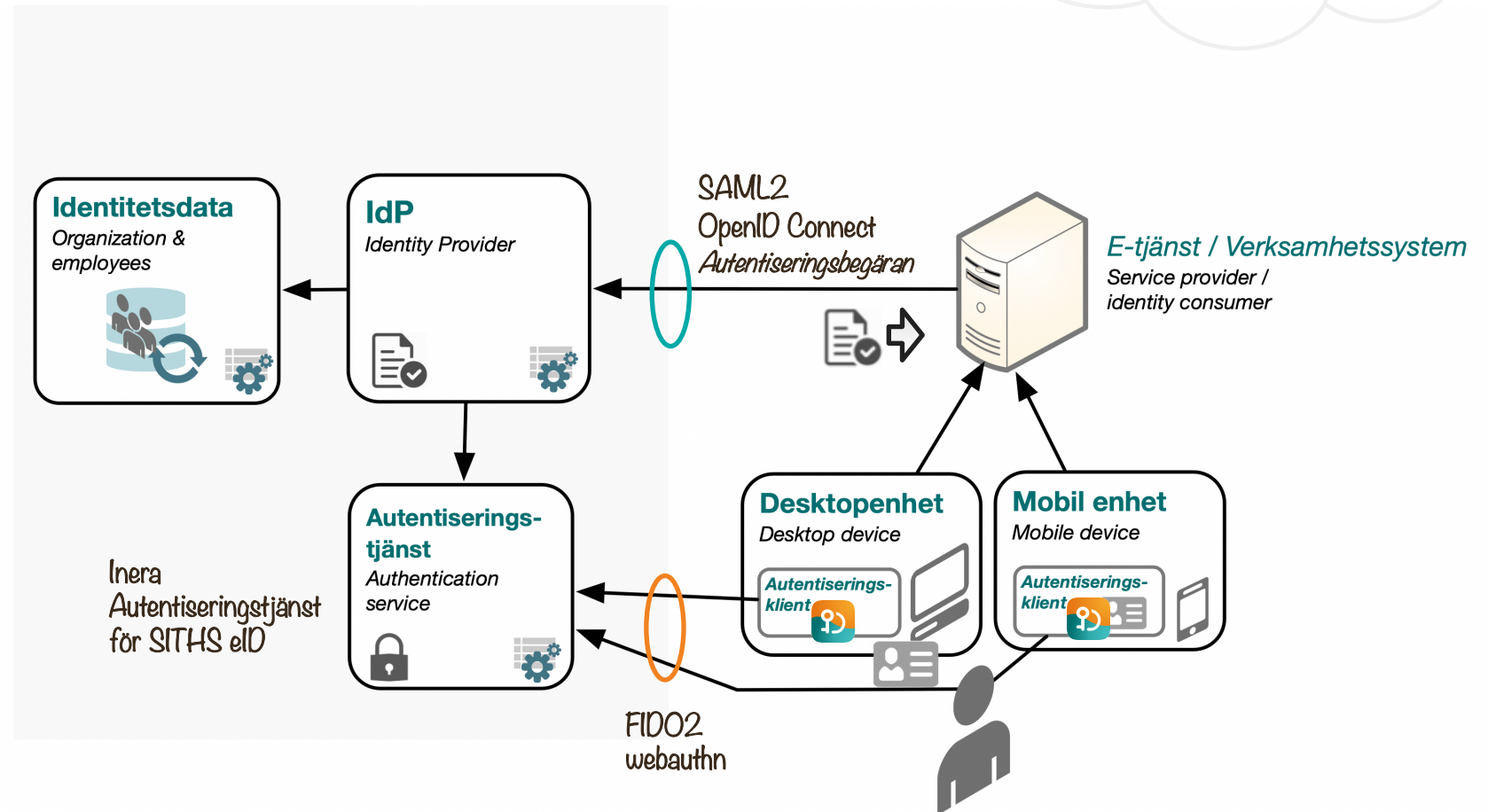
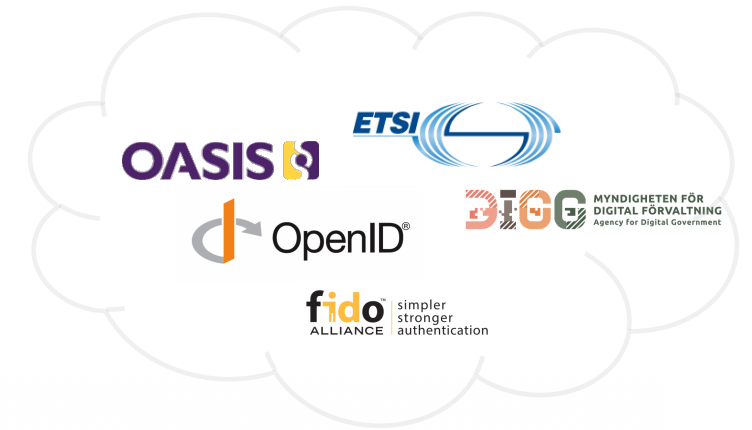


E-legitimering

Arkitekturell översikt & standarder

E-legitimering

Översiktlig arkitektur
Baserad på standarder
och nationell profilering



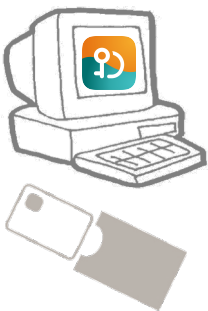
Utfärdande av Mobilt SITHS eID

Självservice

med id-växling från SITHS-kort (LoA3)

Utfärdande av Mobilt SITHS eID - via självservice

Win 10



Hantera SITHS eID

Aktiva Spärrade

⚠ Du har ingen aktiv Mobil SITHS e-id registrerad

Skapa nytt SITHS e-id

Skapa Mobil SITHS eID

Legitimering lyckades. För att ladda ner och aktivera Mobilt SITHS eID till din mobila enhet, starta appen på din mobila enhet och scanna QR-koden som visas

Registrering lyckades. Du kan nu använda ditt registrerade eID för legitimering och signering via din mobila enhet.

Innan du använder ditt eID för första gången rekommenderas att testa det i vår testmiljö.

Testa SITHS eID

iOS/iPadOS
och Android



SITHS eID saknas

Logga in på SITHS Mina sidor för att hämta ett nytt SITHS eID till denna enhet.

Hämta SITHS eID

Hur funkar SITHS eID?

Aktivera SITHS eID

Scanna QR-koden som visas på portalen.

Ditt personnummer

Var vänlig ange ditt personnummer för att verifiera ditt SITHS eID

Personnummer

YYYYMMDD-XXXX

1 2 3
4 5 6
7 8 9
0 ✓

Avbryt

Välj legitimeringskod

Legitimeringskod

• • • • •

Bekräfta legitimeringskod

1 2 3
4 5 6
7 8 9
0 ✓

Avbryt

Ditt SITHS eID är klart

Namn: Johan Äppelkärna med för långt namn som behöver radbryt
Utfärdare: Region Värmland
Giltigt t.o.m.: 2022-06-12

Använd SITHS eID

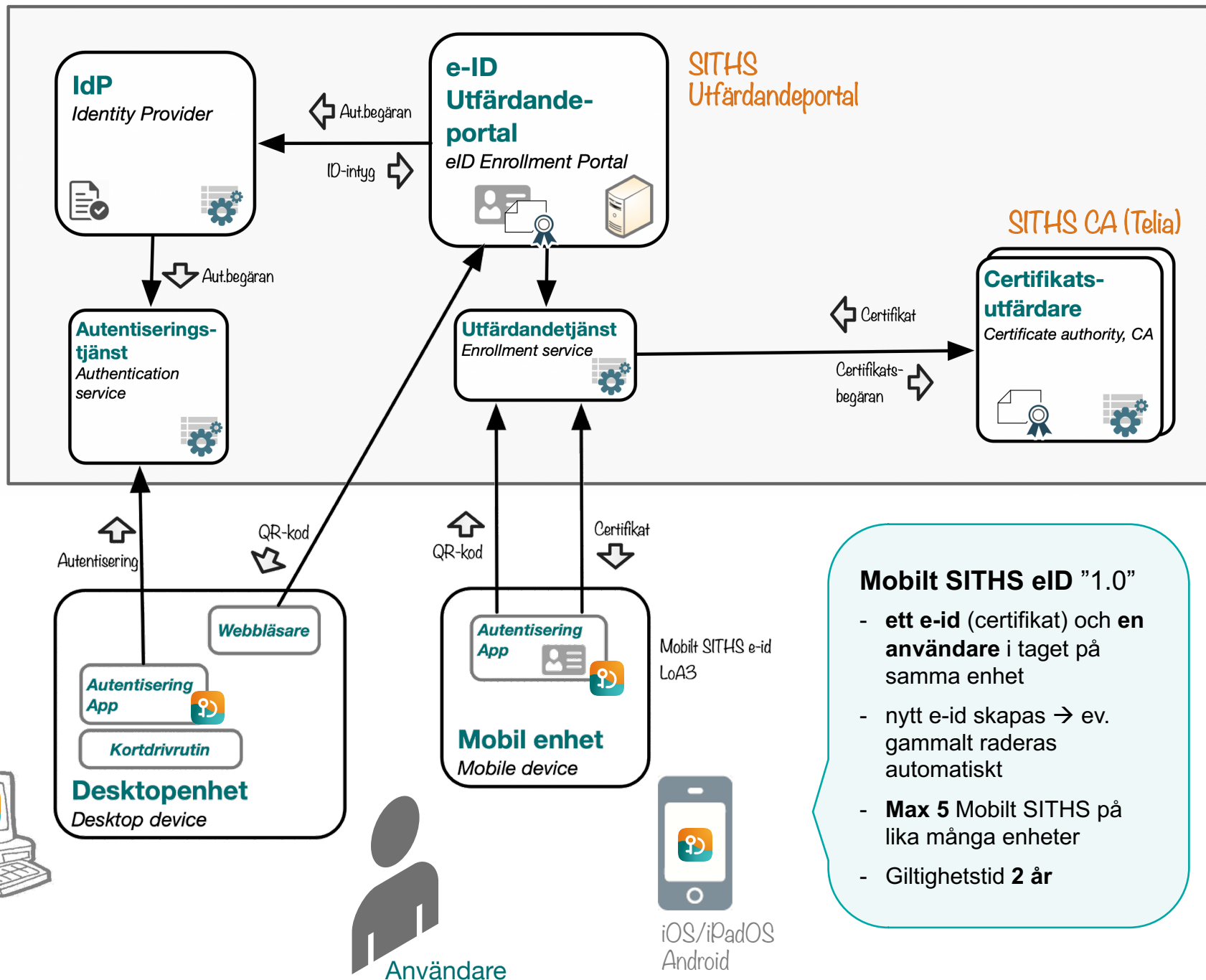
Utfärdande av Mobilt SITHS eID via självservice

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

För granskning enligt Svensk e-legitimation tillitnivå 3

LoA = Level of Assurance = tillitnivå

SITHS eID tillitnivå 3 (LoA3)



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

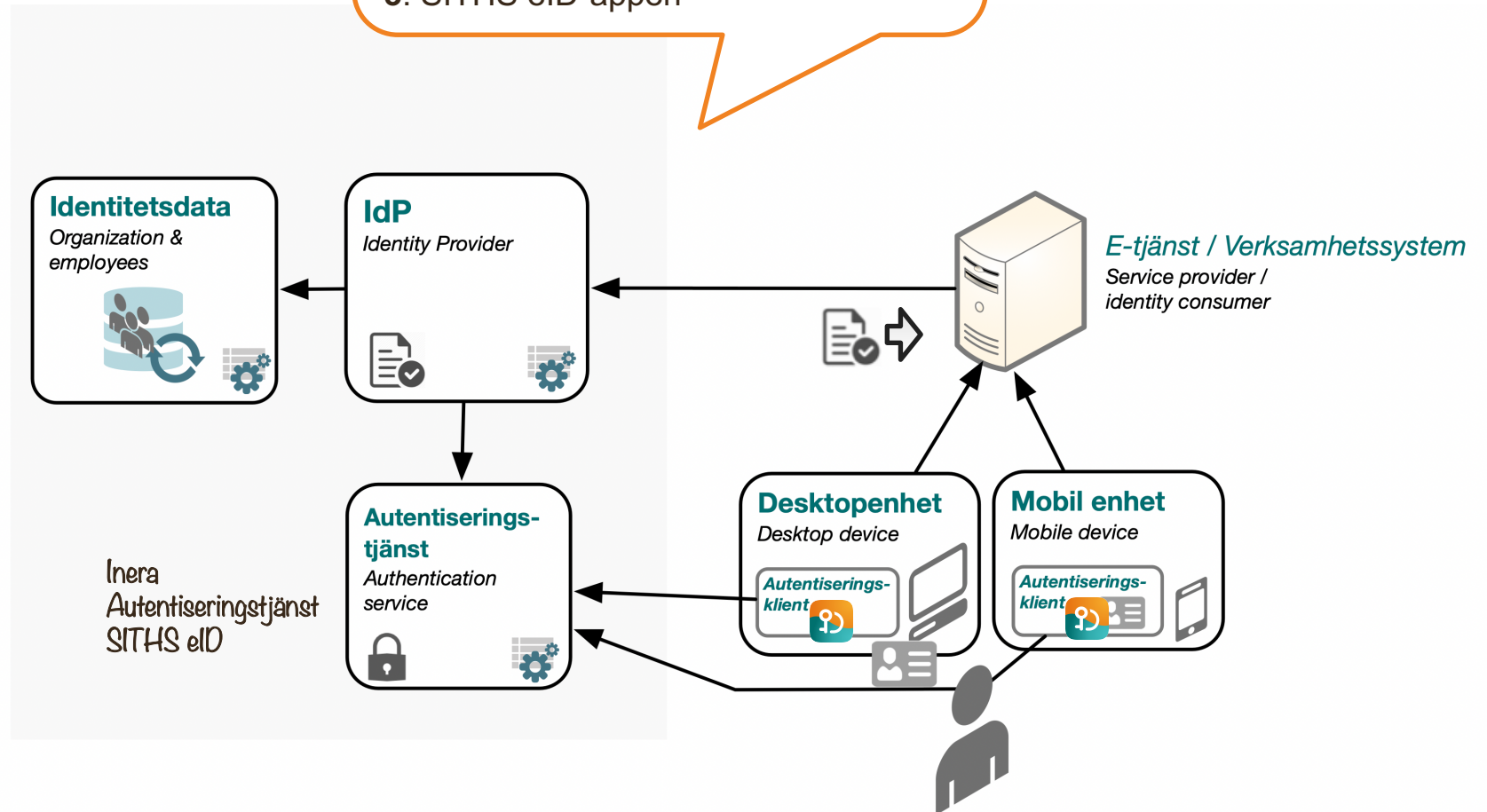
Tillämpningar - Pilotprojekt

E-legitimering

Översiktlig arkitektur

Vad behövs för anslutning?

1. En IdP-tjänst ansluten till Autentiseringstjänst för SITHS eID
2. Systemet anslutet till IdP-tjänsten
3. SITHS eID-appen



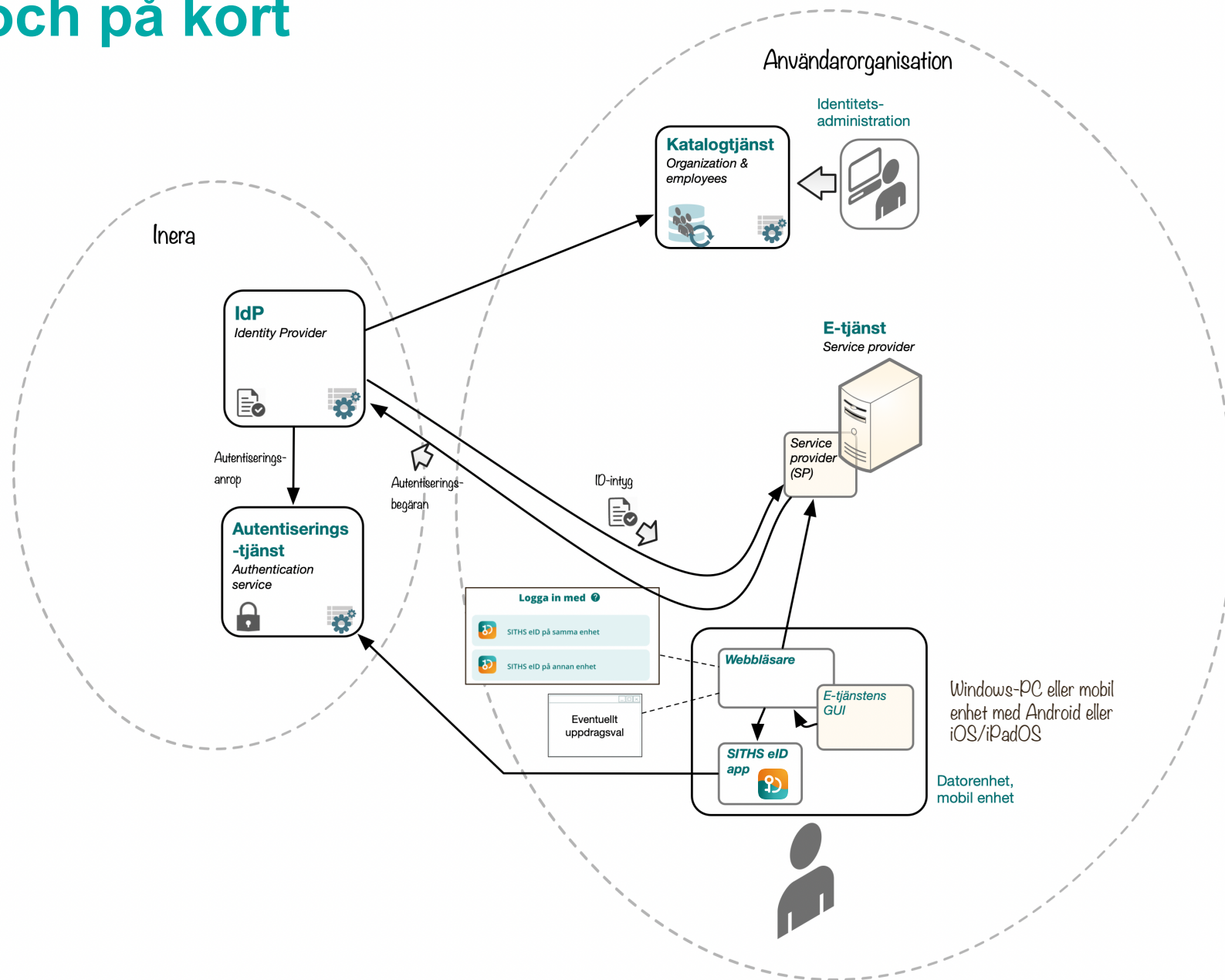
SITHS eID - Mobilt och på kort

Anslutningsmönster

Lokalt system till Ineras IdP

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

➤ Mindre utrymme för lokal anpassning / funktionalitet

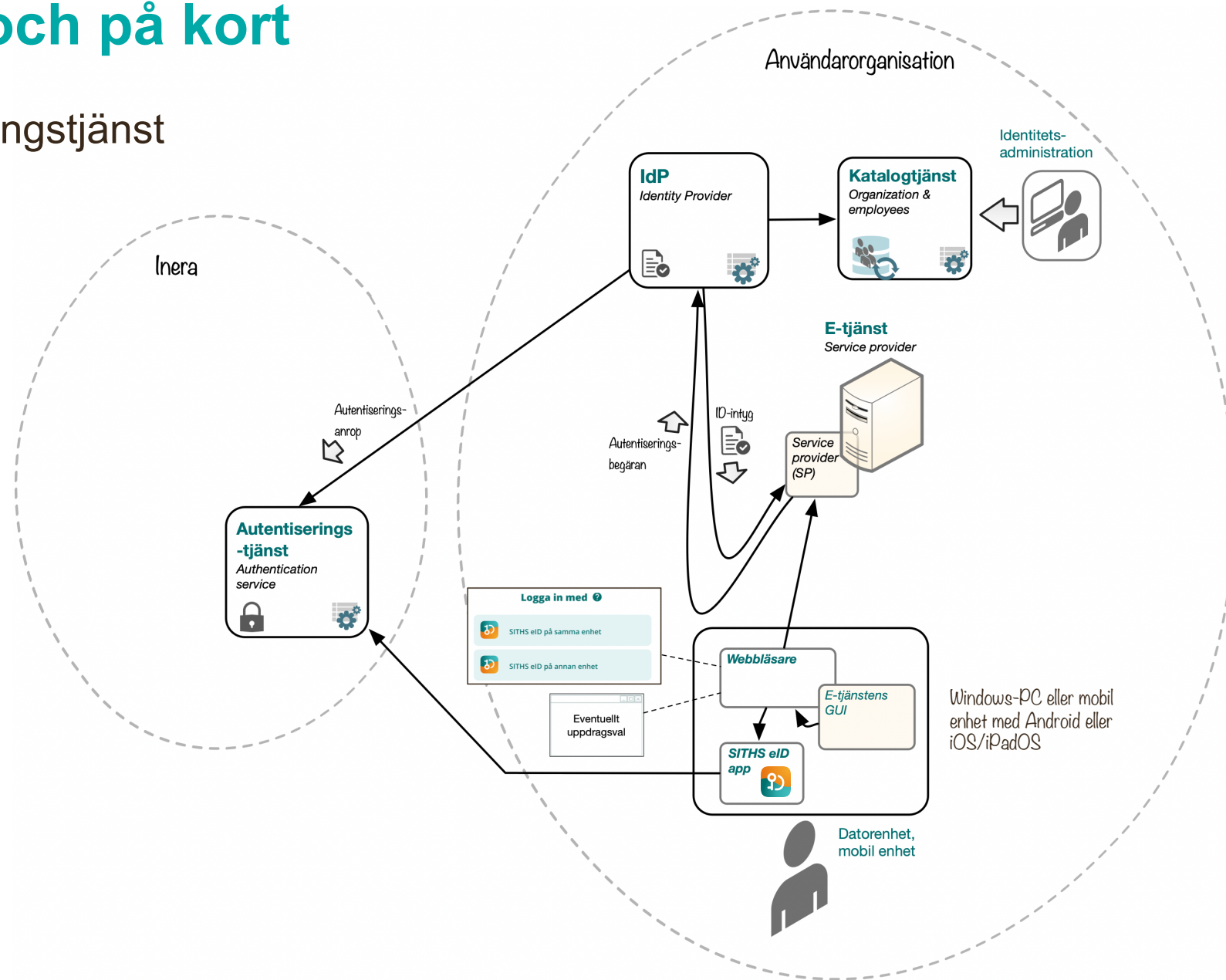


SITHS eID - Mobilt och på kort

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

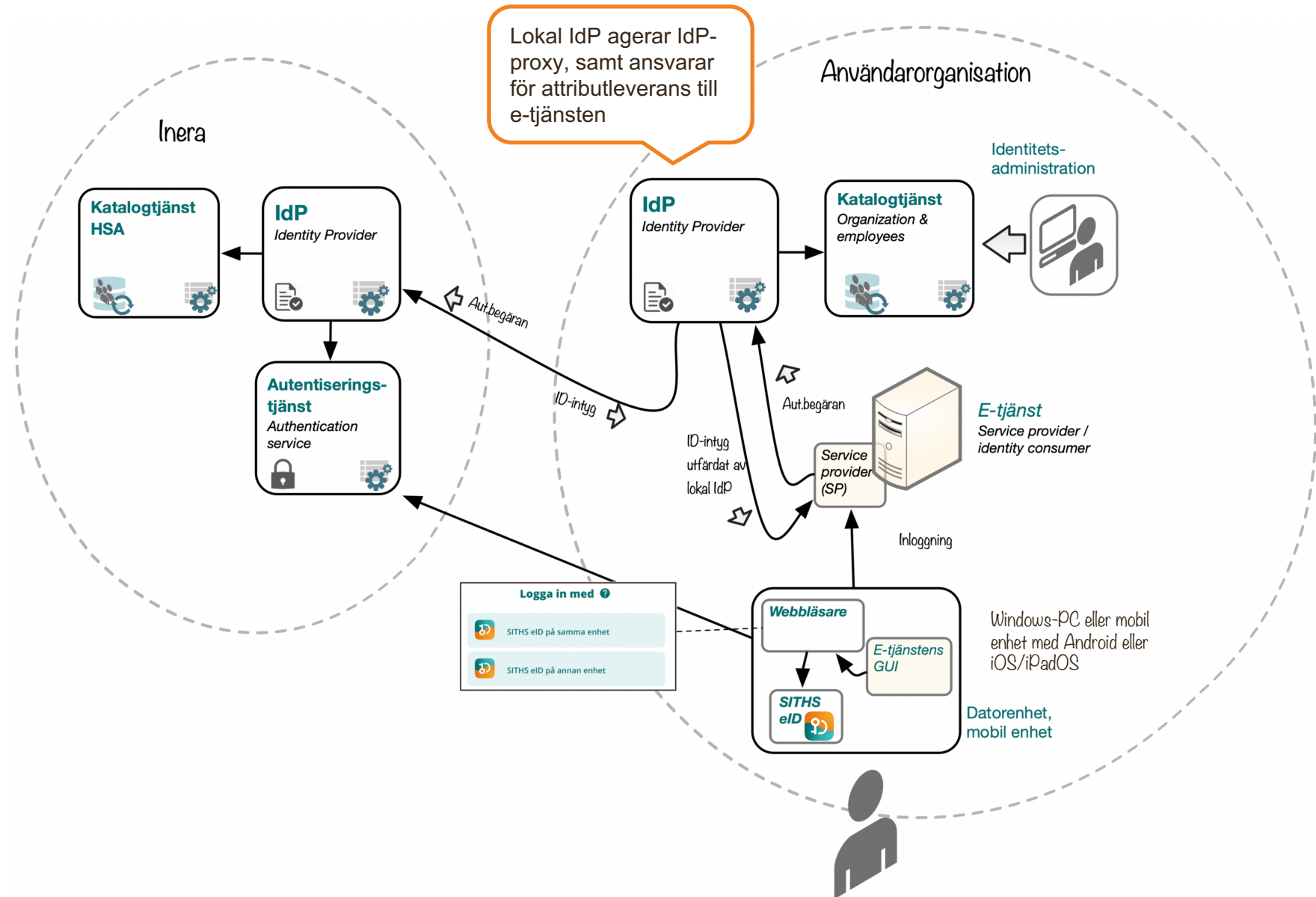


SITHS eID - Mobilt och på kort

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



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)

Dokumentet kan ändras utan att bryta "signeringen"

Löst kopplad information om vem som signerat och när



Lisa Svensson,
2019-08-26



Digital signatur

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

Starkt kopplad information om vem som signerat och när.



Lisa Svensson,
2019-08-26

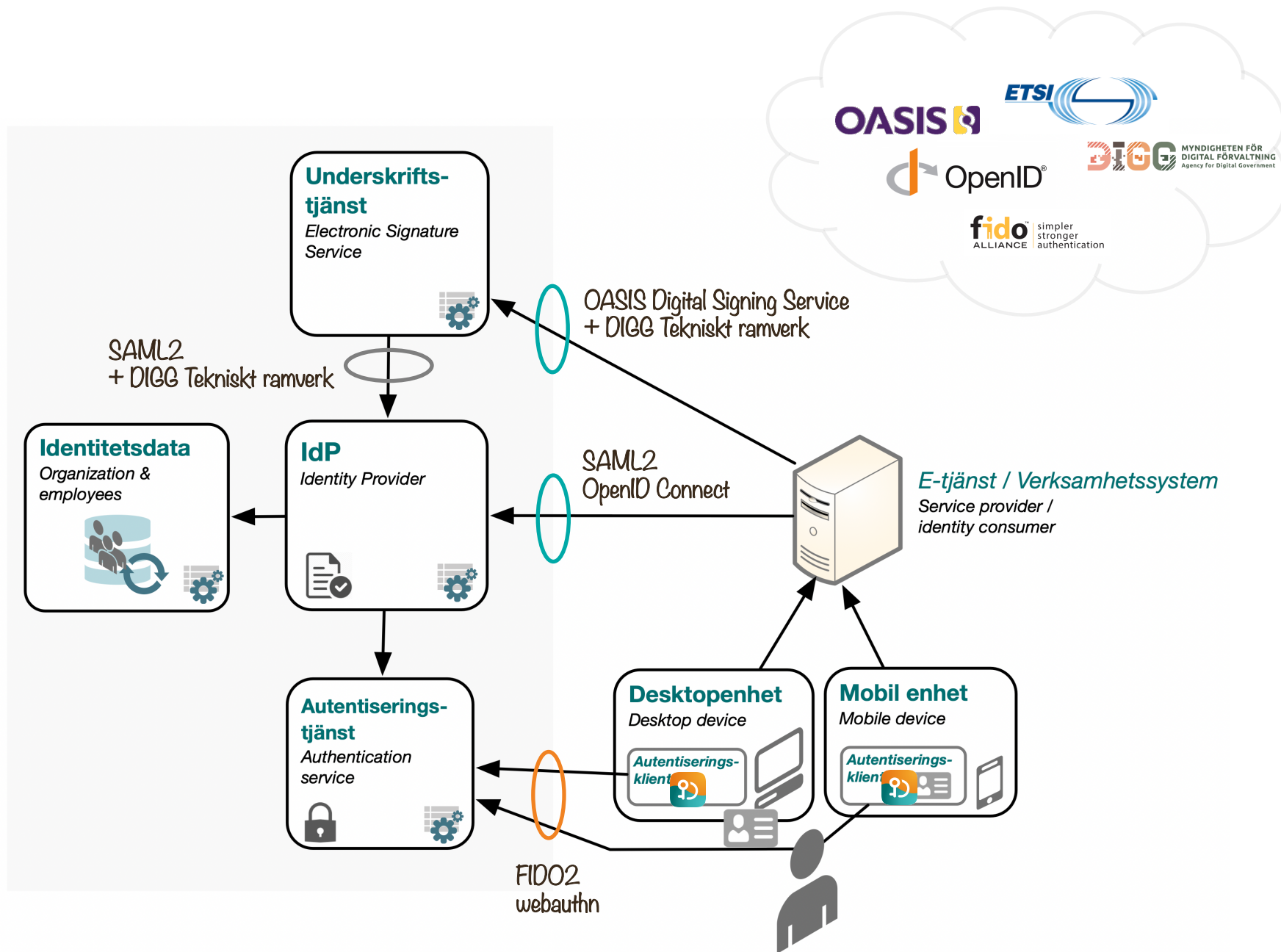
Kan göras verifierbar inom samma IT-system

Verifierbar även hos andra parter med andra IT-system

E-underskrift

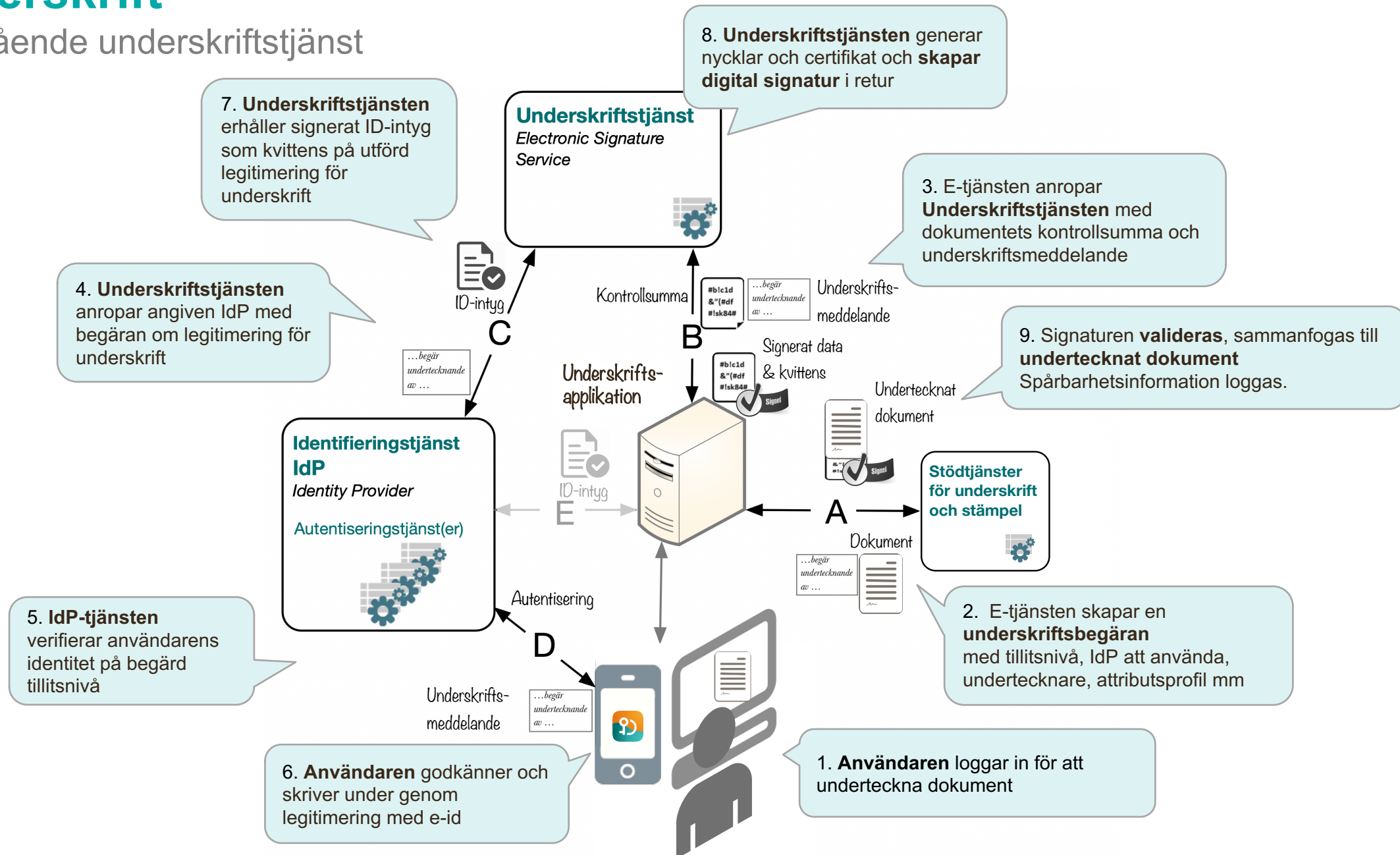
Översiktlig arkitektur
Baserad på standard
och nationell profilering

- ✓ **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



Skriv under med ?

- SITHS eID på samma enhet
- SITHS eID på annan enhet

Följ anvisningar i SITHS eID appen för att slutföra underskrift

Du har skrivit under följande:
Jag gör en testunderskrift.



SITHS eID-app
på iOS och Android



Startar. Var vänlig vänta....

Legitimerar....

Johan Äppelkärna

Jag skriver under hos
Inera Test AB

Jag gör en testunderskrift.

Ange din personliga legitimeringskod

1 2 3
4 5 6
7 8 9
0 ✓

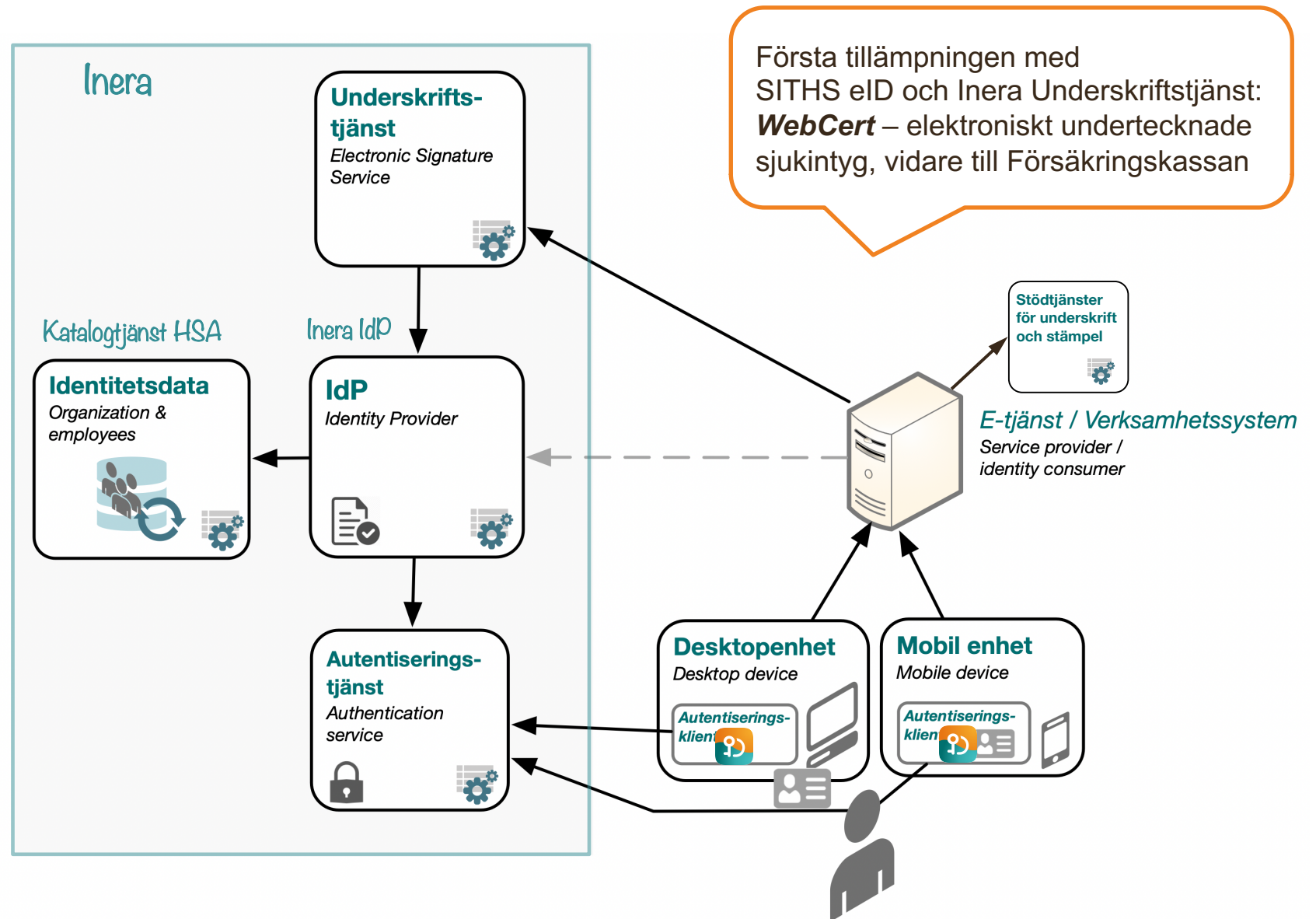
Klar att användas.
Nu kan du använda SITHS eID för
autentisering eller underskrift

Scanna QR-kod

Jag kan inte scanna QR-kod

E-underskrift

Anslutning till Ineras
Underskriftstjänst

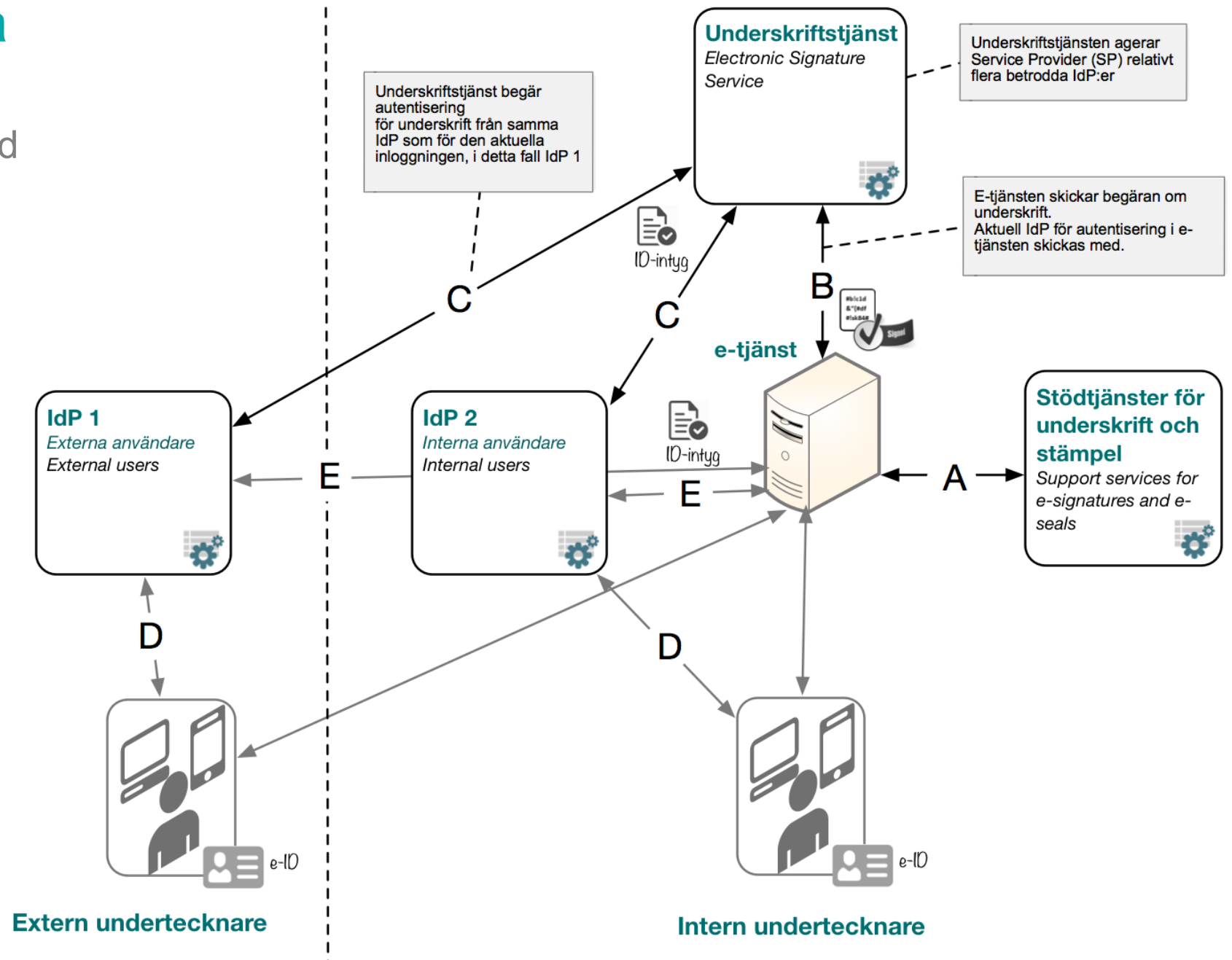


Externa och interna undertecknare

- via federativt samverkan med flera IdP:er

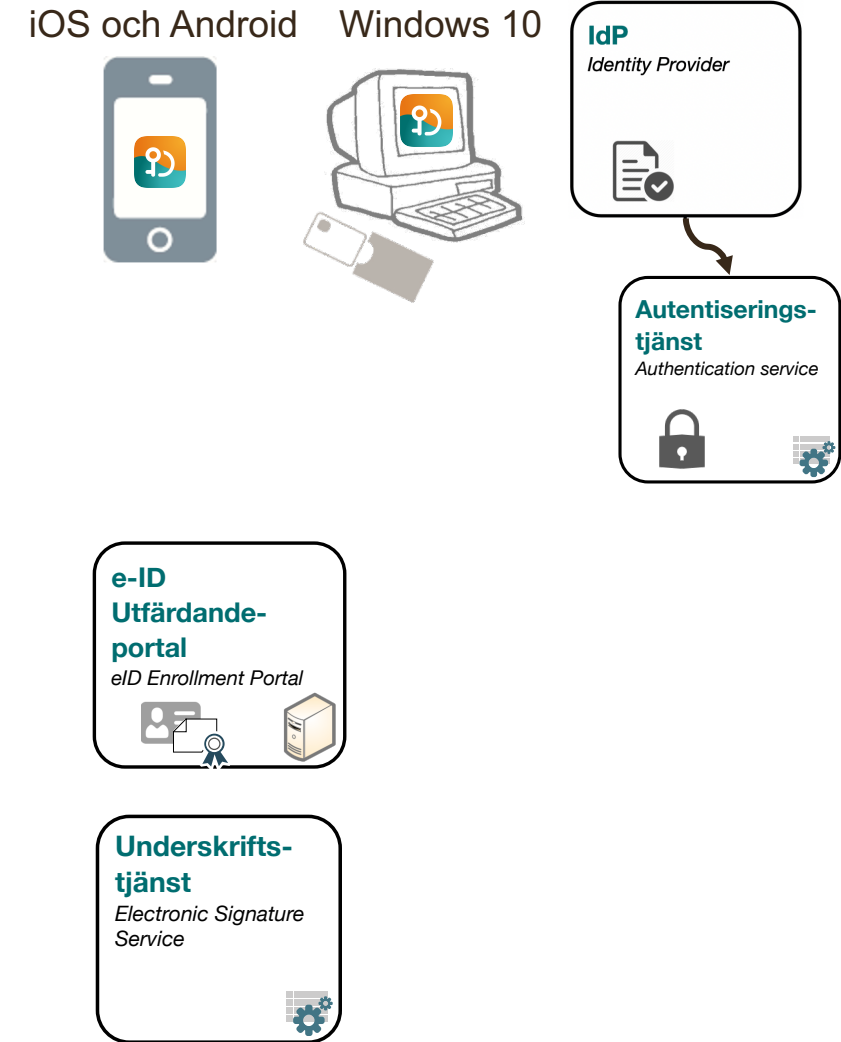
Exempel:

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