Överflygning av VGR:s Identitets- och åtkomsttjänster

Produktområde Identitets- och åtkomsttjänster

VÄSTRA GÖTALANDSREGIONEN

Mål: Användare ska ha tillgång till rätt information på rätt sätt för sin arbetsuppgift och vara medveten om sitt personliga ansvar.

Informationssäkerhet och dataskydd Regional riktlinje 2023 – 2027

6. Åtkomst till informationstillgångar

Vision: Att skapa en säker och sömlös identitets- och åtkomsthantering som möjliggör enkel och trygg tillgång till resurser för alla VGR:s medarbetare, överallt och när som helst. Genom att leverera en robust Identity Fabric strävar vi efter att stärka organisationens säkerhet och användarupplevelse, samtidigt som vi stödjer innovation och tillväxt.

Produktområdeskanvas - Identitets- och åtkomsttjänster

4. Vision och mål

IAM regleras inom EU

EU GDPR – Dataskyddsförordningen
Skyddar personuppgifter och individens rätt till integritet.
Ställer krav på säker hantering, åtkomstkontroll och spårbarhet av persondata.
Utgör grunden för all identitets- och behörighetshantering inom EU.

EU eIDAS 2.0 – Digital identitet och tillitstjänster
Inför den europeiska digitala identitetsplånboken.
Reglerar hur e-legitimationer, signaturer och tillitstjänster fungerar över gränser.
Skapar förtroende och interoperabilitet för elektronisk identifiering i hela EU.

EU NIS2 – Cybersäkerhetsdirektivet
Krav på starkare säkerhet och riskhantering för viktiga och digitala tjänster.
Inkluderar styrning av åtkomst, multifaktorautentisering och incidentrapportering.
Gör IAM till en central del av EU:s cybersäkerhetsarbete.

EU EHDS – European Health Data Space
Skapar ett gemensamt europeiskt ekosystem för hälsodata.
Ger invånare kontroll över sin hälsodata och möjliggör säker datadelning för vård och forskning. Bygger på eIDAS 2.0 och GDPR med särskilt fokus på hälsosektorn.

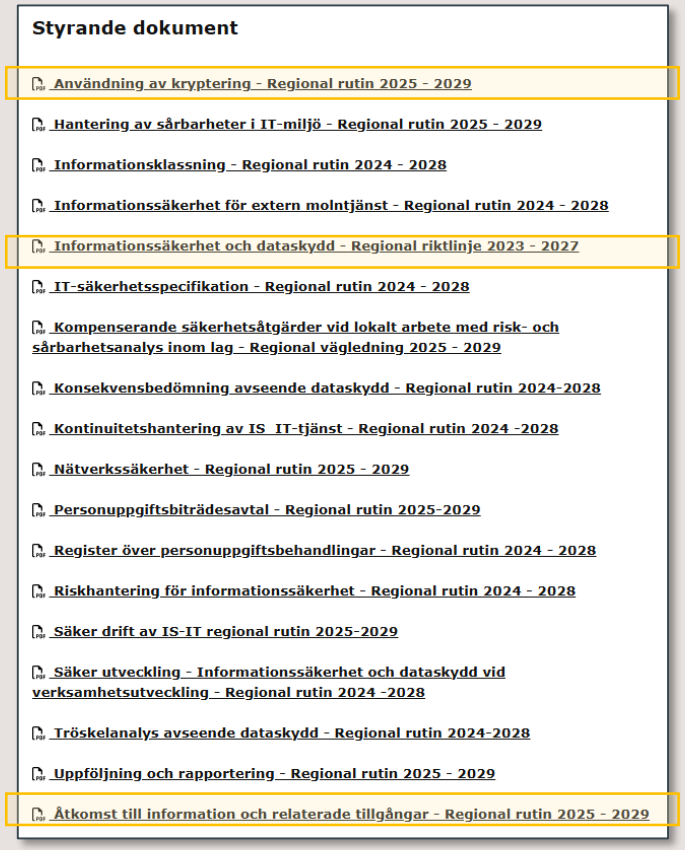
IAM regleras inom LISD

Ledningssystem för informationssäkerhet

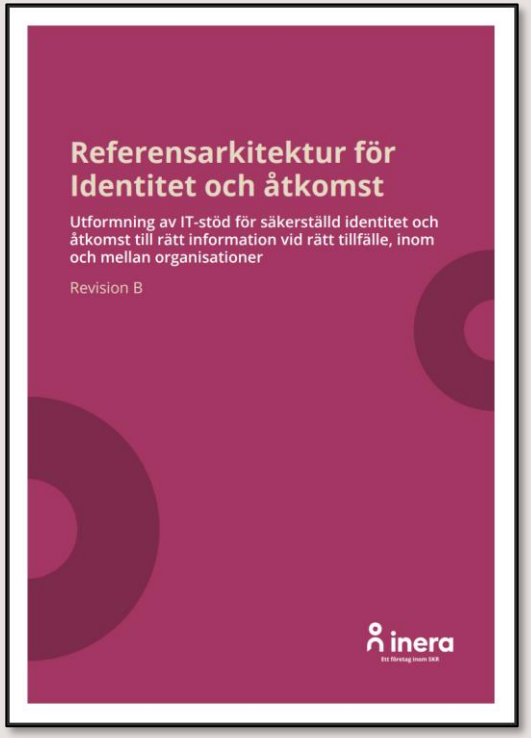
Ledningssystemet innehåller rutiner och instruktioner som konkretiserar krav inom ett antal områden avseende informationssäkerhet. Under Styrande dokument finns riktlinjer och rutiner som kompletterar informationen på denna sida.

Dataskydd och GDPR

Information om dataskyddsförordningen, interna styrdokument rörande dataskydd, dokumentmallar samt frågor och svar.

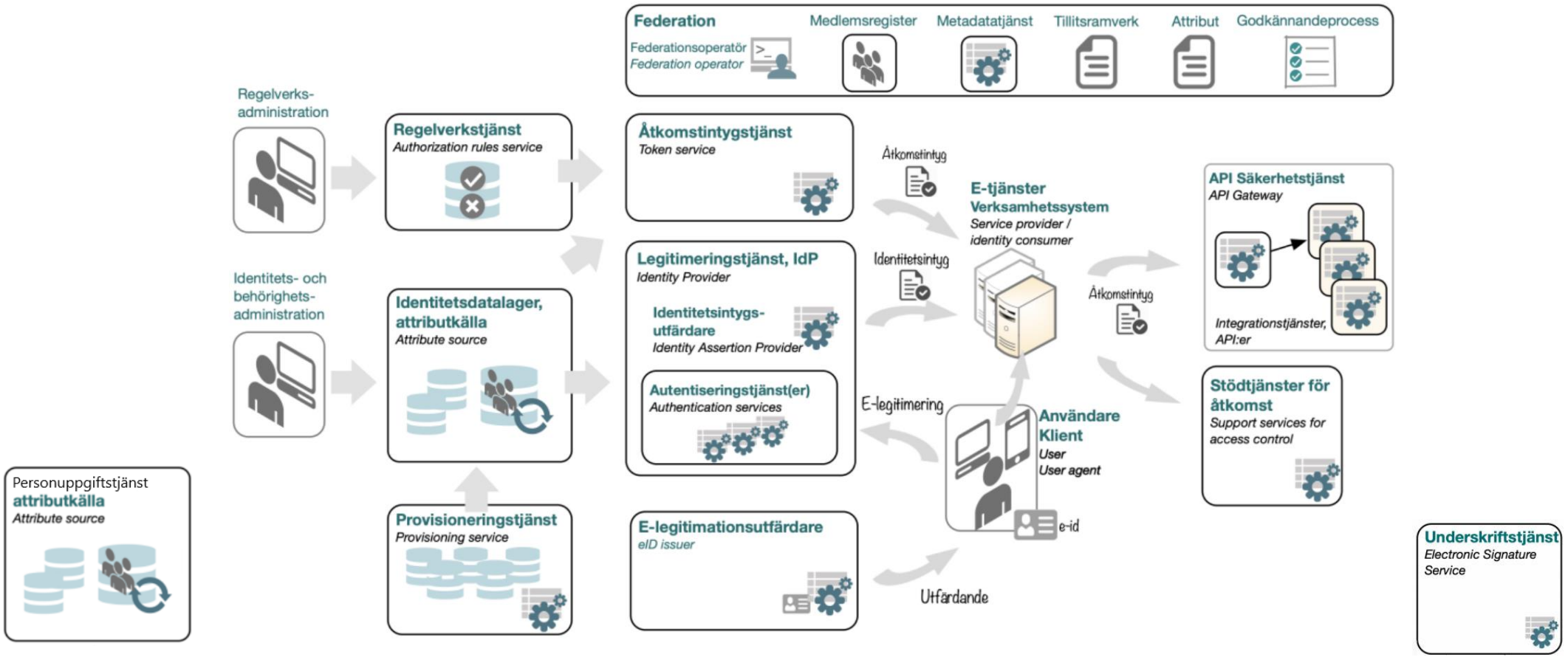


Inera tar fram referensarkitekturer

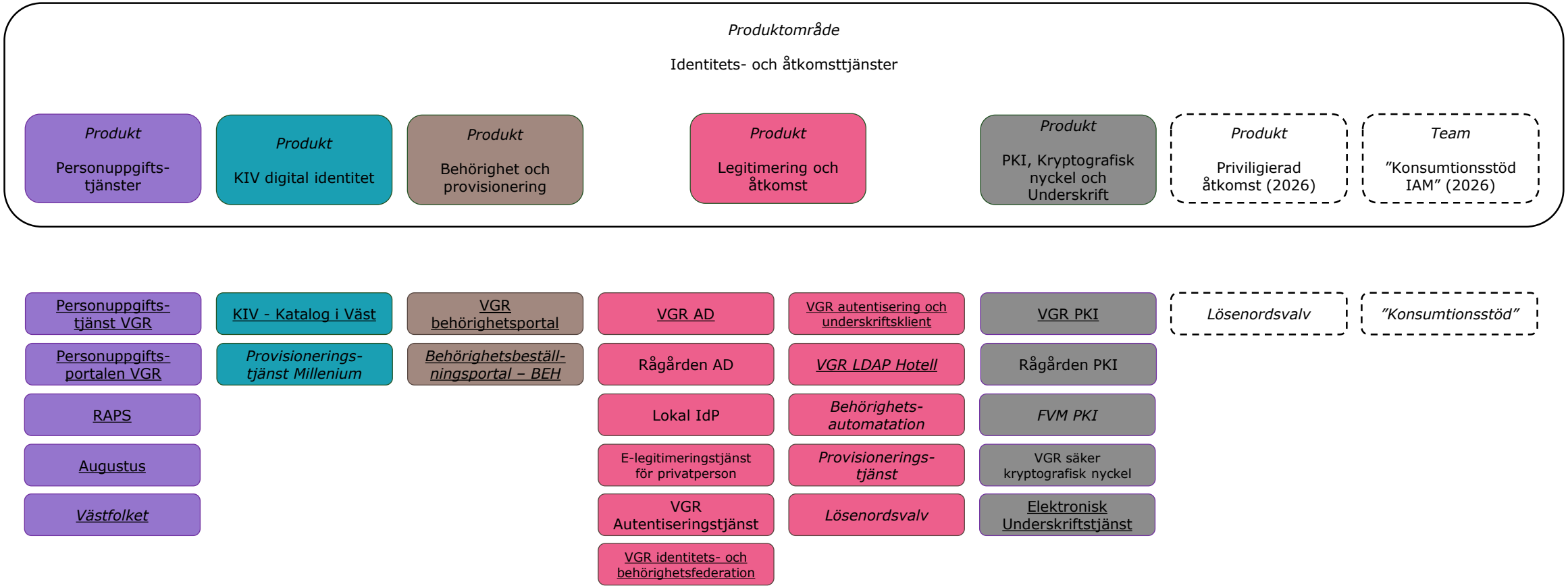


Ineras Referensarkitektur för Identitet och åtkomst

Figur 8 Referensarkitektur Identitet och åtkomst – översikt



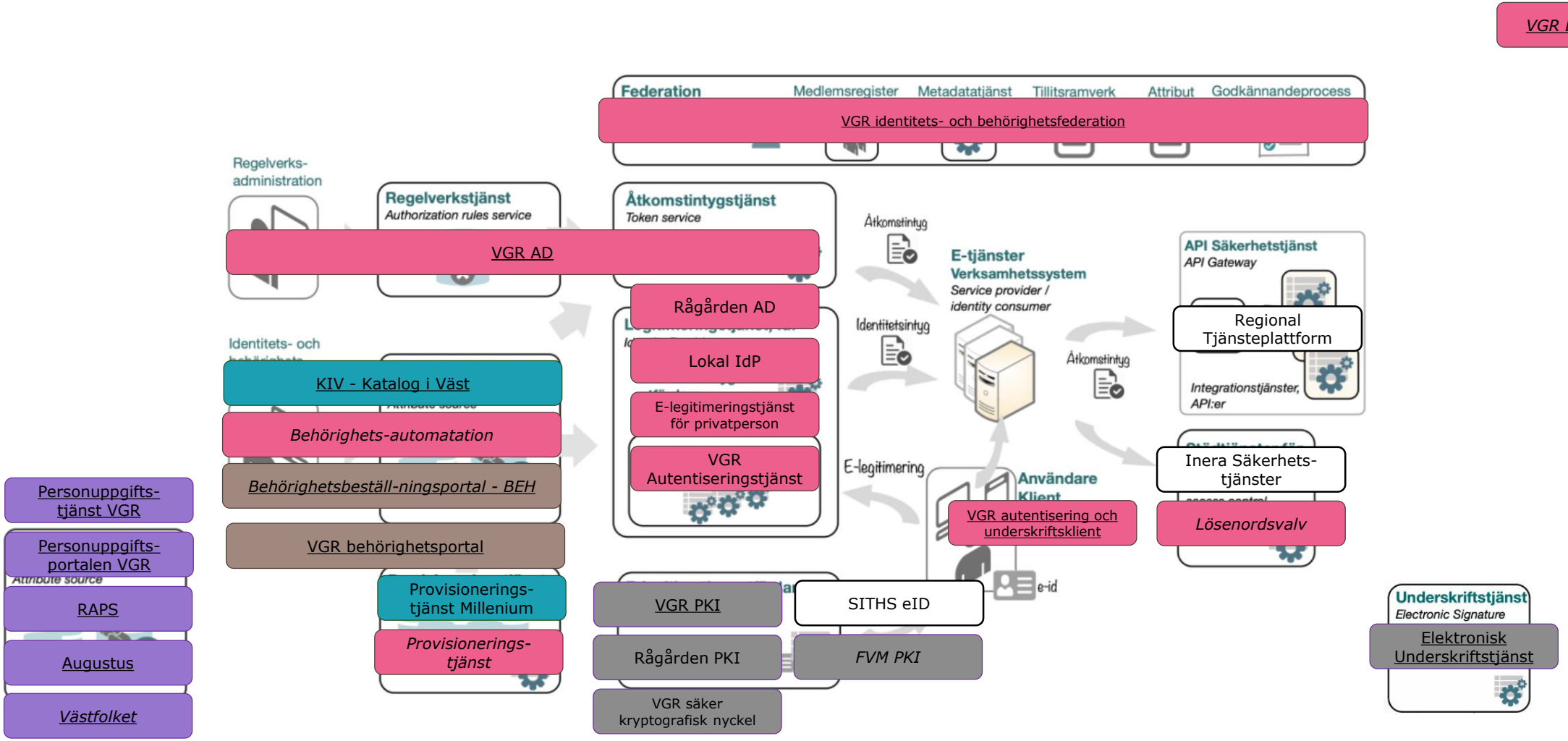
Produktstyrning



kursiv = under avveckling
streckat = planerat att föra in

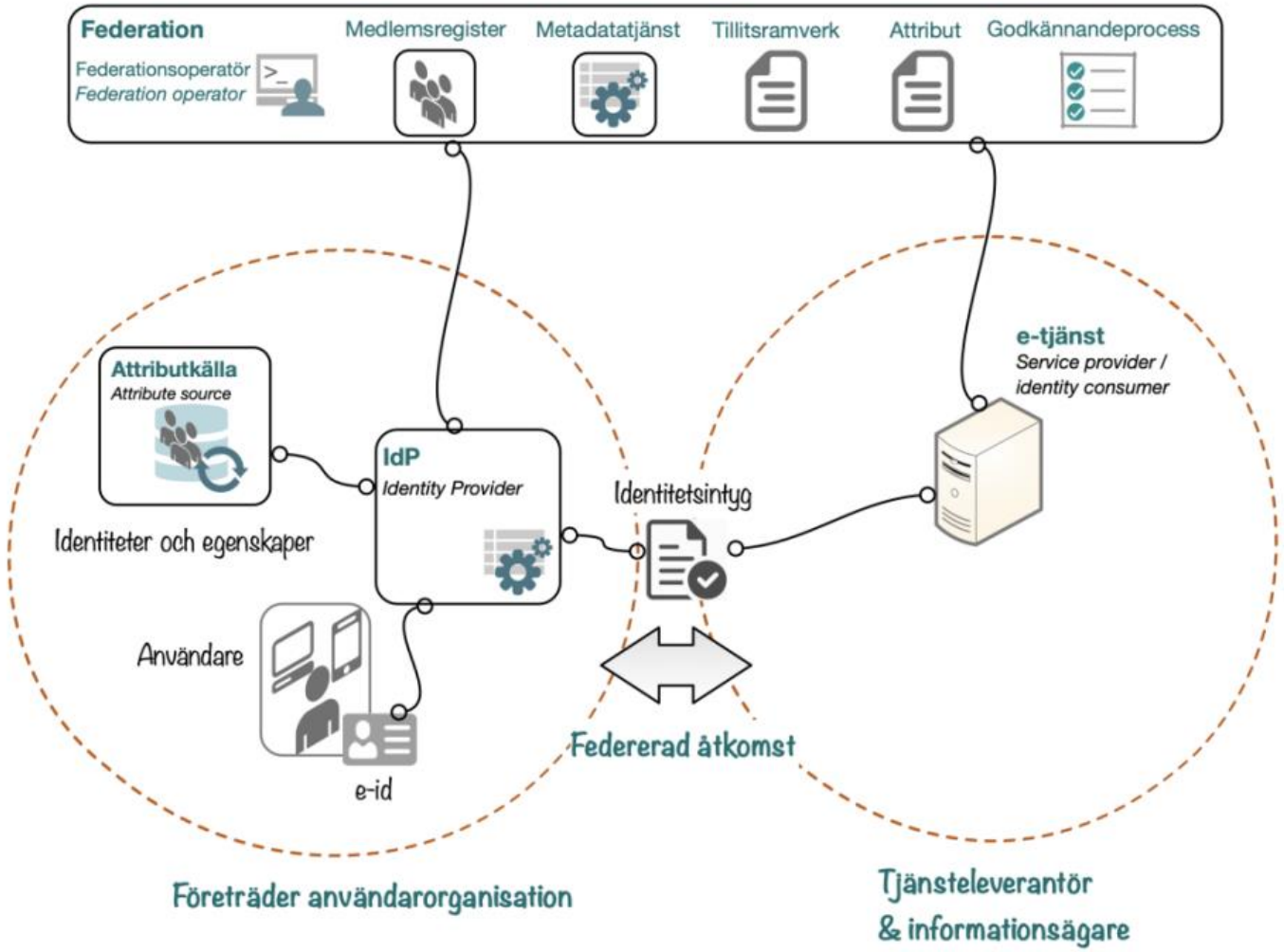
Ineras Referensarkitektur för Identitet och åtkomst

Figur 8 Referensarkitektur Identitet och åtkomst – översikt



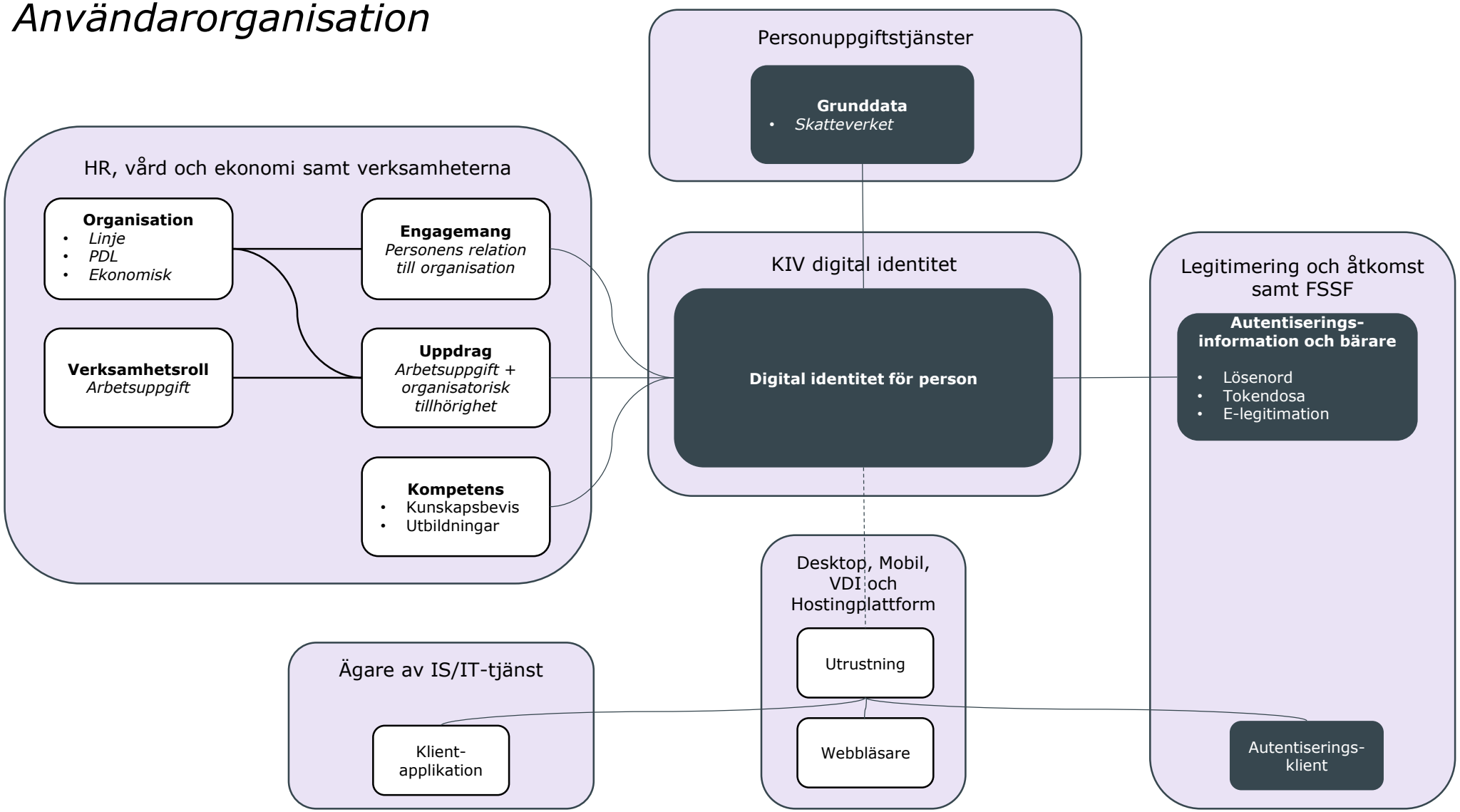
Ineras Referensarkitektur för Identitet och åtkomst

Figur 49. Identitets- och behörighetsfederation. Federativ åtkomst till e-tjänst i annan organisation eller domän.



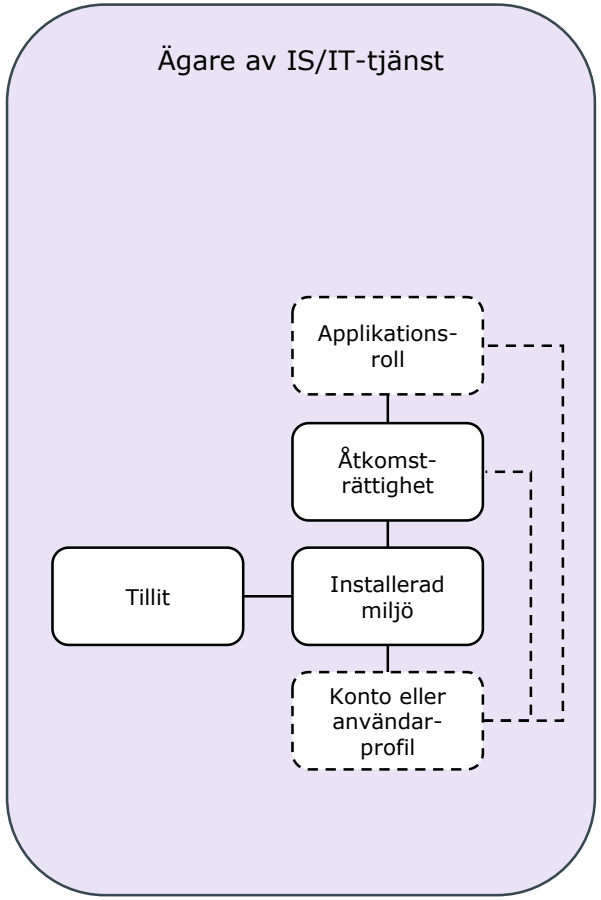
Förutsättningar innan åtkomst

Användarorganisation



Förutsättningar innan åtkomst

Tjänsteleverantör



ansvarar för att säkerställa implementation och efterlevnad av säkerhetsåtgärder utifrån krav på skydd för informations-tillgångarna.

- Informationsklassning
  - *Krav på säkerhetsåtgärder*
- Riskanalys
  - *Krav på säkerhetsåtgärder*

Informationsägare
(kan företrädas av regional processägare)

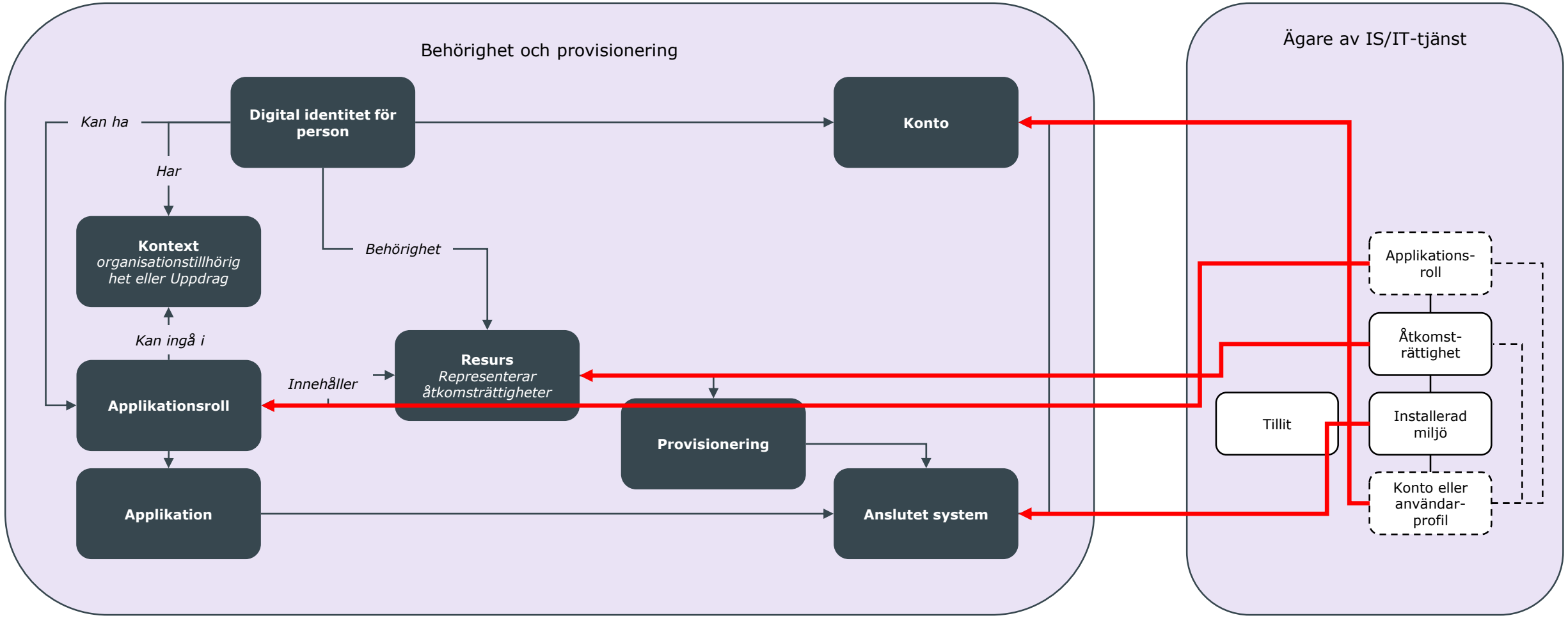
införa, förvalta, följa upp och utvärdera säkerhetsåtgärder

- IT-säkerhetsspecifikation
  - *Implementerade säkerhetsåtgärder*
- Krav för åtkomst

Ägare av IS/IT-tjänst

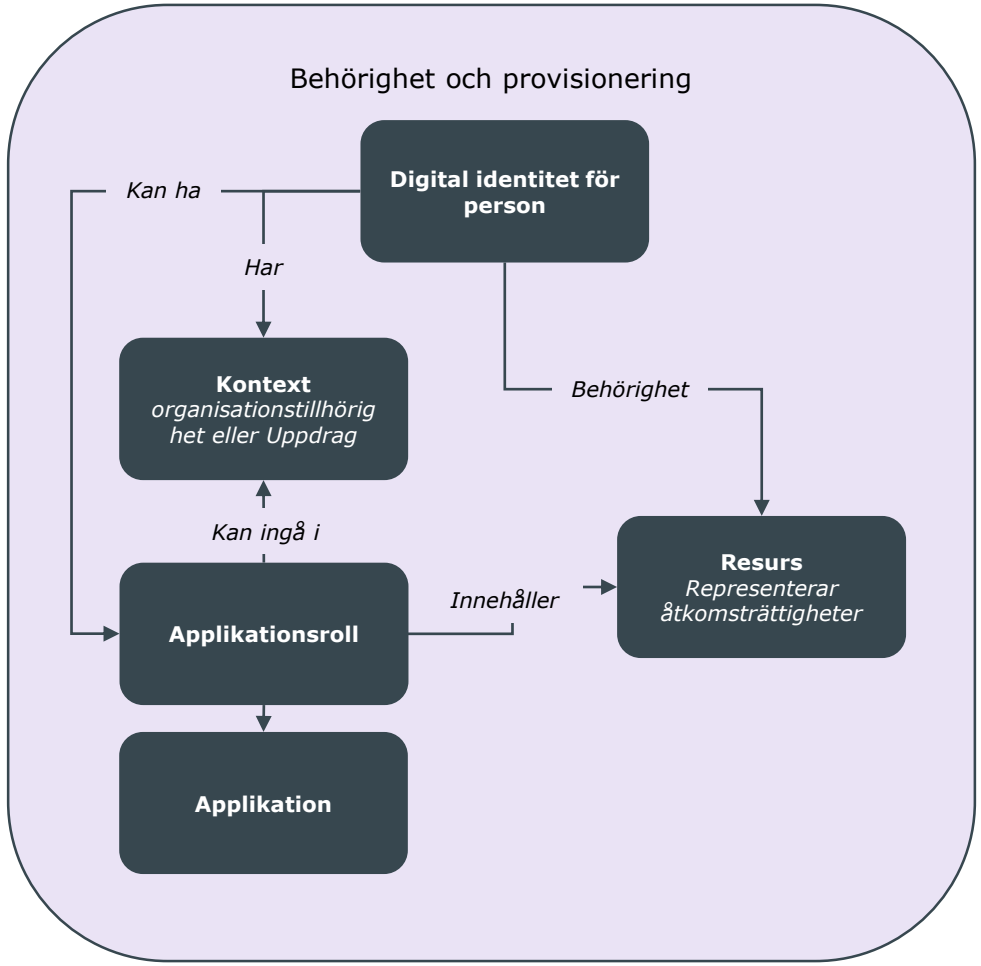
Förutsättningar innan åtkomst

Modellering av IS/IT-tjänst i IGA



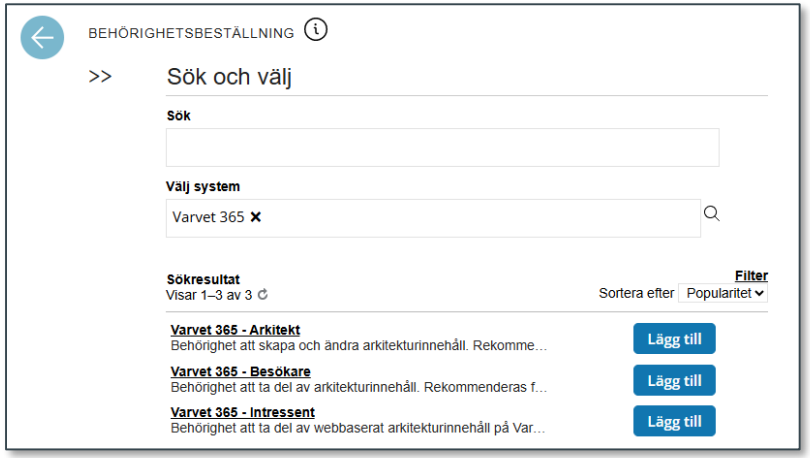
Förutsättningar innan åtkomst

Behörighetstilldelning



Behörighetstilldelning kan ske på tre sätt:

- Applikationsrollen knyts till kontext.
- Applikationsrollen tilldelas via tilldelningspolicy, som byggs utifrån behörighetsgivande attribut.
- Applikationsrollen är beställningsbar.



Förutsättningar innan åtkomst

Provisionering

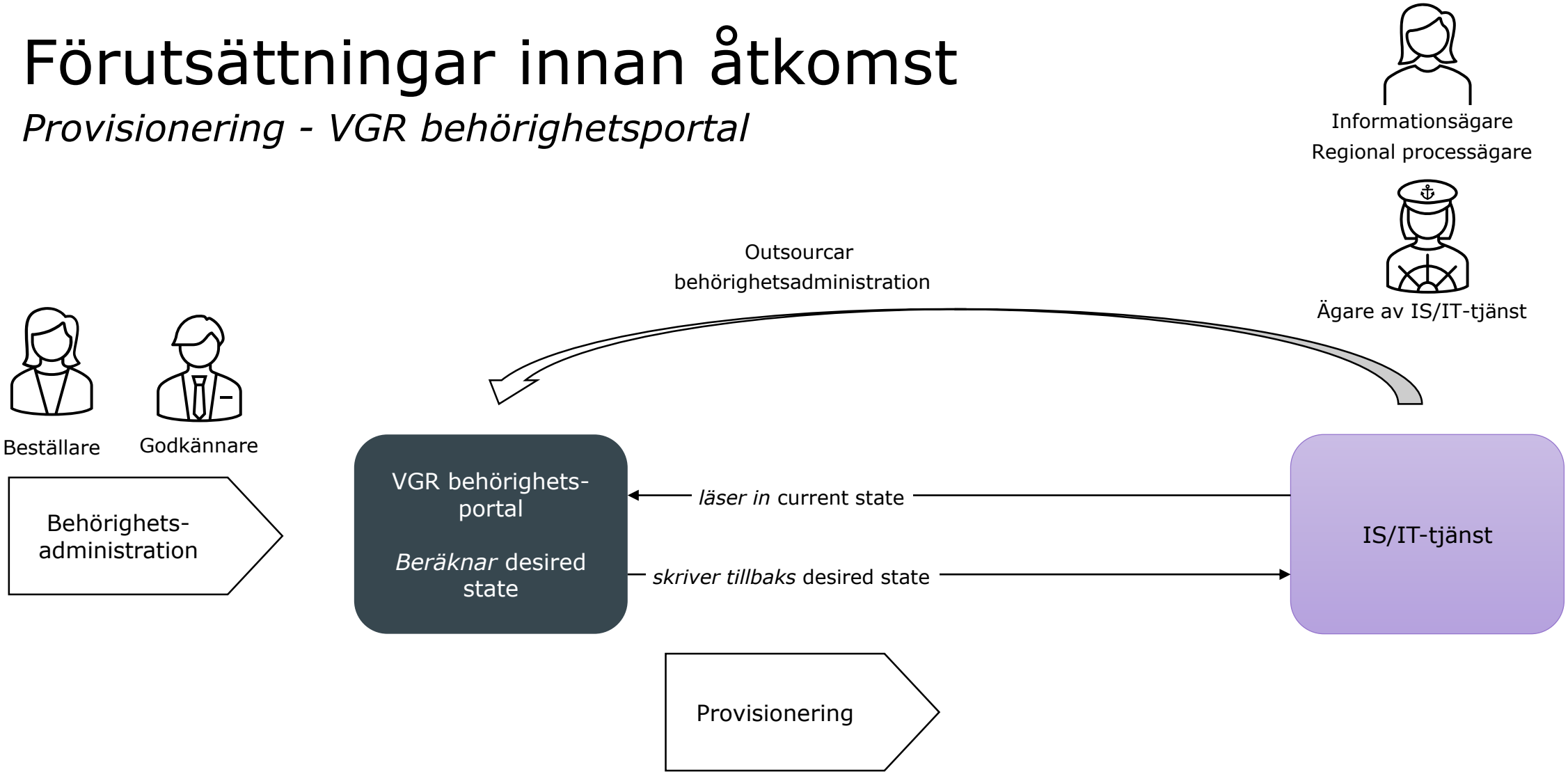
Provisionering handlar om att från centralt håll hantera i konto/användarprofiler samt resultatet av tilldelning av lokala roller/grupper/åtkomsträttigheter.

Provisionering kan ske på olika sätt, men de vanligaste är:

- **JIT (Just In Time):**
  - Identitets och behörighetsinformation finns i identitetsintyget från IdP/OP och skapas lokalt i IS/IT-tjänsten runtime.
  - Legitimerad användare finns i identitetsintyget från IdP/OP och IS/IT-tjänsten för ett direkt uppslag mot attributkällor för att sedan skapas lokalt i IS/IT-tjänsten runtime.
- **AOT (Ahead Of Time):**
  - Identitets och behörighetsinformation trycks (push) från centrala attributkällor till lokalt i IS/IT-tjänsten.
  - Identitets och behörighetsinformation hämtas (pull) från centrala attributkällor till lokalt i IS/IT-tjänsten.

Förutsättningar innan åtkomst

Provisionering - VGR behörighetsportal



Förutsättningar innan åtkomst

Tillit – bilateral federation

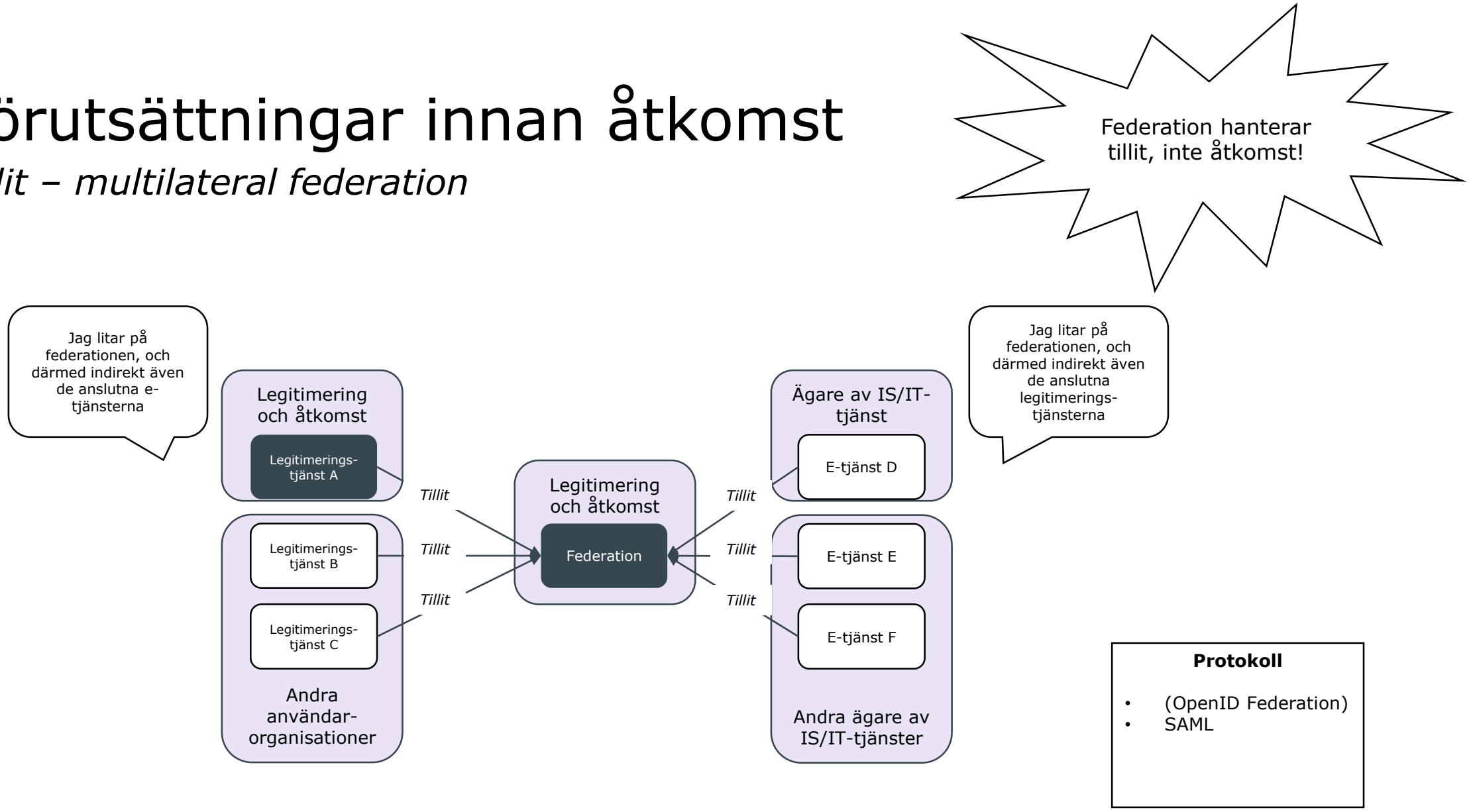
Federation hanterar tillit, inte åtkomst!

Protokoll

- OpenID Connect
- SAML
- WS-fed
- Kerberos
- ~~NTLM~~

Förutsättningar innan åtkomst

Tillit – multilateral federation



Förutsättningar innan åtkomst

Steg

1. Informationsägare/regional processägare:

1. Utför informationsklassning.
   - Förteckning över säkerhetsåtgärder.
2. Utför riskanalys.
   - Uppdaterad förteckning över säkerhetsåtgärder.

2. Ägare av IS/IT-tjänst:

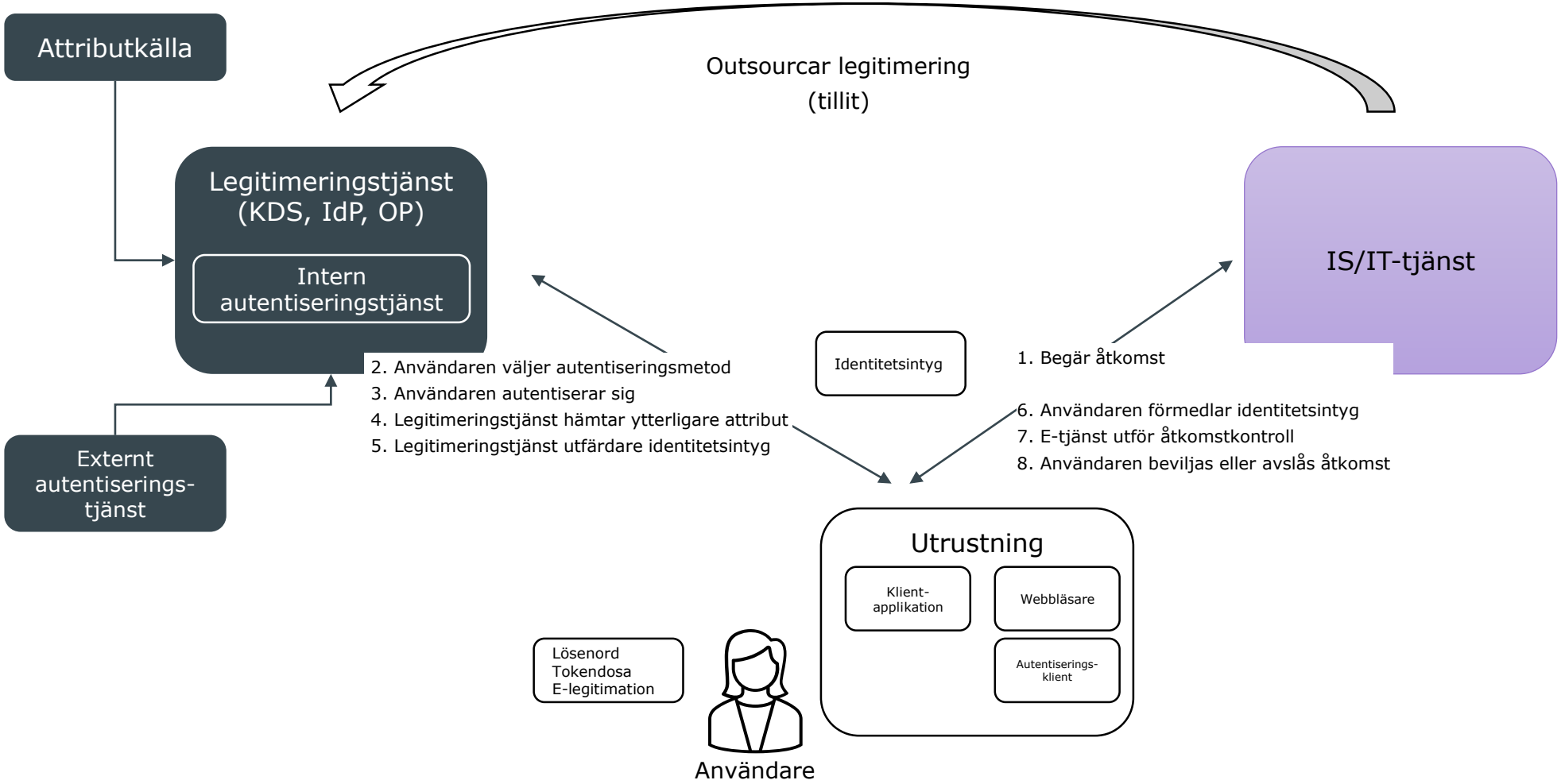
1. Identifiera behov av lokala konto/användarprofiler.
2. Identifiera behov av lokala roller/grupper/åtkomsträttigheter.
3. Identifiera behov av provisionering.
4. Identifiera behov av behörighetstilldelning.
5. Identifiera behov av tillit.
6. Identifiera behov för åtkomstkontroll.

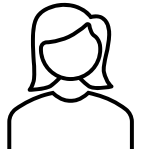
7. Dokumentera lösningsförslag.
8. Dokumentera IS/IT-säkerhetsspecifikation.
   - Krav för åtkomst.

9. Anslut IS/IT-tjänst till VGR behörighetsportal.
10. Konfigurera provisionering till IS/IT-tjänst.
    - JIT (Just In Time).
    - AOT (Ahead Of Time).
11. Anslut IS/IT-tjänst till legitimeringstjänst:
    - till bilateral federation (KDC, IdP eller OP).
    - Anslut till multilateral federation.
12. Konfigurera åtkomstkontroll i IS/IT-tjänst.

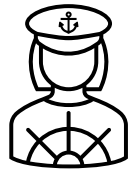
Åtkomst

Legitimering + åtkomstkontroll





Informationsägare
Regional processägare



Ägare av IS/IT-tjänst

Personuppgiftstjänster

Personuppgiftstjänster erbjuder:

- **Västfolket** - Innehåller folkbokföringsuppgifter från Skatteverket för personer i Västra Götaland och Halland med person- eller samordningsnummer.
- **Augustus** - Innehåller folkbokföringshistorik som ligger till grund för vårdfakturering.
- **Befreg/Personuppgiftstjänst VGR** - Innehåller folkbokföringsuppgifter från Skatteverket för personer i Västra Götaland och Halland med person- eller samordningsnummer samt uppgifter för VGR:s reservnummerpatienter, lagrar vissa uppgifter i historik för spårbarhet.
- **Personuppgiftsportalen VGR** - Innehåller folkbokföringsuppgifter från Skatteverket samt funktionalitet för att hantera reservnummer (till exempel skapa, uppdatera och koppla/ länka reservidentiteter).
- **RAPS** - applikation för regional hantering av reservnummersammanslagningar.

KIV digital identitet

KIV digital identitet erbjuder:

- **KIV – Katalog i Väst**: KIV är lagring, administration och tillgängliggörande av kvalitetssäkrade data om medarbetare och organisation. KIV omfattar …
  - KIV-core – datalager och integrationslogik för källsystem (HR, PU mm).
  - KiV-admin - gränssnitt för KiVs administration.
  - FileService – Dagligt exporterade json-filer.
  - WebService – SOAP-tjänst.

Behörighet och provisionering

Behörighet och provisionering erbjuder:

- **VGR behörighetsportal** - plattform för livscykelhantering av konton och behörigheter. Här ansluts nya system som har behov av vår leverans
- **Behörighetsbeställningsportal - BEH** - gammalt digitalt formulär främst för många legacysystem. Här beställs även i nuläget vårdmedarbetaruppdrag (VMU). Inga nya system ansluts, utan hänvisas till VGR behörighetsportal

Legitimering och åtkomst

Multilaterala federationer

Legitimering och åtkomst erbjuder:

- **Sambi**
  Digitalisering av vård, hälsa och omsorg kräver säker digital samverkan mellan olika verksamheter och organisationer. Sambi är en nationell infrastruktur för säker åtkomst och tillitsfull informationsdelning inom vård och omsorg.
- **Skolfederation**
  Skolan hanterar dagligen stora mängder personuppgifter och inloggningar till digitala tjänster som används i undervisningen. Skolfederation möjliggör för lärare och elever att med en enda inloggning nå samtliga digitala tjänster som skolan har avtal med och som är anslutna till federationen.
- **Sweden Connect**
  Sweden Connect är Sveriges anslutningspunkt till eIDAS och innehåller funktioner för elektronisk identifiering. Tjänsten används av offentliga och privata e-tjänster för att möjliggöra inloggning med både svenska och utländska e-legitimationer.

VGR Legitimering och åtkomst planerar att ansluta till:

- **Ena ”federationsinfrastruktur”**
  Ena tillhandahåller en gemensam nationell infrastruktur för federation av digitala identiteter inom offentlig sektor.

VGR Legitimering och åtkomst kan ansluta vid behov till:

- **Swamid**
  Genom identitetsfederationen Swamid kan organisationen erbjuda forskare, lärare och studenter säker och kvalitetssäkrad inloggning till ett brett utbud av tjänster – både nationellt och internationellt.

Legitimering och åtkomst

Legitimeringstjänster för bilaterala federationer

VGR Legitimering och åtkomst erbjuder:

- **VGR AD**
  VGR:s centrala inloggningsmiljö för VGR:s medarbetare och för administrativa e-tjänster för både intern och extern IT-drift.
  - **VGR AD (ADDS)**
    Syfte är VGR:s medarbetare och för administrativa e-tjänster i intern IT-drift (dvs placerade i VGR:s datacenter).
    Stödjer protokollen Kerberos, NTLM (under avveckling) och LDAP (endast för sökningar i VGR AD, ej autentisering).
    Stödjer autentiseringsmetoderna användarnamn/lösenord och SITHS eID på kort.
    Uppnår tillitsnivå 2.
  - **VGR AD (ADFS)**
    Syfte är VGR:s medarbetare och för administrativa e-tjänster i intern IT-drift (dvs placerade i VGR:s datacenter).
    Stödjer protokollen OpenID Connect, SAML och WS*.
    Stödjer autentiseringsmetoderna användarnamn/lösenord, SITHS eID på kort och mobil, Microsoft Authenticator och RSA SecurID.
    Uppnår tillitsnivå 2.
    Är en godkänd legitimeringstjänst i Skolfederation.
  - **VGR AD (ADFS SITHS)**
    Syfte är VGR:s medarbetare och för administrativa e-tjänster i intern IT-drift (dvs placerade i VGR:s datacenter).
    Stödjer protokollen OpenID Connect, SAML och WS*.
    Stödjer autentiseringsmetoderna SITHS eID på kort och mobil.
    Uppnår tillitsnivå 2.
  - **VGR AD (Entra ID)**
    Syfte är VGR:s medarbetare och för administrativa e-tjänster i extern IT-drift (dvs placerade i leverantörernas datacenter).
    Stödjer protokollen OpenID Connect, SAML och WS*.
    Stödjer autentiseringsmetoderna användarnamn/lösenord, SITHS eID på kort och mobil, Microsoft Authenticator och RSA SecurID samt snart Fido2 säkerhetsnyckel för admins.
    Uppnår tillitsnivå 2.

Legitimering och åtkomst

Legitimeringstjänster för bilaterala federationer

VGR Legitimering och åtkomst

- **Lokal IdP**
  Syfte är VGR:s medarbetare och för vård e-tjänster i intern IT-drift (dvs placerade i VGR:s datacenter) och extern IT-drift (dvs placerade i leverantörernas datacenter).
  Stödjer protokollen OpenID Connect och SAML.
  Stödjer autentiseringsmetoderna SITHS eID på kort och mobil.
  Uppnår tillitsnivå 3.
  Är en godkänd legitimeringstjänst i Sambi.
  Plattform kommer att bytas ifrån nuvarande Ineras Legitimeringstjänst Lokal IdP för medarbetare till Fortified Integrity.

- **E-legitimeringstjänst för privatperson**
  Syfte är privatpersoner och för medborgartjänster i intern IT-drift (dvs placerade i VGR:s datacenter) och extern IT-drift (dvs placerade i leverantörernas datacenter).
  Stödjer protokollen OpenID Connect och SAML.
  Stödjer autentiseringsmetoderna BankID på fil, kort och mobil, BankID samt eIDAS.
  Uppnår tillitsnivå 3.
  Är en godkänd e-tjänst (för att få åtkomst till legitimeringstjänsten för Freja eID) i Sweden Connect.
  Kommer att avvecklas under 2027 q1-q2 med hänvisning till Ineras nya Utveckling av invånar-IdP.

Legitimering och åtkomst

Legitimeringstjänster för bilaterala federationer

Inera erbjuder:

- **Legitimeringstjänst IdP för medarbetare**
  Syfte är andra organisationers medarbetare och för vård e-tjänster i intern IT-drift (dvs placerade i VGR:s datacenter) och extern IT-drift (dvs placerade i leverantörernas datacenter).
  Stödjer protokollen OpenID Connect (Bas) och SAML (Plus och Bas).
  Stödjer autentiseringsmetoderna SITHS eID på kort och mobil.
  Uppnår tillitsnivå 3.
  Är en godkänd legitimeringstjänst enligt Sweden Connect.

- **Legitimeringstjänst IdP för medarbetare (2026 q2)**
  Syfte är privatpersoner och för medborgartjänster i intern IT-drift (dvs placerade i VGR:s datacenter) och extern IT-drift (dvs placerade i leverantörernas datacenter).
  Stödjer protokollen OpenID Connect och SAML.
  Stödjer autentiseringsmetoderna BankID på fil, kort och mobil, BankID samt eIDAS.
  Uppnår tillitsnivå 3.

PKI, Kryptografisk nyckel och Underskrift

VGR PKI, Kryptografisk nyckel och Underskrifterbjuder:

- **VGR PKI**.
- **Rågården PKI**.
- **FVM PKI**.
- **VGR Kryptografisk nyckel** – tjänsten är under etablering.
- **Elektronisk underskriftstjänst**.

VÄSTRA GÖTALANDSREGIONEN