

Nya och förändrade lösningar inom SITHS och vägen framåt

SITHS-dagen 2021-05-27

Per Mützell per.mutzell@inera.se

Nytt sätt att logga in och underteckna med SITHS eID

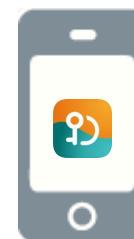
- genom en ny autentiseringsmetod

- **Mobilt SITHS** tillitsnivå 3 som komplement till SITHS eID på kort
- **Utfärdande** av Mobilt SITHS via självservicefunktion och SITHS-kortet
- **E-legitimering** och **e-underskrift** via samma SITHS eID-app, med dator såväl som mobil
- **E-underskrift** med stöd av en fristående **Underskriftstjänst**

SITHS e-legitimation bär kvalitetsmärket [Svensk e-legitimation](#) efter granskning och godkännande av Myndigheten för digital förvaltning, DIGG, på tillitsnivå 3. Granskningen visar att lösningen lever upp till myndighetens högt ställda krav för säkra och flexibla mobila lösningar.



iOS/iPadOS
Android



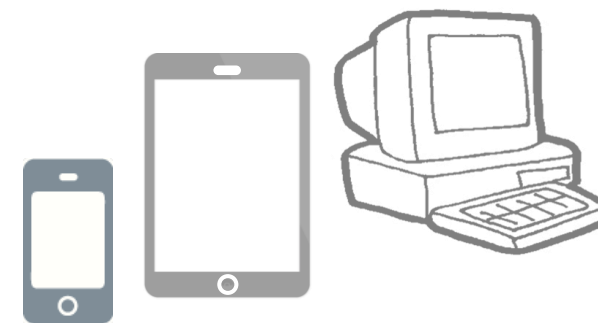
Windows



Varför införs ny autentiseringsteknik i SITHS?

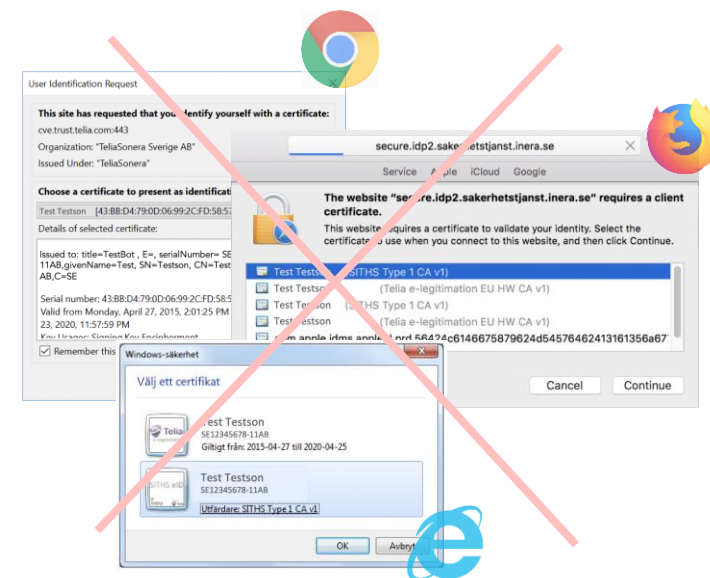
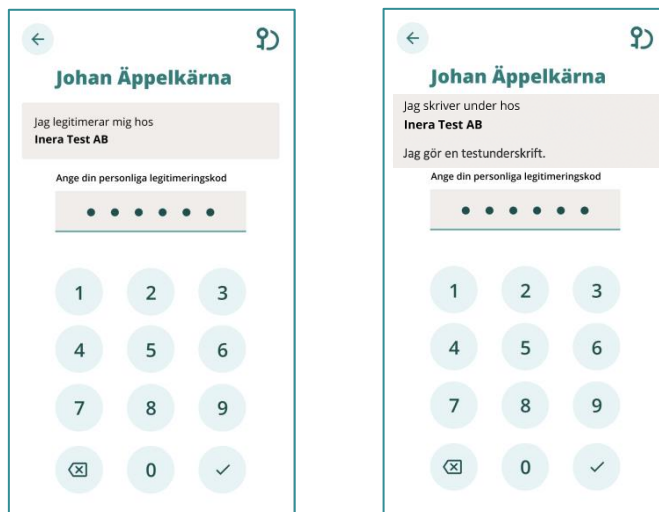
- Möjliggöra **flexibla** och **mobila arbetssätt**

- › använda mobil enhet som arbetsverktyg
- › eller, använda dator men ha sitt eID på en mobil enhet



- **Enhetlig användarupplevelse** och **minskat teknikberoende** vid inloggning och underskrift

- Stöd för **standardteknik** för smarta kort och andra ev. framtida bärare av SITHS eID



Lösningarna följer Ineras referensarkitekturer

Arkitekturen för Mobilt SITHS och Inera Säkerhetstjänster utformas utifrån

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

Källa: <https://rivta.se>



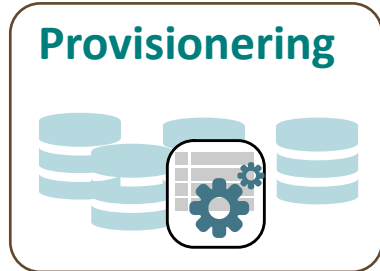
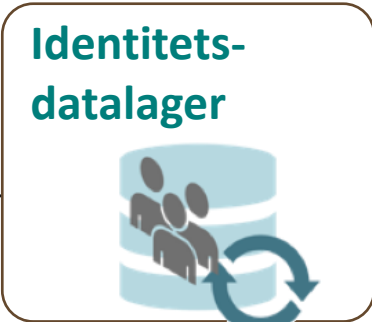
- **Vägledning** – styrande principer, gemensamma krav, mönster
- **Underlag vid anskaffning**
- **Underlag för anpassning av verksamhetssystem**

Referensarkitekturen

Regelverks-
administration



Identitets- och
behörighets-
administration



Federation

Medlemmar



Tillitsramverk



Attribut



Godkännande-
process



**Åtkomstintygs-
utfärdare**



**IdP
Identity Provider**



Autentiseringstjänster



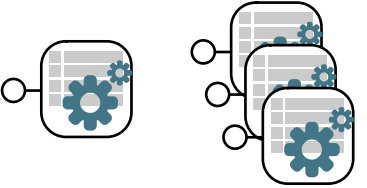
**E-identitets-
utfärdare**



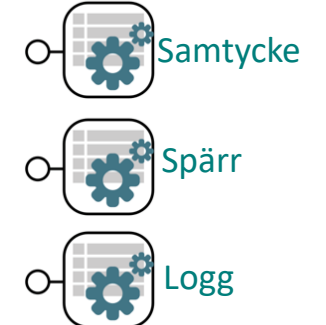
E-tjänster



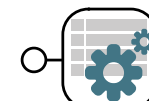
API Säkerhet



Stödtjänster



Underskriftstjänst



Inloggning

Underskrift

e-id

Utfärdande



Referensarkitekturen

Regelverks-
administration



Regelverks-
tjänst



Identitets- och
behörighets-
administration



IdP-tjänsten är "navet"
för säker autentisering av
användaren vid både
inloggning och underskrift

Autentiseringstjänsten (NY)
- stöd för **Mobilt SITHS**
- autentisering på samma eller
annan enhet

Provisionering

**Utfärdande av
Mobilt SITHS (NY)**

Federation

Medlemmar



Tillitsramverk



Attribut



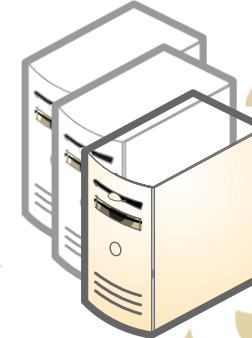
Godkännande-
process



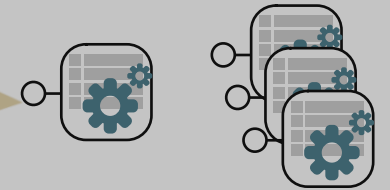
**Standardiserad
anslutningsteknik**
SAML2, OpenID Connect

Åtkomst-
utfärdare

E-tjänster



API Säkerhet



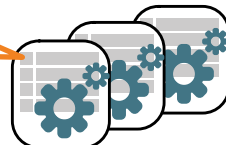
Stödtjänster



**IdP
Identity Provider**



Autentiseringstjänster



Inloggning



e-id

Utfärdande

**E-identitets-
utfärdare**

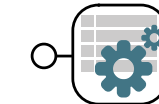


Underskrift

**Underskriftstjänsten
(NY)**

Avancerad elektronisk
underskrift via fristående tjänst

Underskriftstjänst

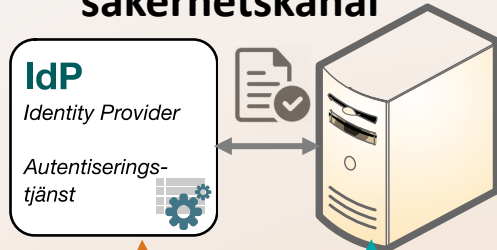


*E-legitimering och e-underskrift
med Mobilt SITHS eller SITHS-kort*

Från delad till separat säkerhetskanal

Ökad flexibilitet - minskat teknikberoende

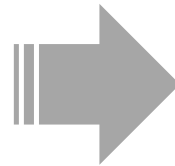
Delad informations- & säkerhetskanal



Tekniska inlåsningar
- webbläsarna
- kortläsarna måste
finnas "överallt"

Försvårar mobilitet!

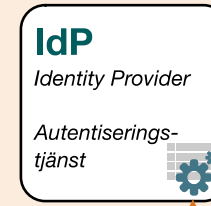
Separat
säkerhetskanal
"Out-of-band"-teknik



- ✓ Använd **samma eller annan enhet** för legitimering och underskrift
- ✓ **Minskat teknikberoende**, stöd för "nedlåst" utrustning, moderna webbläsare
- ✓ Stöd för **mobilitet**

Säkerhetskanal

Informationskanal

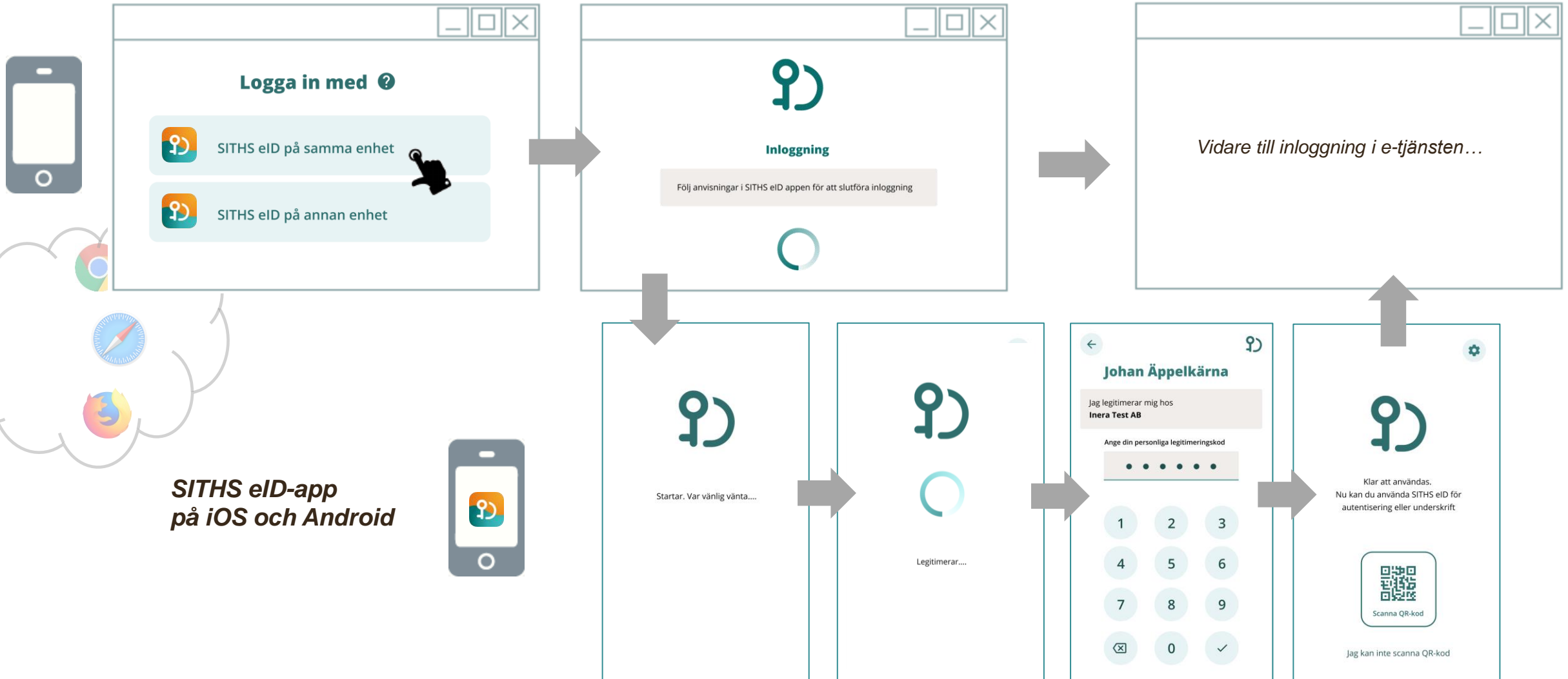


Mobil inloggning

på samma enhet

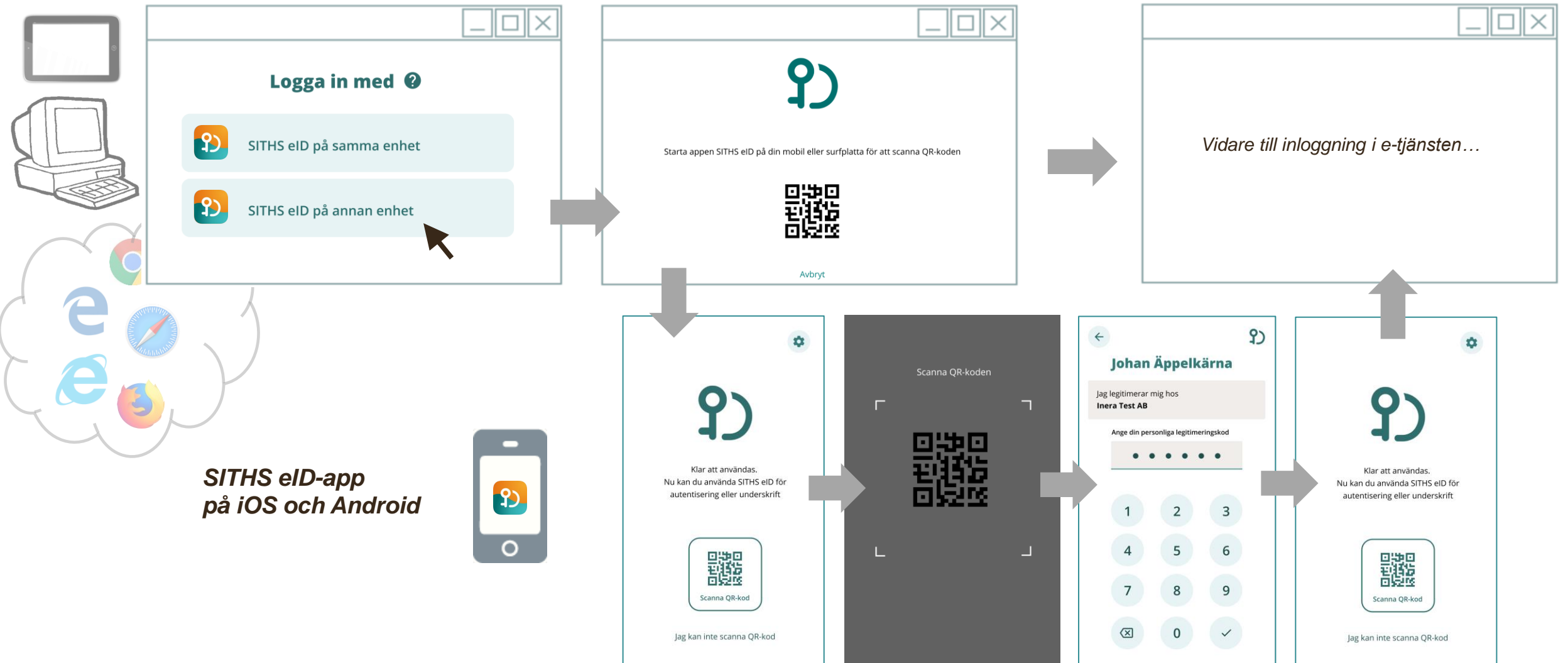
Enhetlig användarupplevelse

på såväl mobil/surfplatta som dator och olika webbläsare



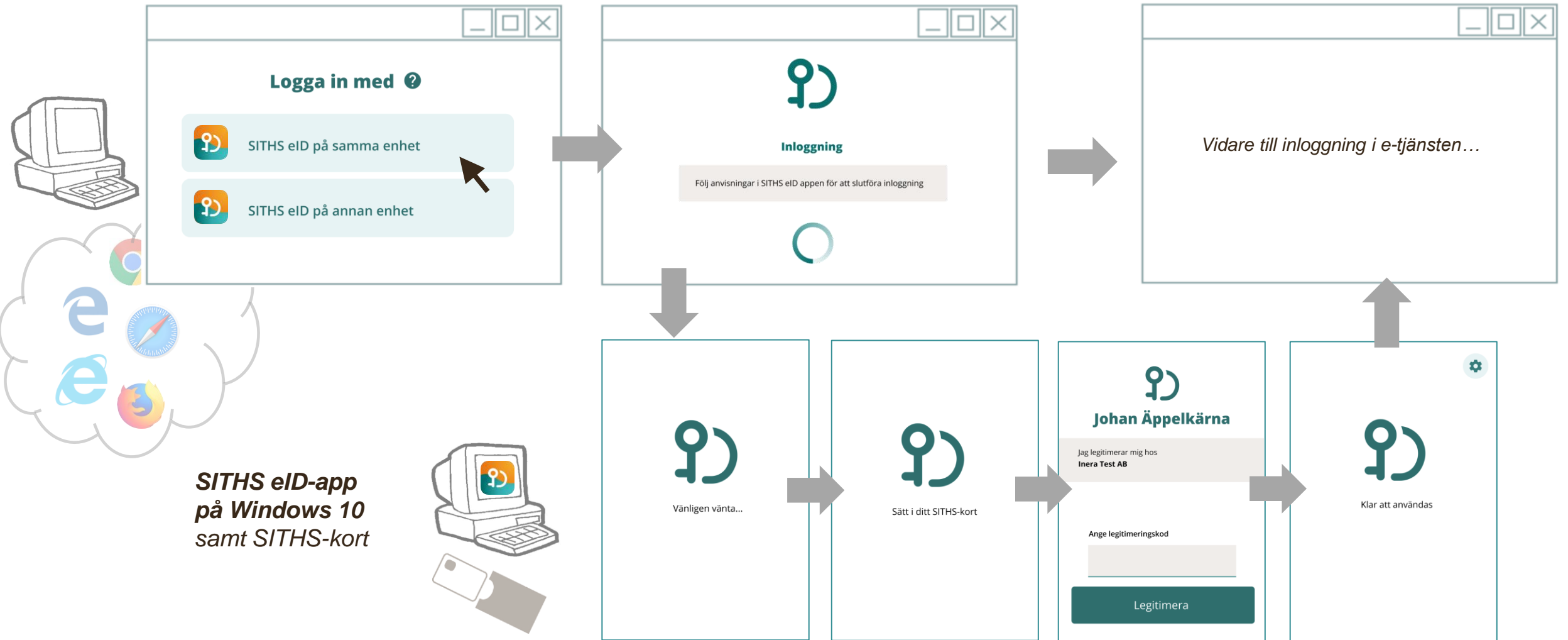
Mobil inloggning

på annan enhet



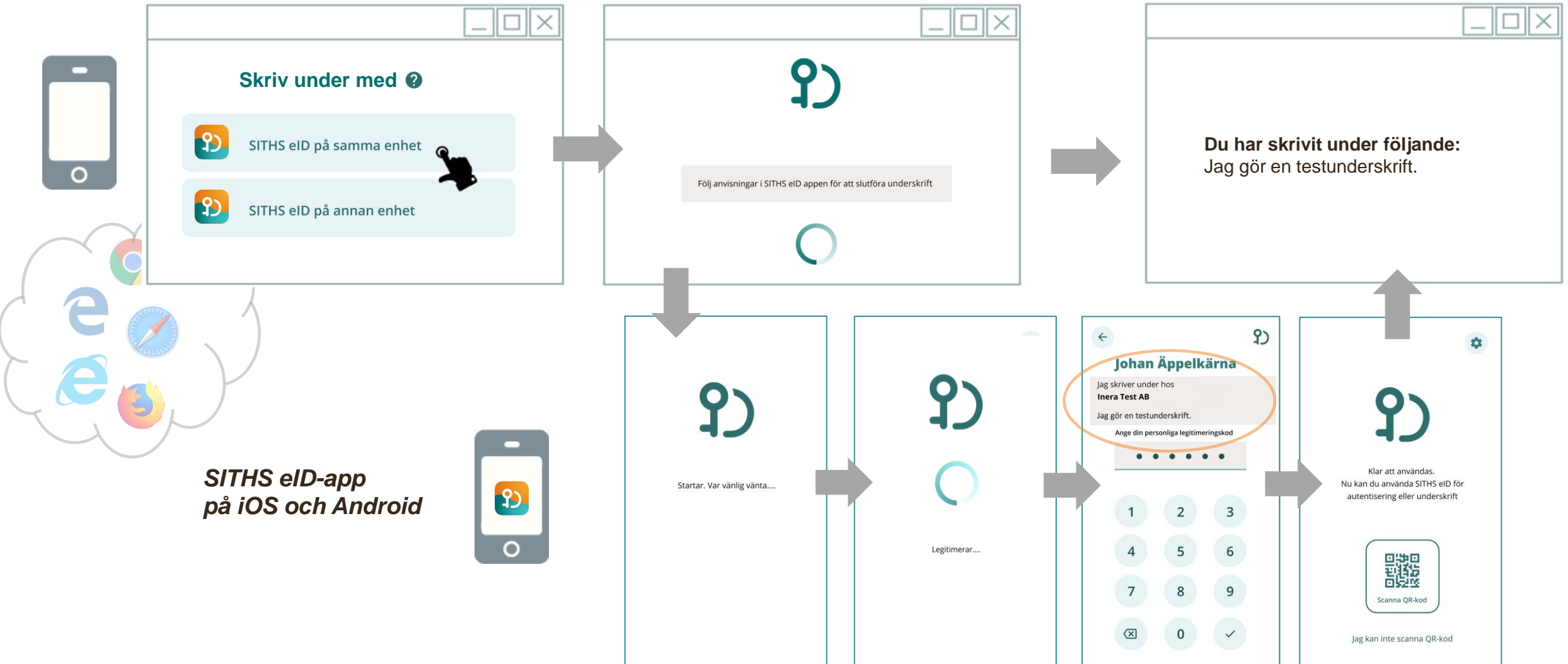
...och förstås även inloggning med smart kort på dator

på samma enhet enbart



Mobil underskrift

på samma eller annan enhet med stöd av Underskriftstjänst



Utfärdande av Mobilt SITHS

Självservice

med id-växling från SITHS eID med tillitsnivå 3

Utfärdande av Mobilt SITHS via självservice



SITHS-kort
tillitsnivå 3

iOS/iPadOS
och Android



Hantera SITHS eID

Aktiva Spärrade

⚠ Det finns inga mobila SITHS eIDn att visa här.

Skapa nytt SITHS eID

Skapa nytt SITHS eID

Användarvillkor

Jag har tagit del av och är införstådd med vilka regler som gäller vid användning, hantering och förlust av min elektroniska identitetshandling och de tillhörande koderna.

SITHS e-legitimation med tillhörande koder är personliga och ska hanteras som värdehandlingar.

För fullständiga villkor se dokumentet "Allmänna villkor för SITHS e-legitimation" som finns tillgängliga på:
<https://www.inera.se/siths/repository>

Accepteras användarvillkoren behöver du legitimera dig på nytt.

Acceptera användarvillkor Avböj användarvillkor

Logga in med ?

SITHS eID på samma enhet

SITHS eID på annan enhet

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?

Utfärdande av Mobilt SITHS via självservice



SITHS-kort
tillitsnivå 3

iOS/iPadOS
och Android



Hantera SITHS eID

Aktiva Spärrade

⚠ Det finns inga mobila SITHS eID:n att visa här.

Skapa nytt SITHS eID

Skapa nytt SITHS eID

Legitimering lyckades. För att skapa ett SITHS eID, starta applikationen SITHS eID på din mobila enhet och scanna QR-koden som visas nedan.

Aktiveringskoden är endast giltig i 15 minuter. Om aktiveringskoden inte använts inom 15 minuter behöver du hämta en ny.

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

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

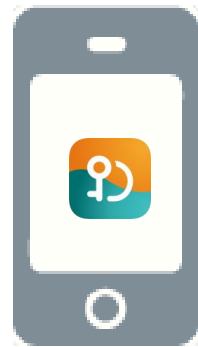
Ditt SITHS eID är klart

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

Använd SITHS eID

Om Mobilt SITHS

- **Svensk e-legitimation tillitsnivå 3**
- Kräver **personnummer** samt växling från **SITHS e-legitimation tillitsnivå 3** från utfärdande organisation
- **Max 1st aktiv på samma mobil** (= en användare i taget)
Befintligt Mobilt SITHS tas bort om ett nytt laddas ned.
- **Max 5st per användare** (på olika mobiler)
- Kan **spärras** av användaren själv i Utfärdandeportalen, av ID-administratör i SITHS-admin, eller 24x7 via Telia servicetelefon



- AppStore / Google Play eller organisationsstyr (MDM)
- **iOS , iPadOS 12+** men 14 rekommenderas
- **Android 7.1.1+** men 10 eller 11 rekommenderas
- Kräver **säkerhetschip i mobilen**
- **Biometri** som alternativ till kod i kommande version kräver hårdvarustöd för fingeravtryck och/eller ansiktsigenkänning

Leverans 2
(2022)

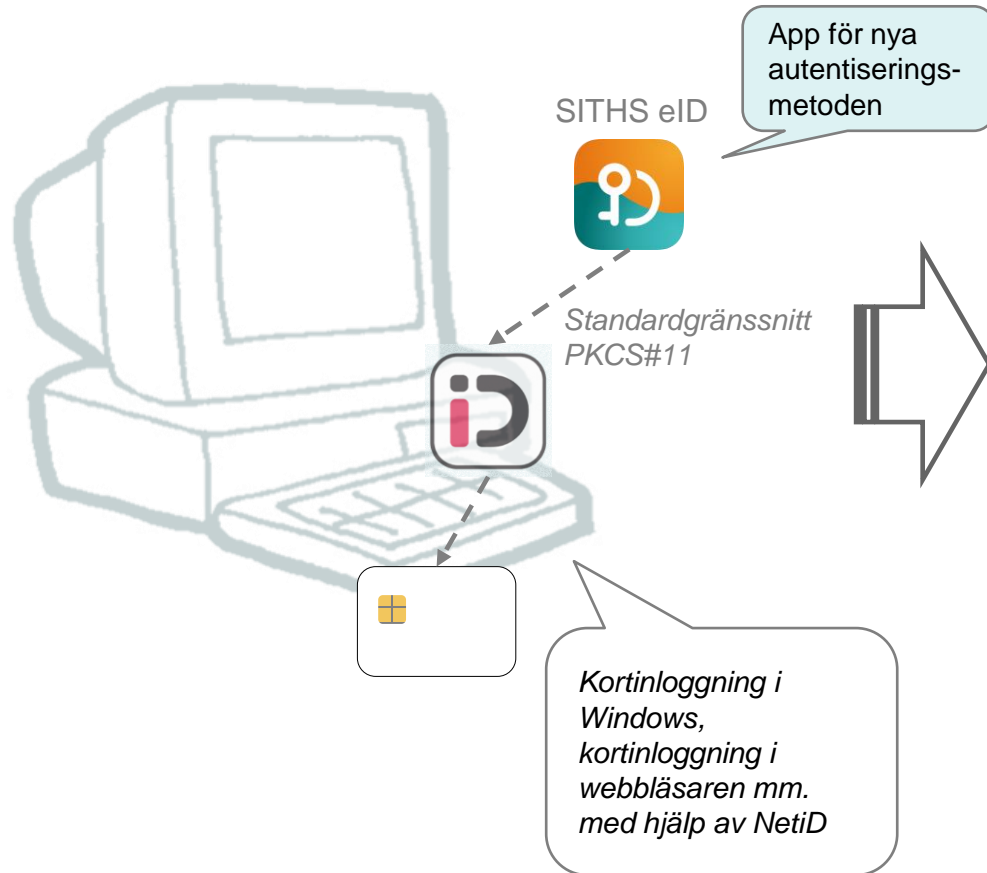


*Använda **SITHS**-kortet i datorn*

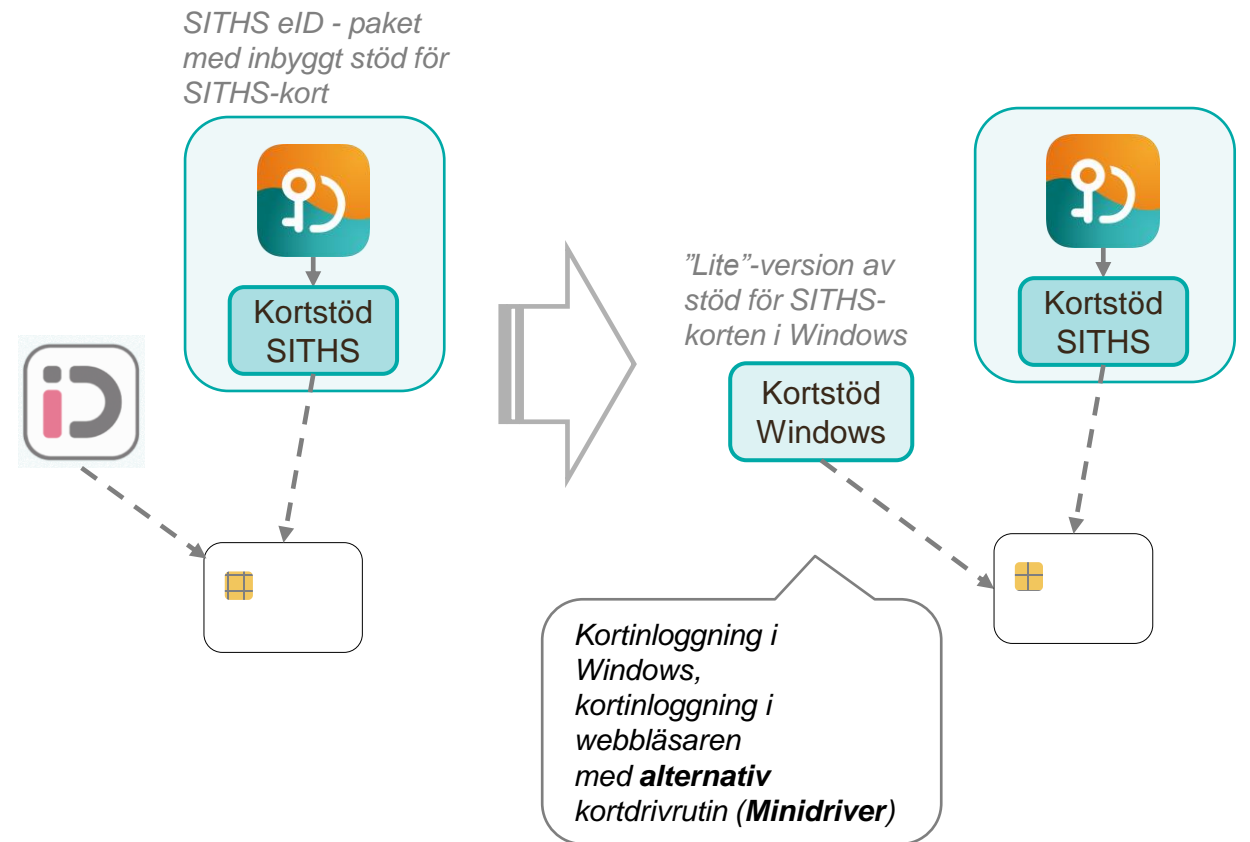
- Vilka förändringar kommer här?

Programvara för SITHS-kort på datorn - stegvis leverans

Leverans 1 (tillgängligt idag)



Leverans 2 (2022)



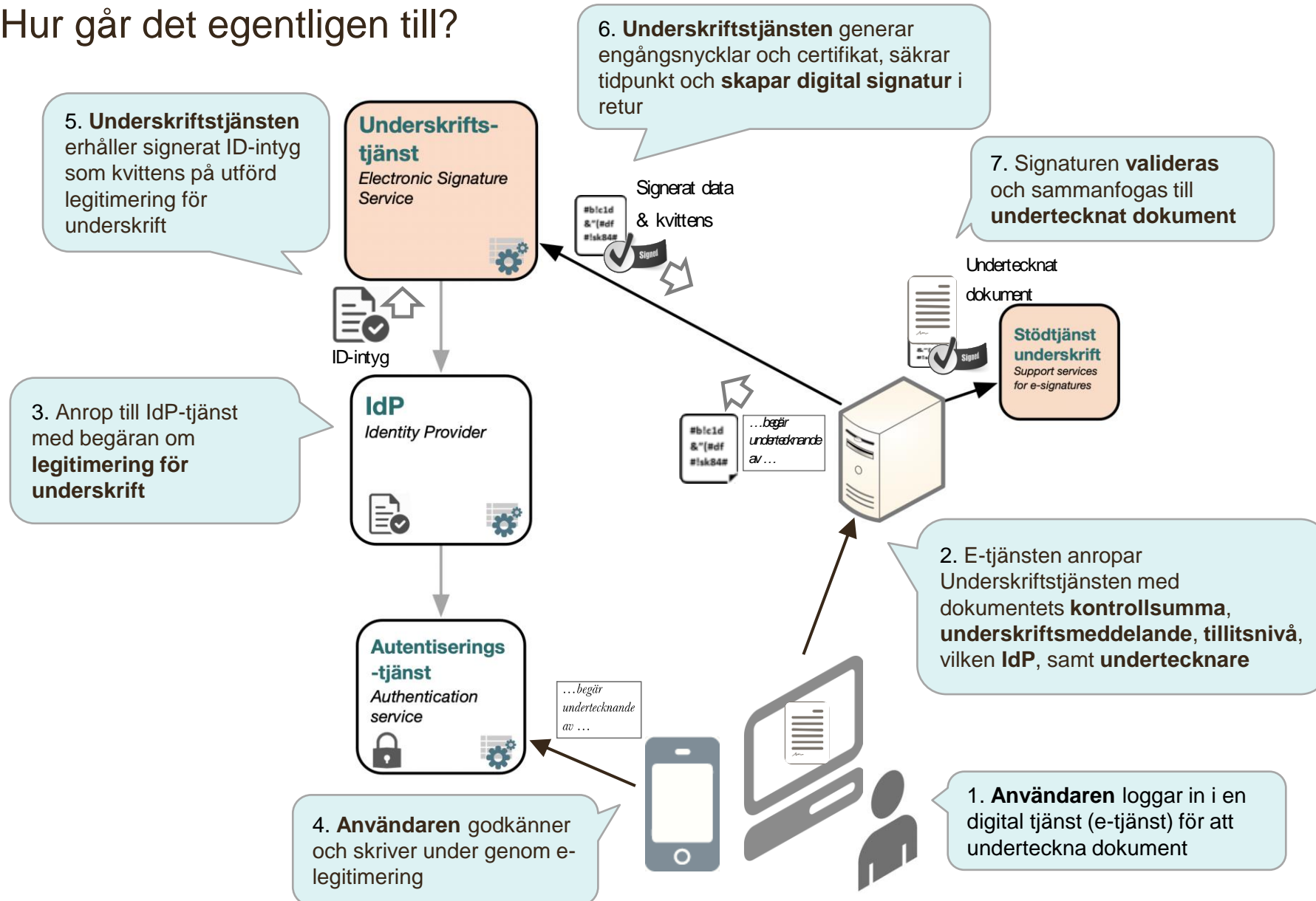
Mer om *elektroniska underskrifter*

- *Varför Underskriftstjänst? Varför inte digital signatur direkt med SITHS-kortet?*
- *Hur kommer man igång, vem blir först ut?*



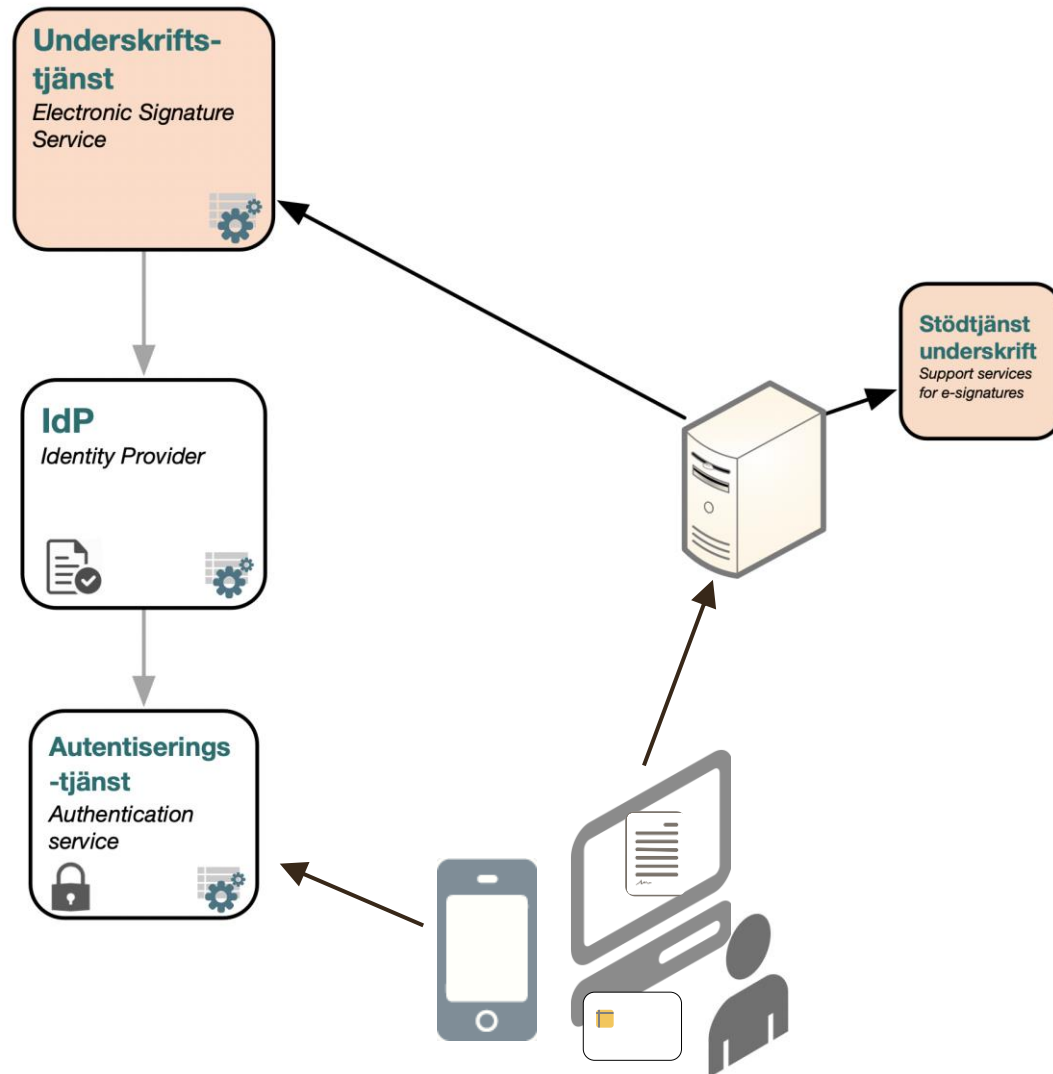
Underskriftstjänsten

Hur går det egentligen till?



Underskriftstjänsten

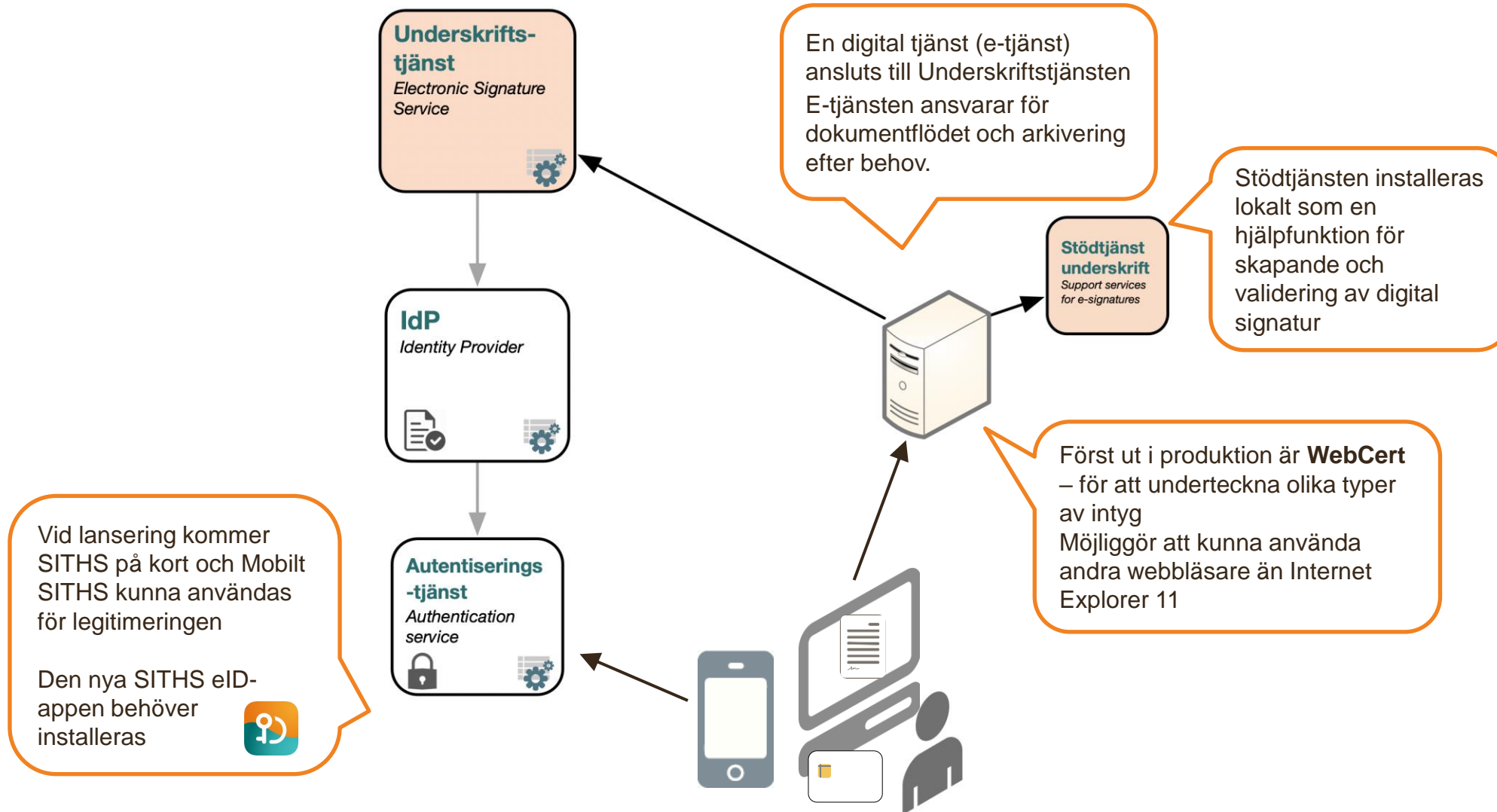
Vilka fördelar ger den fristående Underskriftstjänsten?



- ✓ **Avancerad elektronisk underskrift** enligt DIGG Tekniskt ramverk baserat på ETSI/OASIS standarder
- ✓ **Kvalitetsstämpel - granskad av DIGG** – följer en normativ specifikation
- ✓ **Flexibilitet** - Jobba på datorn – underteckna med mobilen, eller underteckna på datorn direkt.
- ✓ **Tar bort teknisk inlåsning** till äldre webbläsare
- ✓ Använd **samma PIN-kod** som vid inloggning (legitimeringscertifikatet)
- ✓ Alla e-legitimationer är *tekniskt sett* möjliga att ansluta, även de som saknar speciellt underskriftscertifikat, t.ex. utländska e-leg
- ✓ Signaturen kan anpassas till **underskrift i tjänsten** resp. som **privatperson**

Underskriftstjänsten

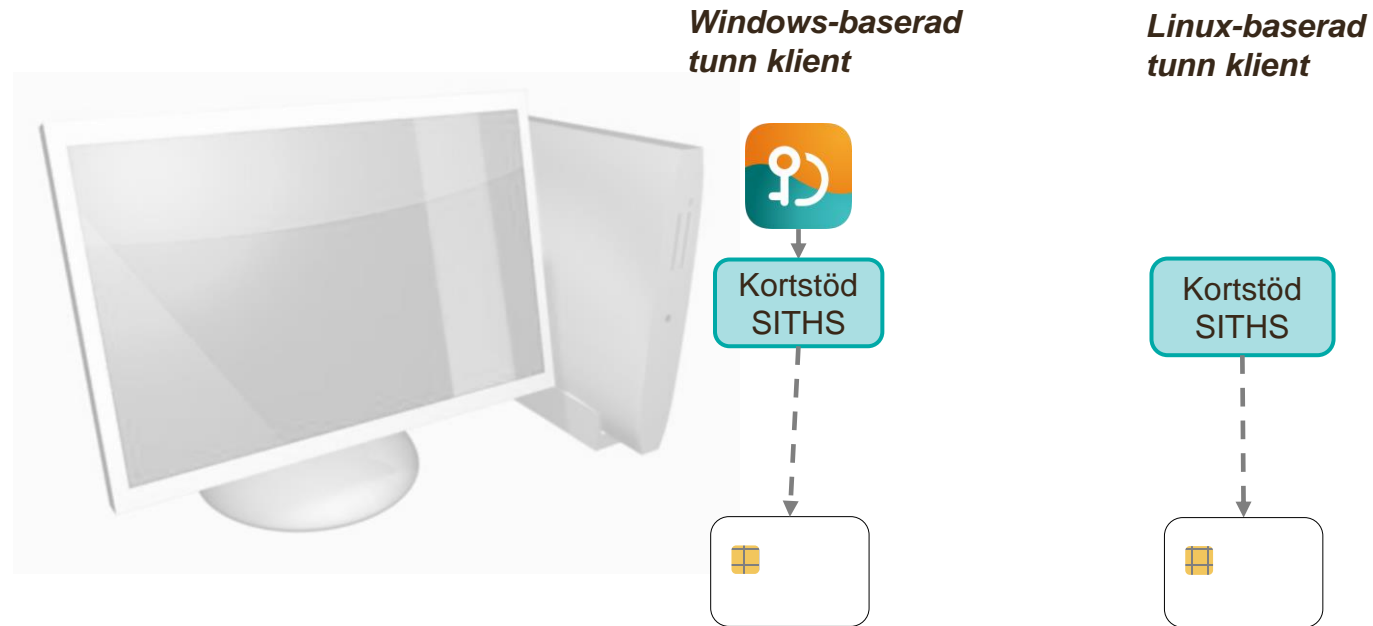
Hur ansluta och använda?



*Hur kommer inloggning via
tunna klienter till virtuella skrivbord
påverkas?*

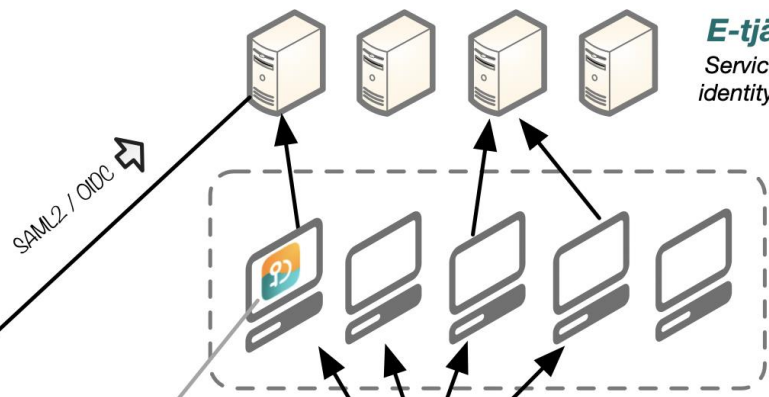
Programvara för SITHS-kort på tunn klient

Leverans 2 (2022)



Inloggning till virtuella skrivbord/appar med SITHS-kort och Mobilt SITHS

Virtuella plattformen kopplas till en IdP ansluten till SITHS Autentiseringstjänst



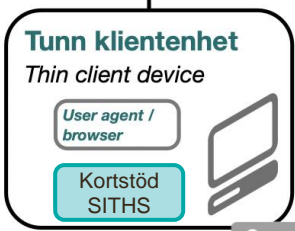
E-tjänster
Service provider / identity consumer

De digitala tjänster användaren behöver åtkomst till

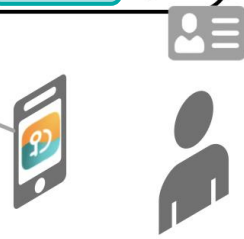
Virtualiserade skrivbord och appar



Citrix ADC / Storefront
Vmware Horizon
...



Linux-baserad tunn klient (i detta exempel)



SAML2 / OIDC

SAML2 / OIDC

Device in Linux

*Arbete med **nästa generation***

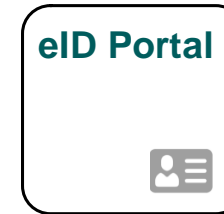
SITHS eID-portal

*för utgivning av SITHS eID på kort och
andra bärare*

Nästa generation SITHS eID-portal

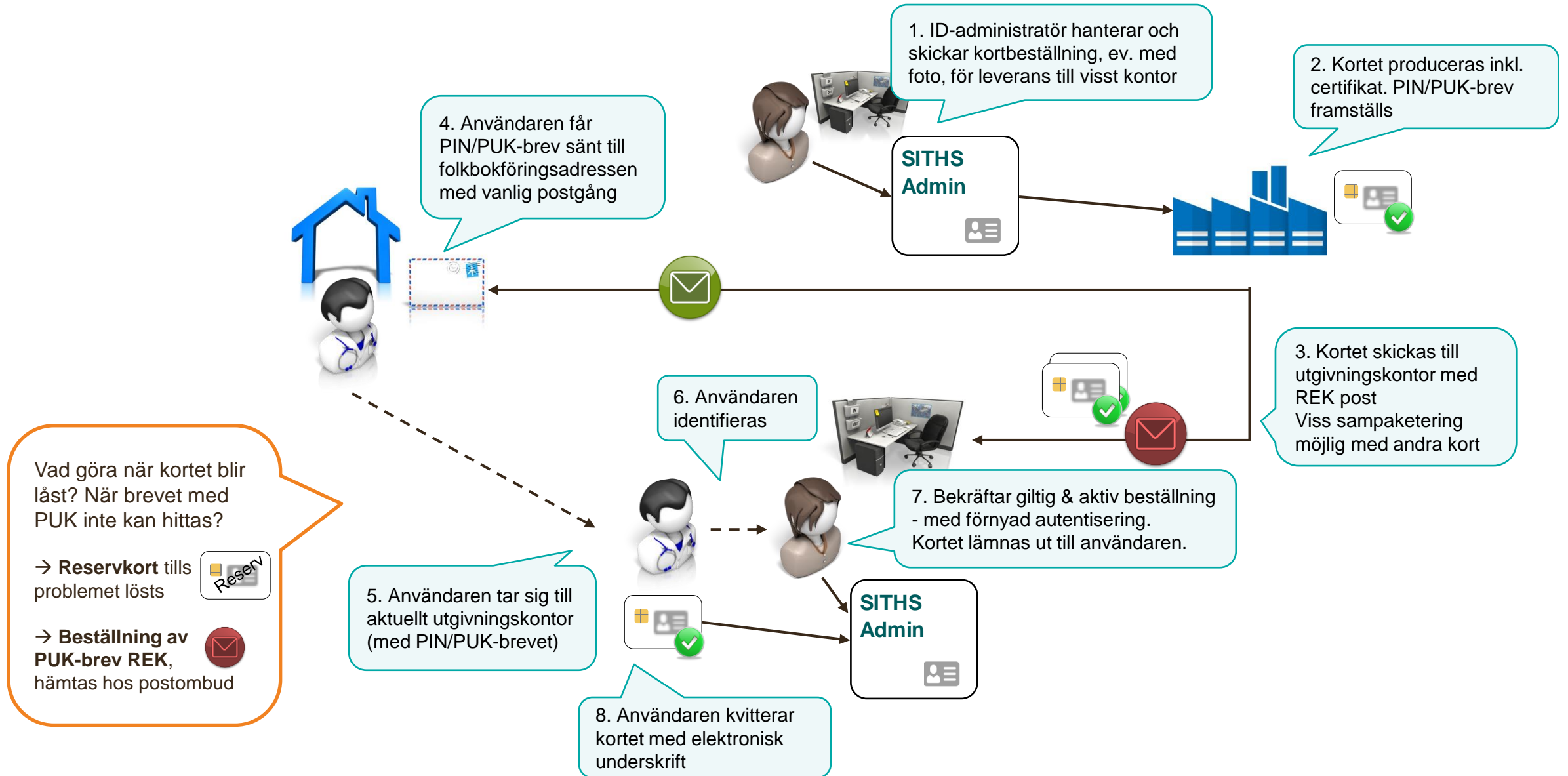
- Vad kan komma bli annorlunda? Några exempel

- **Hela arbetsflödet hålls ihop** i eID-portalen
beställning av SITHS-kort, identifiering, inläsning av foto, utlämnade av kort, ladda ner certifikaten osv.
 - Ersätter *SITHS Admin* samt *Mina Sidor*.
 - Det separata systemet "*SIS Capture Station*" kommer inte att behövas
- **Utreds** om **utgivningsflödet för SITHS-kort** ska "vändas" så att korten skickas hem istället för till utgivningskontoren
 - Den fysiska bäraren hos e-legitimationsinnehavaren från början!
 - Kan t.ex. möjliggöra smartare och snabbare sätt att hjälpa användare med låsta kort

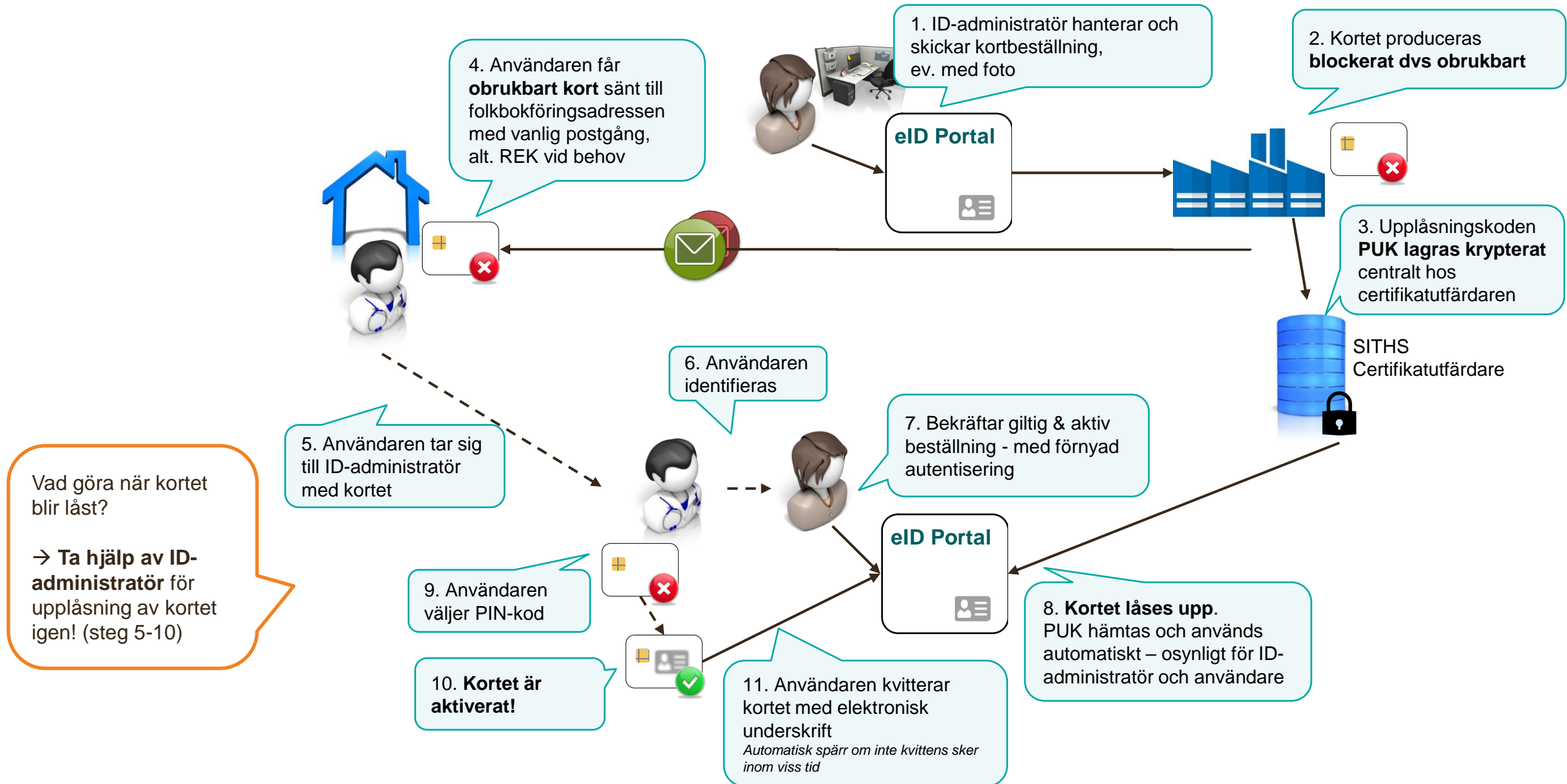


Kravarbetet pågår

Idag: Kortet skickas till utgivningskontor



Alternativ som utreds: Kortet skickas till folkbokföringsadressen



FRÅGOR?

SITHS-dagen 2021-05-27

Per Mützell: per.mutzell@inera.se



inera