


FHIR

- for RITA





FHIR er primært en veldokumenteret, standardiseret domænemodel

- resten er teknik hvori modellen indgår ...

Leverandørens strategi

Brug <indsæt standard her> alle steder hvor det giver mening

Nedenstående gør sig især gældende for FHIR

- Det fremmer genbrugbarhed (80/20)
- Det gør det lettere at tale sammen (på tværs) om hvad der menes
- Værktøjer, værktøjer, værktøjer (tooling, frameworks, osv.)
- Et fantastisk professionelt fagfællesskab hvor lysten til at hjælpe hinanden ikke influeres stærkt af hvor man er ansat



Leverandørens strategi

Konsekvens af strategien (Citius, Altius, Fortius)

Hensigtsmæssig brug af standarden giver følgende afkast

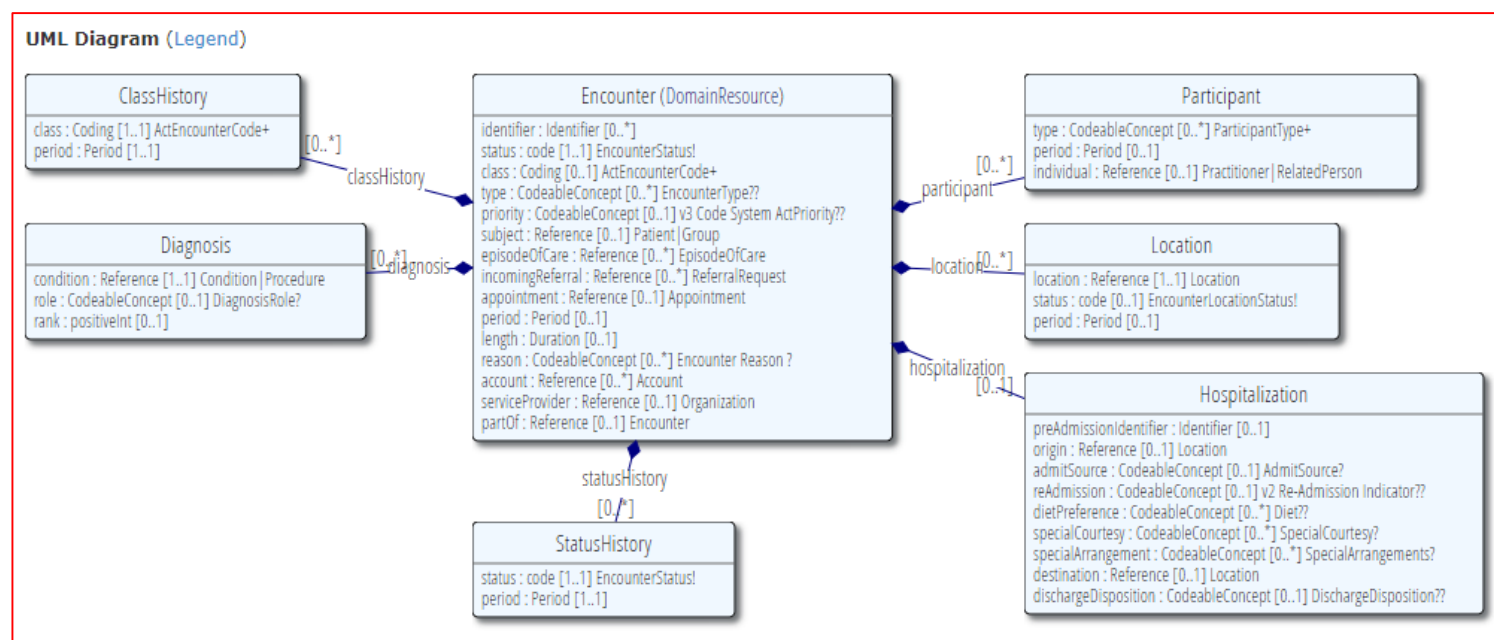
- Det er lettere at få løst en given problemstilling
- Det er lettere at integrere systemer
- Det er lettere at levere kvalitet

Dette er til gavn for kunden og leverandøren

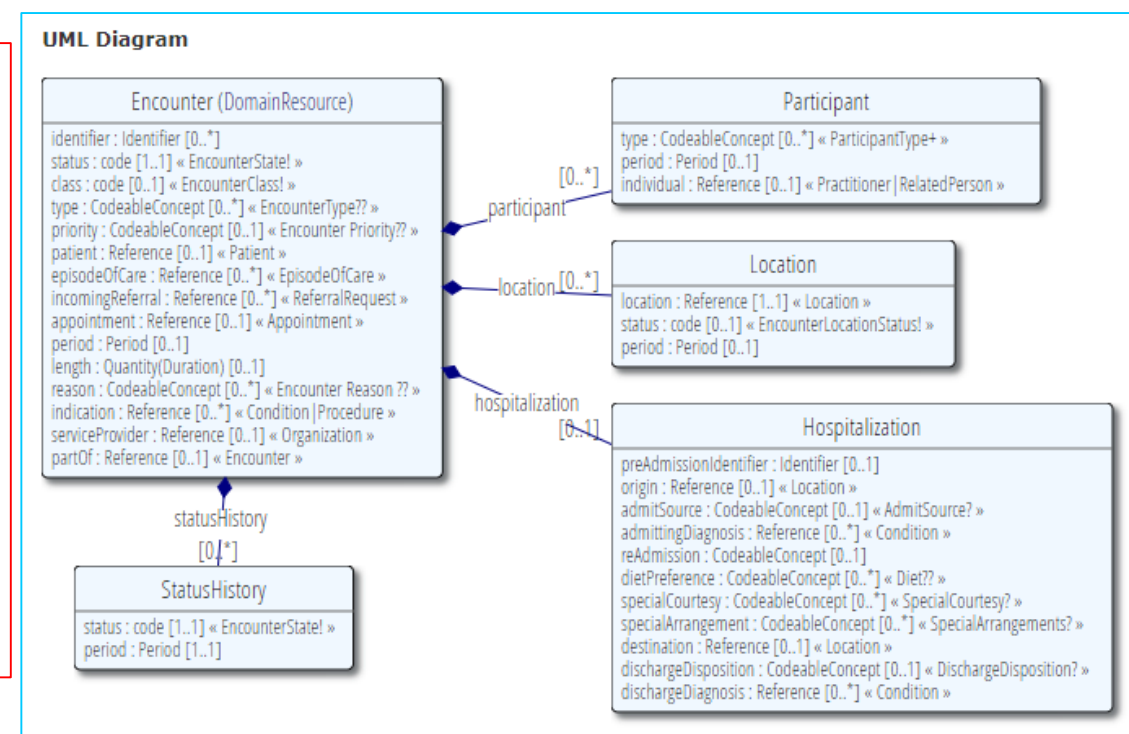
Resten er teknik hvori modellen indgår ...

- FHIR er pt. i status "standard for trial use" - (den er ikke længere i draft)
- FHIR er moving target som alt andet er – f.eks. FMK eller MedCom, men det ændrer ikke på at man godt kan låse sin brug og versionere brugen og dermed fastholde en version

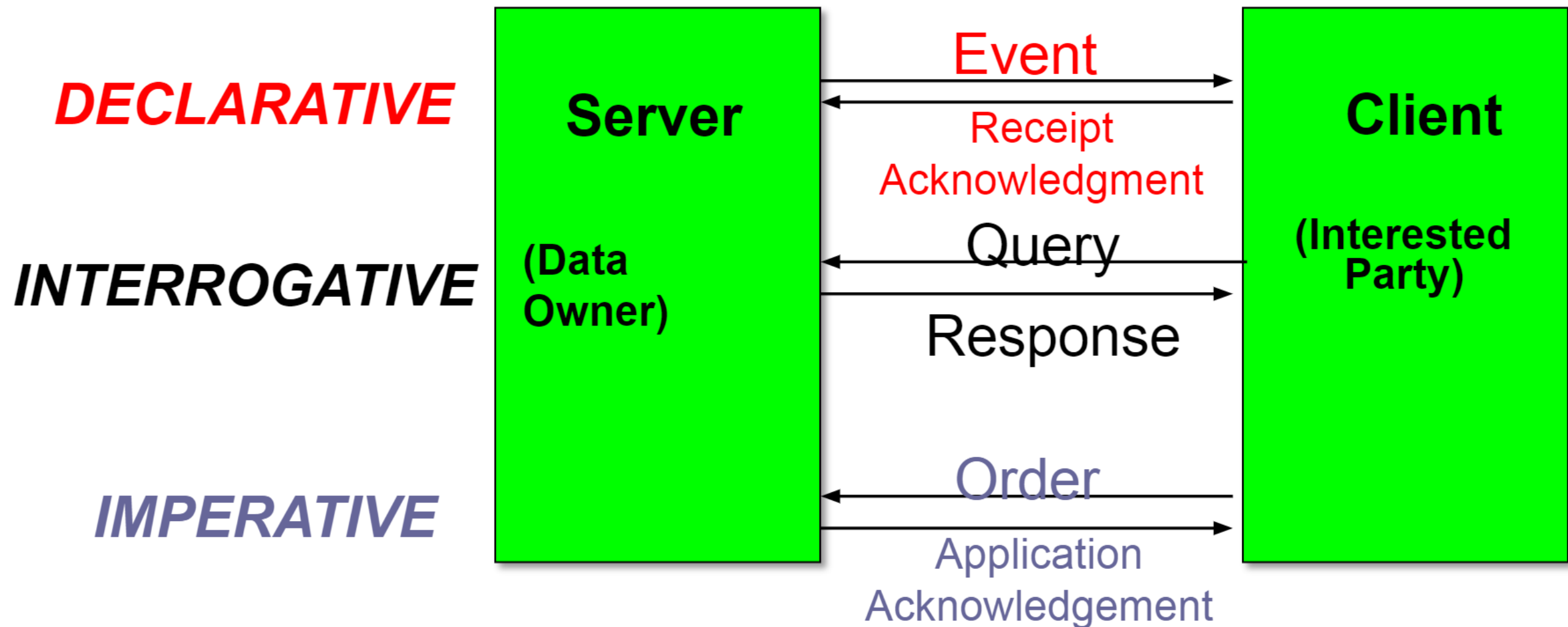
STU3



DSTU2



Message Exchange Mechanisms



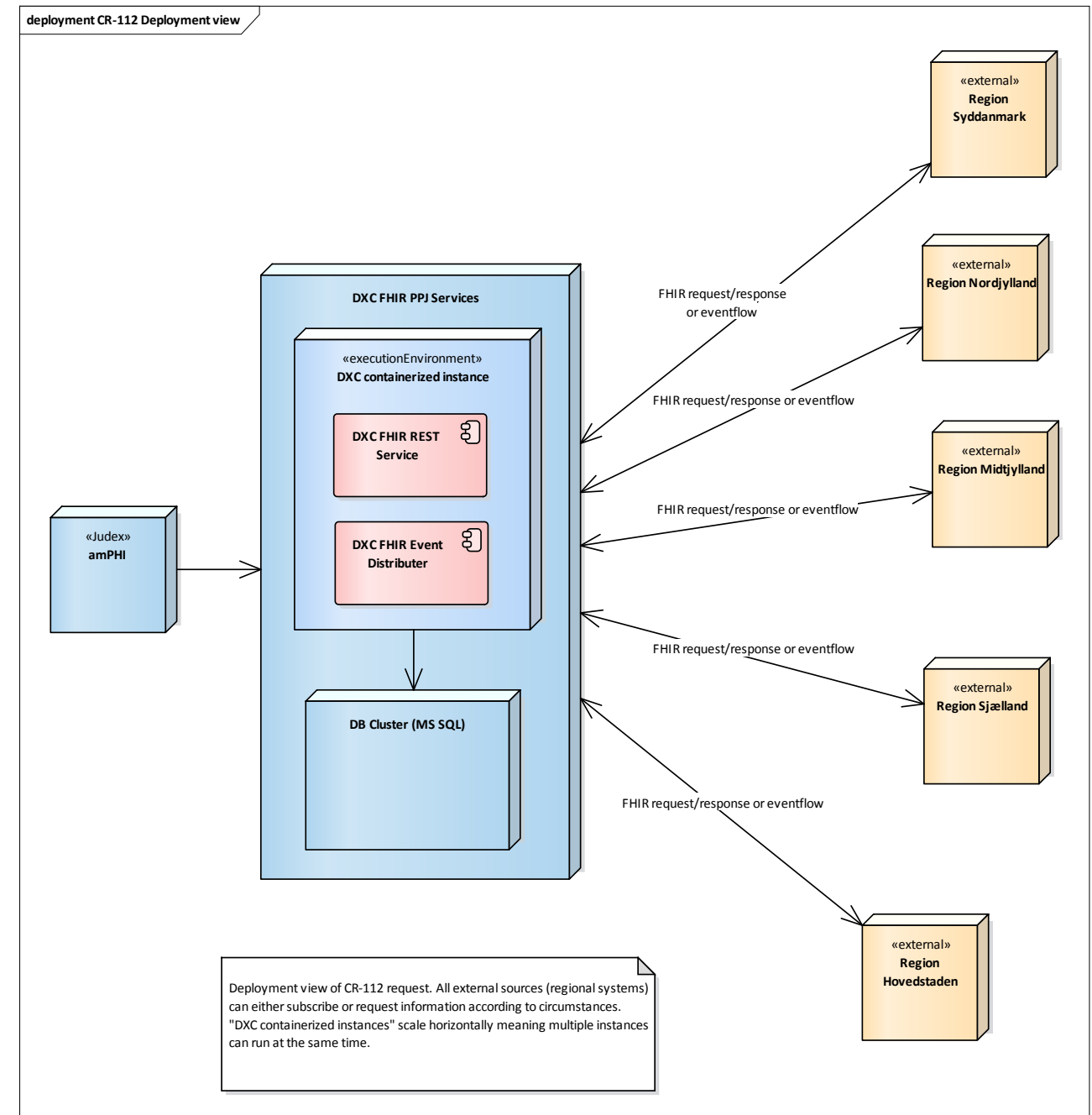


Anvendelsesmuligheder

- **Som services aka. Web Services**
- **Dokumentorienteret – aka. selvindeholdte dokumenter**
- **RESTful – aka. Udstilling af ressourcer/model**
- **Messageorienteret – modellen distribueret i form af beskeder**

PPJ on FHIR

- PPJ on FHIR indeholder en række integrationsmuligheder
 - Eventing
 - Notification
 - Queries
- Udstillede profilerede FHIR centrale ressourcer er bl.a. *Patient, Encounter, Observation, Procedure*



FHIR og sikkerhed

“Fast Healthcare Interoperability Resources (FHIR) is not a security protocol, nor does it define any security related functionality. However, FHIR does define exchange protocols and content models that need to be used with various security protocols defined elsewhere”

- <http://hl7.org/fhir/security.html>

SMART on FHIR

- **Der kan ikke være tvivl om sikkerhedsmodellen i FHIR – for den er der ikke.**
- SMART definerer måder hvorpå man kan etablere sikkerhed – f.eks. Ifbm. REST
- OpenID og OAuth 2.0 (Bruger-til-System)
- SMART Backend Services (System-til-System) integration
- <http://docs.smarthealthit.org/authorization/>



FHIR er en standard der har vundet stor udbredelse på kort tid og vil formentligt være de facto i løbet af meget få år.

Tak for opmærksomheden

