Vejen til en ny, fælles sikkerhedsstandard på sundhedsområdet

Esben Dalsgaard
Chefarkitekt, Sundhedsdatastyrelsen

SUNDHEDSDATA-
STYRELSEN

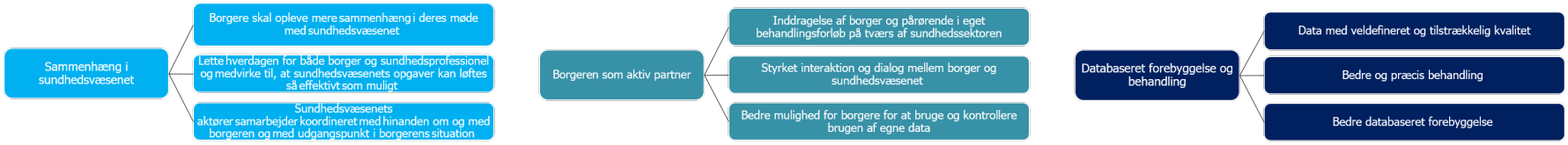
Forventningsafstemning

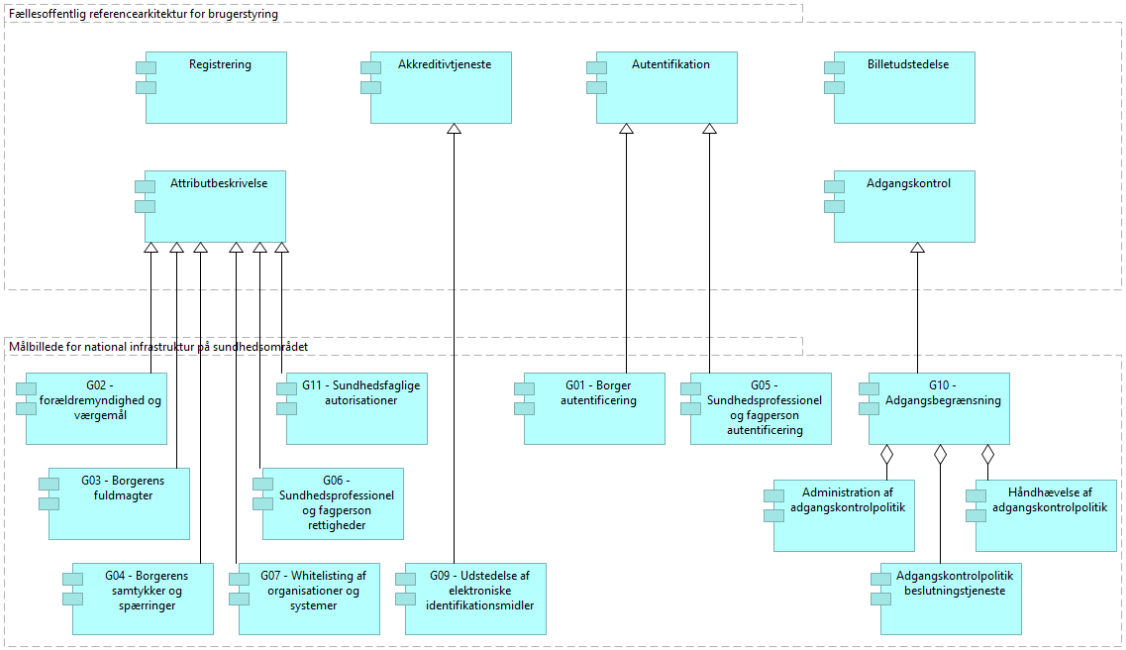
- Der er mange sikkerhedsstandarder, der adresserer såvel organisatoriske som tekniske aspekter – dette indlæg har tyngden på tekniske standarder, der understøtter adgangs-/brugerstyring
- Indlægget vedrører adgangsstyring baseret på validering af brugerens identitet. Der er også behov for at se på teknologier, der har fokus på beskyttelse af identitet (se min præsentation "Sikkerhedsmodeller på sundhedsområdet" fra sidste års eSundhedsobservatorium: http://2018.e-sundhedsobservatoriet.dk/wp-content/uploads/sites/2/2018/10/4Esben.pdf)
- Der er udarbejdet et oplæg til beskrivelse af et Proof of Concept projekt: "Tillidsskabende registerforskning og kunstig intelligens baseret på reelt ikke-identificerbare data", men det er udenfor emnet for denne præsentation (måske indlæg på næste års konference?).

Agenda

- Kort om moderniseringen set i et bredere perspektiv
- Hvorfor modernisering?
- Hvad er status?
- Hvornår udfases gamle standarder?
- Next step

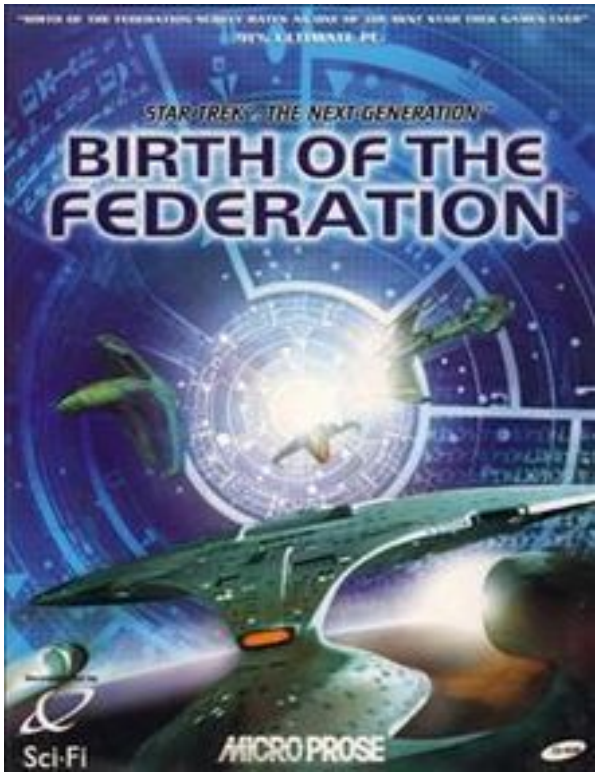
Sammenhæng med målbillede for national infrastruktur





SUNDHEDSDATA-STYRELSEN

Indflyvning ...



- Nationale løsninger har fra sidste halvdel af 00'erne bygget på Internet- og webteknologi, hvor autentifikation og brugeradministration er adskilt fra selve løsningen (føderative, tokenbaserede teknologier).
- Referencearkitektur for informationssikkerhed på sundhedsområdet diskuterer i 2013 forskellige sikkerhedsmodeller, herunder den føderative model, hvor de parter, der indgår i en føderation gensidigt har tillid til hinandens løsninger.
- En fællesoffentlig analyse af sikkerhedsløsninger og standarder (for brugerstyring), peger i 2014 på at man med en relativ beskeden indsats kunne skabe sammenhæng mellem forskellige parters føderative løsninger.
- Regioner og kommuner begynder at etablere fællesregionale og fælleskommunale løsninger baseret på fødererede sikkerhedsmodeller (hvor brugerstyring og autentifikation sker lokalt).
- Fællesoffentligt udarbejdes strategi og referencearkitektur for brugerstyring (2017) og national standard for identitetssikringsniveauer, NSIS (2018). Ved overgang til ny NemLogin tillades opkobling af lokale autentifikationsløsninger baseret på lokale identifikationsmidler (dvs. etablering af en føderation).
- Der pågår arbejde med at beskrive målbillede for sammenhængende brugerstyring på sundhedsområdet ved etablering af en national føderation. Målbilledet og oplæg vedr. sikringsniveauer på sundhedsområdet forventes forelagt den nationale bestyrelse for sundheds-IT.

Problem med eksisterende standard (DGWS)

DGWS (Den Gode WebService) blev udviklet i 2005-2006. Profilen er implementeret i mere end 50 løsninger, og der foretages et stort antal kald af webservices baseret på denne profil. I december 2018 blev der alene på den nationale serviceplatform (NSP) foretaget mere end 100 mio. kald (svarende til ca. 2.000 i minuttet).

Da verden har ændret sig siden profilen blev udviklet, gav man den et ”servicetjek” i 2013-2014 (analyse i den ”Nationale Strategi for Digitalisering af Sundhedsvæsenet 2013 – 2017 – Digitalisering med effekt”, initiativ 3.4).

Her påpeges, at DGWS har anvendelsesmæssige og sikkerhedsmæssige udfordringer, og mangler kompliance til standarder og markedet.

Udfordringer ved DGWS

1. Anvendelsesbegrænsninger ved DGWS
   - understøtter kun system- og medarbejderadgang - ikke borgeradgang
   - bør ikke anvendes i usikre miljøer
   - er låst til et fast og begrænset attributindhold
2. Sikkerhedsmæssige udfordringer ved DGWS
   - understøtter udelukkende SHA-1, som af flere kryptografer vurderes usikker
   - token er langtidsgyldige og kan ikke bindes til brugskontekst - fx patient, service-aftager og –udbyder
   - det er ikke muligt at kryptere tokens eller indhold heraf
3. DGWS er en propritær standard
   - manglende kompliance til standarder og svær at integrere til markedsprodukter
   - har ringe synergi fra nationale og internationale fremskridt med standarder, protokoller, værktøjer, ”best practice” og øvrig innovation

IDWS-projektet (2017 – 2019)

Analysen anbefalede, at man fremover benytter den fællesoffentlige web service profil (OIO IDWS) samt overholder internationale standarder på sundhedsområdet (IHE XUA profilen).

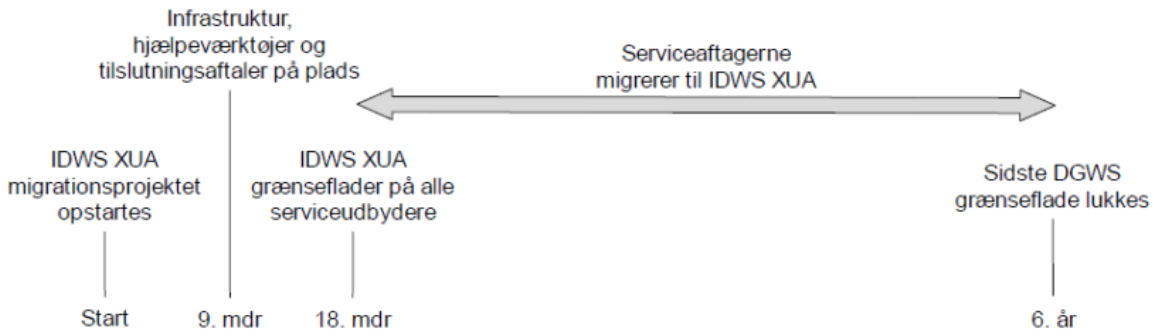
Dette har krævet mindre tilretninger af OIO IDWS og de værktøjer, der understøtter denne (er gennemført).

Der blev herefter nedsat et profilerings- og afprøvningsprojekt, hvis formål har været at tilvejebringe og afprøve den nye IDWS XUA sikkerhedsprofil og afprøve denne i tre piloter. Denne afprøvning er del af den fællesoffentlige digitaliseringsstrategis initiativ 7.2 ”Fælles standarder for sikker udveksling af information”.

IDWS-projektets leverancer

- IDWS XUA profil er udarbejdet af en arbejdsgruppe (profilering af den fællesoffentlige IDWS-standard)
- Java og .Net hjælpeværktøjer og vejledninger tilvejebragt (udvidelse af DIGST værktøjer)
- NSP infrastruktur (DCC, STS og sundheds IdP) tilpasset den nye profil
- Fælles Medicinkort (FMK) og DokumentDelingsServicen (DDS) opdateret til IDWS XUA
- DDS afprøvet i en regional pilot, FMK afprøvet i en kommunal og en lægepraksis pilot
- Governancemodel, migrationsplan og beslutningsoplæg udarbejdet
- IDWS XUA profilen forelægges det rådgivende udvalg for standarder og arkitektur på sundhedsområdet (RUSA) mhp. optagelse i kataloget over nationale standarder
- Migrationsstrategi er forelagt Kommunernes it-arkitekturråd, Regionernes it-arkitekturråd (RITA) og RUSA, og forelægges Den Nationale Bestyrelse for Sundheds-it

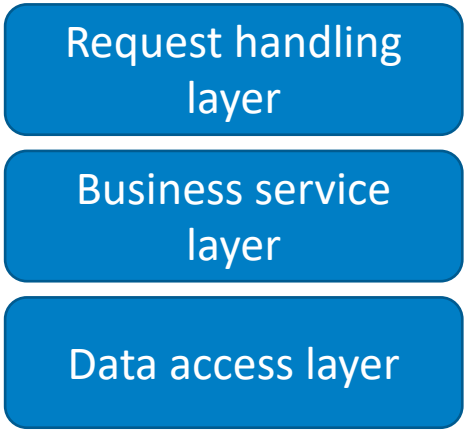
Migrations-strategi fra DGWS til IDWS XUA



1. Nye nationale services på sundhedsområdet udstilles kun med IDWS XUA
2. Eksisterende nationale services tilbydes opkobling via IDWS2DGWS proxy
   - Proxyservices udfases ved migrationsperiodens afslutning.
   - Serviceudbydere, der ikke ønsker proxy, skal etablere en IDWS indenfor 18 mdr.
3. Fagsystemer indenfor sundhedsområdet (fx EPJ, EOJ og LPS) får en lang tidsfrist (6 år) til gennemføre at skriftet fra DGWS til IDWS.

Kan man gøre noget allerede nu?

- Hvis man ikke allerede har separat kode, der tager sig af håndtering af protokol og dataformat, kan man forberede sin service på nye standarder ved at separere denne kode ud i et eget lag. Herved vil det være lettere at køre med duale snitflader (DGWS og IDWS XUA) en periode og udfase den gamle DGWS snitflade senere.



Next step

- IDWS XUA profil, værktøjer og infrastrukturkomponenter skal færdiggøres og tilrettes ud fra de erfaringer man har opnået i pilotprojekterne.
- Tilrettet profil skal forelægges RUSA med henblik på optagelse som anbefalet national standard.
- Migreringsstrategi skal forelægges den nationale bestyrelse for sundheds-it
- Migreringsprojekt skal finansieres og igangsættes
- Målbillede for sammenhængende brugerstyring på sundhedsområdet (beskrivelse af en national sundhedsføderation og dennes sammenhæng til andre føderationer) skal færdiggøres og forelægges RUSA og den nationale bestyrelse sammen med et oplæg til identitetssikringsniveauer på sundhedsområdet

Next step (2)

- Implementeringsprojekt (sammenhængende brugerstyring) skal finansieres og igangsættes
  - I første omgang dækkes kun XML-baserede standarder (sundhedsområdets profileringer af OIO SAML og OIO IDWS)
  - Tilretning af eksisterende infrastrukturkomponenter (kald af andre infrastrukturkomponenter, omveksling af tokens etc.)
  - Føderationsaftaler, politikker og governance skal på plads
  - Stært ønske blandt nogle parter om, at dette kommer på plads inden NemID og NemLogin udskiftes

- Profiler, værktøjer og infrastruktur til understøttelse af mobile apps og mikroservices skal udvikles og afprøves
  - Er besluttet igangsat af den nationale bestyrelse for sundheds-it (IDWS del 2)
  - Foreløbig er gennemført en analyse af tre internationale profileringer af sikkerhedsstandarden OAuth2
  - Afprøvning af medicinallergiservice baseret på HL7's nyeste FHIR-standard
  - Skal gerne medvirke at få en generel infrastruktur på plads, der understøtter services baseret på FHIR (skal skaleres fra pilotbrug til storskala anvendelse)

Spørgsmål ?