Tillämpning Referensarkitektur IAM i VGR

VÄSTRA GÖTALANDSREGIONEN

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.

Disclamer

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 ☺

VÄSTRA GÖTALANDSREGIONEN

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.
- Komplett 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

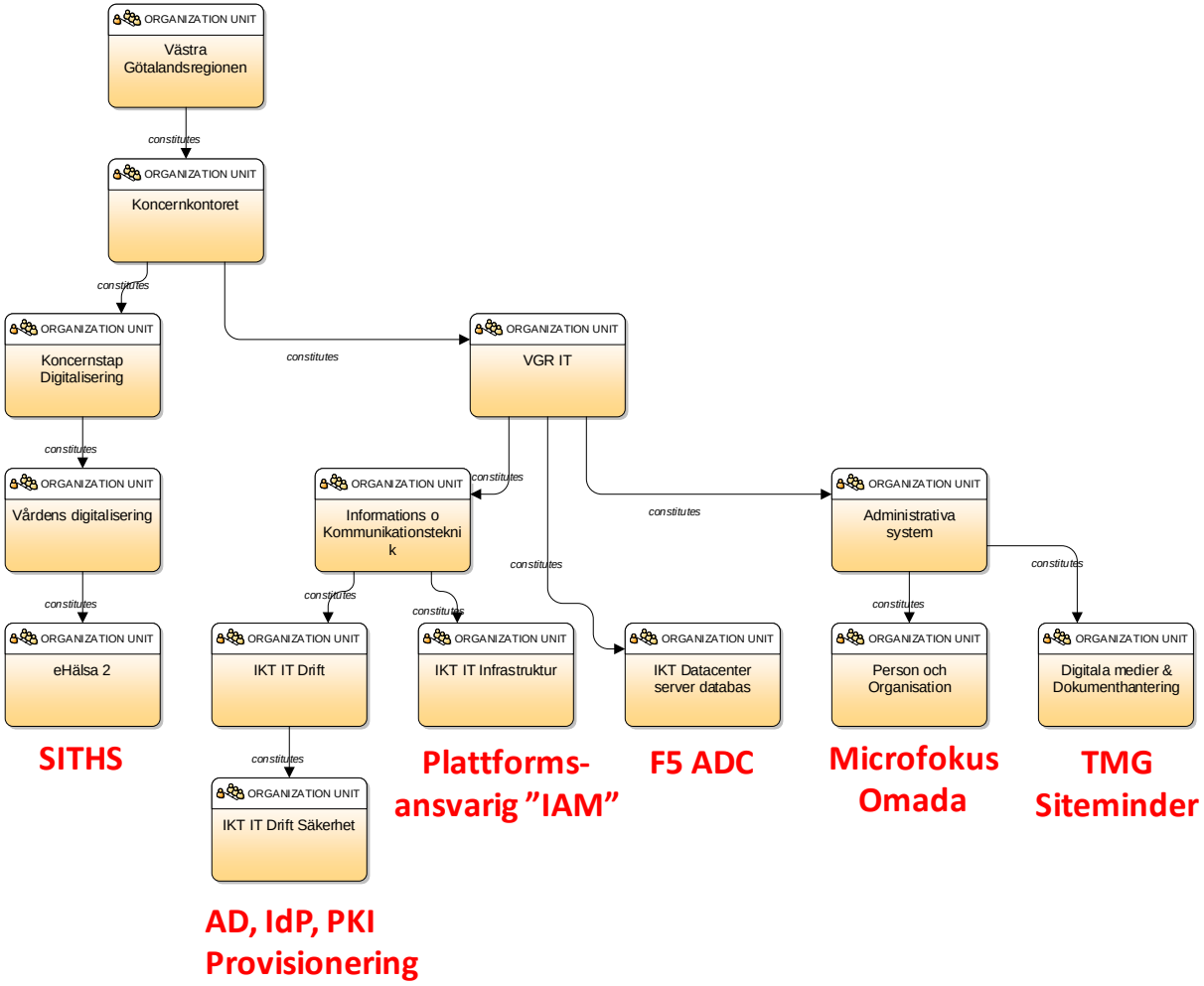
Transport

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.



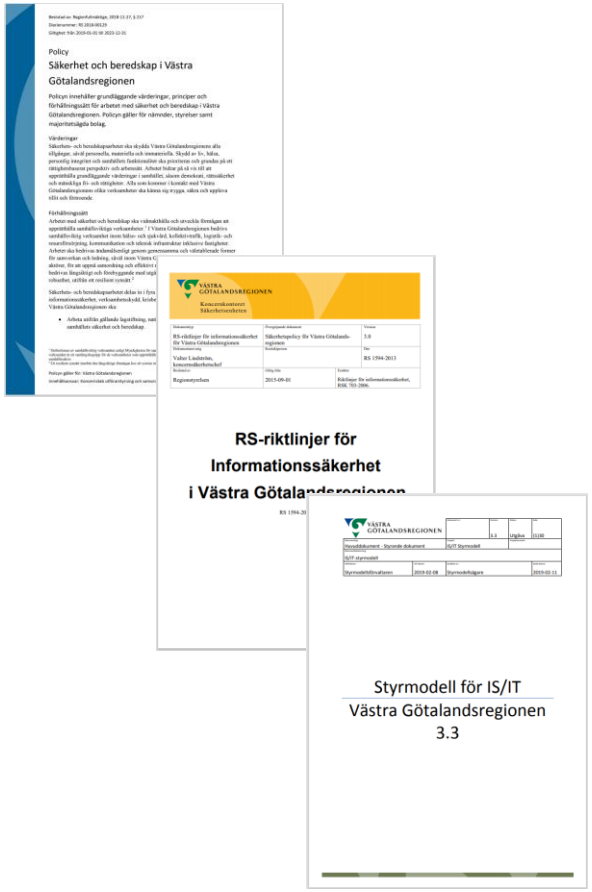
VGR:s leverantörer för IAM

Mycket bra teknik – men en salig blandning.

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

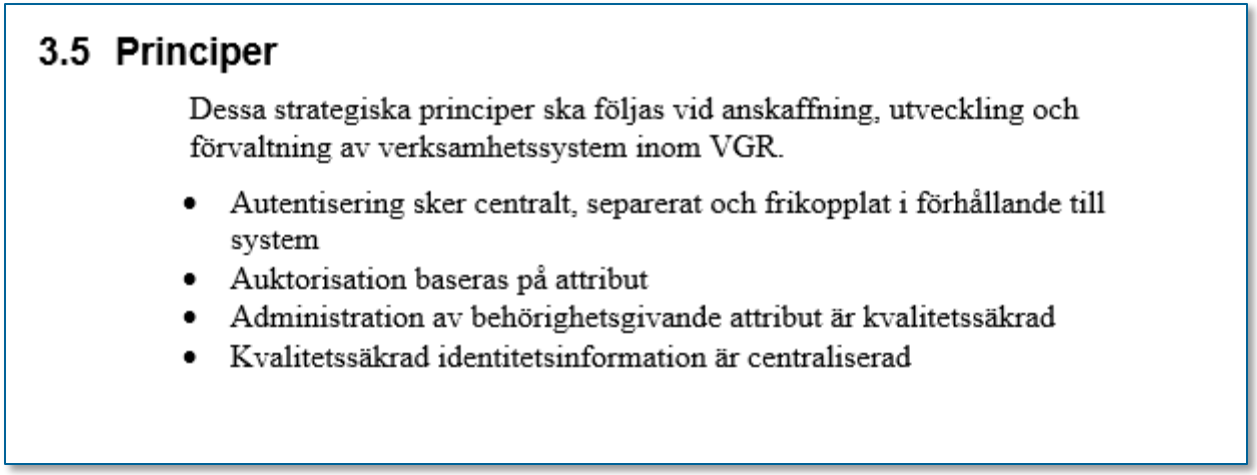
2015 så började VGR arbeta med strategier

Identitet, behörighet och åtkomststrategi för VGR kompletterar övriga styrande dokument



Identitet, behörighet och åtkomst-strategi för VGR.

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



3.5 Principer

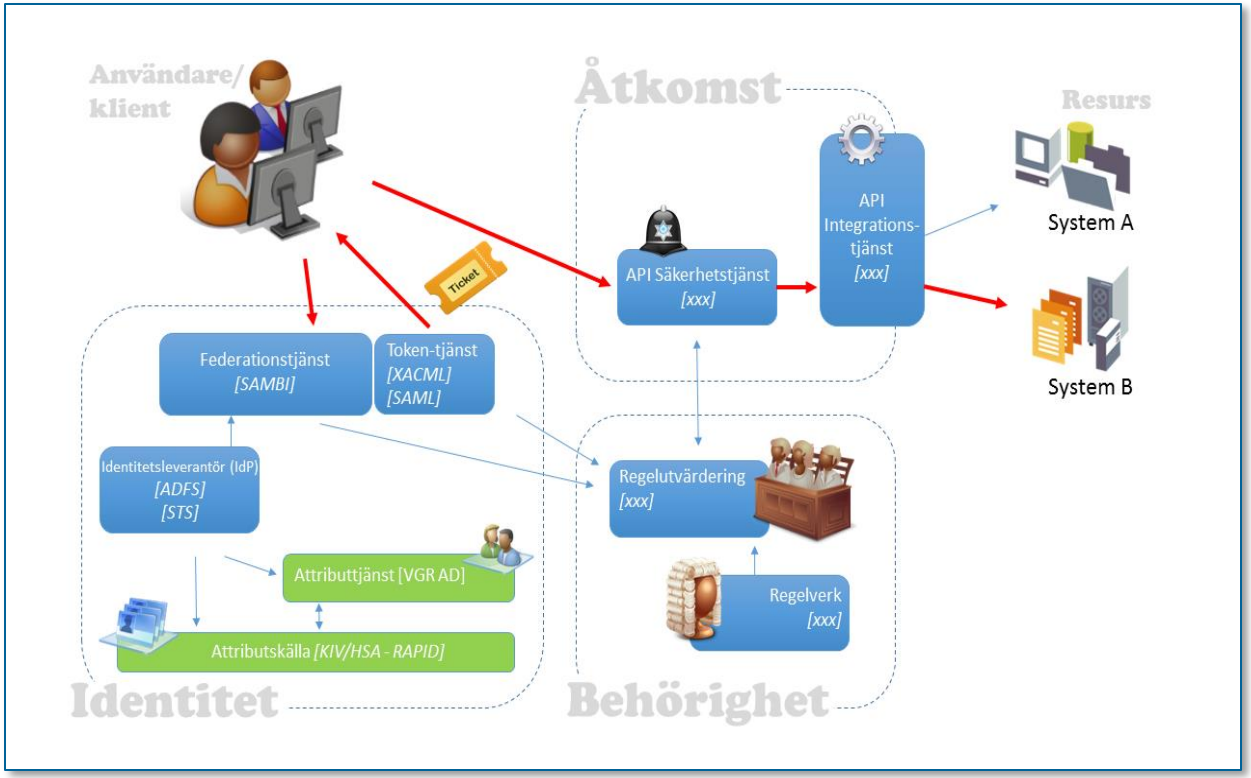
Dessa strategiska principer ska följas vid anskaffning, utveckling och förvaltning av verksamhetssystem inom VGR.

- 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 åtkomst-strategi för VGR.

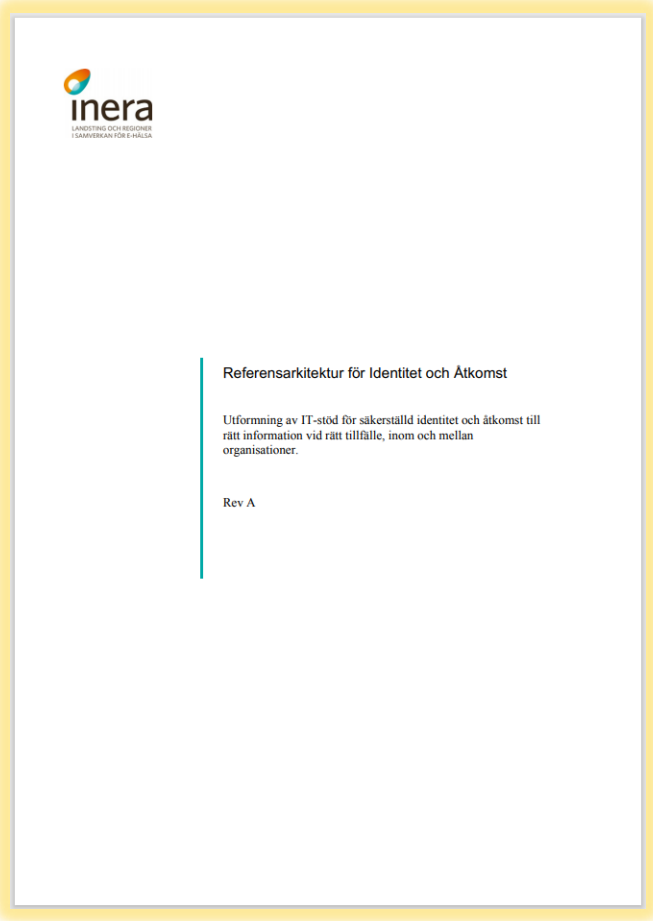
Ett första försök att göra något som kan betecknas som arkitektur – begrepp och samlad översikt

(tack Östergötland)

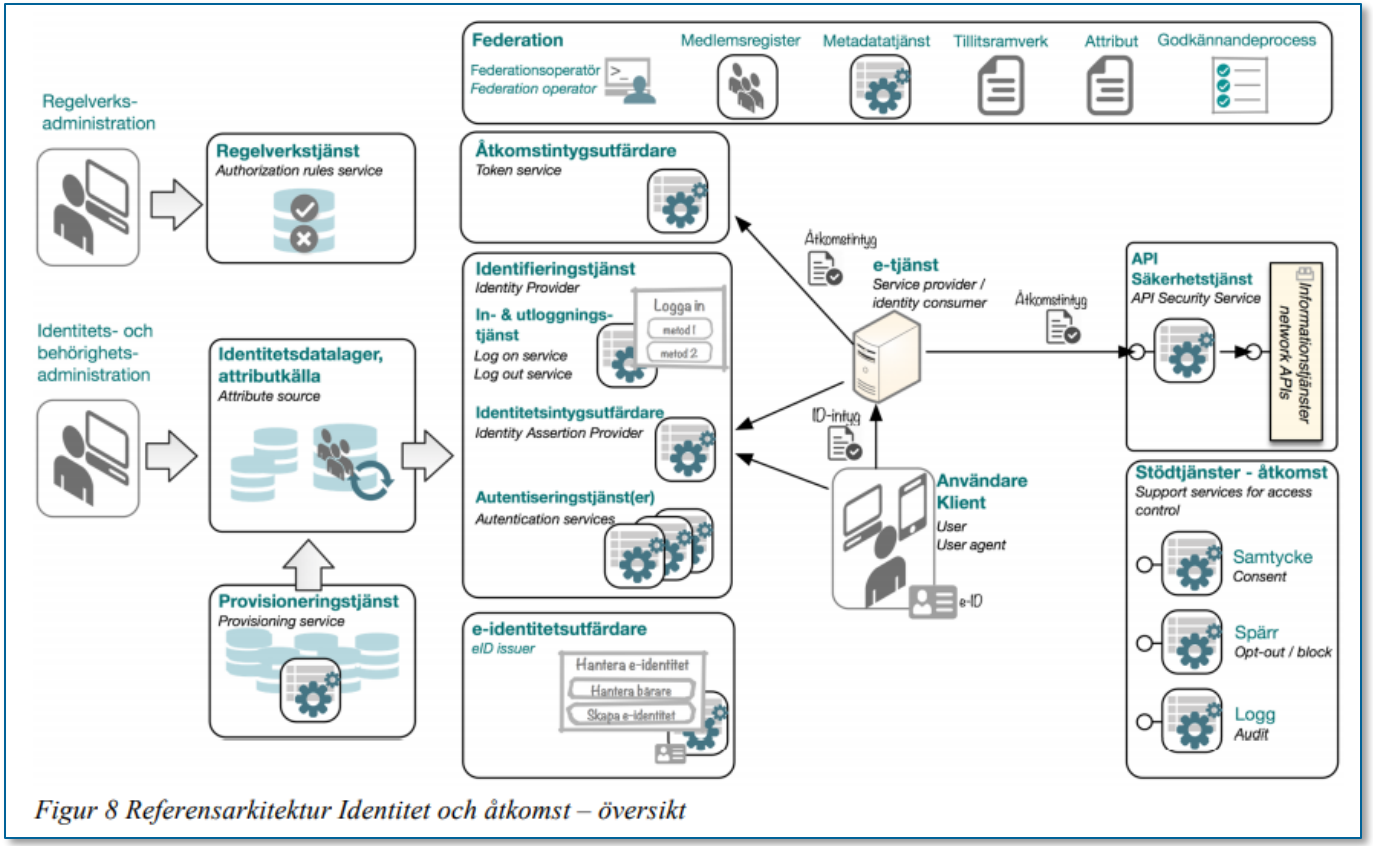


2017 så släpps Inera Referens-arkitektur för Identitet och Åtkomst

77 sidor!

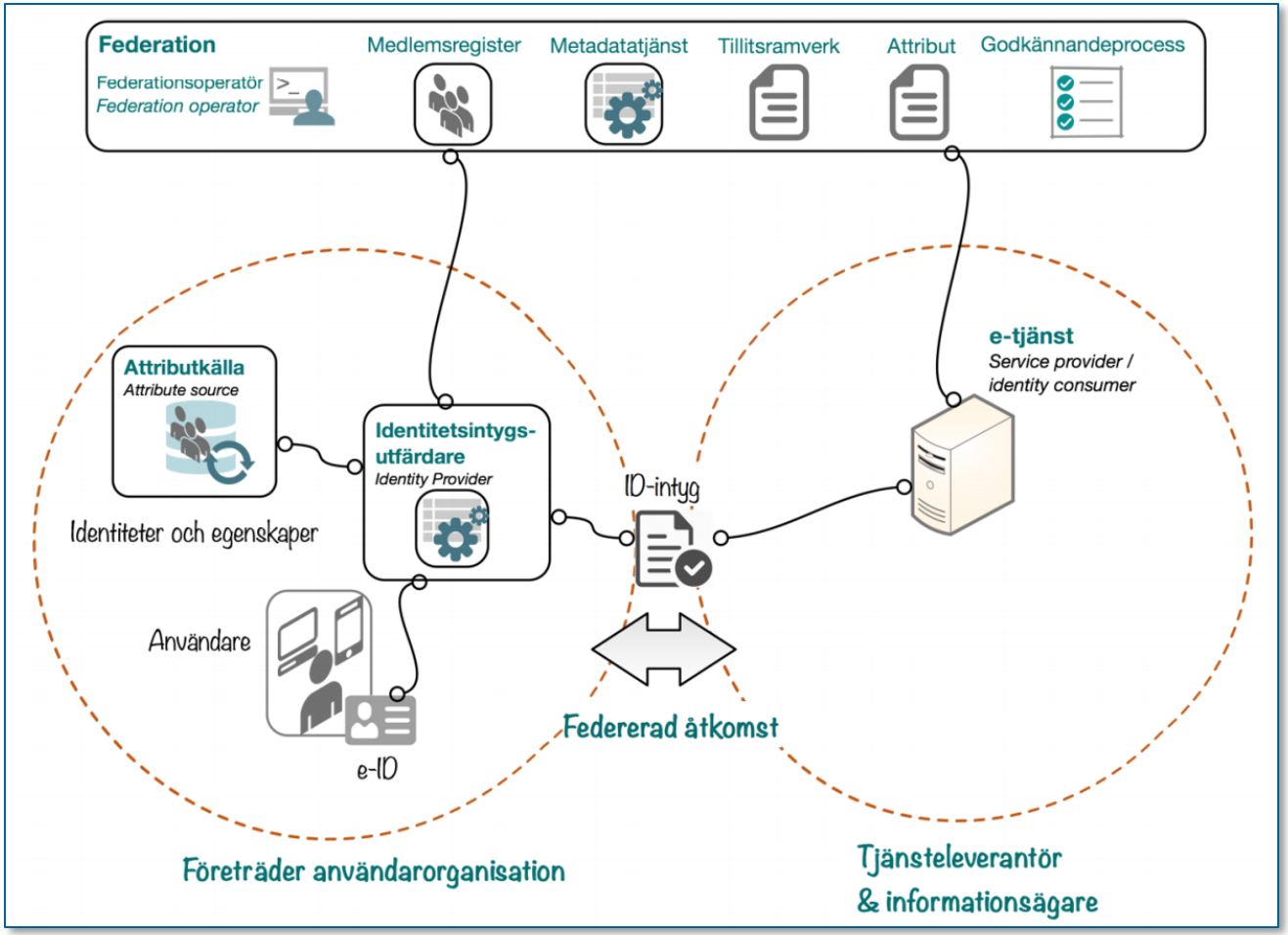


Två bilder är ständigt återkommande



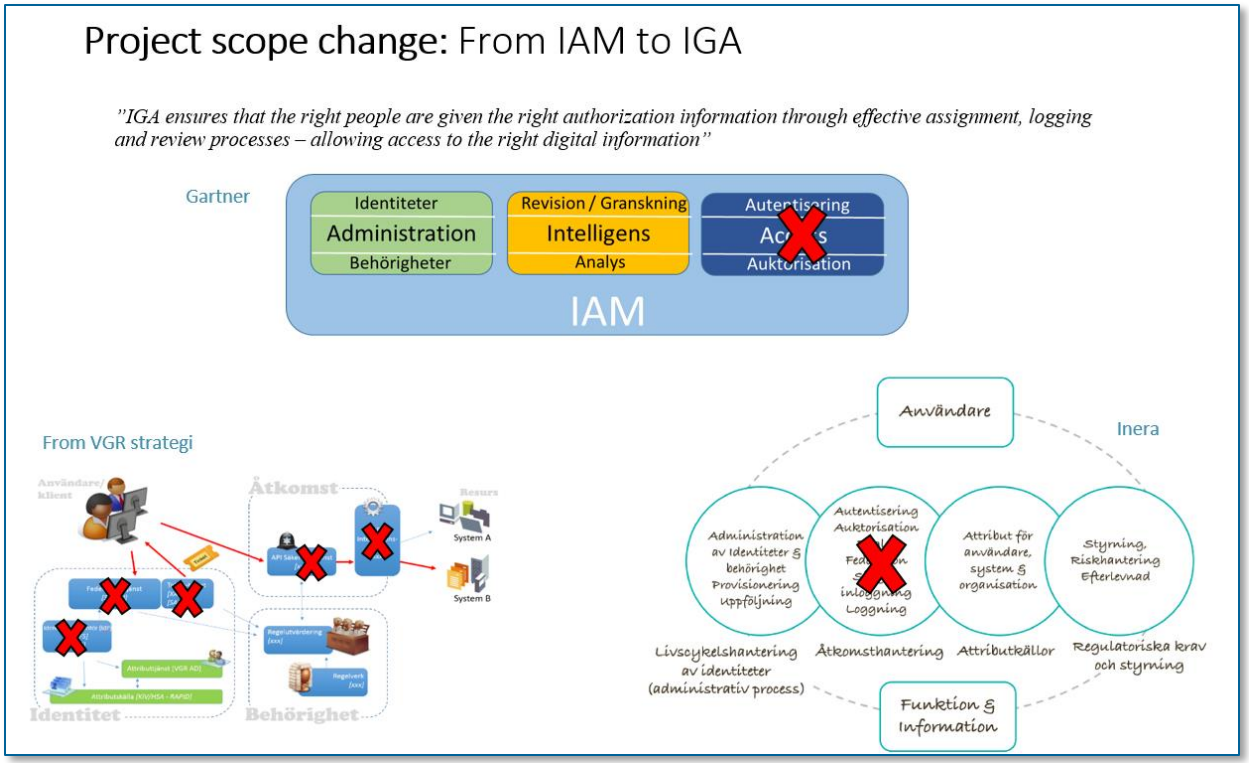
Figur 8 Referensarkitektur Identitet och åtkomst – översikt

Två bilder är ständigt återkommande

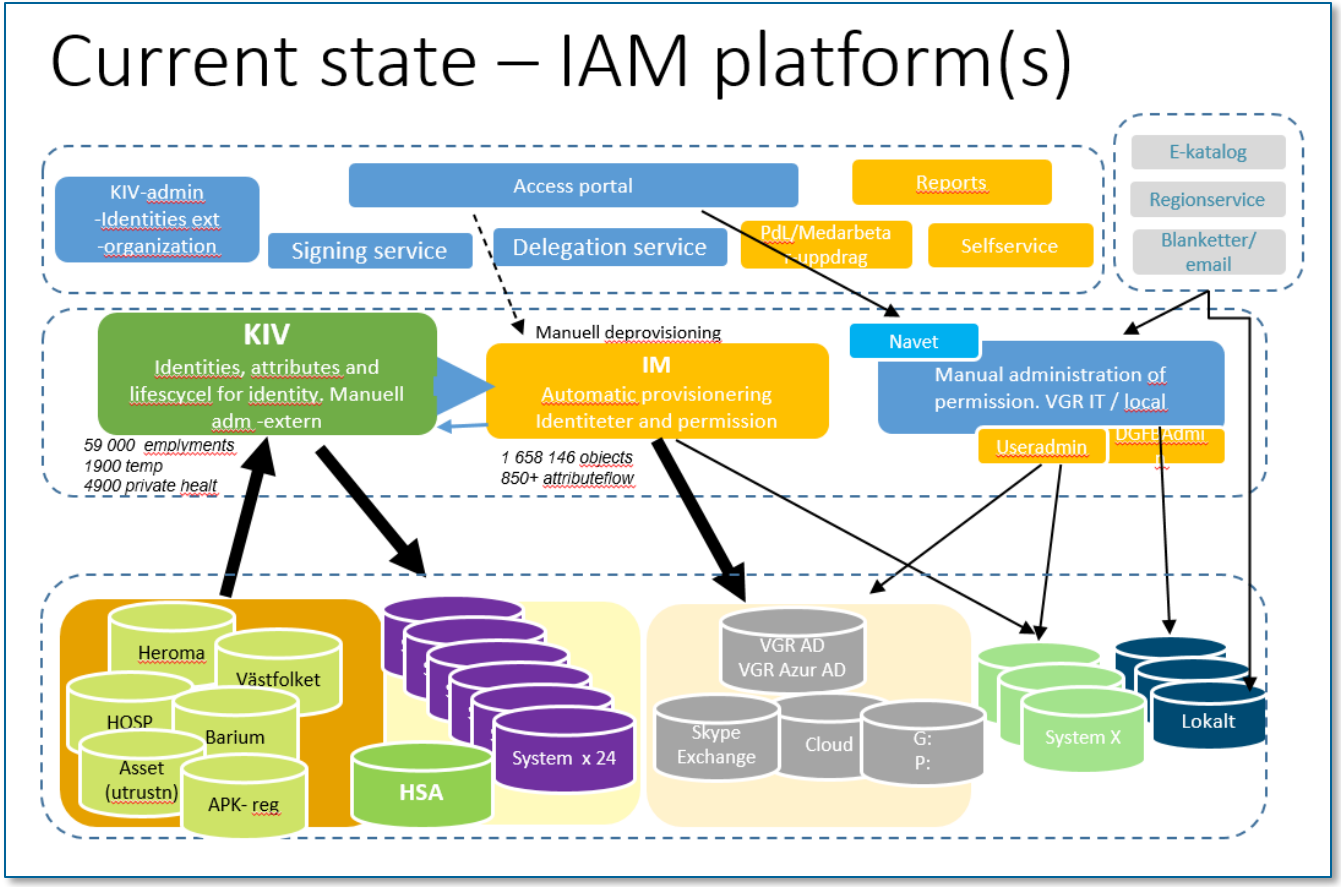


Olika delar inom VGR börjar ta axplock ur arkitekturen

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

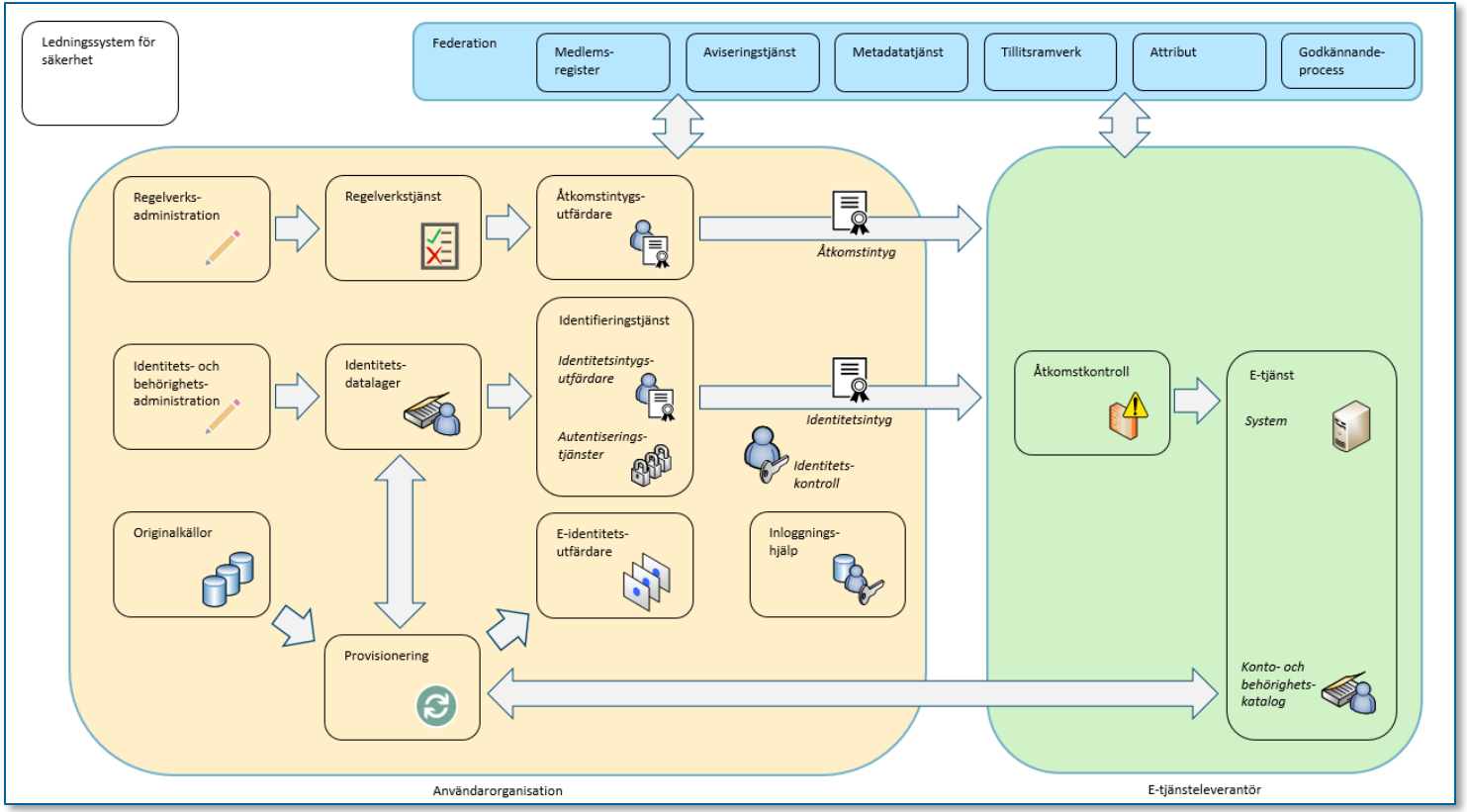


… men fortfarande inget strukturerat sätt att beskriva vår miljö

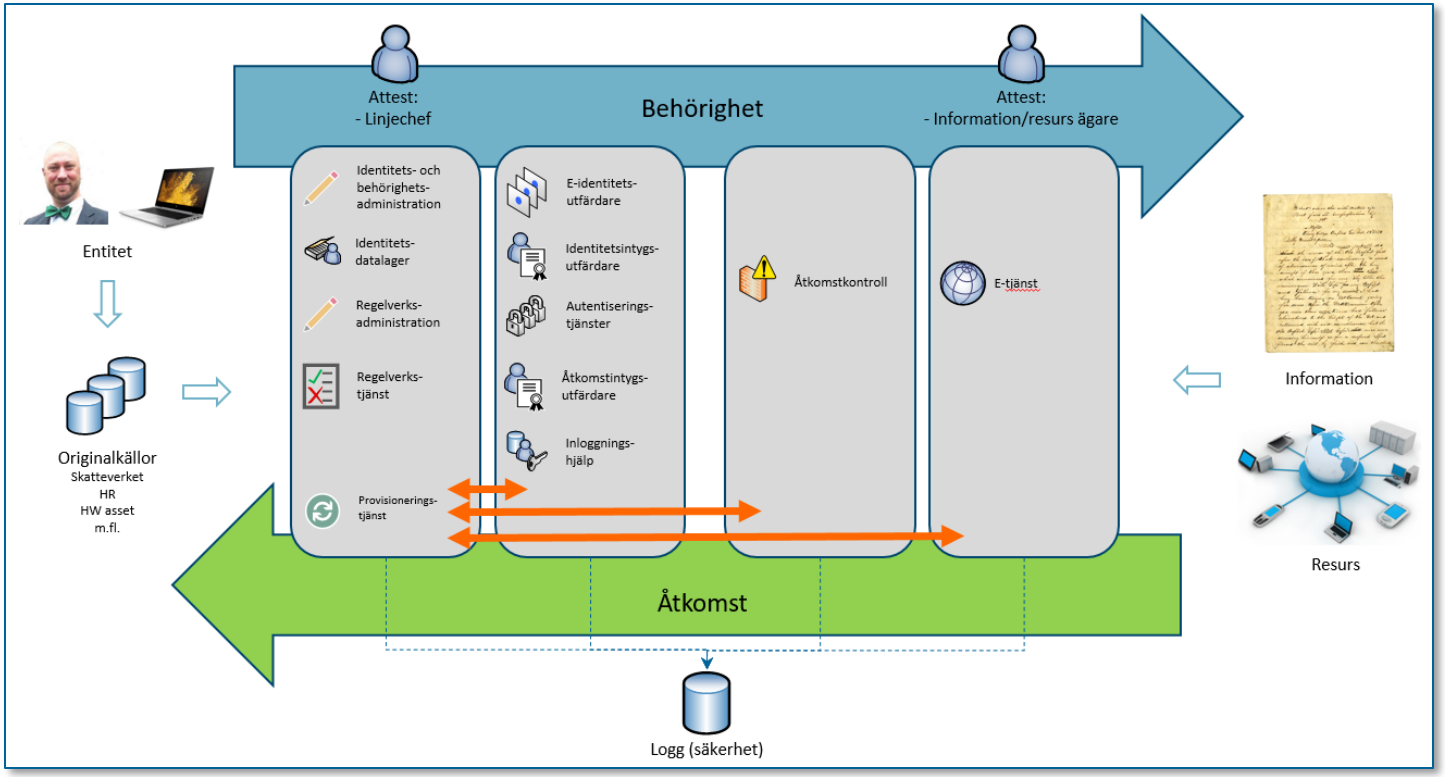


Första försöket att ”VGRifiera” Ineras översiktsbild

Begreppen är med (men inte säkerhets-tjänserna)



Och någon form av processbild

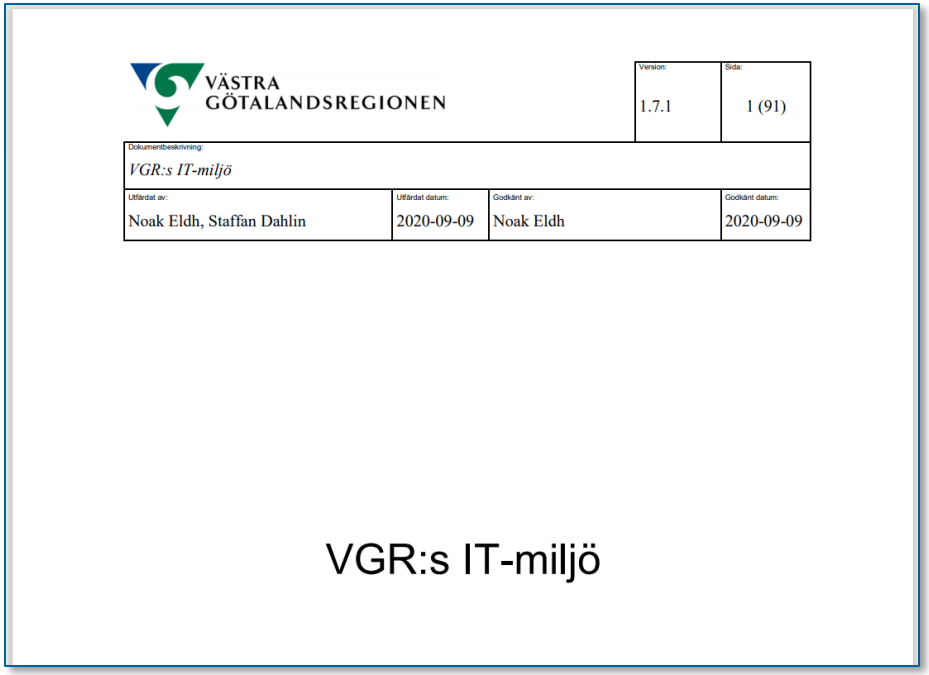


Lärdom 2017

- 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 referens-arkitekturen.



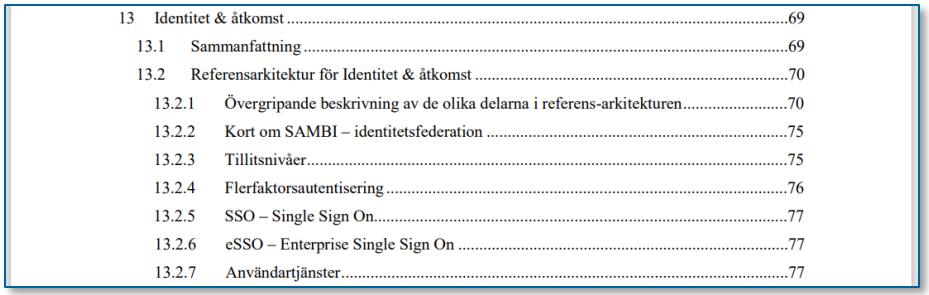
VÄSTRA GÖTALANDSREGIONEN

Version:	Sida:
1.7.1	1 (91)

Dokumentbeskrivning: *VGR:s IT-miljö*

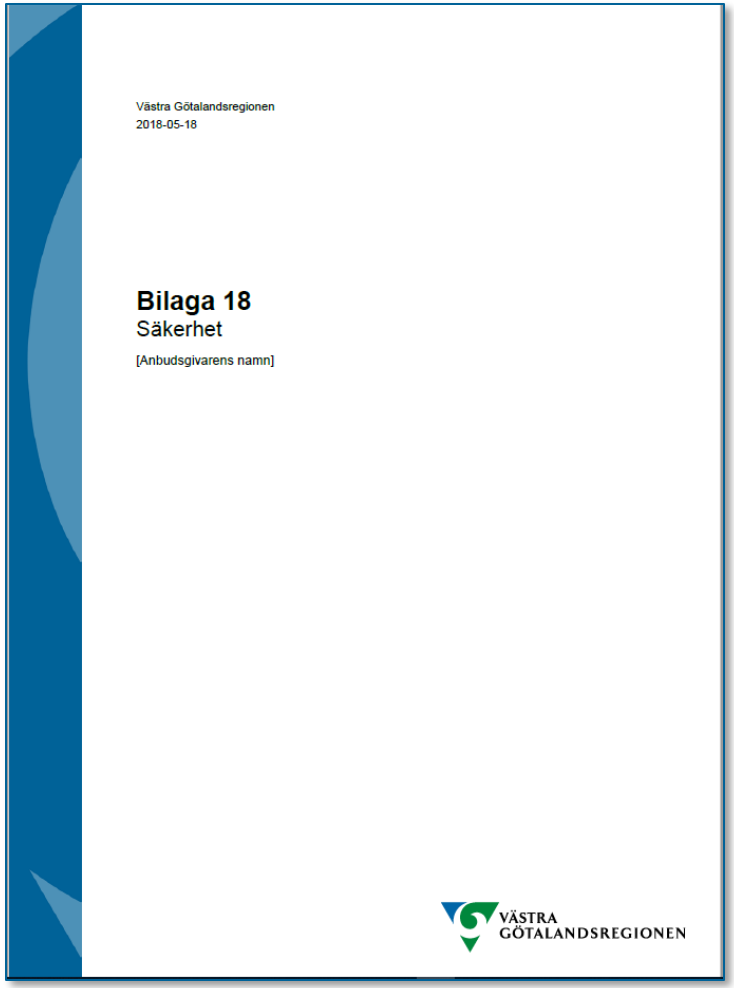
Utfärdat av:	Utfärdat datum:	Godkänt av:	Godkänt datum:
Noak Eldh, Staffan Dahlin	2020-09-09	Noak Eldh	2020-09-09

VGR:s IT-miljö

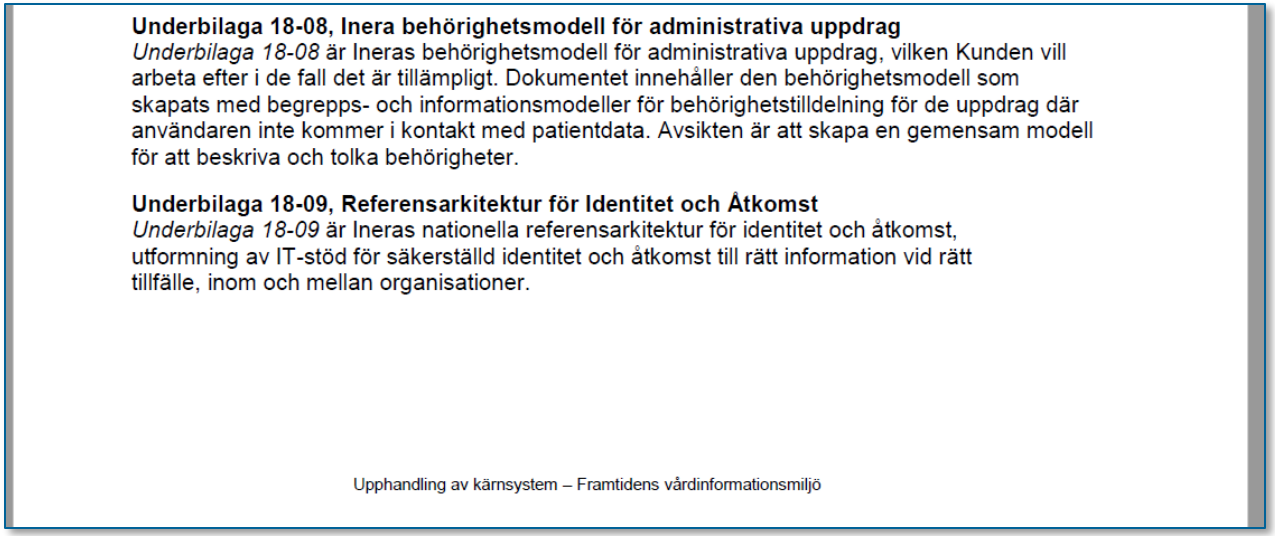


13 Identitet & åtkomst 69
13.1 Sammanfattning 69
13.2 Referensarkitektur för Identitet & åtkomst 70
13.2.1 Övergripande beskrivning av de olika delarna i referens-arkitekturen 70
13.2.2 Kort om SAMBI – identitetsfederation 75
13.2.3 Tillitsnivåer 75
13.2.4 Flerfaktorsautentisering 76
13.2.5 SSO – Single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

Upphandling FVM



Pekar på referens-arkitekturen i upphandling (FVM)

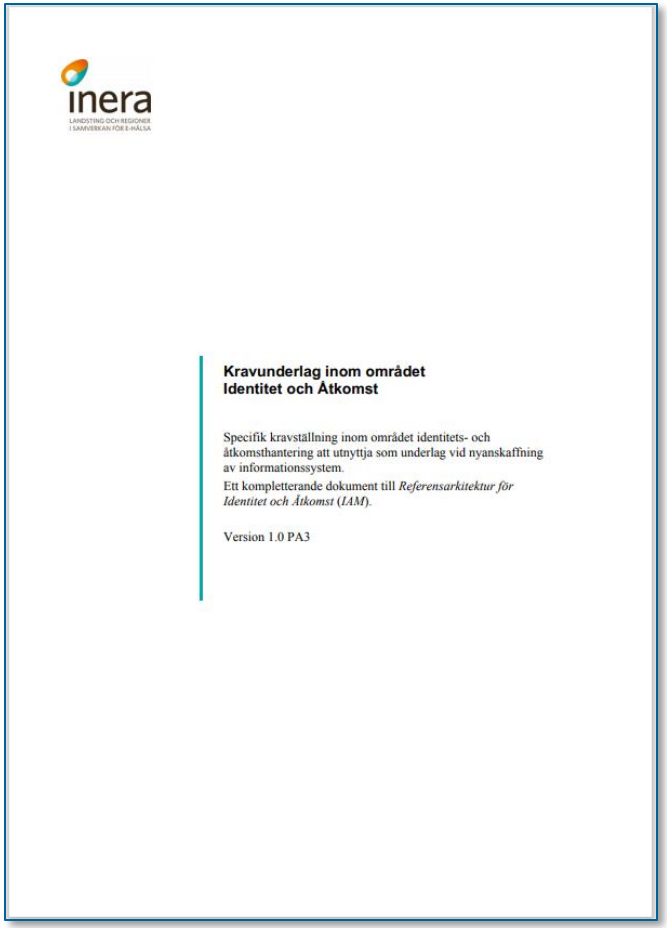


Underbilaga 18-08, Inera behörighetsmodell för administrativa uppdrag
Underbilaga 18-08 är Ineras behörighetsmodell för administrativa uppdrag, vilken Kunden vill arbeta efter i de fall det är tillämpligt. Dokumentet innehåller den behörighetsmodell som skapats med begrepps- och informationsmodeller 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.

Upphandling av kärnsystem – Framtidens vårdinformationsmiljö

Pekar på Kravunderlag inom området Identitet och Åtkomst (FVM)



inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

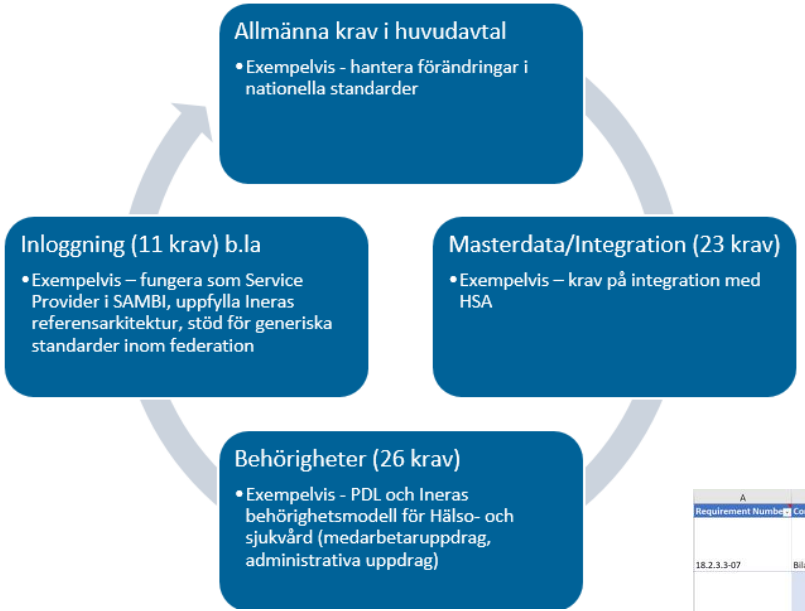
Kravunderlag inom området Identitet och Åtkomst

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

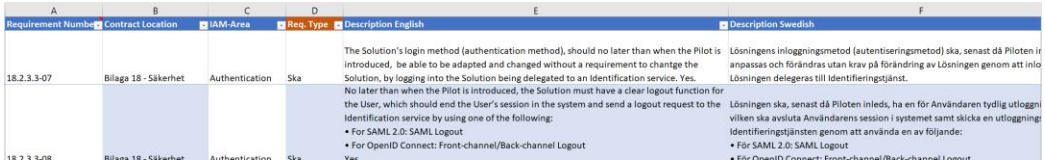
Ett kompletterande dokument till *Referensarkitektur för Identitet och Åtkomst* (*IAM*).

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



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

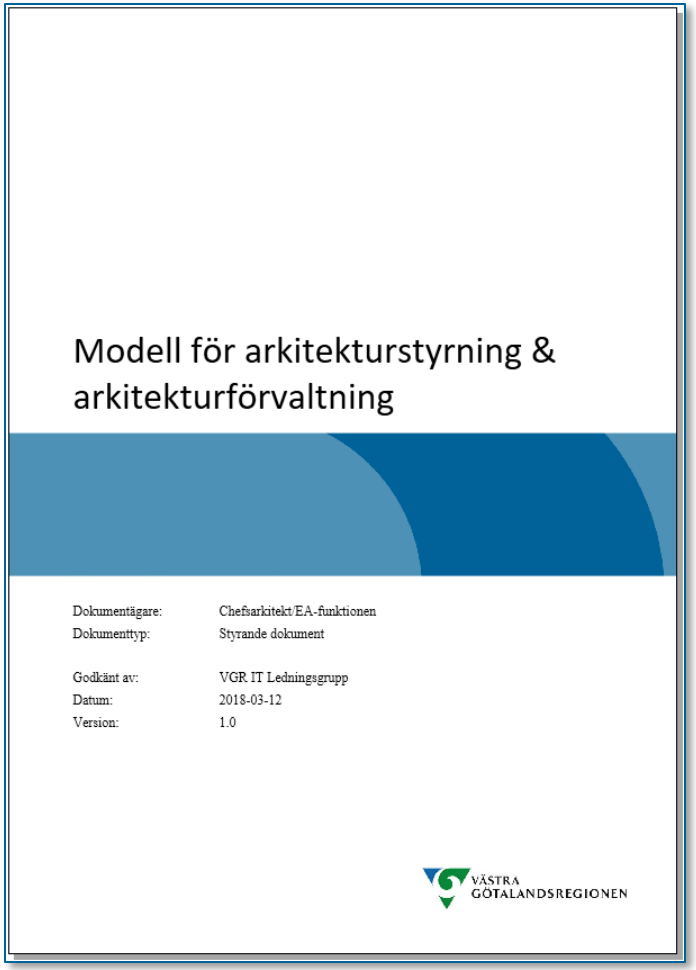
Mobila arbetssätt

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.

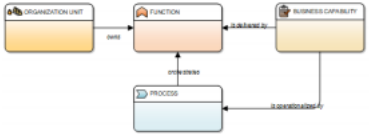


Varvet – VGR:s arkitektur-ramverk. Baseras på TOGAF 9.2 och har anpassats.

Struktur och innehåll

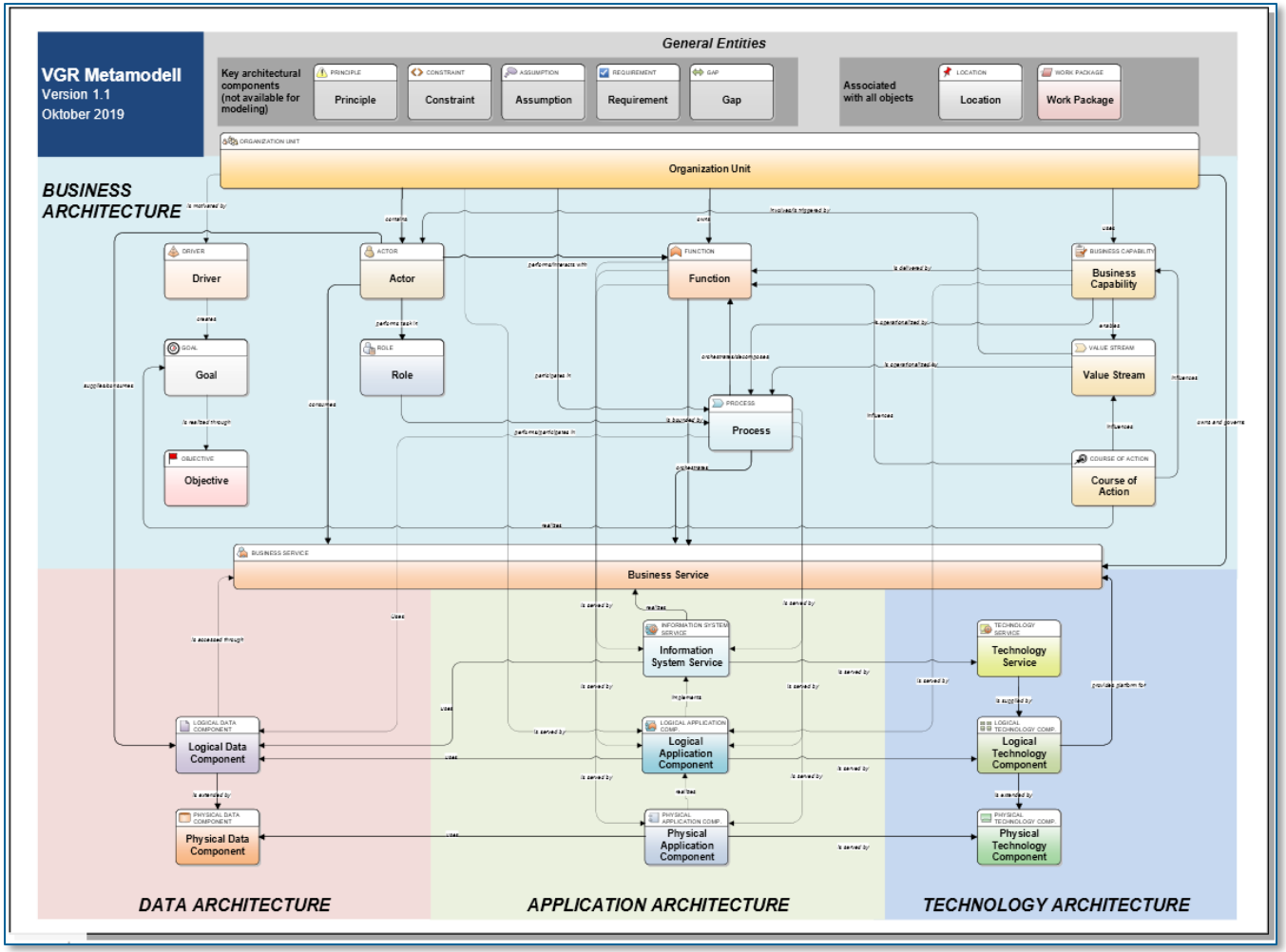
arkitektu´r [-ki- el. -çi-]
substantiv ~*en* ~*er*
ORDLED: arki·tekt·ur·en

- **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.



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.

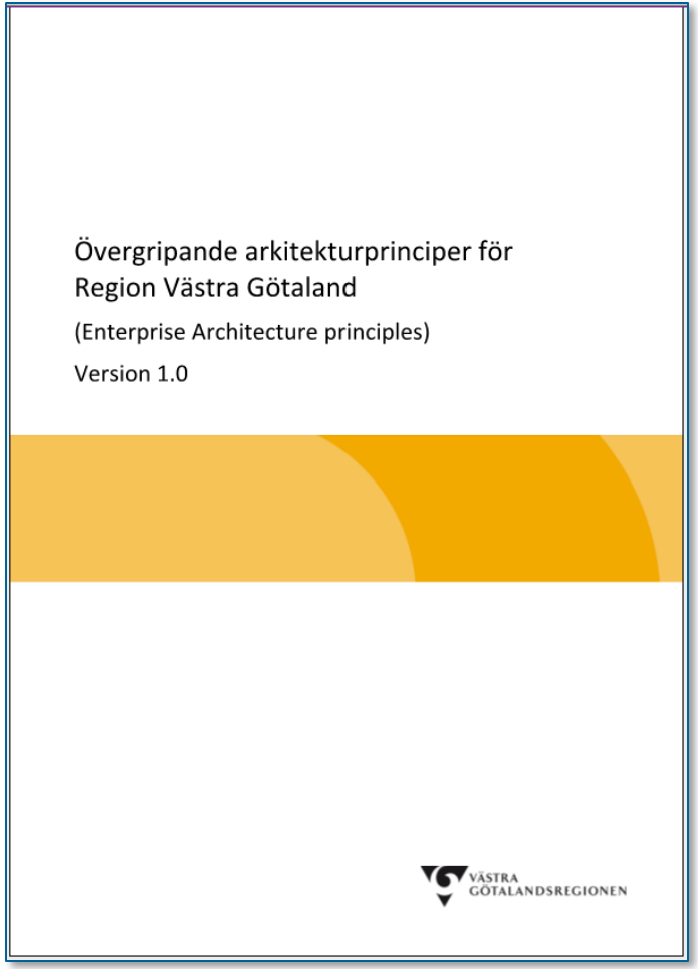
Målbild:
VGR's strategi för behörighet och åtkomst skall användas. Detta leder också till såväl förenklad kontoadministration som förbättrad användarupplevelse genom att användarna använder centrala användarnamn och lösenord och möjligheter kan finnas till single singnon.

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 separarerad 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.

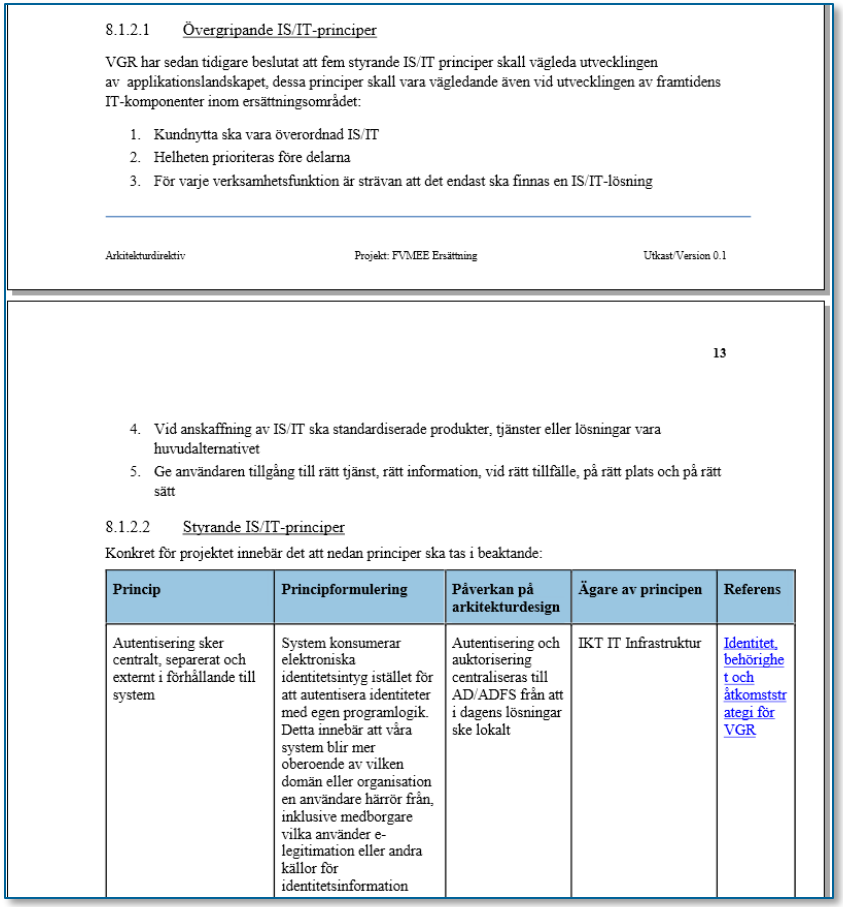
EA-principer tas fram inom Varvet

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



Principer inom IAM används i ADD av lösnings-arkitekter

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: FVMEE 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:

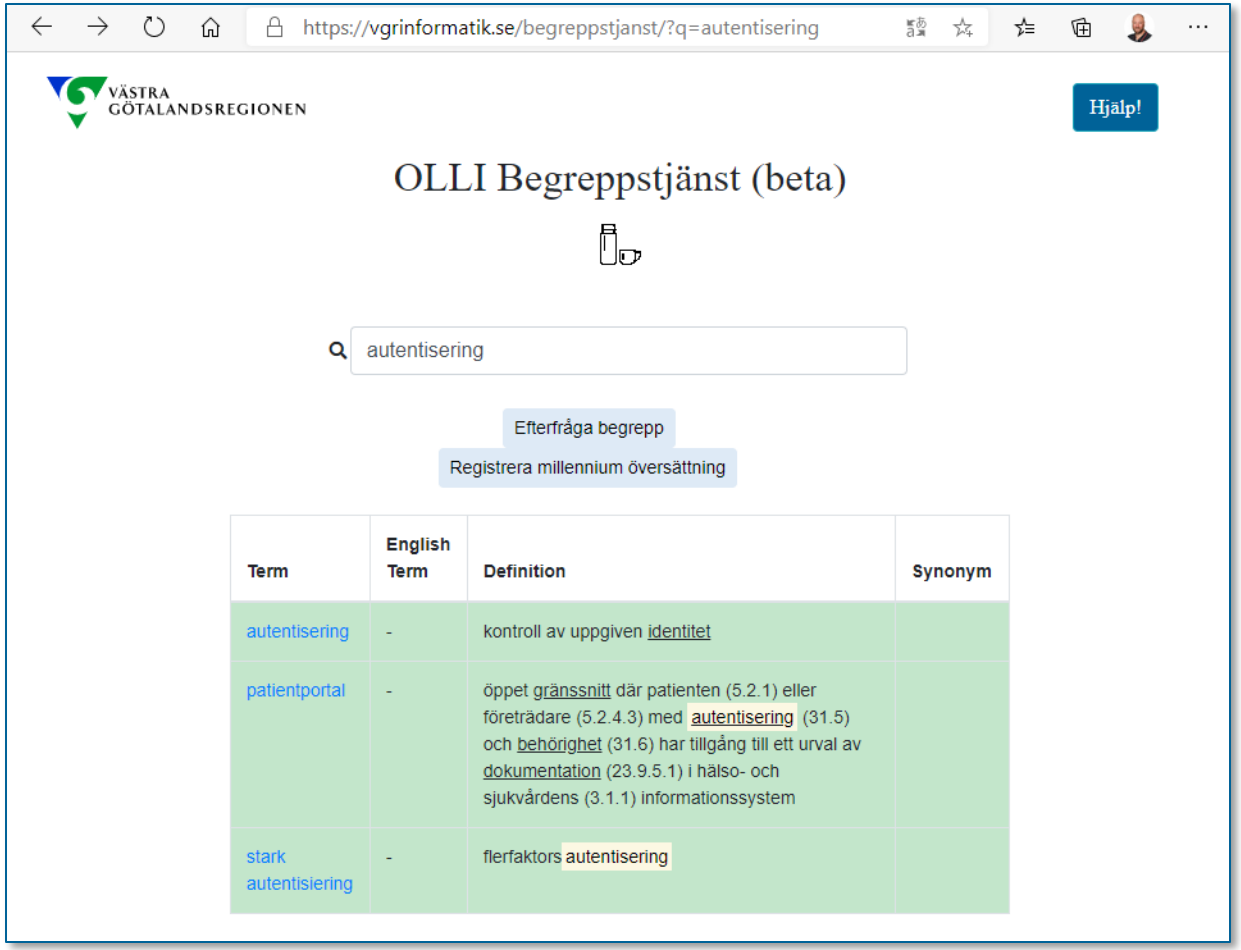
Princip	Principformulering	Påverkan på arkitekturdesign	Ägare av principen	Referens
Autentisering sker centralt, separerat och externt i förhållande till system	System konsumerar elektroniska identitetsintyg istället för att autentisera identiteter med egen programlogik. Detta innebär att våra system 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	Identitet, behörighet och åtkomststrategi för VGR

Lärdom 2019

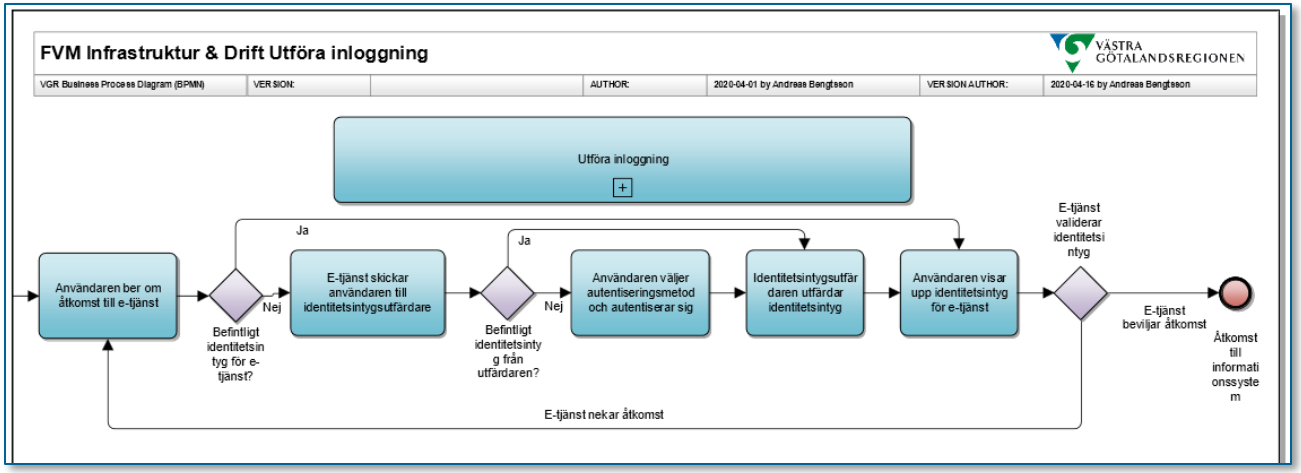
- Referens-arkitekturen fungerar inte bara för Ineras leveranser utan även för andra leverantörers produkter.
- Förståelsen för referens-arkitekturen ökar ju mer arkitektur vi arbetar med inom Varvet.
- Principerna börjar att användas.
- Vissa förvaltare och leverantörer är med på banan till referens-arkitekturen.

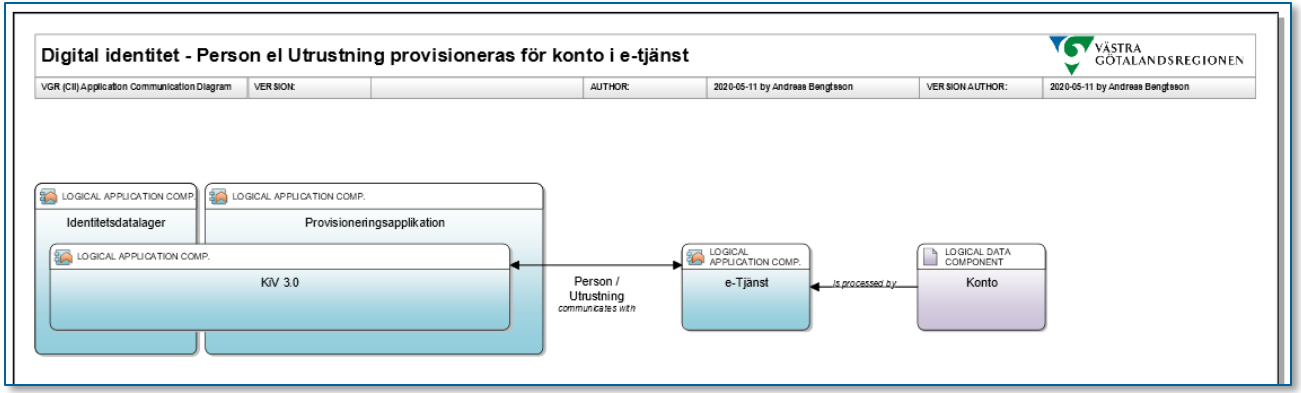
Termer och begrepp (igen)

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

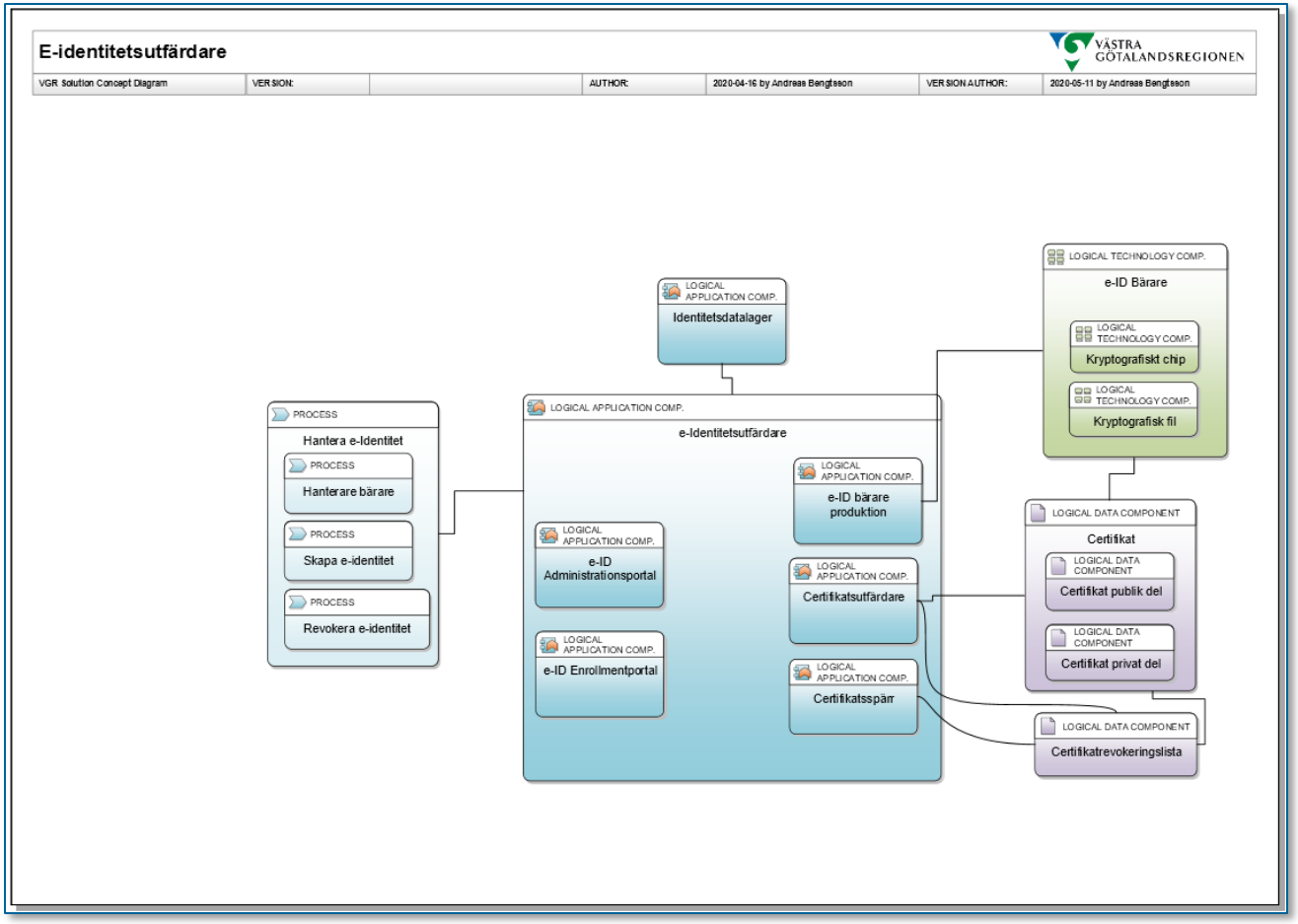


Generella exempel på hur arkitektur för IAM kan modelleras i Varvet tas fram

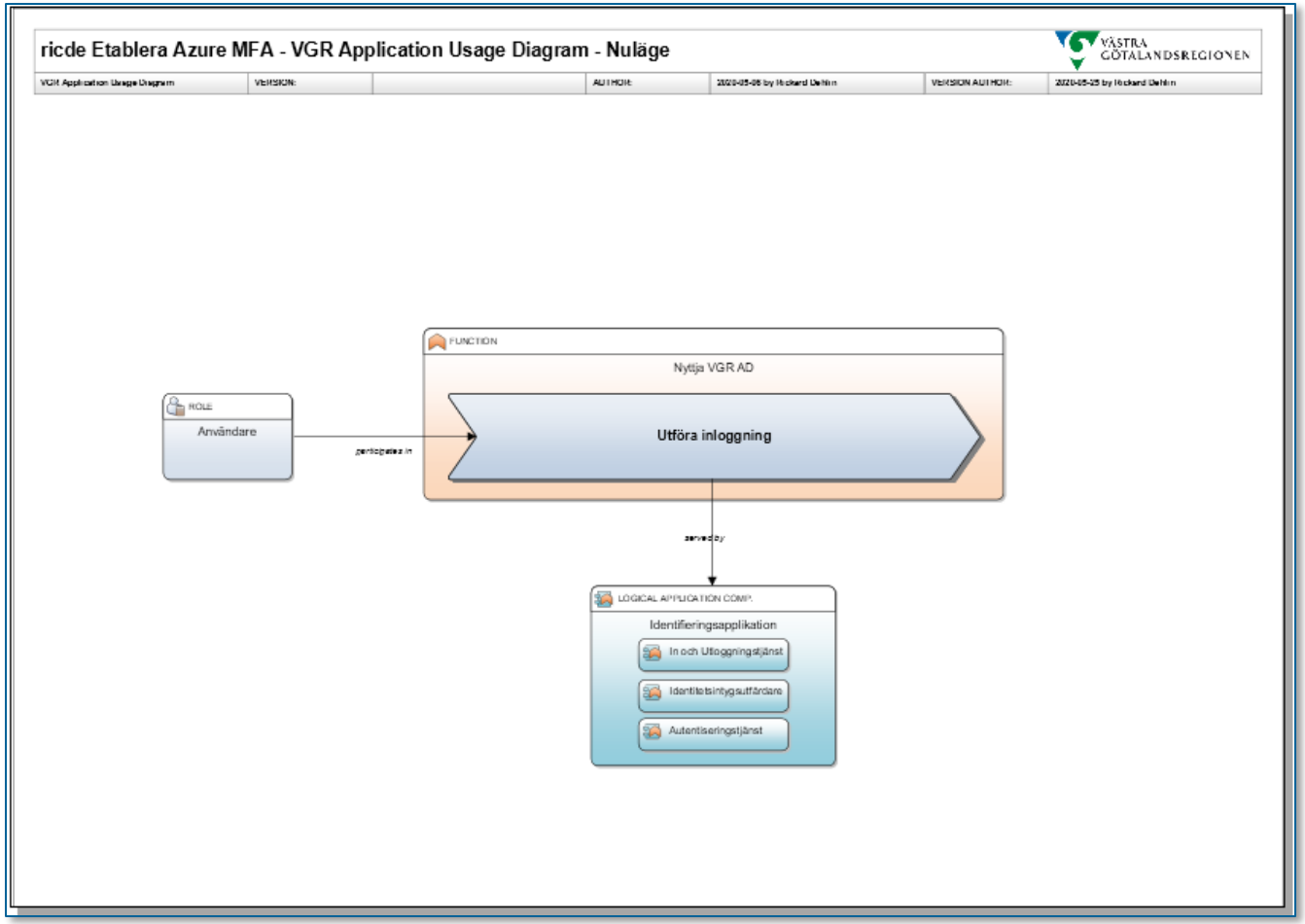




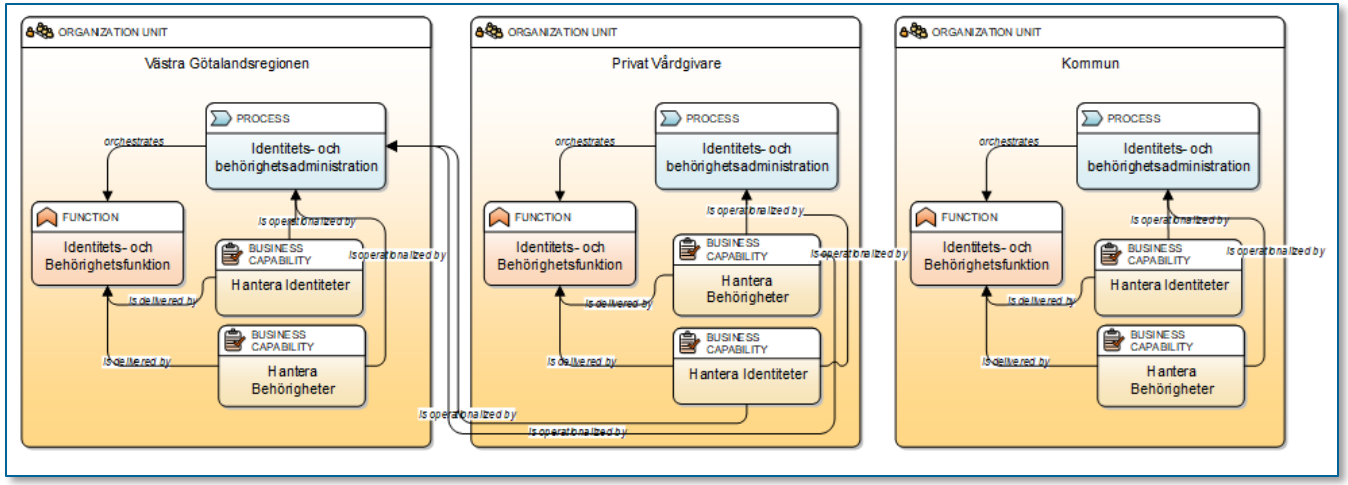
Målarkitektur för E-identitets-utfärdare



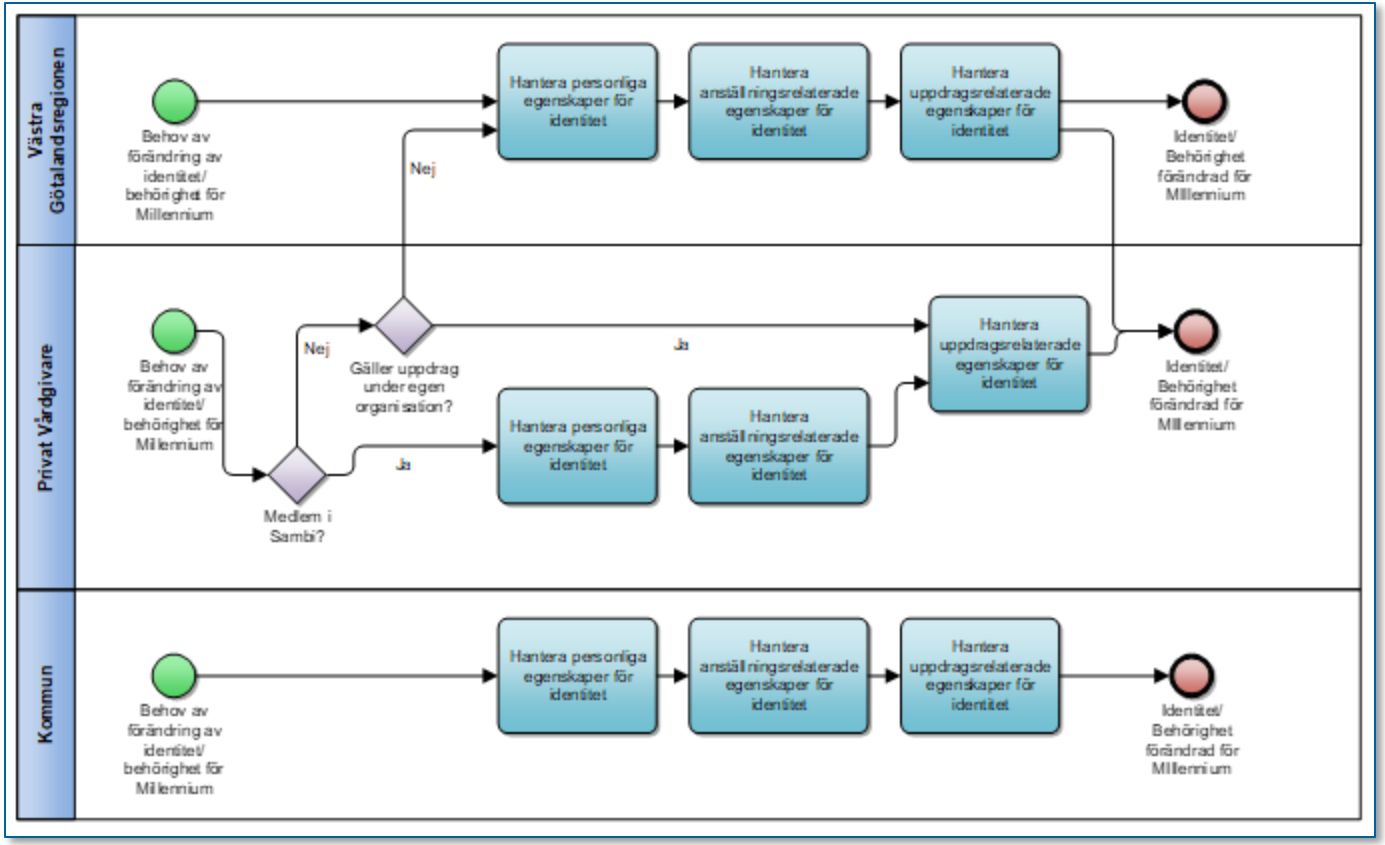
Lösningsarkitekter tar fram IAM artefakter



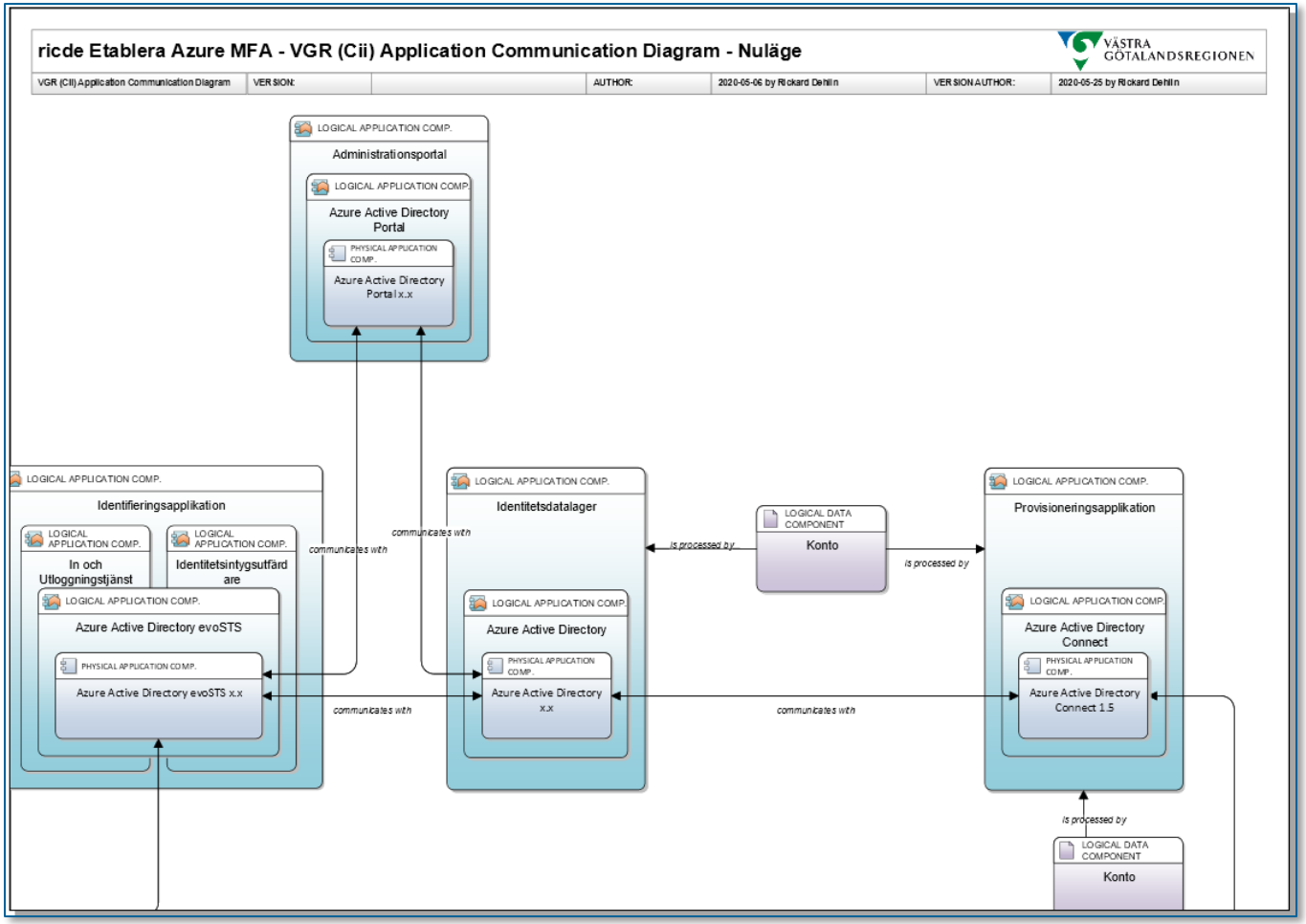
Lösningsarkitekter tar fram IAM artefakter (FVM)



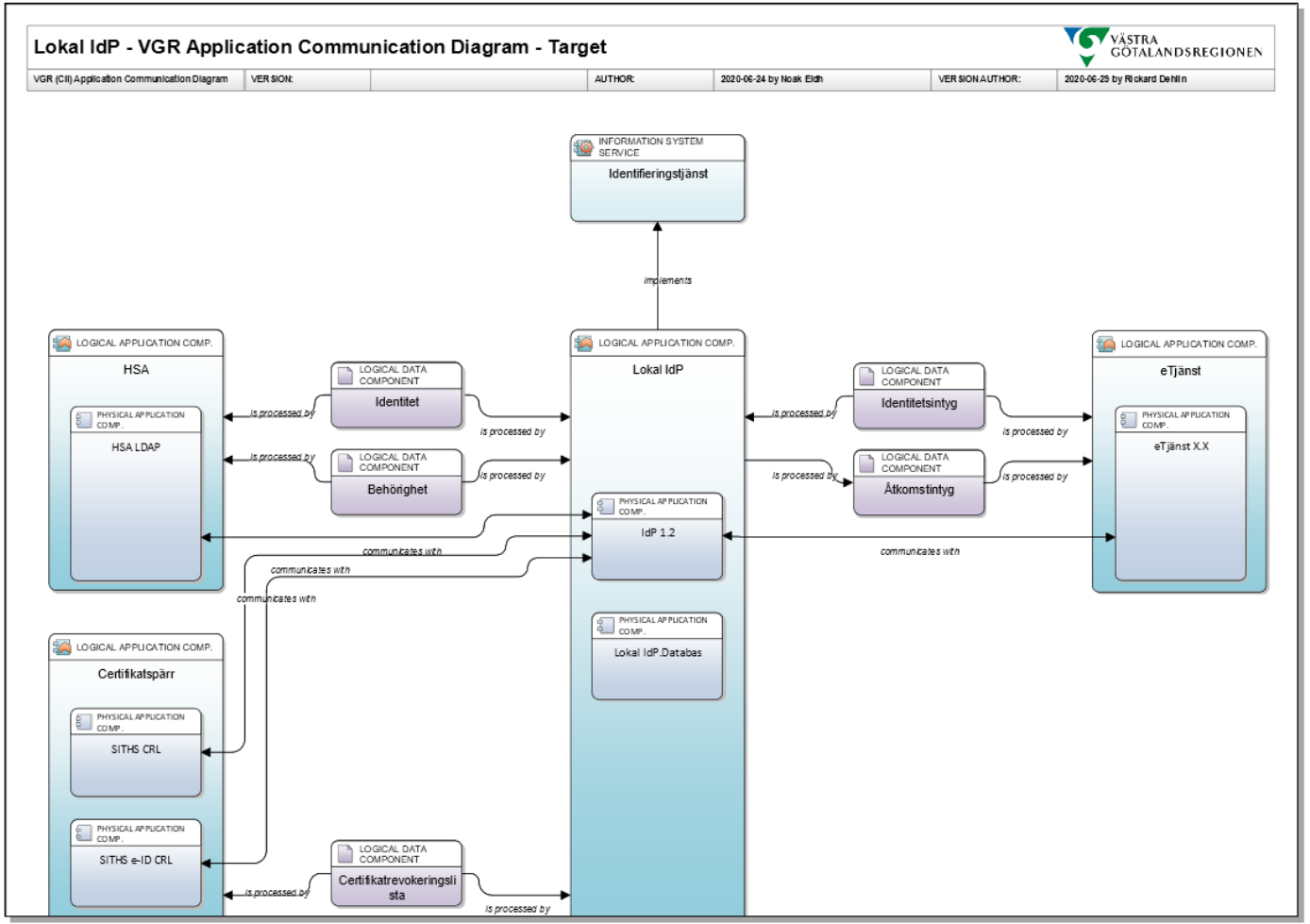
Lösningsarkitekter tar fram IAM artefakter (FVM)



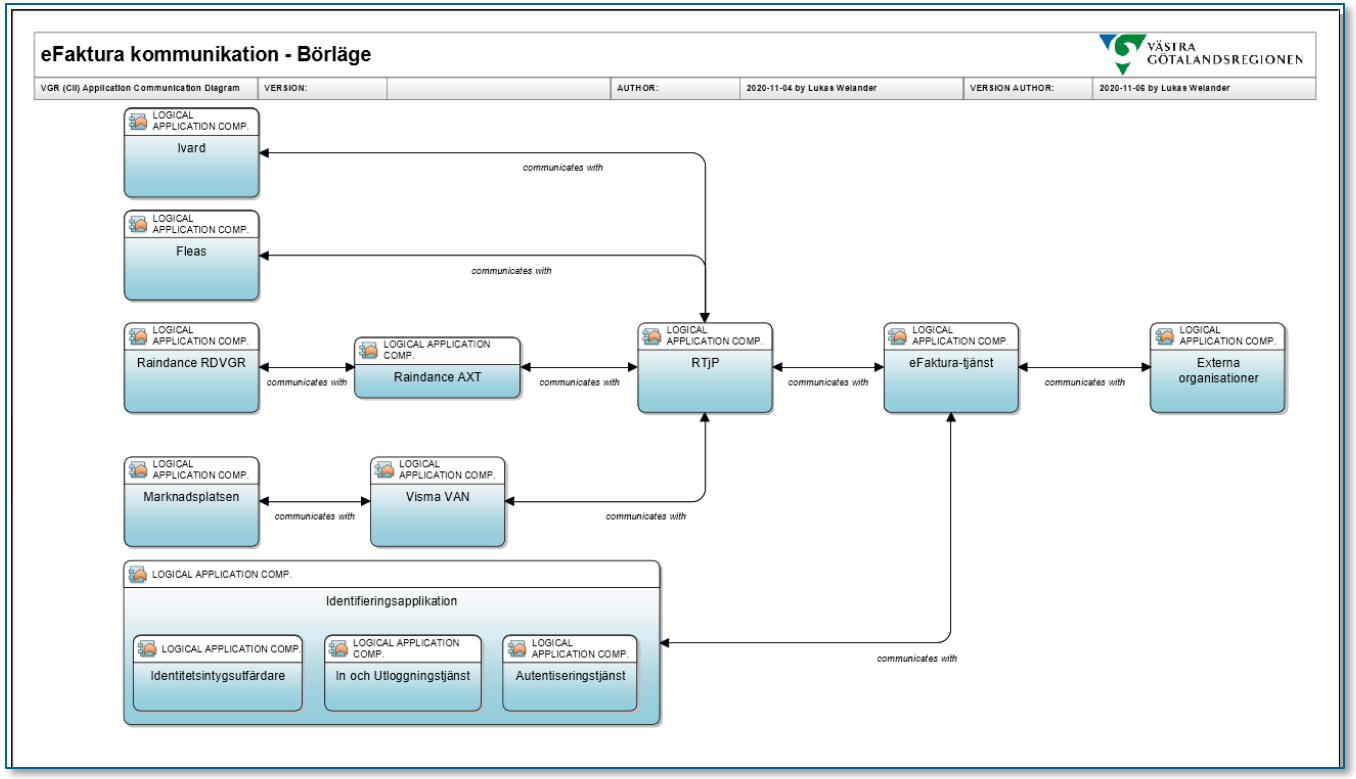
Lösningsarkitekter tar fram IAM artefakter



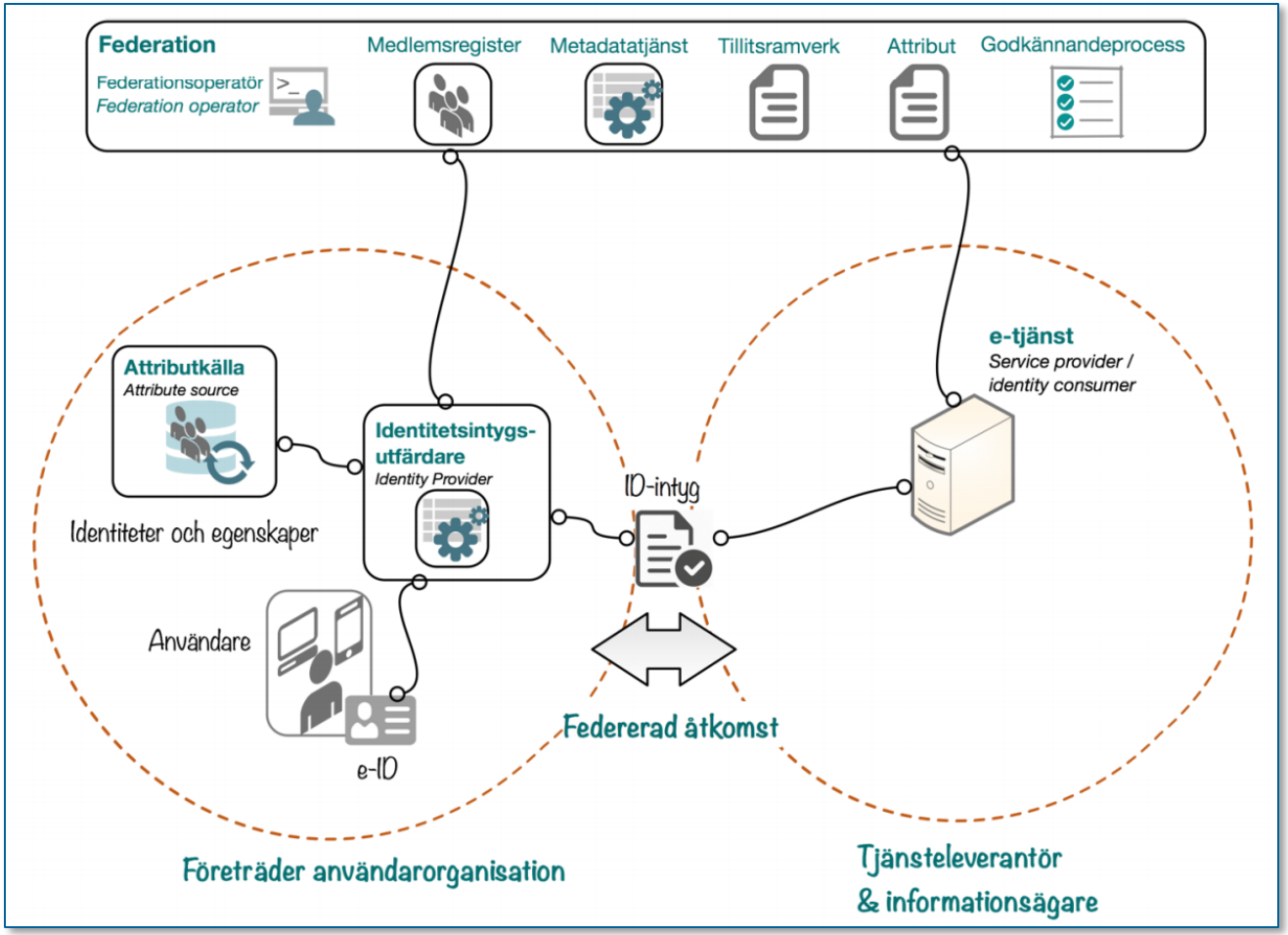
Lösningsarkitekter tar fram IAM artefakter



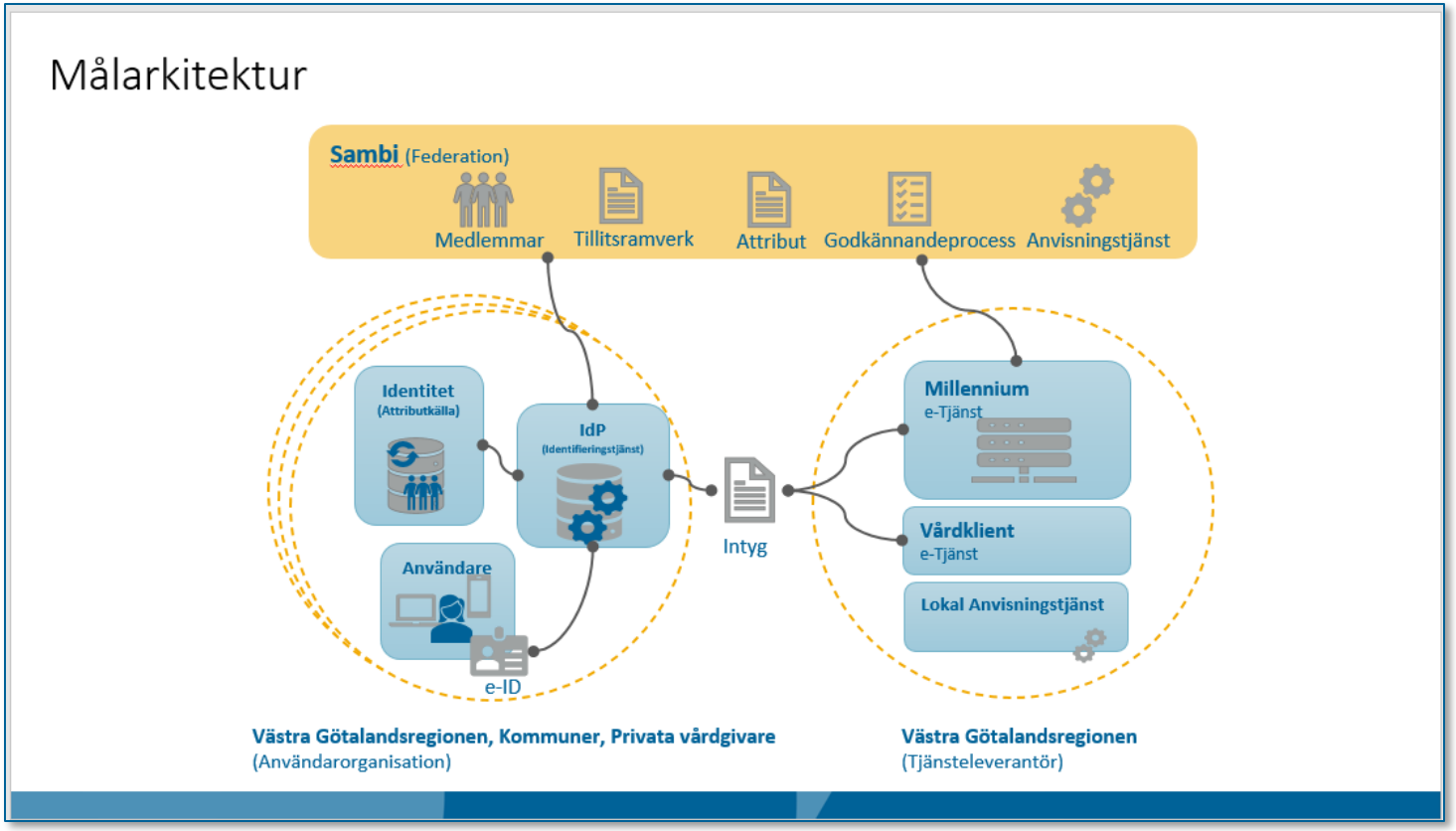
Domän-arkitekter modellerar med publicerade IAM artefakter



Från 2017


Federation
Federationsoperatör
Federation operator
Medlemsregister
Metadatatjänst
Tillitsramverk
Attribut
Godkännandeprocess
Attributkälla
Attribute source
Identiteter och egenskaper
Identitetsintygs-
utfärdare
Identity Provider
ID-intyg
e-tjänst
Service provider /
identity consumer
Användare
e-ID
Federerad åtkomst
Företräder användarorganisation
Tjänsteleverantör
& informationsägare

… blev


Målarkitektur
Sambi (Federation)
Medlemmar
Tillitsramverk
Attribut
Godkännandeprocess
Anvisningstjänst
Identitet
(Attributkälla)
IdP
(Identifieringstjänst)
Användare
e-ID
Intyg
Millennium
e-Tjänst
Vårdklient
e-Tjänst
Lokal Anvisningstjänst
Västra Götalandsregionen, Kommuner, Privata vårdgivare
(Användarorganisation)
Västra Götalandsregionen
(Tjänsteleverantör)

VGR går med i Identitets- och behörighets-federationen Sambi

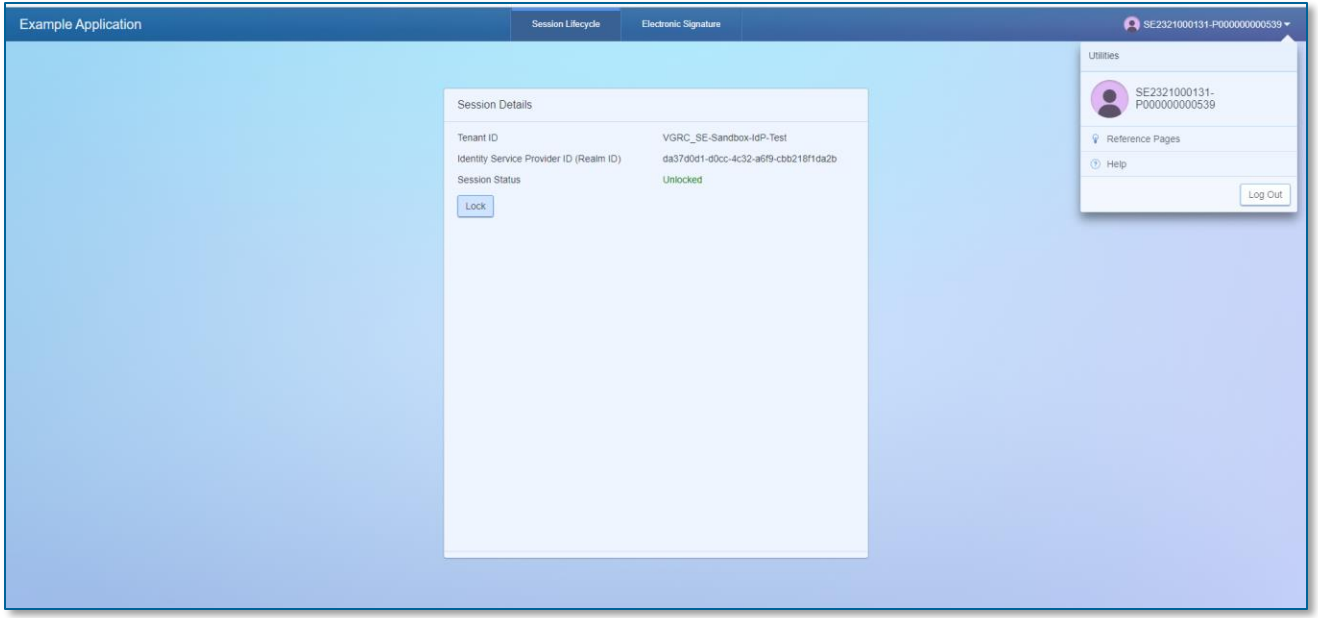
Referensarkitekturen pekar på användarorganisation, tjänsteleverantör och federation.

IdP med i Sambi federationen

Tack vare att FVM kravställt på federerad inloggning

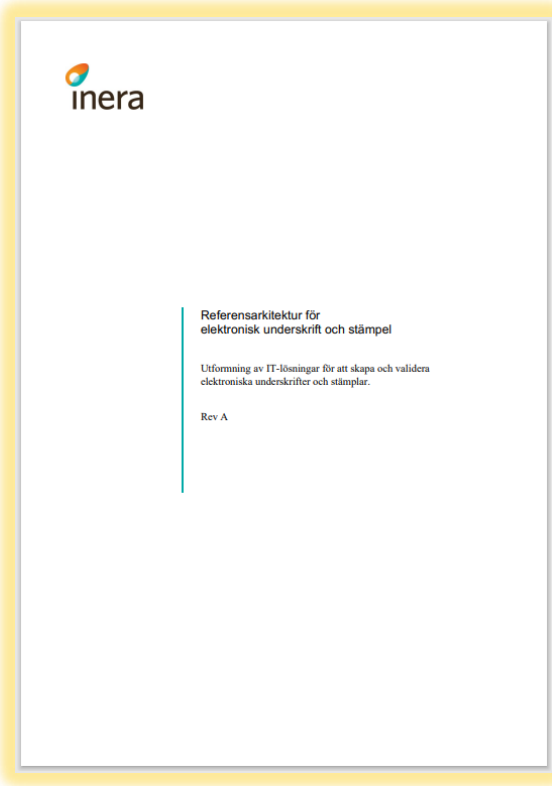
Lyckad inloggning i FVM (sandbox)

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

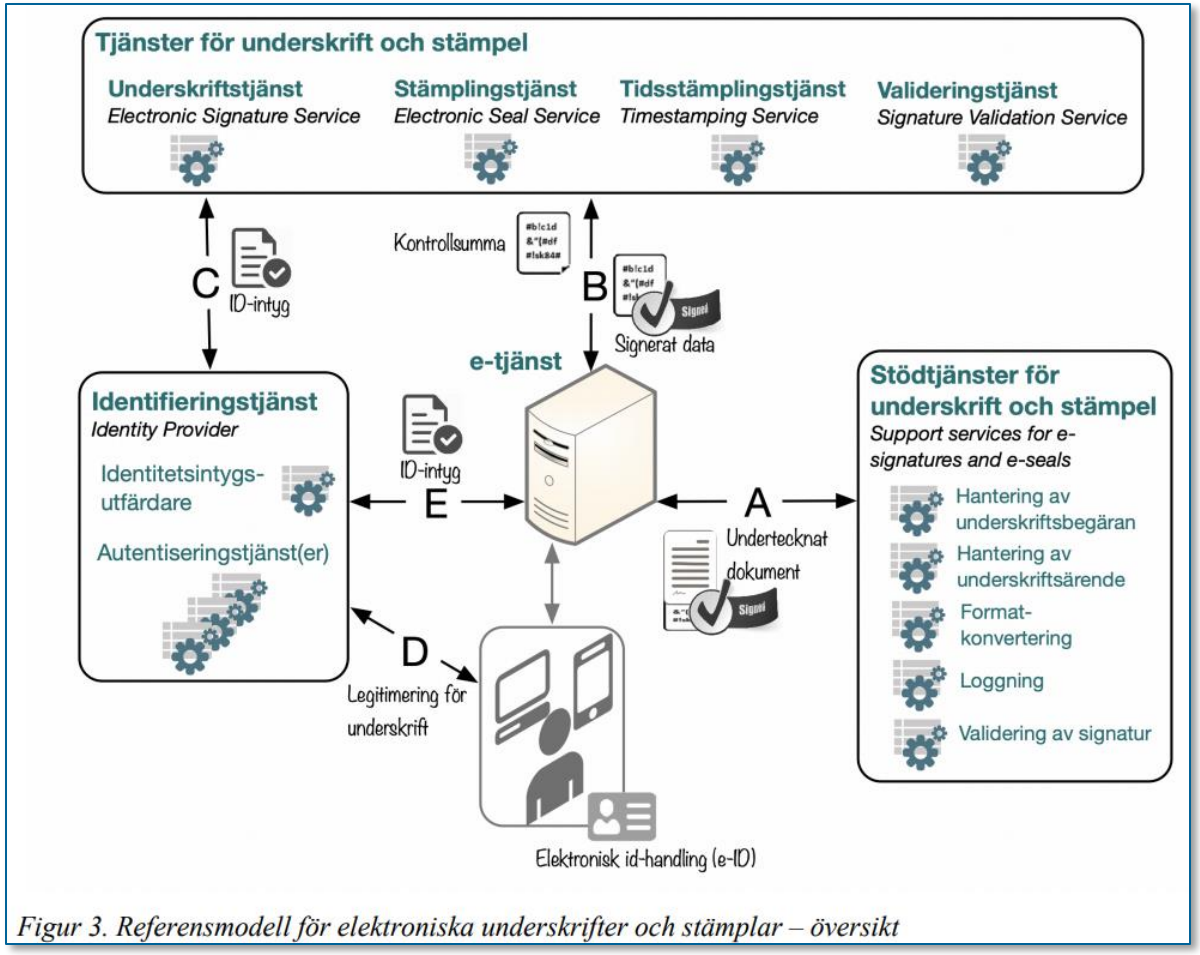


2020 så släpps Inera Referensarkitektur för grunddata och katalog samt Referensarkitektur för elektronisk underskrift och stämpel

- 140 sidor!
- 82 sidor!



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

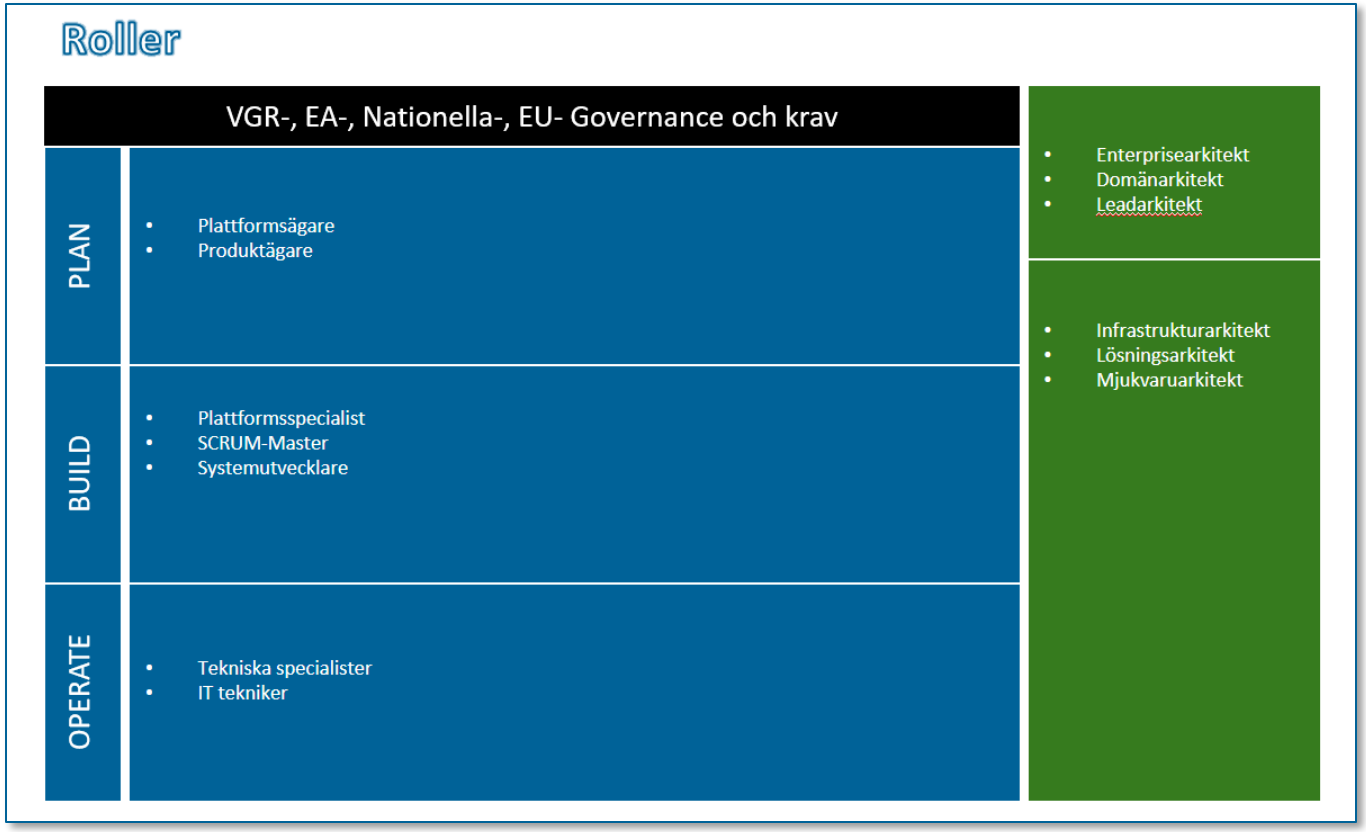


Figur 3. Referensmodell för elektroniska underskrifter och stämplar – översikt

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 referens-arkitekturen.
- Resan fortsätter …


VÄSTRA
GÖTALANDSREGIONEN