

# Tillämpning Referensarkitektur IAM i VGR

Rickard Dehlin

Västra Götalands regionen

IT-arkitekt med plattformsansvar för Identitet & åtkomst.

Hellre dialog än monolog, så ställer mer än gärna frågor i chatten så försöker jag besvara dem eller så ber jag frågeställaren slå på ljudet och ställa frågan.

# Disclaimer

Denna presentation försöker bara beskriva VGR:s resa och så långt som VGR har kommit idag med referensarkitekturen för Identitet & åtkomst, och den gör inga anspråk på att vara det rätta sättet 😊



## VGR

- Offentlig sektor.
- En av Sveriges 21 regioner.
- Grundades 1999, som en pilot för regioner i Sverige.
- 64 000 medarbetare.
- Budget 55 miljarder.
- 1 730 000 invånare (2020).

## VGR IT

- 1 775 medarbetare (1 000 konsulter).
- Grundades in 2007.
- Komplet IT leverantör, från datacenter till användartjänster.
- 83 000 aktiva personkonton i AD.
- 75 000 aktiva datorkonton i AD.
- 240 000 utrustningar på VGRnet.
- 2 000 system.
- Budget 1,5-2 miljarder.



Hälso- och sjukvård



Transport



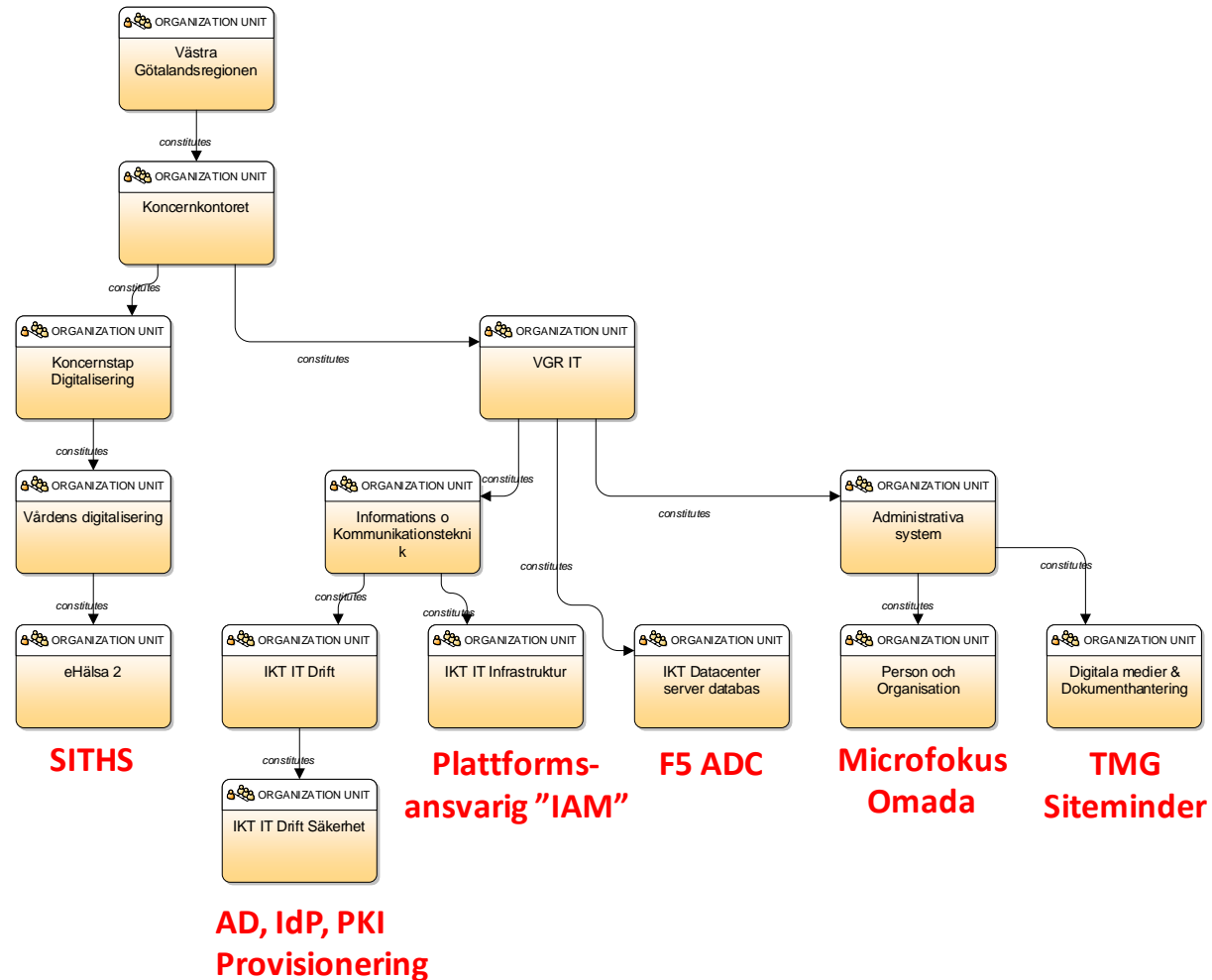
Kultur



Regional utveckling

# VGR:s linje- organisation för IAM

Det finns alltså ingen sammanhållen leverans för "IAM", utan det är utsmetat till var någon historiskt har sett ett behov av en produkt.



# VGR:s leverantörer för IAM

Mycket bra teknik –  
men en salig blandning.

De flesta leverantörer  
har "sin egna  
arkitektur", ur ett  
produktperspektiv.



# 2015 så började VGR arbeta med strategier

Identitet, behörighet och åtkomststrategi för VGR kompletterar övriga styrande dokument

Informationssystem, 2015-11-17, 0:07  
Reviderad: 16/03/2015  
Utgåva: 04/2015 (04 av 04) 01/16

### Policy

#### Säkerhet och beredskap i Västra Götalandsregionen

Policyn innehåller grundläggande riktlinjer, principer och förhållningssätt för arbetet med säkerhet och beredskap i Västra Götalandsregionen. Policyn gäller för västra, sydvästra samt myndighetsägda bolag.

#### Värdegrund

Säkerhet och beredskap innebär att skydda Västra Götalandsregionens aktiver, tillgångar, såväl personella, materiella och immateriella. Skada av t.ex. väder, olycka, terrorist, sabotage och andra hot mot regionen och dess verksamhet är en potentiell risk för regionens verksamhet och dess verksamhet. Detta innebär att säkerhet och beredskap är en grundläggande förutsättning för att kunna tillhandahålla de tjänster som regionen ska erbjuda.

#### Förhållningssätt

Arbetet med säkerhet och beredskap ska utvärderas och utvärderas utifrån en systematisk och strukturerad metod. I Västra Götalandsregionen bedrivs systematisk utvärdering av säkerhet och beredskap i alla verksamheter, lagar och myndigheter, kommuner och andra myndigheter som samarbetar med regionen. Detta innebär att säkerhet och beredskap ska utvärderas i alla verksamheter och myndigheter som samarbetar med regionen. Detta innebär att säkerhet och beredskap ska utvärderas i alla verksamheter och myndigheter som samarbetar med regionen.

#### Säkerhet och beredskapens betydelse för Västra Götalandsregionen

Säkerhet och beredskap är en förutsättning för att kunna tillhandahålla de tjänster som regionen ska erbjuda. Detta innebär att säkerhet och beredskap är en grundläggande förutsättning för att kunna tillhandahålla de tjänster som regionen ska erbjuda.

• Säkerhet och beredskap är en grundläggande förutsättning för att kunna tillhandahålla de tjänster som regionen ska erbjuda.

Informationssystem, 2015-11-17, 0:07  
Reviderad: 16/03/2015  
Utgåva: 04/2015 (04 av 04) 01/16

### RS-riktlinjer för Informationssäkerhet i Västra Götalandsregionen

RS 1704:20

Titel	Utgivningsår	Utgivningsdatum
RS 1704:20	2014-09-01	2014-09-01

Informationssystem, 2015-11-17, 0:07  
Reviderad: 16/03/2015  
Utgåva: 04/2015 (04 av 04) 01/16

### Styrmall för IS/IT Västra Götalandsregionen 3.3

Titel	Utgivningsår	Utgivningsdatum
Styrmall för IS/IT	2014-09-01	2014-09-01

Informationssystem, 2015-11-17, 0:07  
Reviderad: 16/03/2015  
Utgåva: 04/2015 (04 av 04) 01/16

### Identitet, behörighet och åtkomststrategi för VGR

Titel	Utgivningsår	Utgivningsdatum
Identitet, behörighet och åtkomststrategi	2014-09-01	2014-09-01

Informationssystem, 2015-11-17, 0:07  
Reviderad: 16/03/2015  
Utgåva: 04/2015 (04 av 04) 01/16



# Identitet, behörighet och åtkomst- strategi för VGR.

Ett första försök att göra  
något som kan  
betecknas som  
arkitektur - principer

## 3.5 Principer

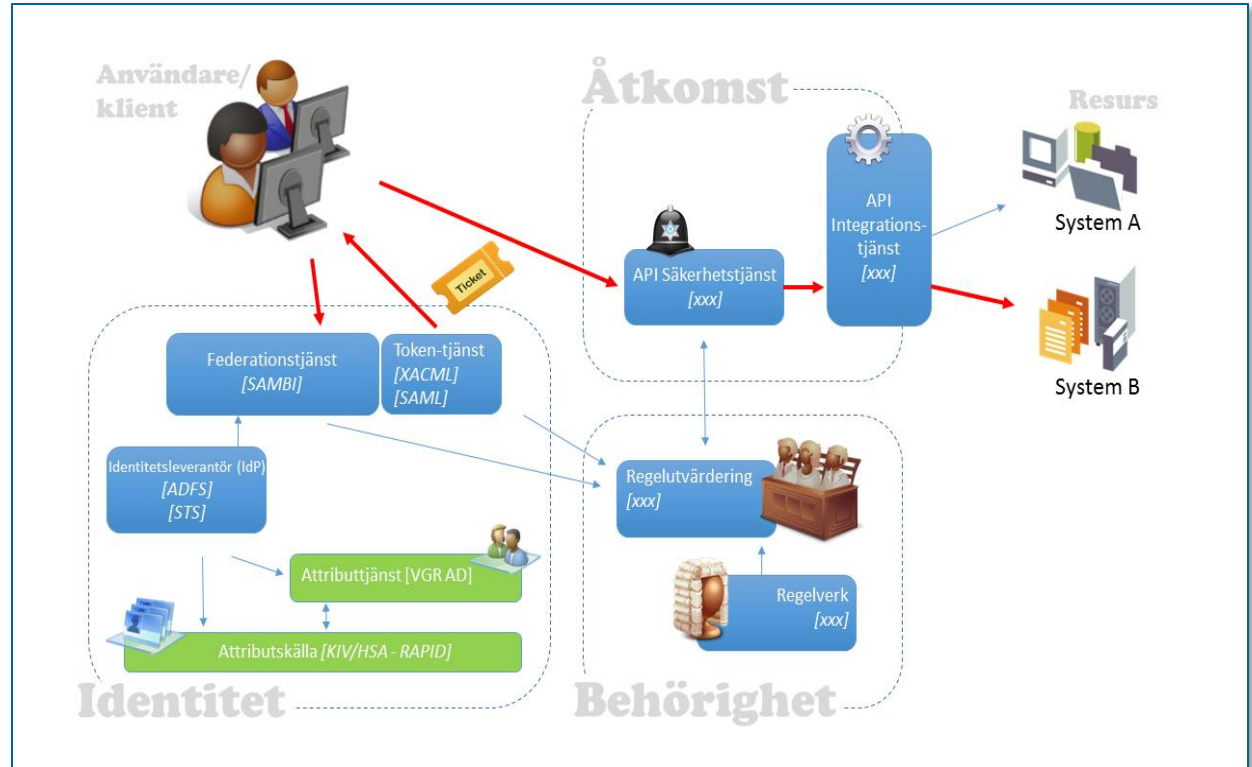
Dessa strategiska principer ska följas vid anskaffning, utveckling och förvaltning av verksamhetssystem inom VGR.

- Autentisering sker centralt, separerat och frikopplat i förhållande till system
- Auktorisation baseras på attribut
- Administration av behörighetsgivande attribut är kvalitetssäkrad
- Kvalitetssäkrad identitetsinformation är centraliserad

# Identitet, behörighet och åtkomststrategi för VGR.

Ett första försök att göra något som kan betecknas som arkitektur – begrepp och samlad översikt

(tack Östergötland)



# 2017 så släpps Inera Referens- arkitektur för Identitet och Åtkomst

77 sidor!

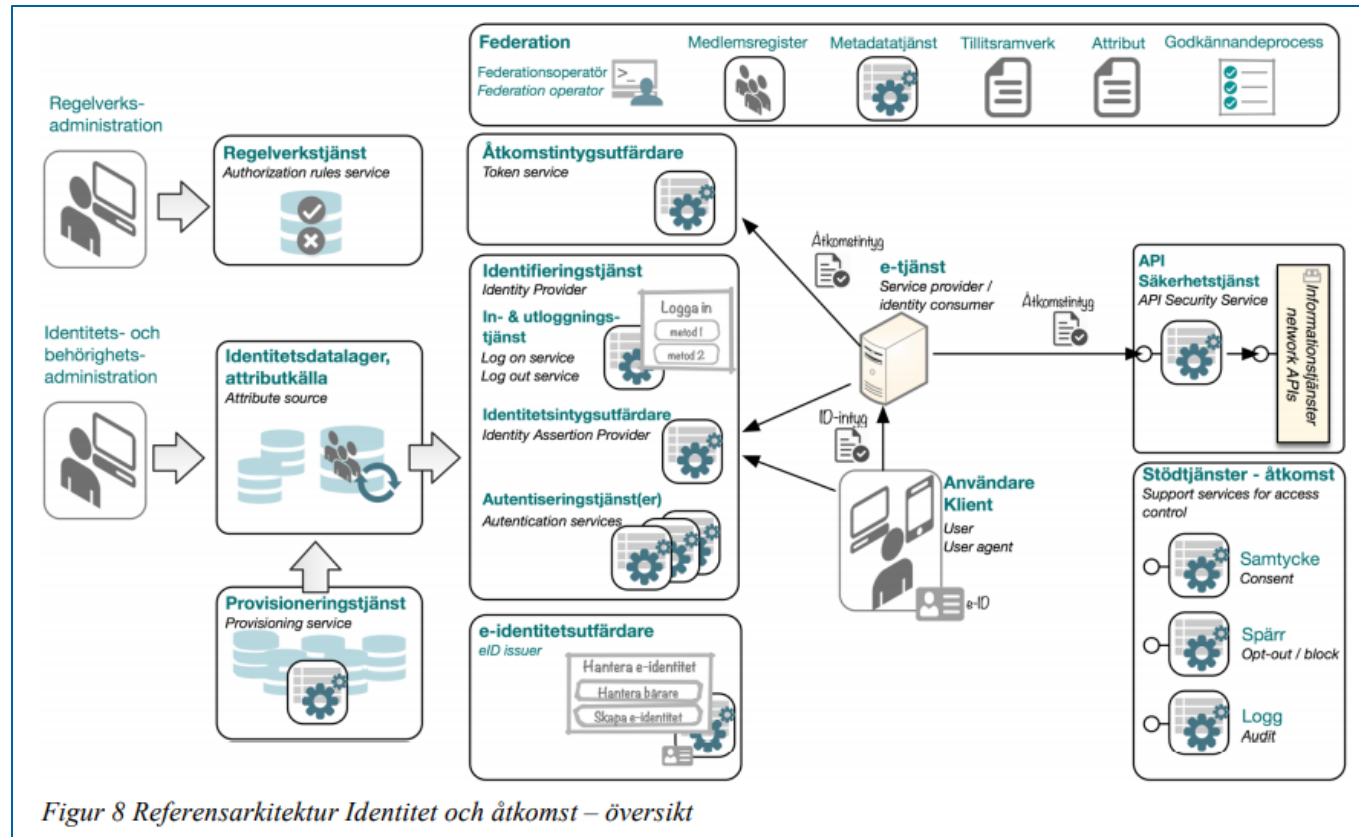


## Referensarkitektur för Identitet och Åtkomst

Utformning av IT-stöd för säkerställd identitet och åtkomst till rätt information vid rätt tillfälle, inom och mellan organisationer.

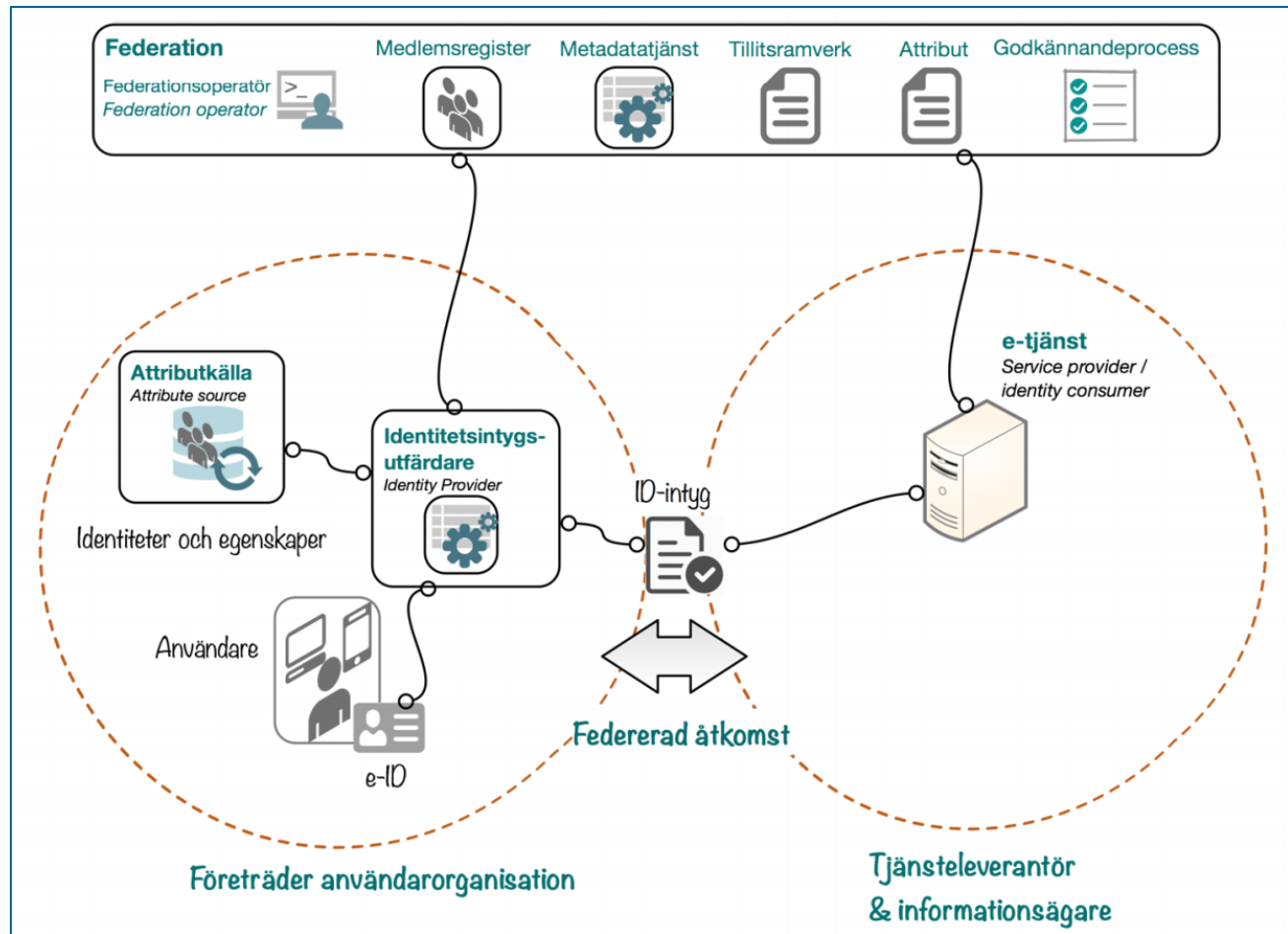
Rev A

Två bilder är  
ständig  
återkommande



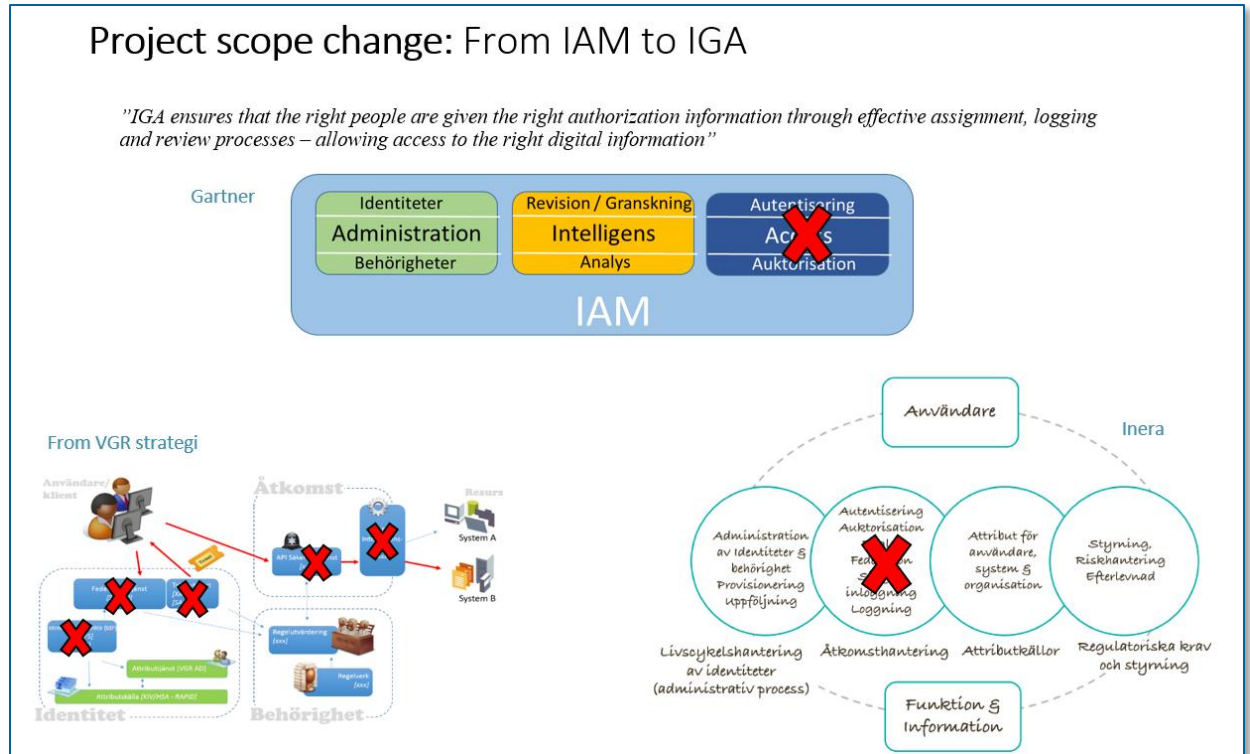
Figur 8 Referensarkitektur Identitet och åtkomst – översikt

Två bilder är  
ständig  
återkommande



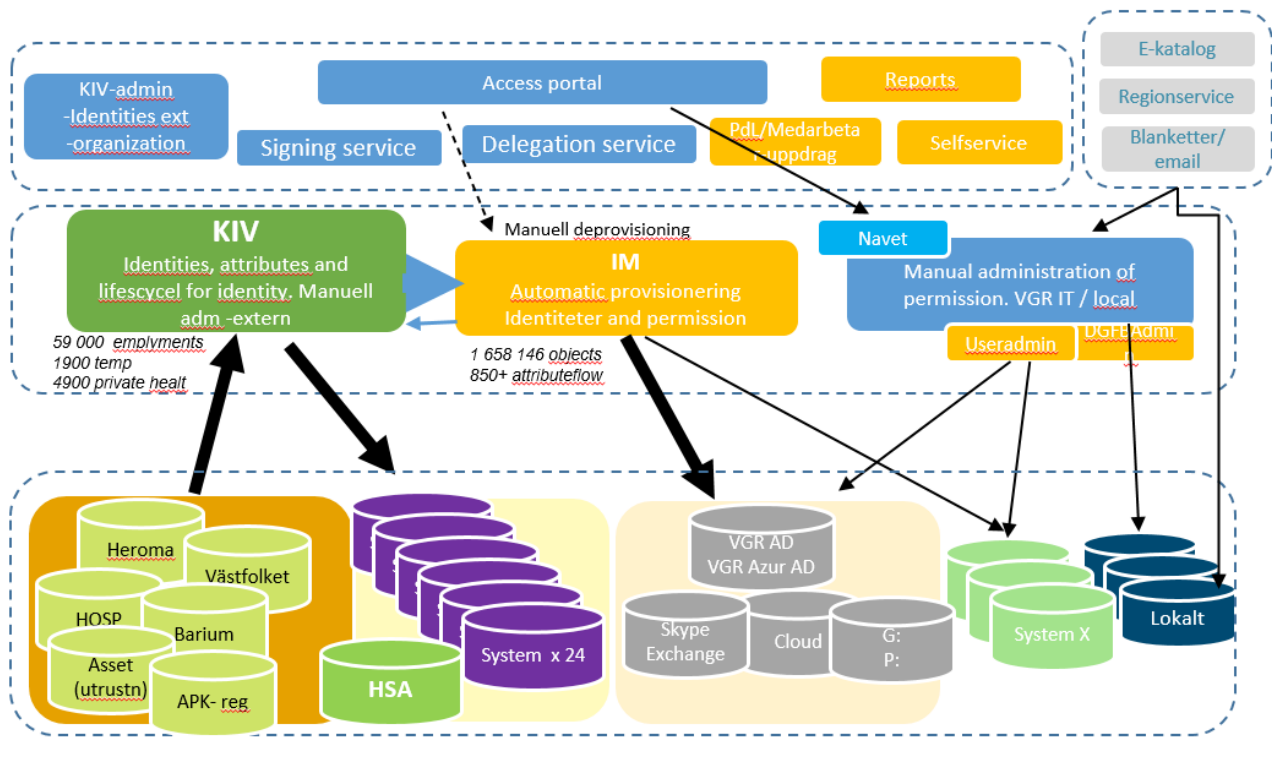
# Olika delar inom VGR börjar ta axplock ur arkitekturen

Exempelvis VGR:s projekt för att byta till en IGA plattform (som inte innefattar autentisering och auktorisation)



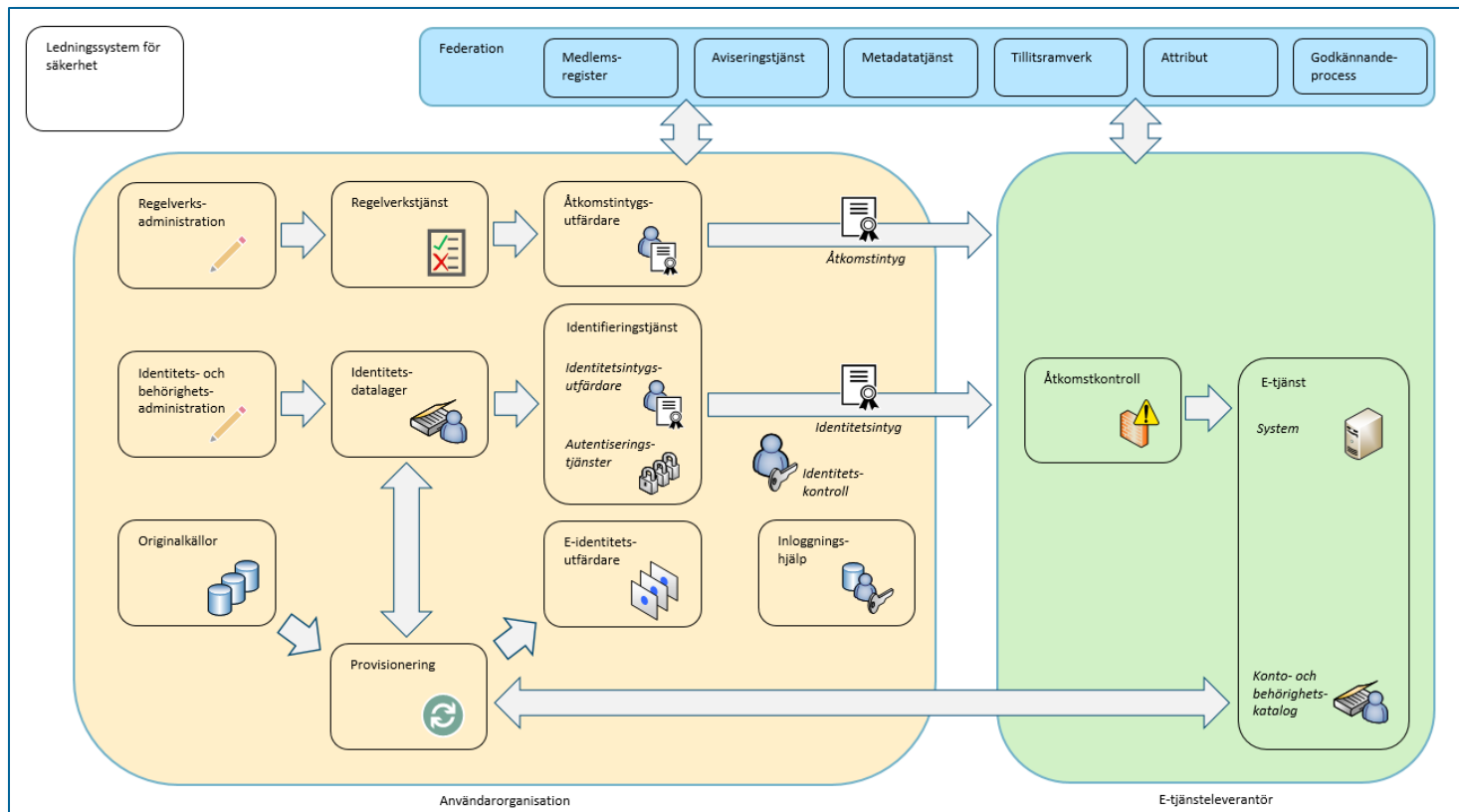
... men  
fortfarande  
inget  
strukturerat  
sätt att  
beskriva vår  
miljö

## Current state – IAM platform(s)



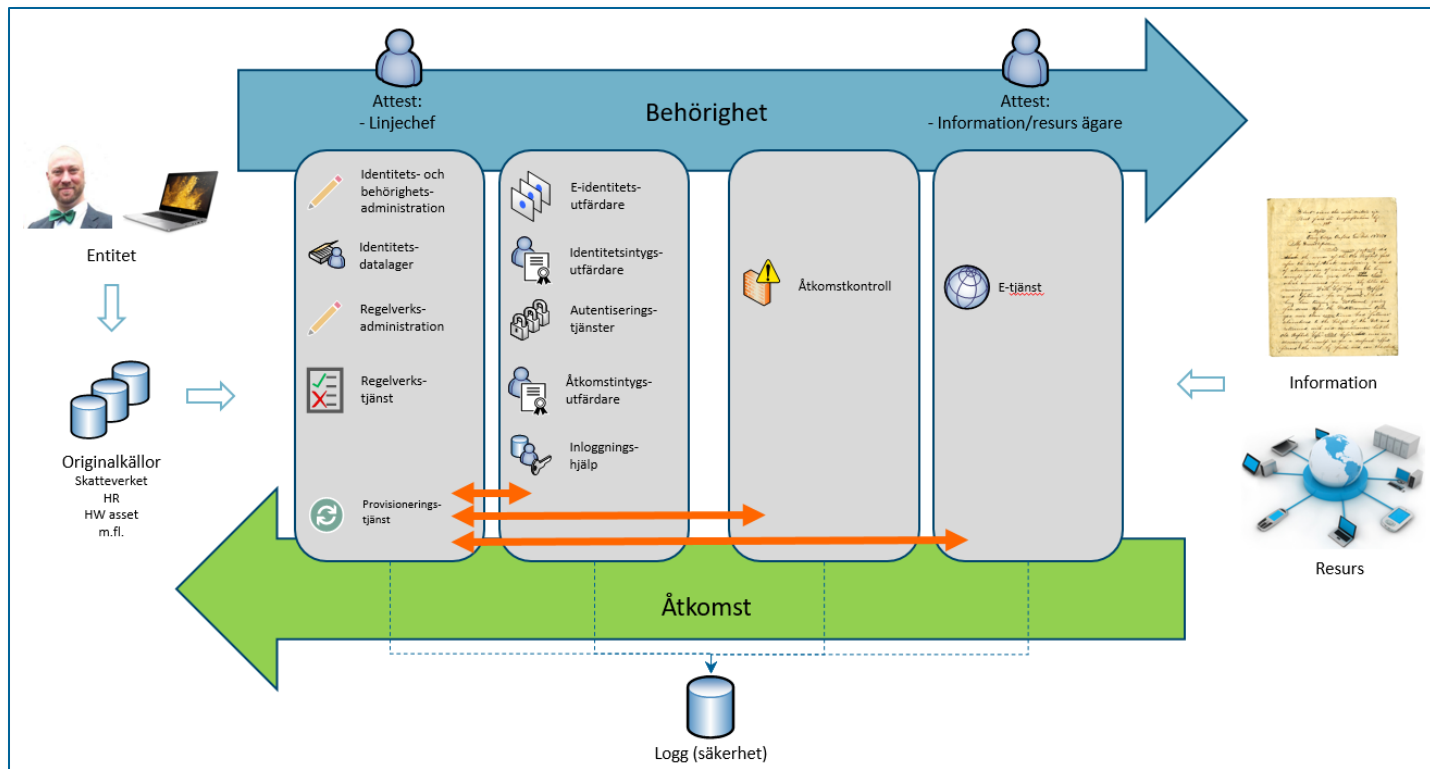
# Första försöket att "VGRifiera" Ineras översiktsbild

Begreppen är med (men inte säkerhetstjänserna)





Och någon form av processbild




# Lärdom 2017

- Gemensam begreppsmodell
- **Referens**-arkitektur, inte lagbok (vi började nog med att se den som en sådan)
  - Våga förändra/förädla utifrån VGR:s perspektiv.
- Flera förvaltare och leverantörer är fortfarande omogna/oförstående till referens-arkitekturen.

# VGR:s IT-miljö dokumenterad

Även här pekar vi nu internt på referensarkitekturen.

 VÄSTRA GÖTALANDSREGIONEN		Version: 1.7.1	Side: 1 (91)
Dokumentbeskrivning: <i>VGR:s IT-miljö</i>			
Utfärdat av: Noak Eldh, Staffan Dahlin	Utfärdat datum: 2020-09-09	Godkänt av: Noak Eldh	Godkänt datum: 2020-09-09

## VGR:s IT-miljö

13	Identitet & åtkomst .....	69
13.1	Sammanfattning .....	69
13.2	Referensarkitektur för Identitet & åtkomst .....	70
13.2.1	Övergripande beskrivning av de olika delarna i referens-arkitekturen .....	70
13.2.2	Kort om SAMBI – identitetsfederation .....	75
13.2.3	Tillitsnivåer .....	75
13.2.4	Flerfaktorsautentisering .....	76
13.2.5	SSO – Single Sign On .....	77
13.2.6	eSSO – Enterprise Single Sign On .....	77
13.2.7	Användartjänster .....	77

# Upphandling FVM

Västra Götalandsregionen  
2018-05-18

## **Bilaga 18** Säkerhet

[Anbudsgivarens namn]

# Pekar på referens- arkitekturen i upphandling (FVM)

## **Underbilaga 18-08, Inera behörighetsmodell för administrativa uppdrag**

*Underbilaga 18-08* är Ineras behörighetsmodell för administrativa uppdrag, vilken Kunden vill arbeta efter i de fall det är tillämpligt. Dokumentet innehåller den behörighetsmodell som skapats med begrepps- och informationsmodeller för behörighetstilldelning för de uppdrag där användaren inte kommer i kontakt med patientdata. Avsikten är att skapa en gemensam modell för att beskriva och tolka behörigheter.

## **Underbilaga 18-09, Referensarkitektur för Identitet och Åtkomst**

*Underbilaga 18-09* är Ineras nationella referensarkitektur för identitet och åtkomst, utformning av IT-stöd för säkerställd identitet och åtkomst till rätt information vid rätt tillfälle, inom och mellan organisationer.

# Pekar på Kravunderlag inom området Identitet och Åtkomst (FVM)



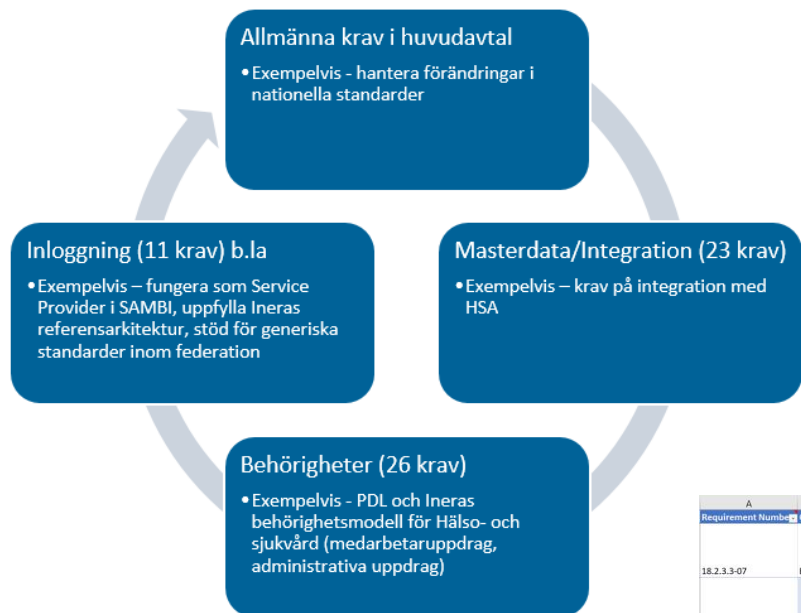
## **Kravunderlag inom området Identitet och Åtkomst**

Specifik kravställning inom området identitets- och åtkomsthantering att utnyttja som underlag vid nyanskaffning av informationssystem.

Ett kompletterande dokument till *Referensarkitektur för Identitet och Åtkomst (IAM)*.

Version 1.0 PA3

# Pekar på referens-arkitekturen i upphandling (FVM)



Projekttillhörighet	Antal krav i IAM
Care Professional Documentation	5
Core	24
Informatics	2
Integration	7
Maintenance and Support	2
Reporting	6
Technical Infrastructure	16

A	B	C	D	E	F
Requirement Number	Contract Location	IAM-Area	Req. Type	Description English	Description Swedish
18.2.3.3-07	Bilaga 18 - Säkerhet	Authentication	Ska	The Solution's login method (authentication method), should no later than when the Pilot is introduced, be able to be adapted and changed without a requirement to change the Solution, by logging into the Solution being delegated to an Identification service. Yes. No later than when the Pilot is introduced, the Solution must have a clear logout function for the User, which should end the User's session in the system and send a logout request to the Identification service by using one of the following: <ul style="list-style-type: none"> <li>For SAML 2.0: SAML Logout</li> <li>For OpenID Connect: Front-channel/Back-channel Logout</li> </ul> Yes	Lösningens inloggningsmetod (autentiseringsmetod) ska, senast då Piloten är anpassad och förändras utan krav på förändring av Lösningen genom att info Lösningen delegeras till Identifieringstjänst.  Lösningen ska, senast då Piloten inledd, ha en för Användaren tydlig utloggning vilken ska avsluta Användarens session i systemet samt skicka en utloggning Identifieringstjänsten genom att använda en av följande: <ul style="list-style-type: none"> <li>För SAML 2.0: SAML Logout</li> <li>För OpenID Connect: Front-channel/Back-channel Logout</li> </ul> Yes

# Drivkrafter används för att presentera "varför"

## Drivkrafter

- I nuläget
  - Många konton
  - Lösenord
  - Låg igenkänningsfaktor
  - Krångligt med behörigheter
  - Tidskrävande administration

**Singelinloggning**  
snabb, enkel och säker  
tillgång till information

**Nya inloggnings-  
metoder**

**Mobila  
arbetsätt**



**Kvalitetssäkring**  
av e-identiteter

**Standardisering**  
minska inläsning och  
kostnader

**Säker samverkan** över  
organisationsgränser



Varvet – VGR:s  
arkitektur-  
ramverk.  
Baseras på  
TOGAF 9.2 och  
har anpassats.

## Modell för arkitekturstyrning & arkitekturförvaltning

Dokumentägare:	Chefarkitekt/EA-funktionen
Dokumenttyp:	Styrande dokument
Godkänt av:	VGR IT Ledningsgrupp
Datum:	2018-03-12
Version:	1.0

Varvet – VGR:s  
arkitektur-  
ramverk.

Baseras på  
TOGAF 9.2 och  
har anpassats.

## Struktur och innehåll

### ■ Termer och Begrepp

- Ett gemensamt språk och synsätt; en parlör för arkitektur.

### ■ Metamodell

- Hur objekt hänger samman; grammatik för modellering.

### ■ Vyer och symboler

- Presentation ur ett visst perspektiv; delmängder och visuell design.

### ■ Dokument och leverans

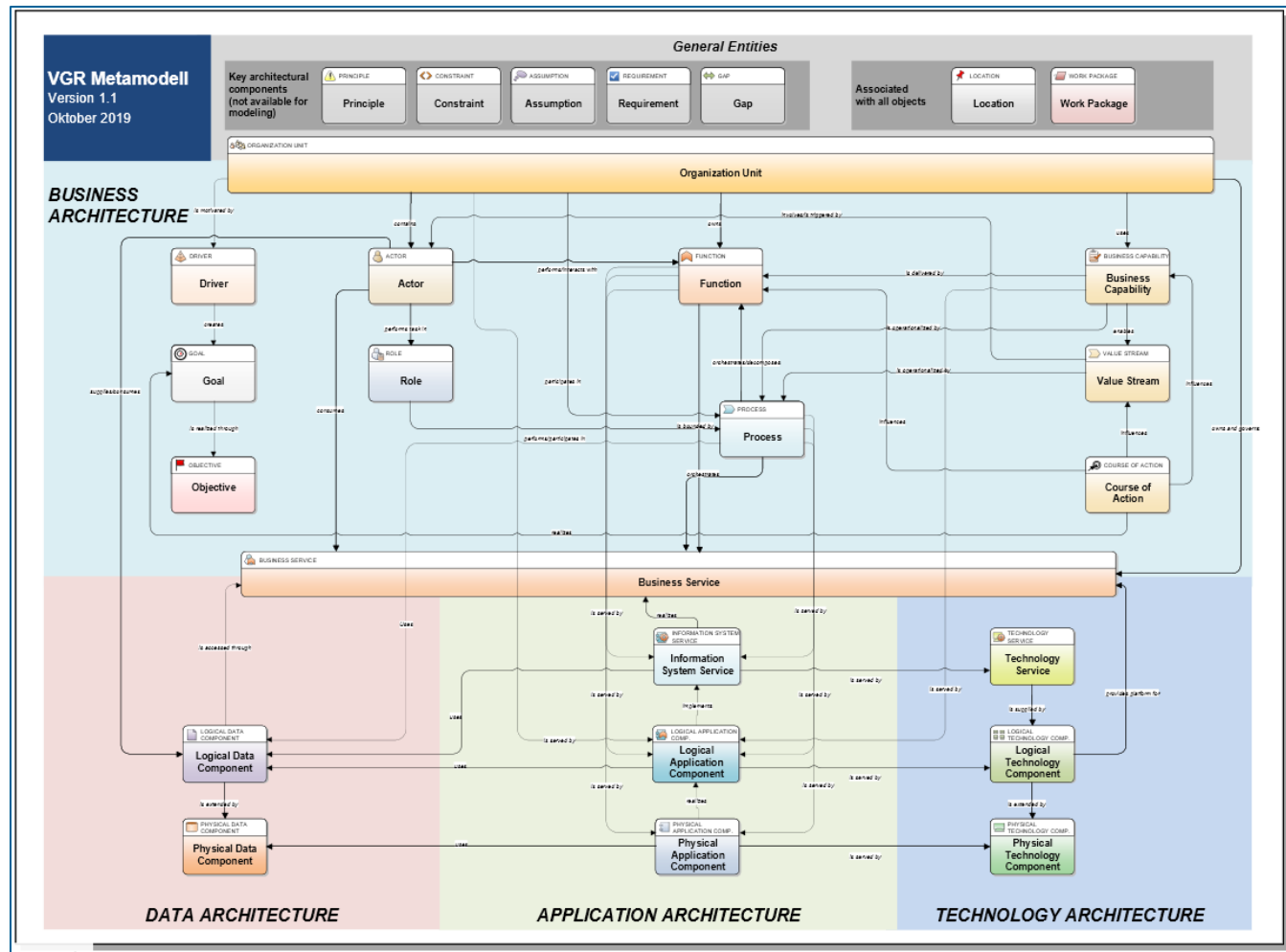
- Hur arkitektur sammanställs, dokumenteras och levereras.

**arkitektu'r**   [-ki- el. -çi-]  
substantiv ~en ~er  
ORDLED: arki-tekt-ur-en



# Varvet – metamodell

VGR använder iServer  
som verktyg för Varvet



# Lärdom 2018

- I och med införandet av Varvet så finns det något att ”häkta på” för referensarkitekturen.
- Se området logiskt, fokusera inte på tekniska produkter.
- Drivkrafter börjar att användas.
- Referensarkitekturen är inte bara för IAM:s förvaltning och produkter utan för flera intressenter.
- Referensarkitekturen håller för upphandling.

# 2019 – Förvaltande objekt tar fram objektplaner

Referensarkitekturen  
anas ...

Förstudien ser viss problematik inom följande områden

- 1) Kontohantering  
Livscykelhantering saknas. Ej koppling till VGR's AD. Konton och lösenord skapas lokalt i <system X>.
- 2) Behörighetstilldelning  
Sker lokalt i <system X>.
- 3) Identifiering  
Inloggning med användaridentifiering sker i <system X> mot konton som lagras med lokala användarnamn och lösenord.

Målbild:

VGR's strategi för behörighet och åtkomst skall användas. Detta leder också till såväl förenklad kontoadministration som förbättrad användarupplevelse genom att användarna använder centrala användarnamn och lösenord och möjligheter kan finnas till single signon.

Förstudien rekommenderar förändringar inom följande områden.

- 1) Kontohantering  
VGR's centrala system Kiv 3.0 skall användas för kontoadministration.
- 2) Behörighetstilldelning  
VGR's centrala system Kiv 3.0 skall användas för behörighetstilldelning.
- 3) Identifiering  
Dagens Informationsklassning av <system X> är gemensam för <instans Y> och <instans Z>. Denna bör uppdateras och göras separat för <instans Y> och <instans Z> för att ge underlag till risk och sårbarhetsanalys om det kan finnas olika krav kring stark authenticering för <instans Y> respektive <instans Z> som innehåller patientinformation.  
<system X> ska stödja federerad inloggning via en federeringstjänst som sköter identifiering av användare separerad från <system X>. Beroende på om t.ex stark authenticering krävs för enbart <instans Y> eller både <instans Y> och <instans Z> behöver detta inte hanteras lokalt i <system X> utan kan hanteras på olika sätt i ADFS. Djupare analys behöver göras kring vilka protokoll som <system X> stödjer.

# EA-principer tas fram inom Varvet

Detta ger en ram för att  
föra in principerna #IA1 -  
#IA10 ifrån  
referensarkitekturen till  
Varvet.

Övergripande arkitekturprinciper för  
Region Västra Götaland  
(Enterprise Architecture principles)  
Version 1.0

# Principer inom IAM används i ADD av lösningsarkitekter

Dessa är ännu inte formaliserade

## 8.1.2.1 Övergripande IS/IT-principer

VGR har sedan tidigare beslutat att fem styrande IS/IT principer skall vägleda utvecklingen av applikationslandskapet, dessa principer skall vara vägledande även vid utvecklingen av framtidens IT-komponenter inom ersättningsområdet:

1. Kundnytta ska vara överordnad IS/IT
2. Helheten prioriteras före delarna
3. För varje verksamhetsfunktion är strävan att det endast ska finnas en IS/IT-lösning

Arkitekturdirektiv

Projekt: FVM/EE Ersättning

Utkast/Version 0.1

13

4. Vid anskaffning av IS/IT ska standardiserade produkter, tjänster eller lösningar vara huvudalternativet
5. Ge användaren tillgång till rätt tjänst, rätt information, vid rätt tillfälle, på rätt plats och på rätt sätt

## 8.1.2.2 Styrande IS/IT-principer

Konkret för projektet innebär det att nedan principer ska tas i beaktande:

Princip	Principformulering	Påverkan på arkitekturdesign	Ägare av principen	Referens
Autentisering sker centralt, separerat och externt i förhållande till system	System konsumerar elektroniska identitetsintyg istället för att autentisera identiteter med egen programlogik. Detta innebär att våra system blir mer oberoende av vilken domän eller organisation en användare härrör från, inklusive medborgare vilka använder e-legitimation eller andra källor för identitetsinformation	Autentisering och auktorisering centraliseras till AD/ADFS från att i dagens lösningar ske lokalt	IKT IT Infrastruktur	<a href="#">Identitet, behörighet och åtkomststrategi för VGR</a>

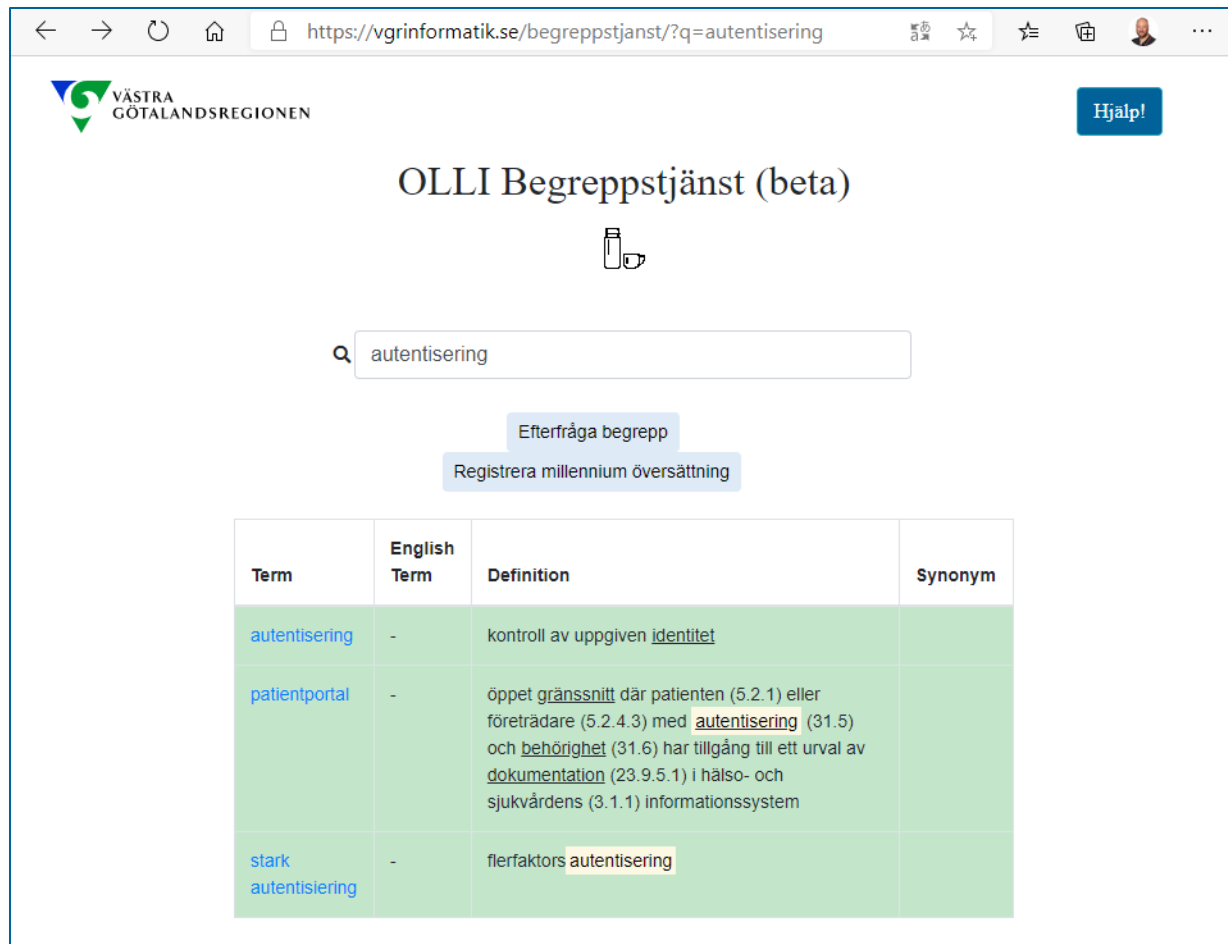
# Lärdom 2019

- Referens-arkitekturen fungerar inte bara för Ineras leveranser utan även för andra leverantörers produkter.
- Förståelsen för referens-arkitekturen ökar ju mer arkitektur vi arbetar med inom Varvet.
- Principerna börjar att användas.
- Vissa förvaltare och leverantörer är med på banan till referens-arkitekturen.



# Termer och begrepp (igen)

Äntligen så har vi  
möjlighet att få till en  
enhetlig begreppsmodell  
för IAM över hela VGR



VÄSTRA  
GÖTALANDSREGIONEN

Hjälp!

## OLLI Begreppstjänst (beta)

🍷

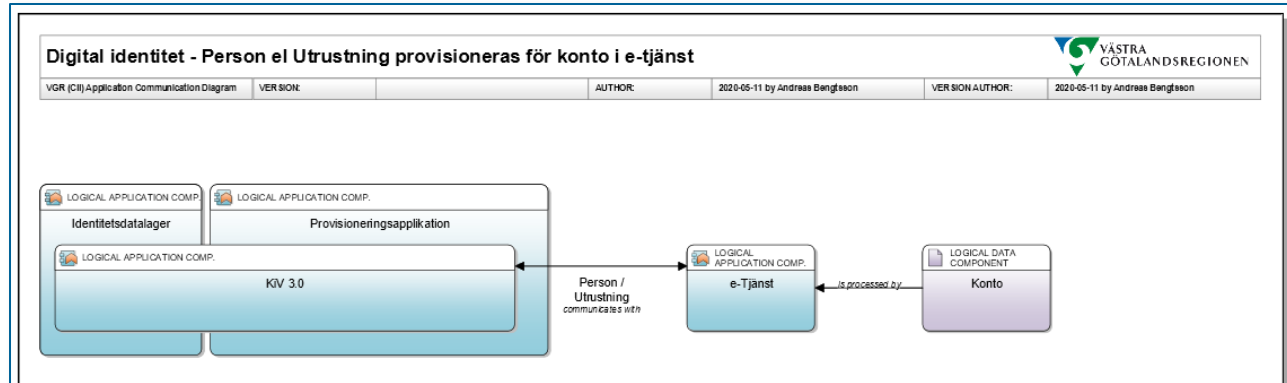
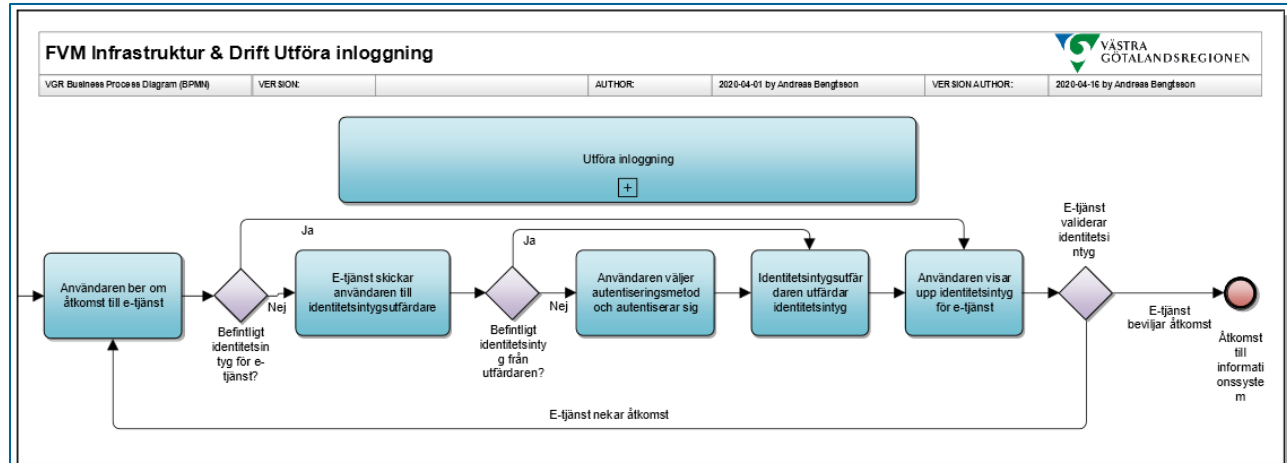
🔍 autentisering

Efterfråga begrepp

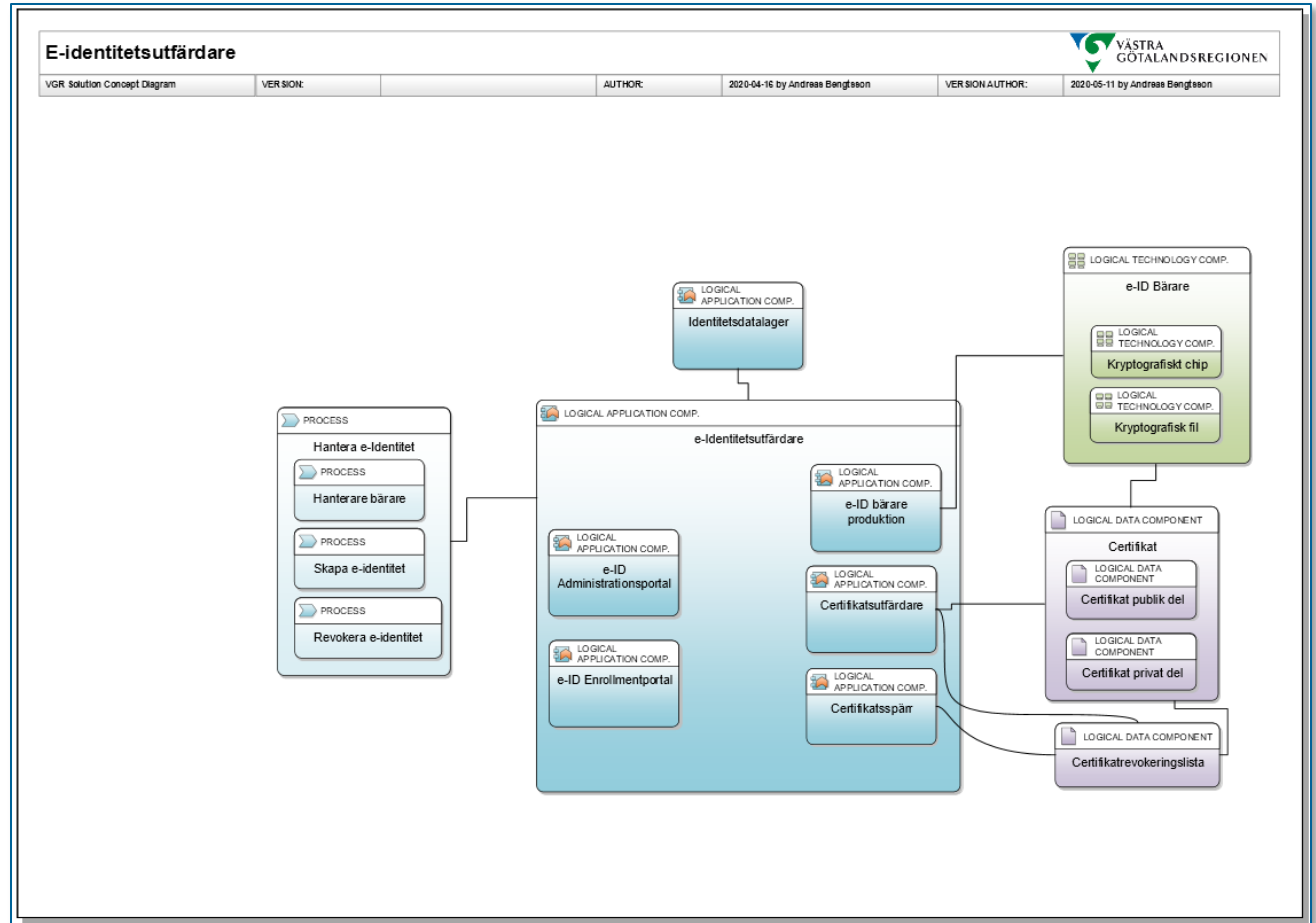
Registrera millennium översättning

Term	English Term	Definition	Synonym
<a href="#">autentisering</a>	-	kontroll av uppgiven <u>identitet</u>	
<a href="#">patientportal</a>	-	öppet <u>gränssnitt</u> där patienten (5.2.1) eller företrädare (5.2.4.3) med <u>autentisering</u> (31.5) och <u>behörighet</u> (31.6) har tillgång till ett urval av <u>dokumentation</u> (23.9.5.1) i hälso- och sjukvårdens (3.1.1) informationssystem	
<a href="#">stark autentisering</a>	-	flerfaktors <u>autentisering</u>	

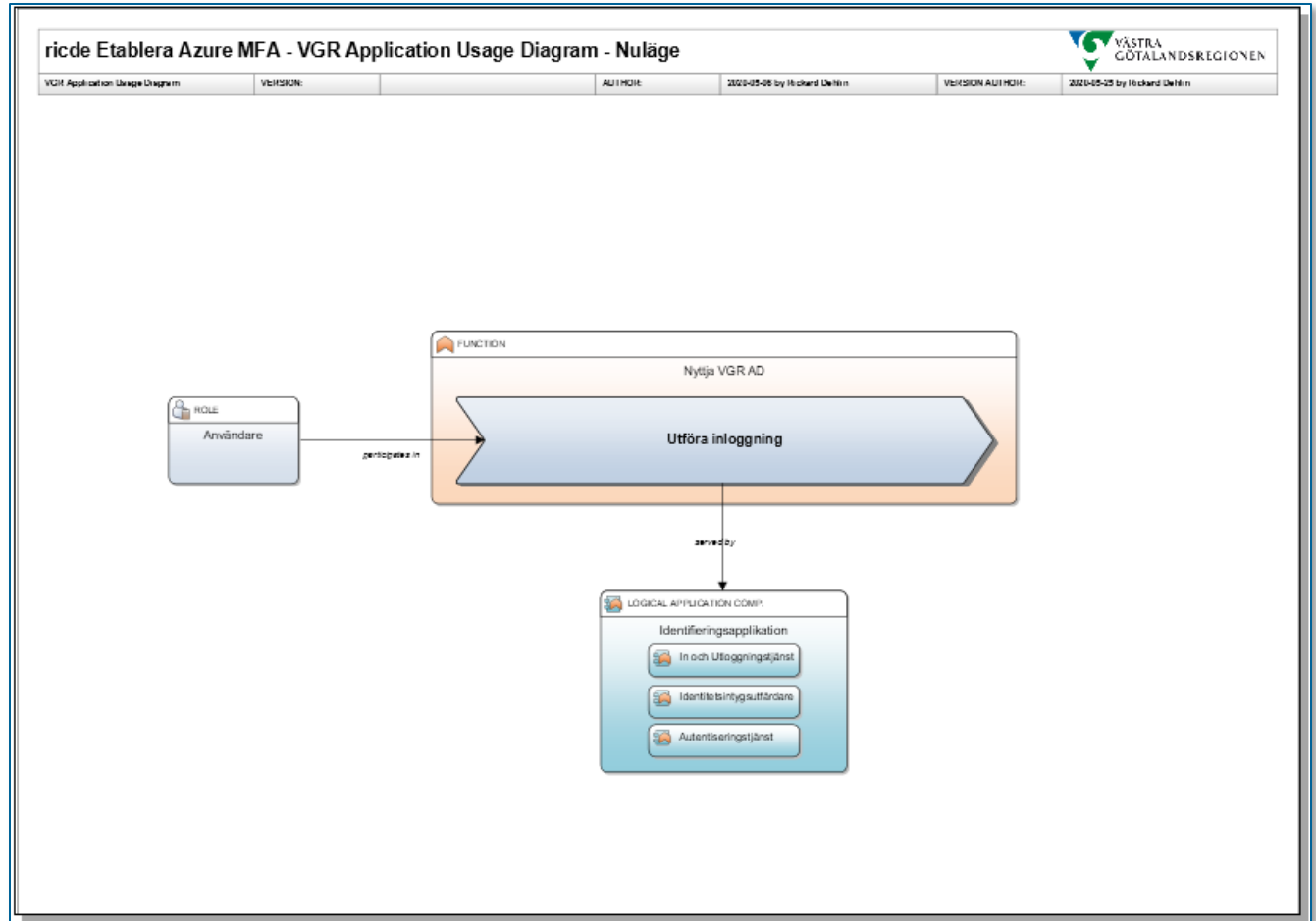
Generella exempel på hur arkitektur för IAM kan modelleras i Varvet tas fram



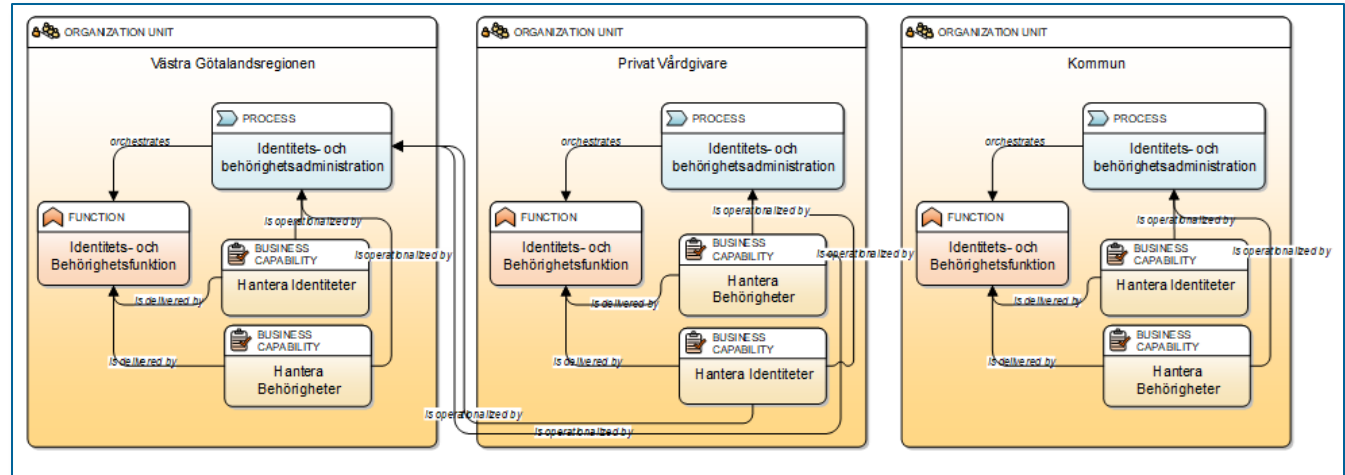
# Målararkitektur för E-identitets- utfärdare



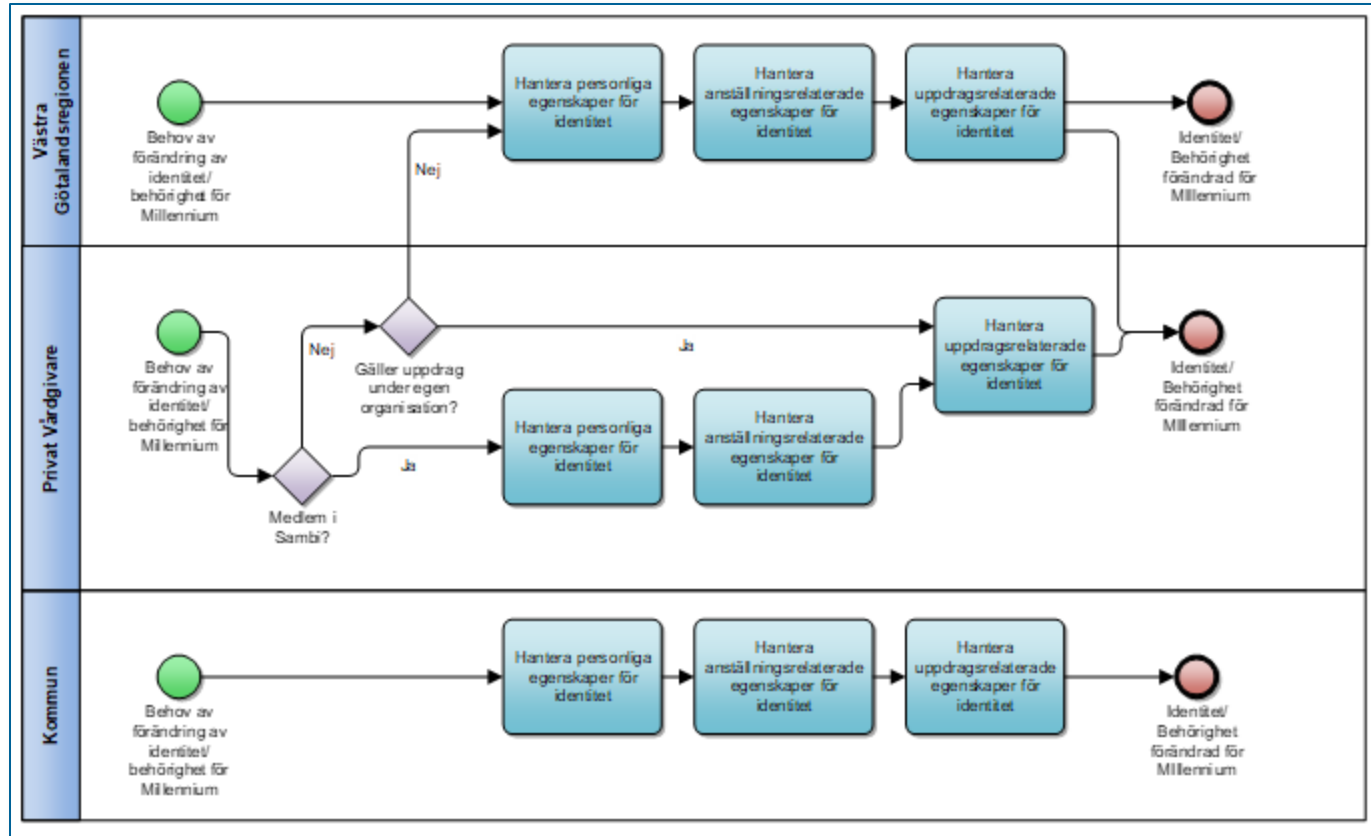
Lösningsarkitektur tar fram IAM artefakter



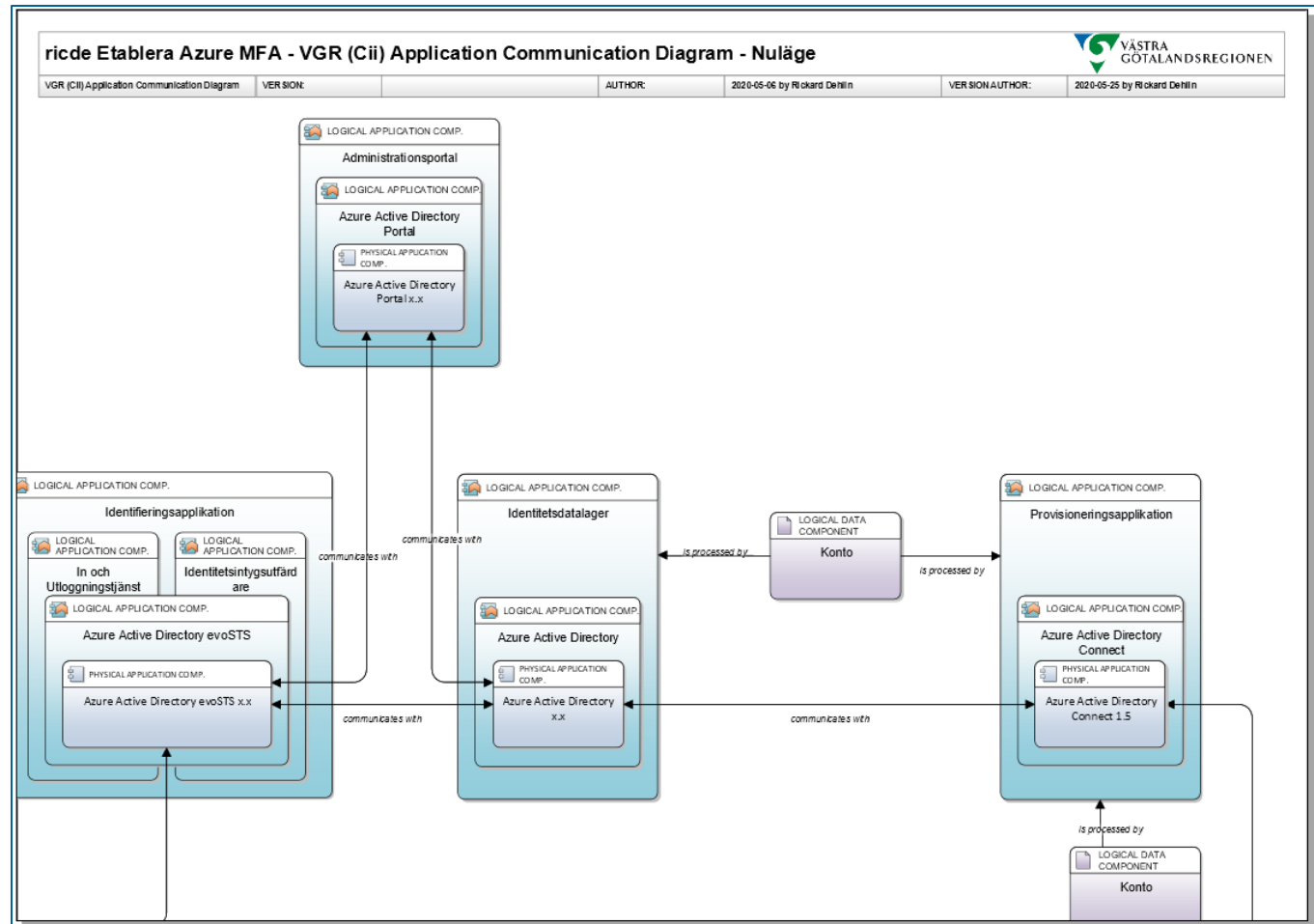
# Lösningsarkitektur tar fram IAM artefakter (FVM)



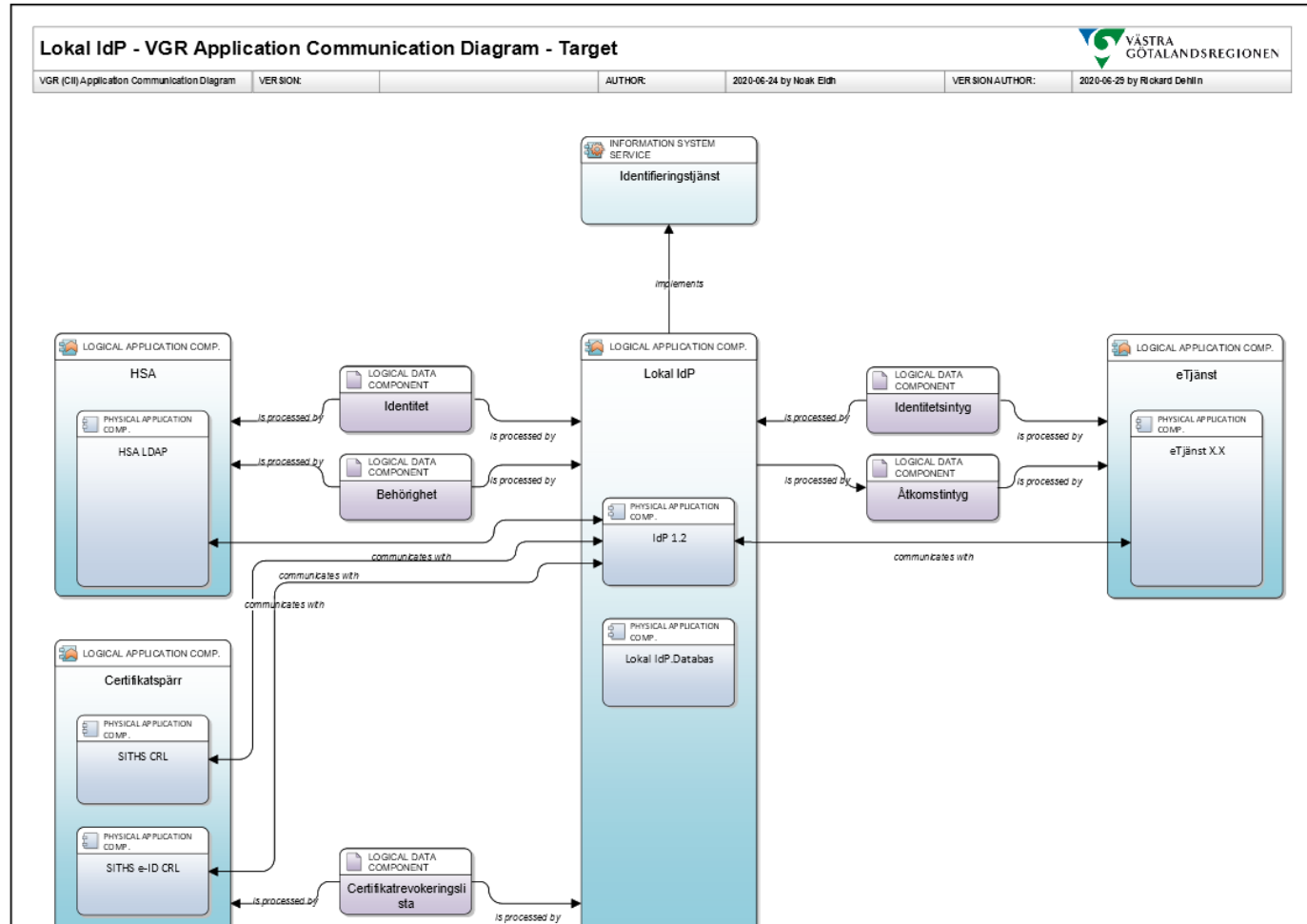
# Lösningssarkitektur tar fram IAM artefakter (FVM)



Lösningssarkitektur tar fram IAM artefakter

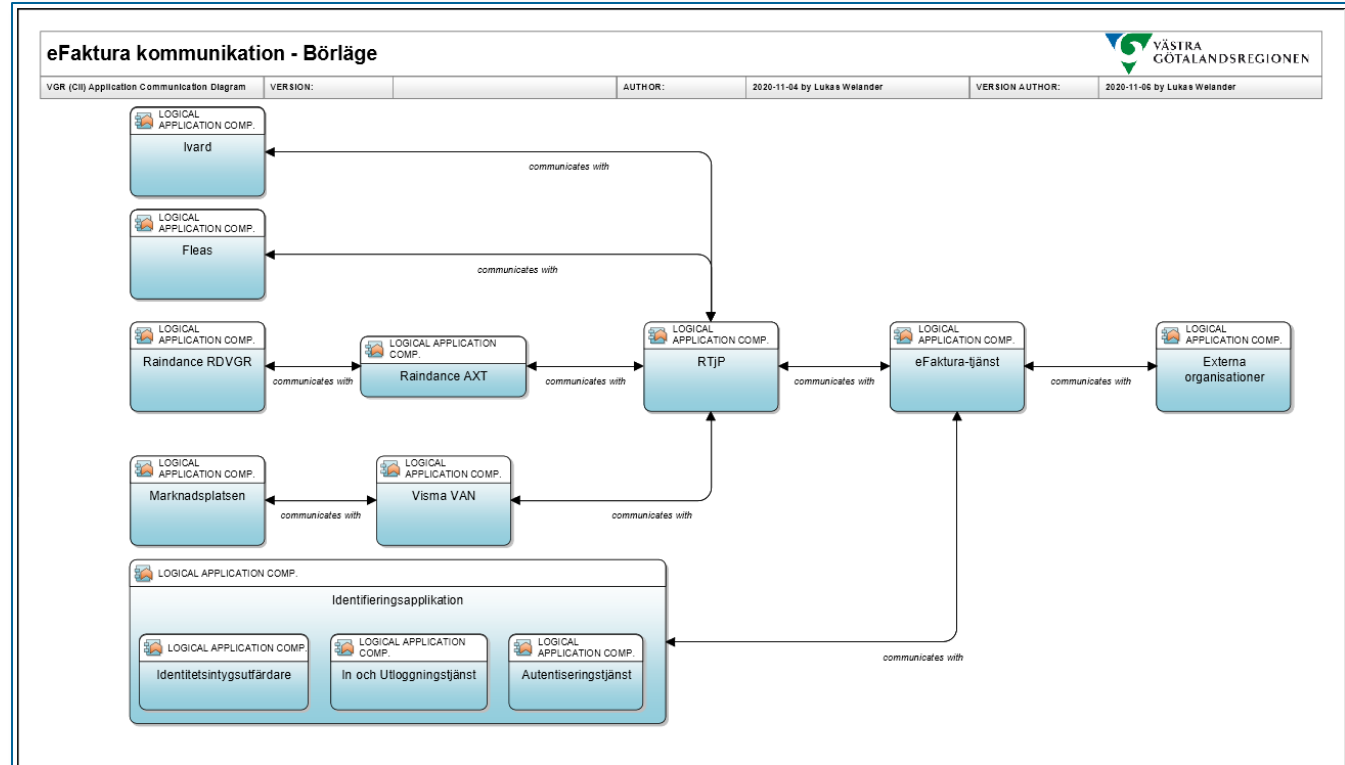


# Lösningssarkitektur tar fram IAM artefakter

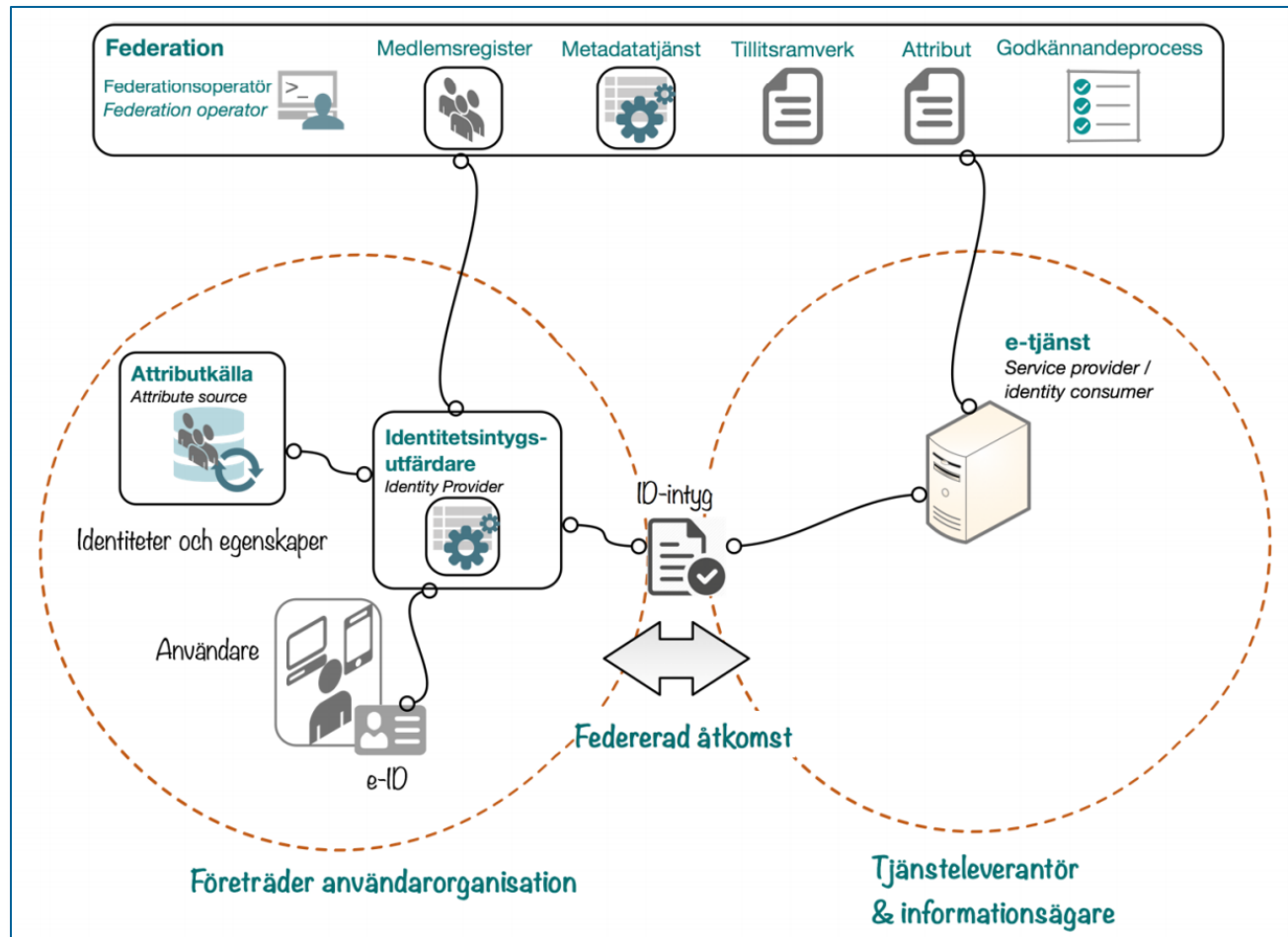




Domän-  
arkitekter  
modellerar  
med  
publicerade  
IAM artefakter

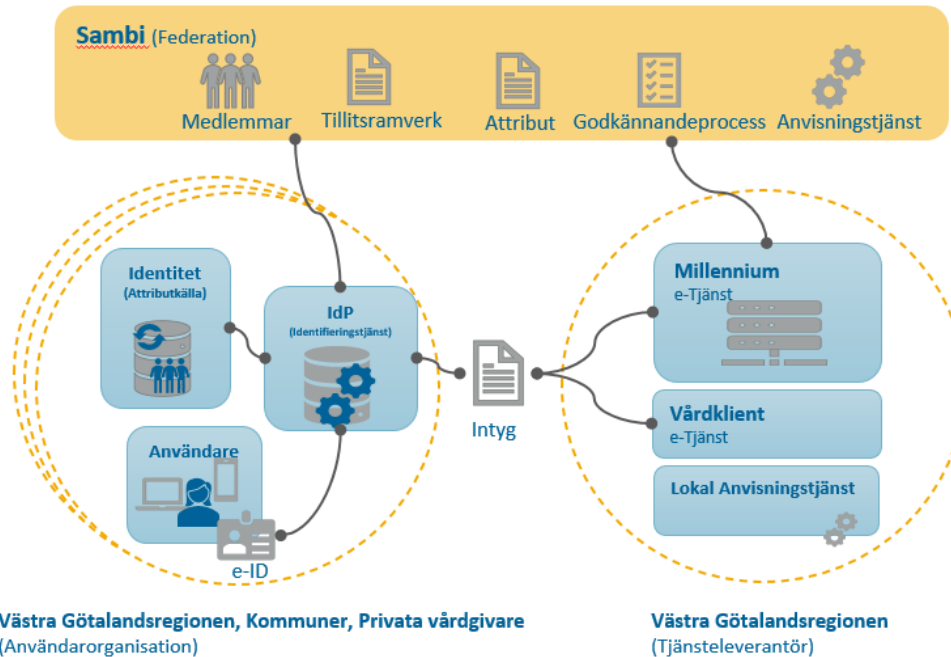


Från 2017



... blev

## Målarkitektur



# VGR går med i Identitets- och behörighets- federationen Sambi

Referensarkitekturen  
pekar på  
användarorganisation,  
tjänsteleverantör och  
federation.



Sambi 

[Om Sambi](#) | [Kontakt](#)

Sök...

Hem | Medlem i Sambi | Tillitsgranskning | Sambiombud | Gruppföreträdare | Teknik | Aktuellt | Kurser i Sambi | Om Sambi

[Hem](#) > [Aktuellt](#) > [2020](#) > [juli](#) > [02](#) > Västra Götalandsregionen (VGR) har slutit femårsavtal om Sambi

## Västra Götalandsregionen (VGR) har slutit femårsavtal om Sambi

2 jul, 2020



VÄSTRA  
GÖTALANDSREGIONEN

Västra Götalandsregionen (VGR) har skrivit ett femårsavtal med [Internetstiftelsen](#) avseende medlemskap i federationen Sambi. Identitets- och behörighetsfederationen kommer att vara lösningen för säker och enkel inloggning till det nyligen upphandlade journalsystemet Millenium. VGR är därmed medlem i Sambi och har också genomfört en tillitsgranskning.

# IdP med i Sambi federationen

Tack vare att FVM  
kravställt på federerad  
inloggning



```
← → ↻ 🏠 🔒 https://fed.sambi.se/accept/md/metadata.xml ☆ ⌵ 🗄 👤 ...
▼ <md:EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:idpdisco="urn:oasis:names:tc:SAML:profiles:SSO:idp-
discovery-protocol" xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xenc="http://www.w3.org/2001/04/xmenc#" entityID="https://lokalidp-acceptans.vgregion.se:443/saml1">
  ▼ <md:Extensions>
    ▼ <mdattr:EntityAttributes>
      ▼ <saml2:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>http://id.sambi.se/loa/loa2</saml2:AttributeValue>
        <saml2:AttributeValue>http://id.sambi.se/loa/loa3</saml2:AttributeValue>
        <saml2:AttributeValue>http://id.sambi.se/loa/loa4</saml2:AttributeValue>
        </saml2:Attribute>
      </mdattr:EntityAttributes>
    </md:Extensions>
  ▼ <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼ <md:KeyDescriptor use="signing">
      ▼ <ds:KeyInfo>
        ▼ <ds:X509Data>
          <ds:X509Certificate>MIIG6jCCBdKgAwIBAgIMVgj2IQUqyrD444heSMA0GCSqGSIb3DQEBCwUAMFAx CzAJBgNVBAYTAKJFMRkwFwYDVQQKExBHbG91YW
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
```

# Lyckad inloggning i FVM (sandbox)

Tack vare kraven i  
upphandlingen från  
2018.  
IdP, SP, federation

The screenshot displays a web application interface with a blue header and a light blue background. The header includes the text "Example Application" on the left and "Session Lifecycle" and "Electronic Signature" in the center. On the right side of the header, there is a user profile icon and the text "SE2321000131-P00000000539".

In the center of the page, there is a "Session Details" panel with the following information:

Tenant ID	VGRC_SE-Sandbox-idP-Test
Identity Service Provider ID (Realm ID)	da37d0d1-d0cc-4c32-a6f9-cb8218f1da2b
Session Status	Unlocked

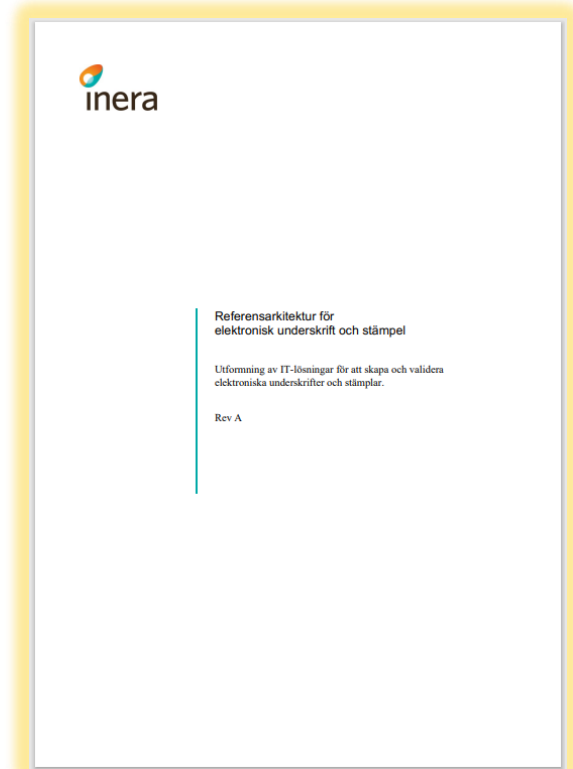
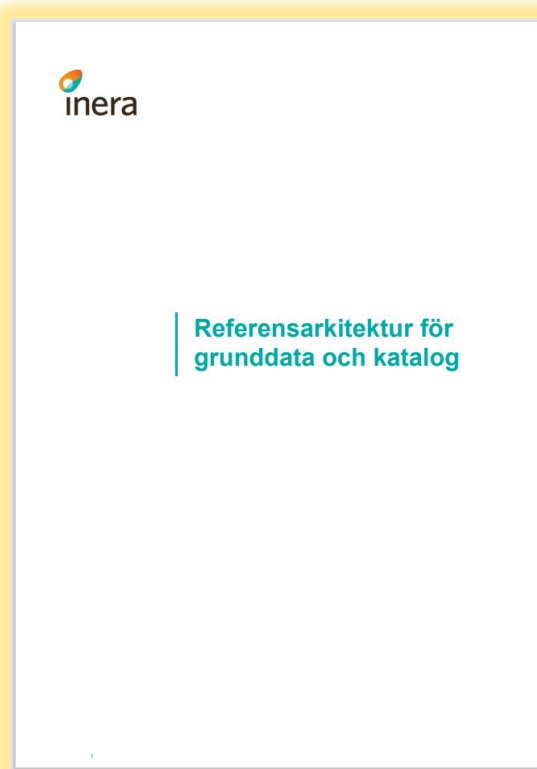
Below the session details, there is a "Lock" button.

On the right side of the page, there is a "Utilities" panel with the following elements:

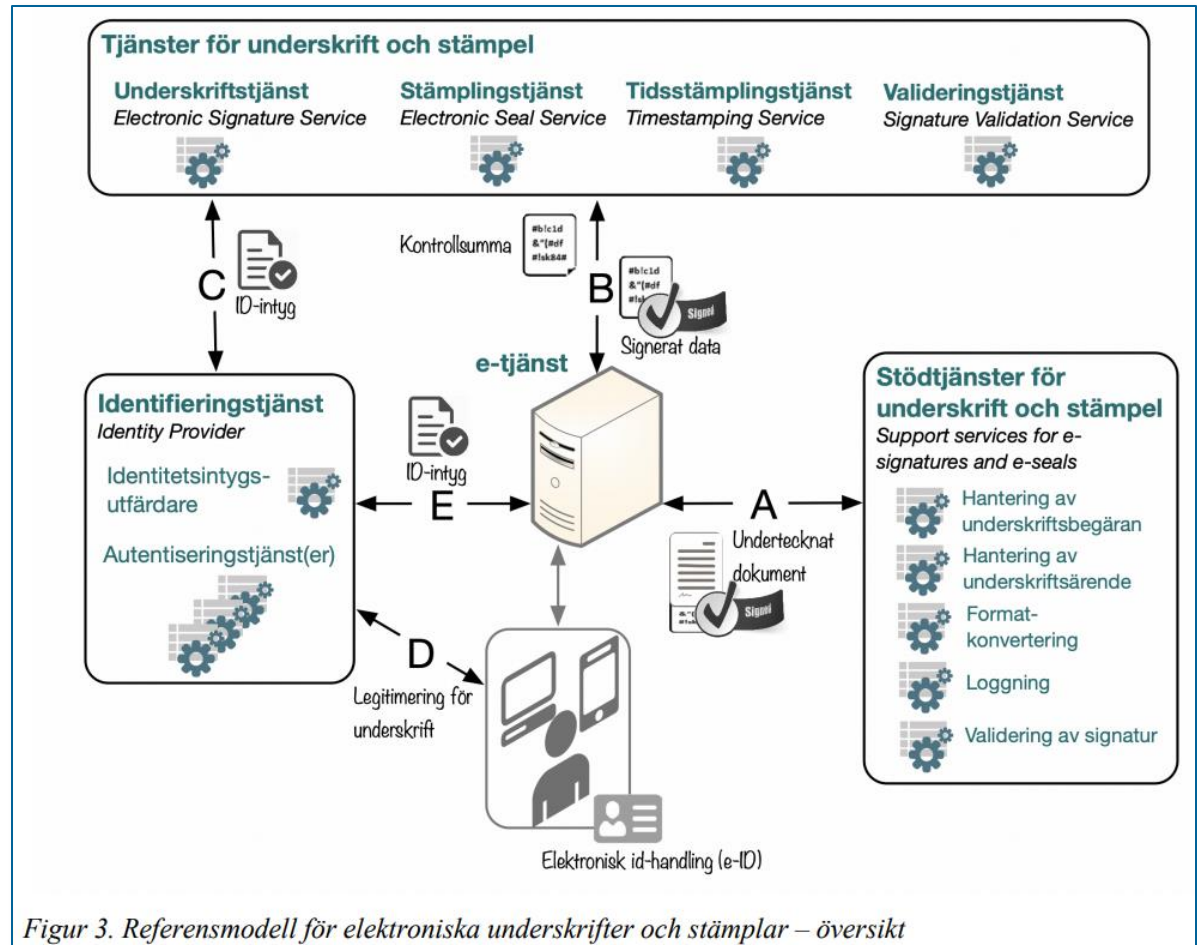
- A user profile icon and the text "SE2321000131-P00000000539".
- A "Reference Pages" link with a downward arrow.
- A "Help" link with a question mark icon.
- A "Log Out" button.

2020 så släpps Inera  
Referensarkitektur  
för  
grunddata och  
katalog samt  
Referensarkitektur  
för  
elektronisk  
underskrift och  
stämpel

- 140 sidor!
- 82 sidor!



Även här finns översiktsbild som är den vi börjar med att förstå och arbeta med



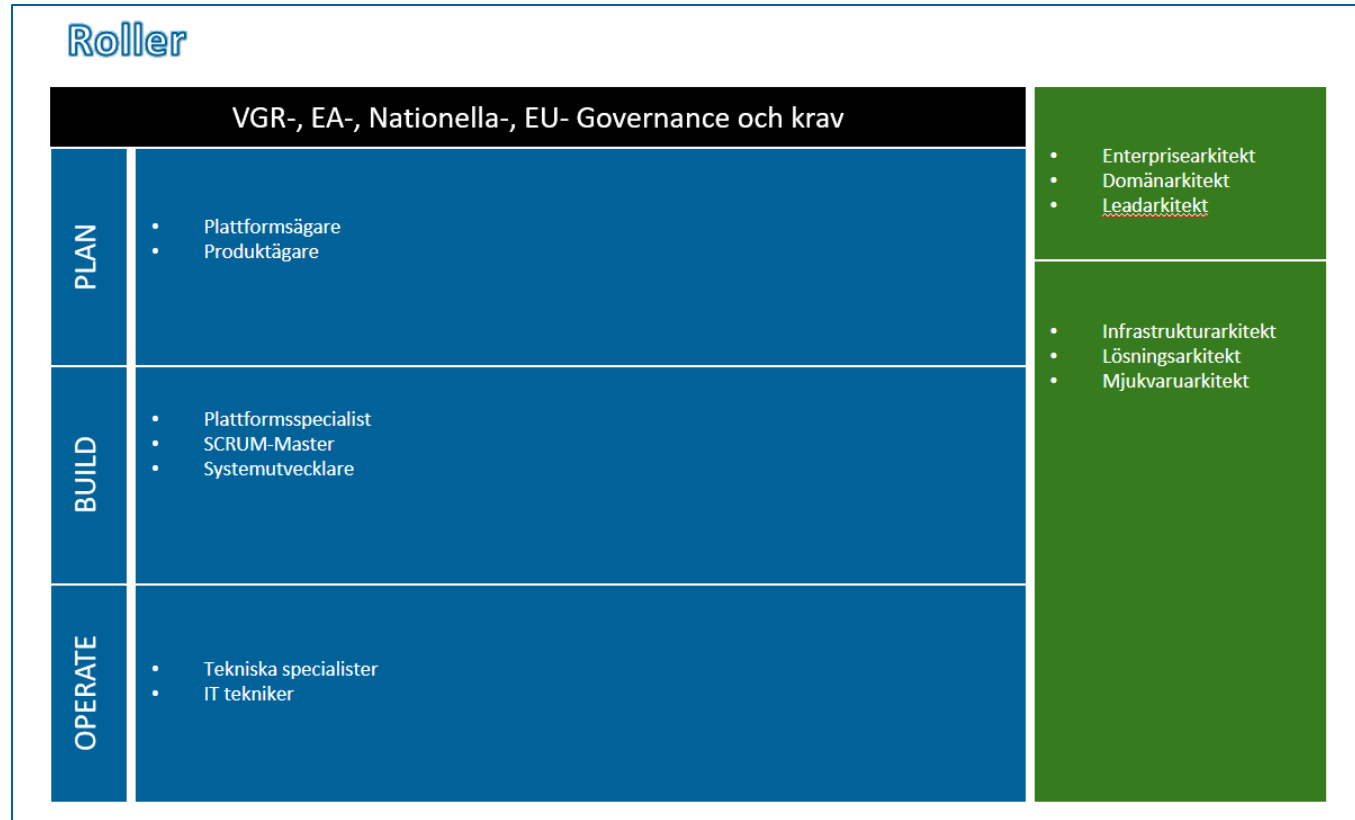
Figur 3. Referensmodell för elektroniska underskrifter och stämplatser – översikt



Ny organisation är på väg att föras in.

Arkitekterna är en naturlig del i modellen.

Modellen klarar att spänna över organisationen.



# Lärdom 2020

- IAM spänner över stora delar av IT-organisationen (ansvar och nyttjande). Förvaltning och arkitektur måste gå hand i hand.
- Referensarkitekturen är en naturlig del av arbetet, både i Varvet modellering, upphandling, lösningsarkitektur osv.
- Flera förvaltare och leverantörer är helt med på banan till referensarkitekturen.
- Resan fortsätter ...

