eHälsomyndighetens nya säkerhetskrav

för åtkomst till tjänster kring läkemedelsförskrivning, recept och uttag

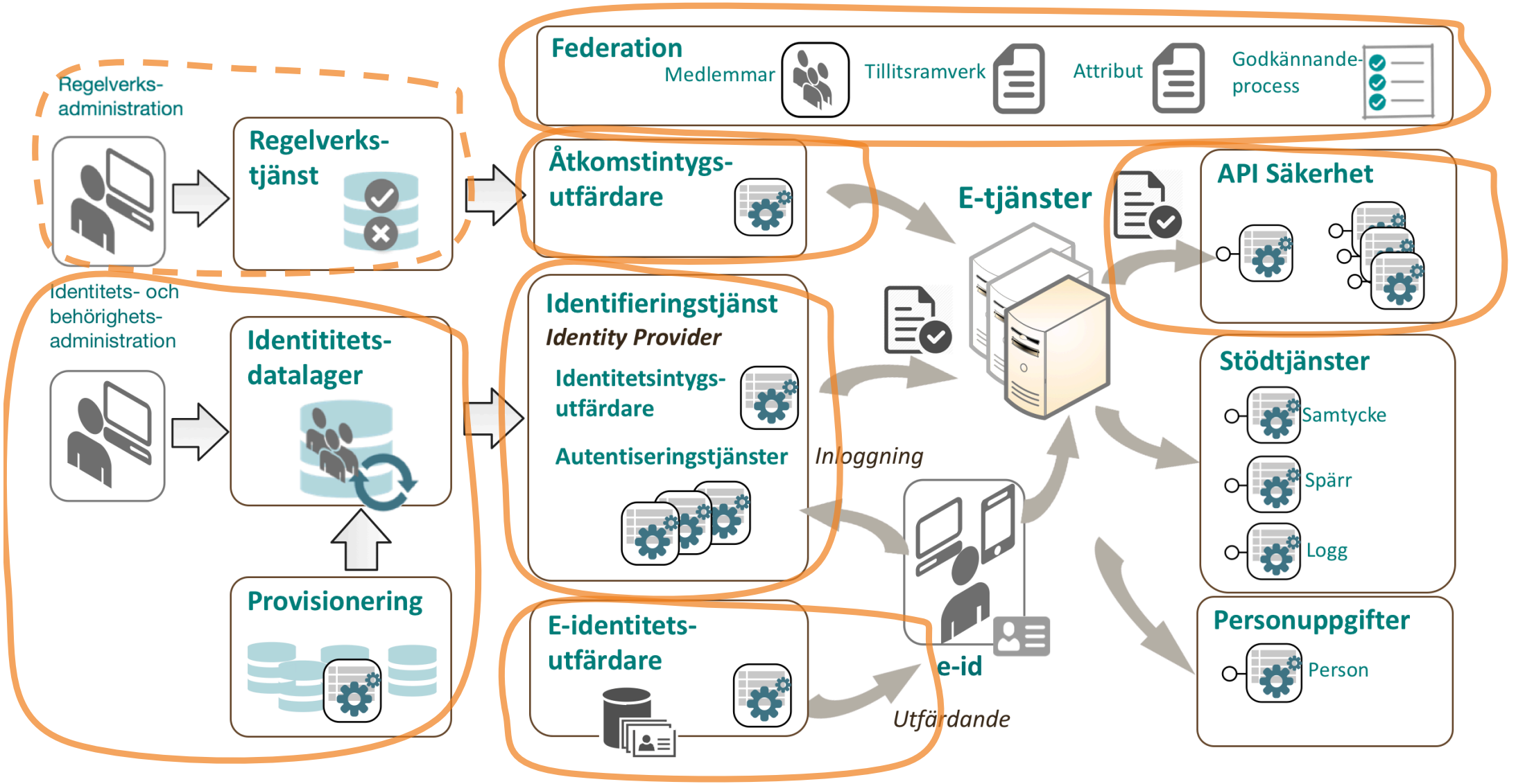
Vad påverkas? Vem gör vad och hur?

2017-09-28

Per Mützell, Inera

- *Hur påverkar myndighetens beslut vårdgivarna och möjligheten att komma åt information om patienternas läkemedel?*
- *Hur kan vårdgivare förbereda sig?*
- *Vad kan Inera bidra med?*

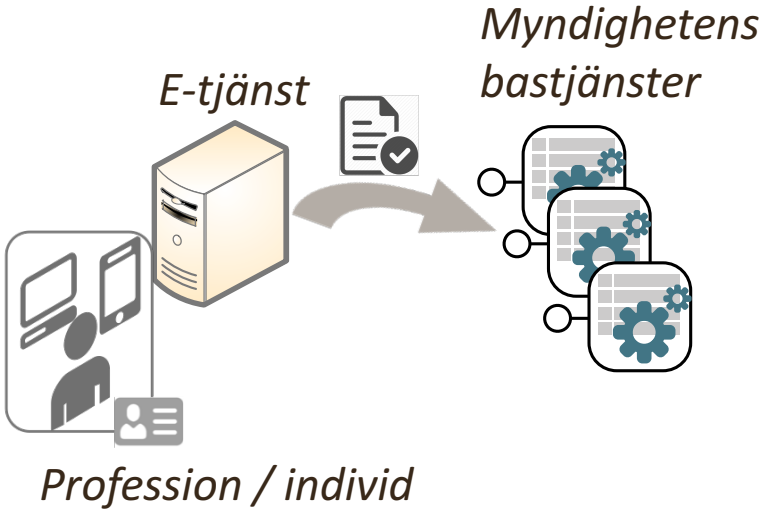
OCH - hänger detta ihop med referensarkitekturen för identitet och åtkomst?


Federation
Medlemmar
Tillitsramverk
Attribut
Godkännande-process
Regelverks-administration
Regelverks-tjänst
Åtkomstintygs-utfärdare
E-tjänster
API Säkerhet
Identitets- och behörighets-administration
Identitetsdatalager
Identifieringstjänst
Identity Provider
Identitetsintygs-utfärdare
Autentiseringstjänster
Inloggning
Stödtjänster
Samtycke
Spärr
Logg
Provisionering
E-identitets-utfärdare
e-id
Utfärdande
Personuppgifter
Person

Bakgrund

Säker åtkomst för vård- och apoteksaktörer

- Ny säkerhetslösning införs av eHälsomyndigheten baserat på påpekande från Datainspektionen
- Berör bastjänster kopplade till **Receptregistret** **Läkemedelsförteckningen** m.fl. register.
  - E-recept, dosrecept, uttagna (expedierade) läkemedel på apotek
  - Administrativa uppgifter kring dospatienter
- Kräver förändringar i säkerhetstekniken i vård- och omsorgssystem som ansluter till myndighetens bastjänster



inera

eHälsomyndighetens tidplan

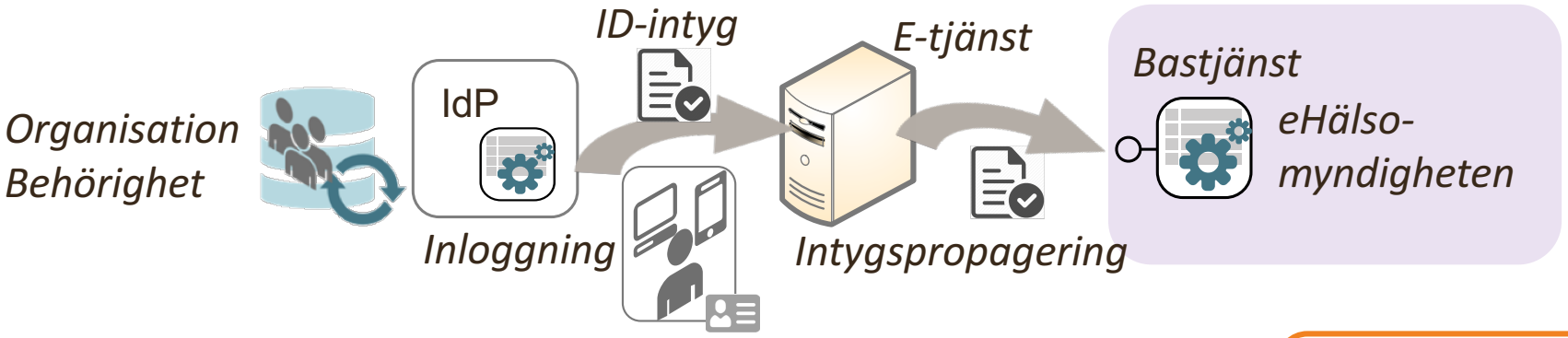
- 2017: Referenstjänster/Testmiljöer, Informations- och utbildningsprogram.
- 2017 Q4: Produktion ny säkerhetslösning och anpassade tjänster
- 2019 Q2: Gamla säkerhetslösningen stängs ned

inera

Vilka krav ställer myndighetens nya lösning?

Federationsanslutning

och propagering av ID-intyg (SAML)



- **Sambi - identitet- och behörighetsfederation** för hälsa, vård och omsorg
  - Godkänd **identifieringstjänst** (**IdP**) för inloggning
  - Godkänd **stark autentiseringslösning** (LoA3 enligt ELN)
  - Godkänt **verksamhetssystem** (e-tjänstens anslutning)
  - Godkänd **organisation** (LIS, rutiner)
- **ID-intyget** (SAML) ska skickas med från inloggningen ”i original”

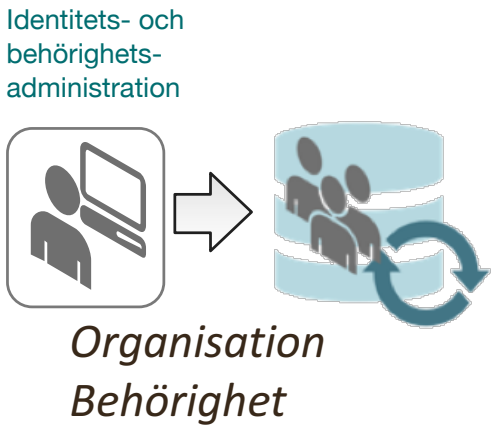
Följsamhet, tillit, säkerhetsgranskning
Se sambi.se

Behörighetsstyrning och spårbarhet baserat på digitala intyg

inera

Nya krav på attribut i ID-intyget - vårdaktörer

- **Person-id**
  - **Personnummer** eller **personlig förskrivarkod** eller **legitimationskod** (källa: Socialstyrelsen)
- **Utökad yrkeskod**
  - *AT-läkare*
  - *Läkare med förordnande*
  - *Administratör av dospatientuppgifter*
- **Förskrivarkod**
  - Personlig eller gruppförskrivarkod
- **Vårdgivare-id** (organisationstillhörighet)
  - **Organisationsnummer** eller **HSA-id**



Vilka och vad berörs?

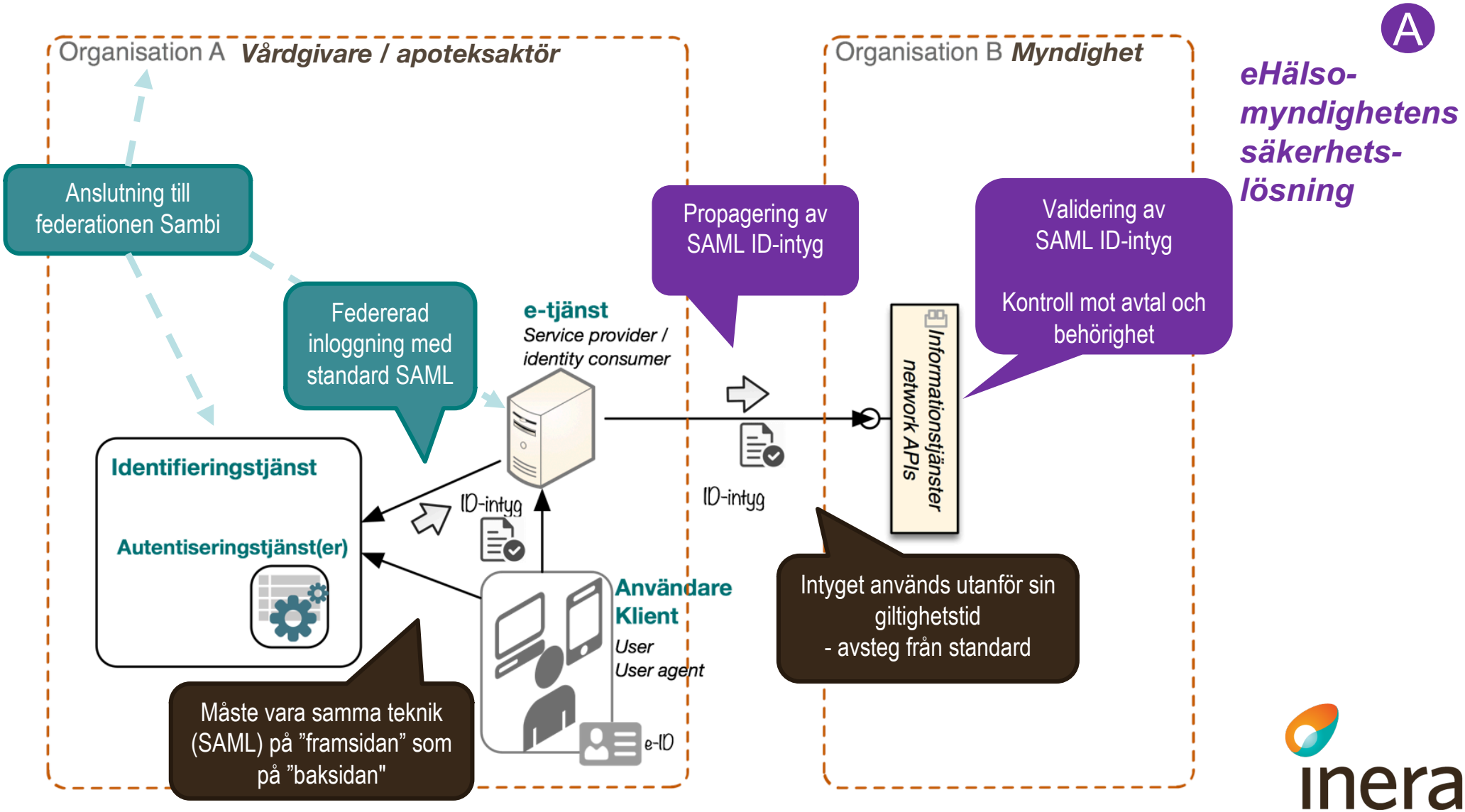
- Vilka IT-system berörs?
  - Förskrivarstöd läkemedel, e-recept, dosrecept
  - Administration kring dospatienter
  - Läkemedelsförteckningen, uttag på apotek
  - För professionen resp. individens egen åtkomst
  - IT-infrastruktur för Identitet och åtkomsthantering (IAM)

- Vilka organisationer berörs?
  - Alla som använder och/eller tillhandahåller sådant IT-system som har åtkomst till myndighetens bastjänster

inera

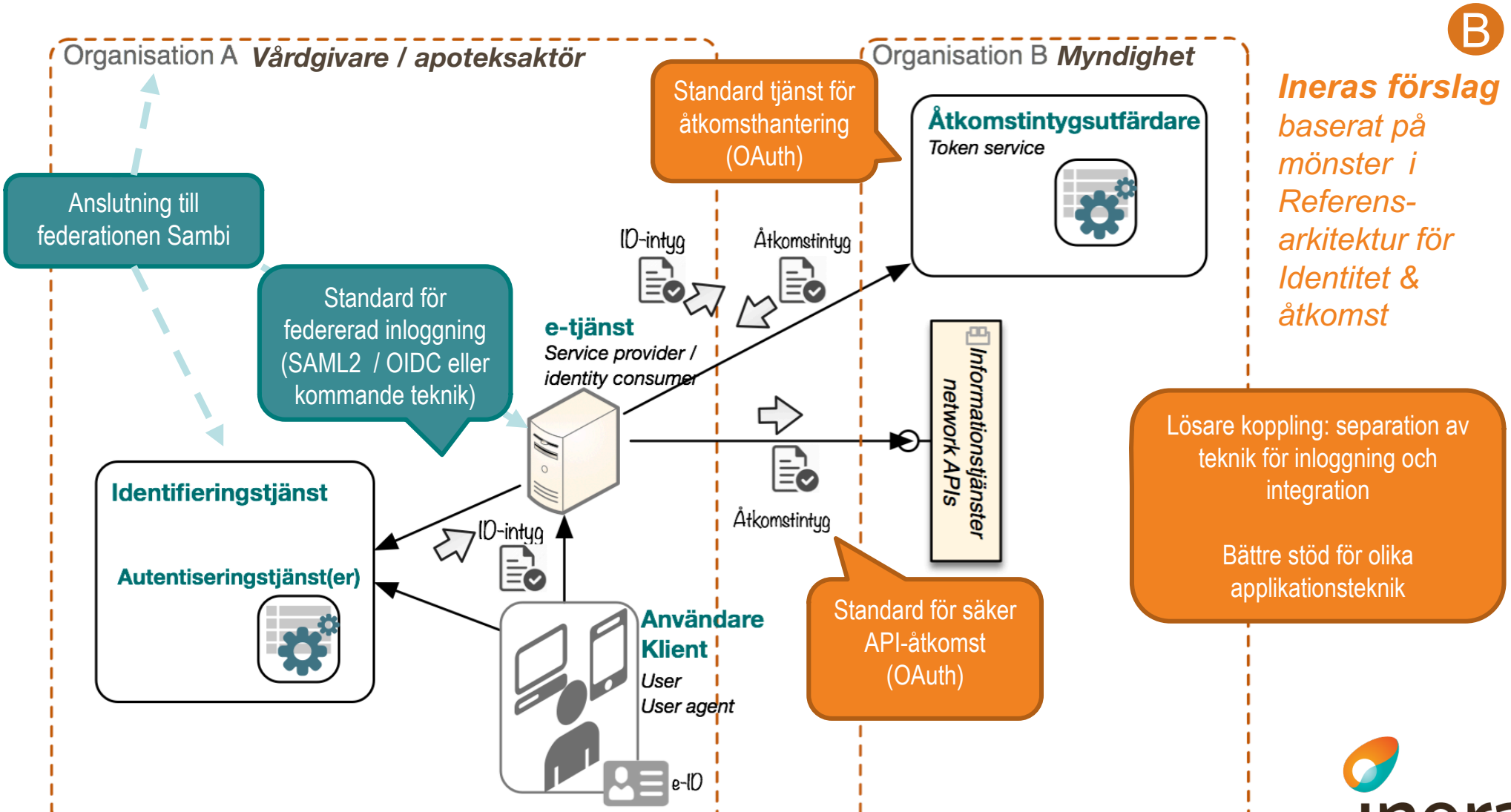
Mer om lösningsarkitekturen

- Hur relaterar den till Referensarkitekturen?


A
eHälso-myndighetens säkerhets-lösning
Organisation A Vårdgivare / apoteksaktör
Organisation B Myndighet
Anslutning till federationen Sambi
Federerad inloggning med standard SAML
e-tjänst
Service provider / identity consumer
Propagering av SAML ID-intyg
Validering av SAML ID-intyg
Kontroll mot avtal och behörighet
Informationstjänster network APIs
Identifieringstjänst
Autentiseringstjänst(er)
ID-intyg
ID-intyg
Användare
Klient
User
User agent
e-ID
Intyget används utanför sin giltighetstid
- avsteg från standard
Måste vara samma teknik (SAML) på ”framsidan” som på ”baksidan"
inera

Synpunkter på eHälsomyndighetens lösning

- Onödigt **”hård” teknisk koppling**
  - Knyter samma teknik på ”fram-” och ”baksidan” - inloggning resp. backendintegration
  - Risk för inlåsningseffekter – hur stöds andra industristandarder anpassade till t.ex. mobila tillämpningar (läs OpenID Connect) för säker inloggning?
- Vissa **avsteg ifrån SAML-standard**
- Systemanpassningar riskerar att inte kunna **återanvändas** för säker åtkomst till api:er i andra sammanhang



B

Ineras förslag
baserat på mönster i Referens-arkitektur för Identitet & åtkomst

inera

B

Sammanfattning
– Ineras lösningsalternativ baserat på referensarkitekturen

- Tillämpa **standardmönster** för säker delegerad åtkomst – bygg för **återanvändning**
- **Lösare koppling** mellan inloggningsteknik och integrationsteknik
- **Förbered arkitekturen** för kommande säkerhetsstandarder och tekniker (OpenID Connect, HTTP/REST, stöd för mobila plattformar…)

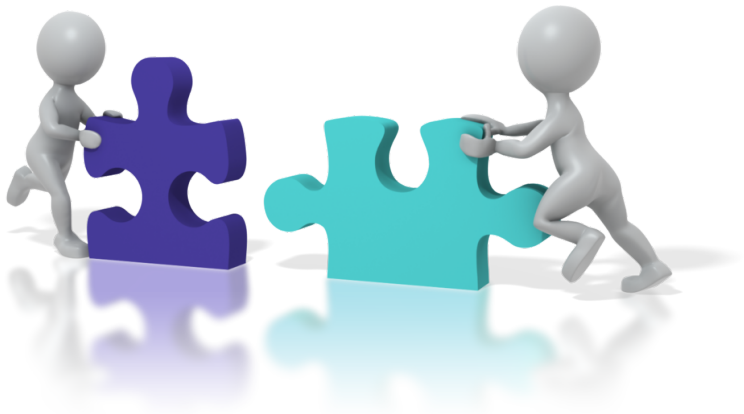
inera

Men, vad innebär då detta?

Vad händer nu?

Samverkan kring lösningsutformning - med sikte på att möjliggöra alternativ B

- Lösning alternativ A implementeras enligt plan
- Samverkan pågår kring utformning av alternativ B
- eHälsomyndigheten tar fram beslutsunderlag för alternativ B
- Återstår beslut om och tidplan för alternativ B

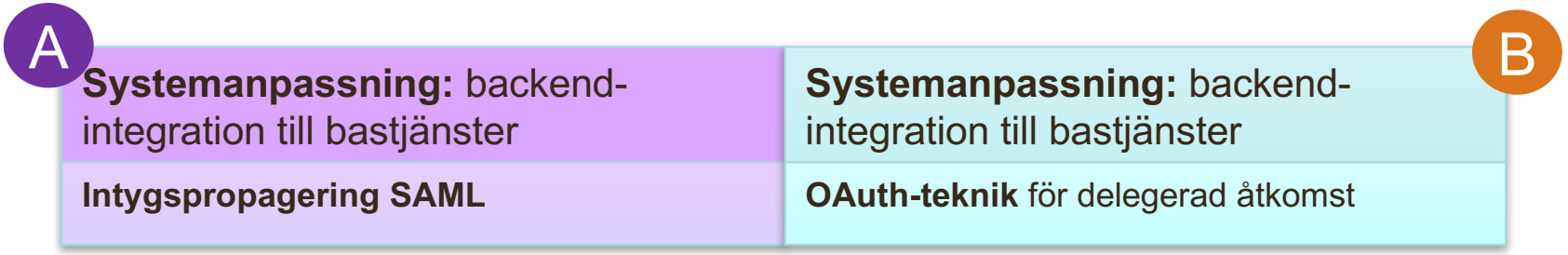


inera

Vad innebär detta i praktiken?

- Vad behöver göras lokalt?
- Vad kan Inera göra?
- Hur ser en översiktlig tidplan ut?

Vad behöver respektive organisation göra?



inera

Vad kan Inera bidraga med?

Systemanpassning och federationsanslutning nationella system: Pascal, NPÖ, Katalogtjänst HSA, Säkerhetstjänster IdP osv.

Godkända i Sambi idag:
Inera IdP, Katalogtjänst HSA som leverantör till användarorganisation

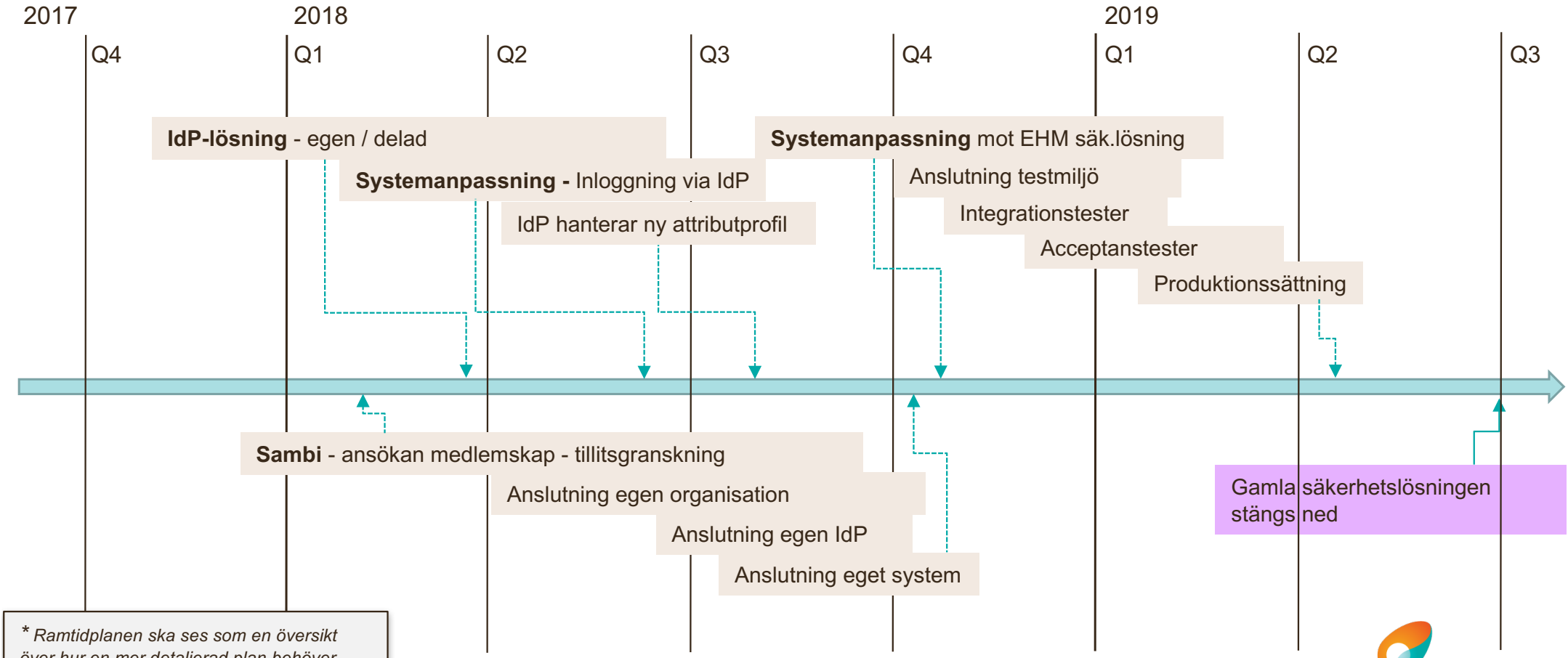
Samverkan med Sambi attributförvaltning

Samordna och ta fram **regelverk för attributförsörjning** inom ramen för HSA-samverkan
Anpassning **gemensamma verktyg** (HSA-admin)
Vidareutveckla **tjänstekontrakt** för attributförsörjning

Godkännande **SITHS och Efos** som **e-legitimation**

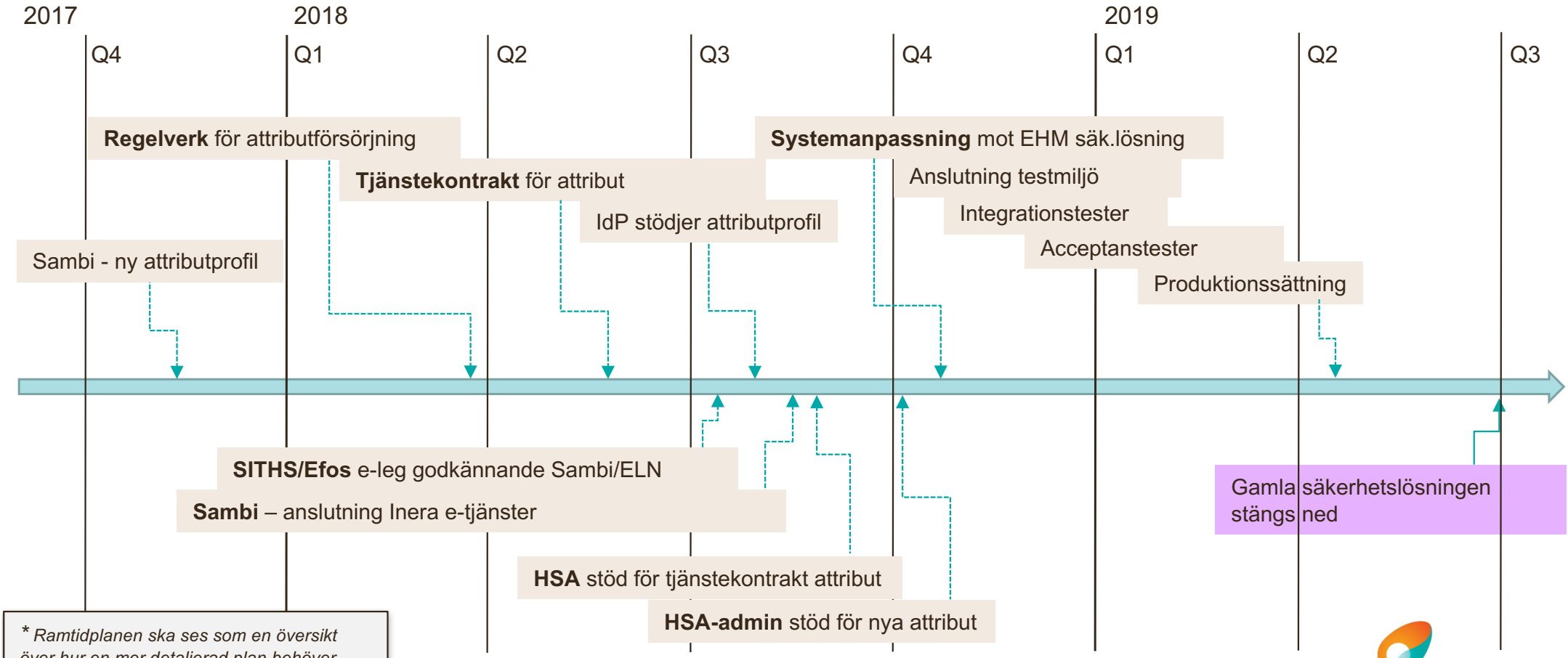
Granskning utförs av E-legitimationsnämnden

Ramtidplan* – lokala aktiviteter



* *Ramtidplanen ska ses som en översikt över hur en mer detaljerad plan behöver utformas och vad den behöver innehålla. De enskilda placeringarna på tidsaxeln kan skilja sig åt i det enskilda fallet*

Ramtidplan* – Inera aktiviteter



* *Ramtidplanen ska ses som en översikt över hur en mer detaljerad plan behöver utformas och vad den behöver innehålla. De enskilda placeringarna på tidsaxeln kan skilja sig åt i det enskilda fallet*

inera

Tack!

Frågor?