Sikkerhedsmodeller på sundhedsområdet

eSundhesobservatoriet 3. oktober 2018

En par indledende bemærkninger

- Sikkerhed er mange ting
  - Hvordan sikrer vi at data ikke forvanskes?
  - Hvordan sikrer vi at data ikke forsvinder?
  - Hvordan sikrer vi at data er tilgængelige, når der er brug for dem?
  - Hvordan sikrer vi at data ikke kommer uretmæssige i hænde / misbruges?

- Hvornår er rette tidspunkt at adoptere ny teknologi?
  Tidlig adoption giver tidlig udnyttelse af teknologiske muligheder, men rummer også en række risici:
  - Teknologi indeholder ”børnesygdomme” (f.eks. manglende skaleringsevne)
  - Teknologi stadig i forandring (kræver mere vedligeholdelse)
  - Teknologi udkonkurreres af andre teknologier (support og vedligehold stopper)
  - Teknologi understøttes af få parter (leverandørafhængighed, sårbarhed)
  - Vanskelig at implementere i effektiv daglig brug

Agenda

- Fokusområder ved digitaliseringen af sundhedsvæsenet
- Hvor kom vi fra sikkerhedsmæssigt og hvor er vi nu?
- Hvad er den fremtidige retning?

Fokusområder ved digitaliseringen af sundhedsvæsenet

- Det sammenhængende sundhedsvæsen
  - Mulighed for at tilgå de samme oplysninger
  - Koordinering af indsats
  - Lette kommunikation

- Borgeren som aktiv partner
  - Overskuelighed og gennemskuelighed
  - Deling af informationer
  - Understøtte kommunikation og dialog
  - Varetagelse af ønsker og rettigheder

- Det datadrevne sundhedsvæsen
  - Big-data analyse
  - Prædiktionsmodeller
  - Beslutningsstøtte

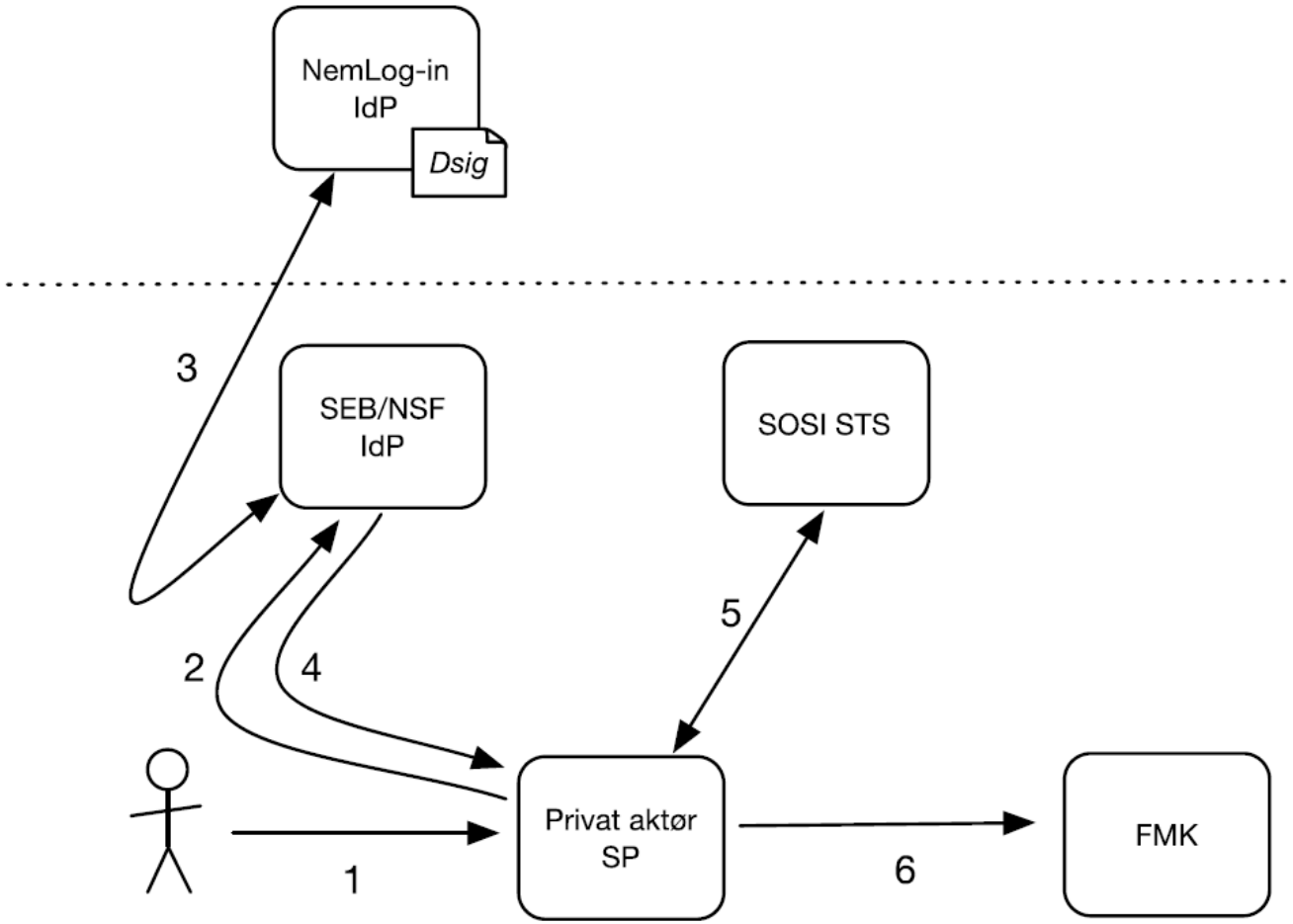
Lidt historie

- Før midt 00'erne blev der kun tilgået data opbevaret af egen organisation (og som egen organisation var ansvarlig for).
- Der kunne videregives (kopi) af data til andre parter.
- Store organisationer på sundhedsområdet konsoliderede brugerstyring omkring valgte Identity Management (IM) løsninger
- Man prøvede fejlagtigt at overføre disse løsningsmodeller til nationalt plan
- Der var i stedet brug for sikkerhedsmodeller, der understøtter at brugere i en organisation kan tilgå data der opbevares af en anden organisation
  - Sundhedsloven blev ændret
  - Der blev udarbejdet sikkerhedsmodel til FMK baseret på fælles OCES politikker
  - Der blev udarbejdet en referencearkitektur for informationssikkerhed
  - Analyse af sikkerhedsstandarder pegede videre ad denne vej
- Man er også fællesoffentligt begyndt at gå i denne retning (NSIS, nyt Nem-ID for erhverv)

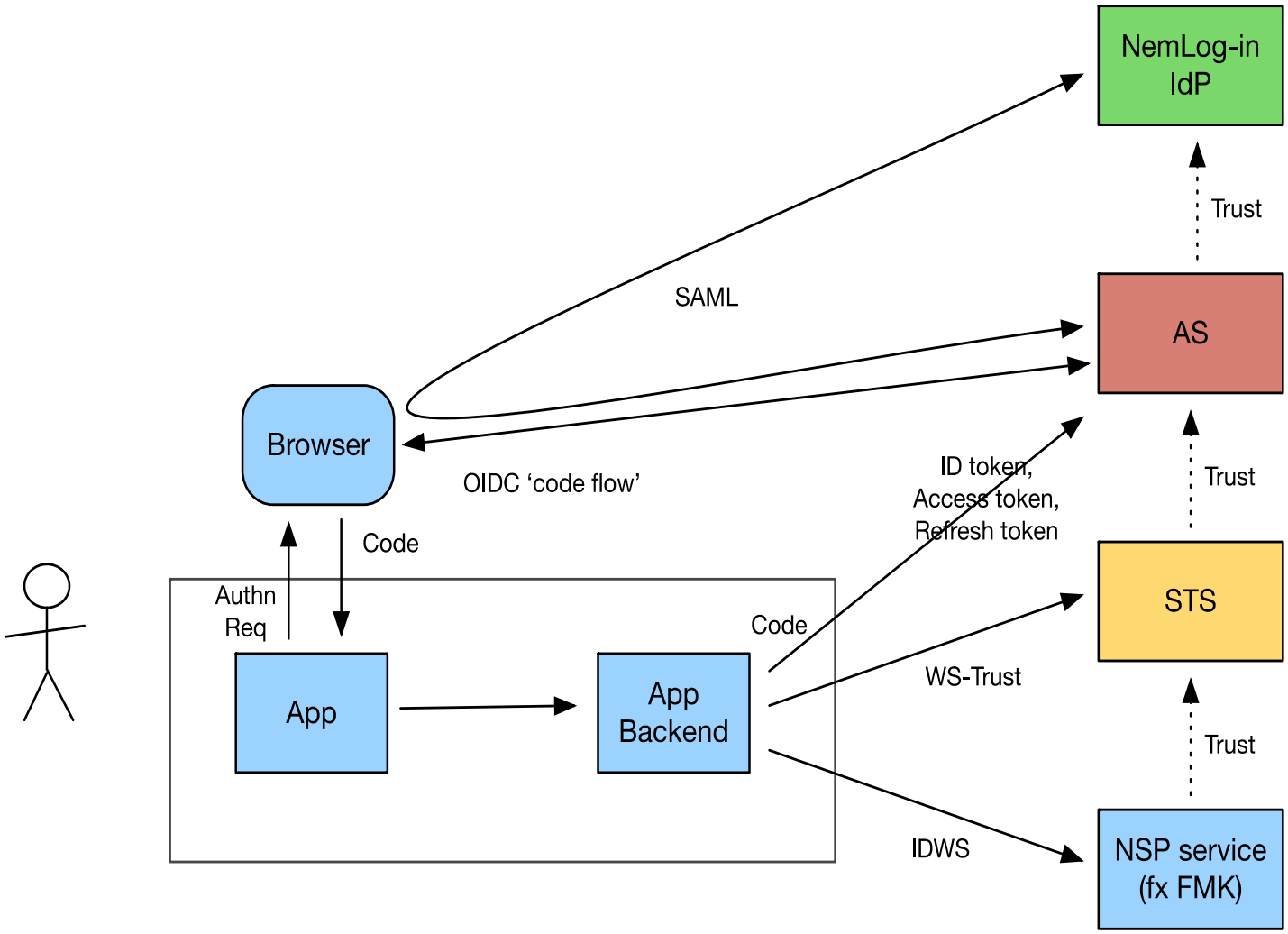
Eksempler på sikkerhedsteknologi der anvendes på sundhedsområdet i dag

- Digital signatur er udbredt for medarbejdere
- Borgere benytter NemID
- Stærk autentifikation / identifikation af brugere (baseret på signatur)
  - Borgere på sundhed.dk og apoteksportaler
  - Borgere fra apps (Medicinkortet)
  - Sundhedspersoner på sundhed.dk
  - Sundhedspersoner i fagsystemer, der tilgår nationale tjenester (f.eks. Fælles Medicinkort)
- Systemer autentificeres og forbindelser krypteres gennem brug af signaturer (FOCES / X.509 certifikater).

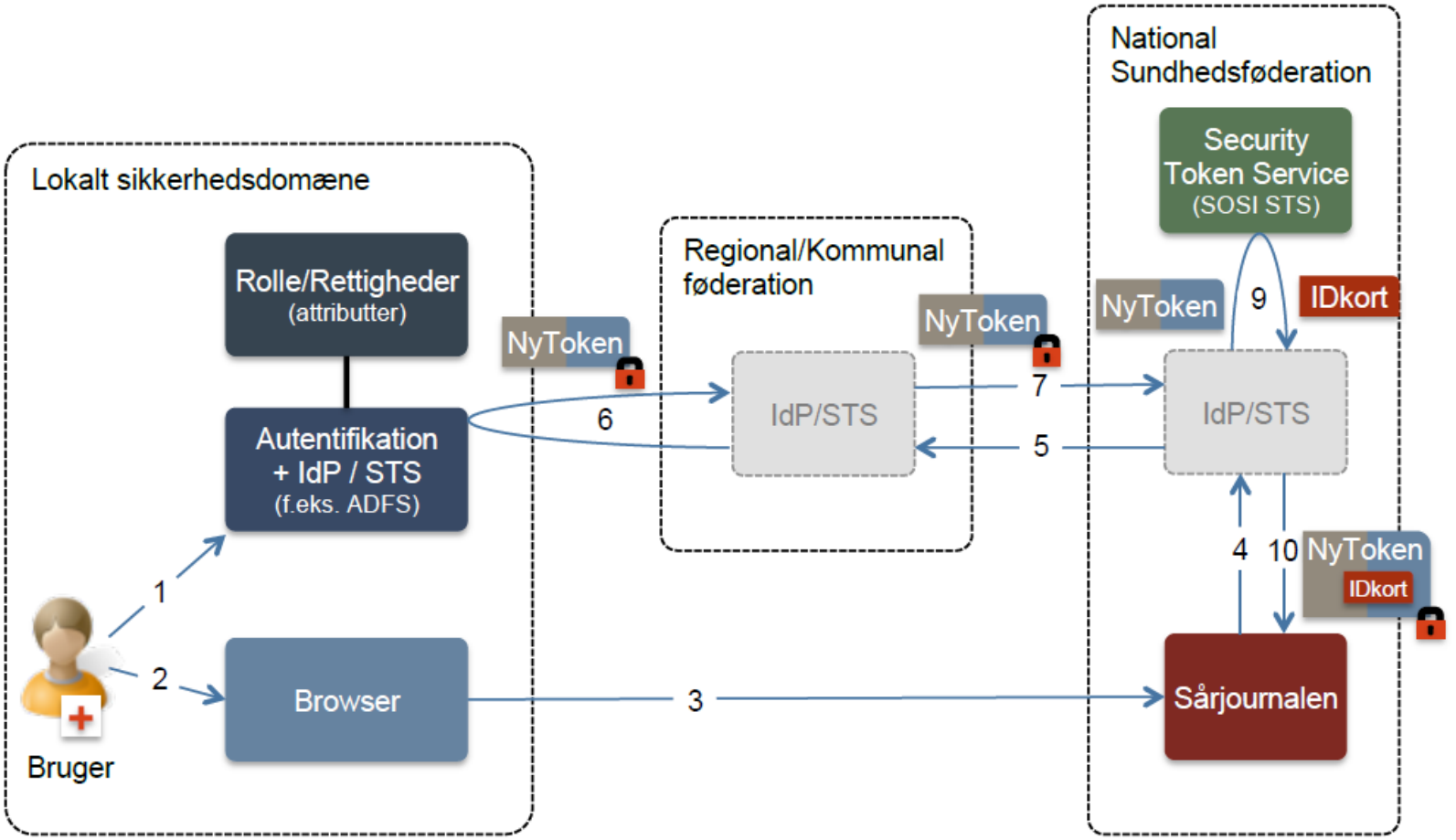
Eksempel: Web-apoteker (og lægepraksis)



Eksempel: Medicinkort-app (og Min Læge app)



Eksempel: Sårjournal (og FUT)



SUNDHEDSDATA-
STYRELSEN

Hvad arbejdes der mere på?

- Modernisering af SOAP standarder, så disse både dækker borgere og sundhedsprofessionelle (igangværende projekt)
- Udarbejdelse af REST / FHIR standarder, så disse både dækker borgere og sundhedsprofessionelle (projektgrundlag godkendt af national bestyrelse)
- Projekterne rummer såvel specifikation af standarder, som tilretning af understøttende værktøjer samt nødvendige ændringer til infrastruktur.
- Ovenstående afprøves i praksis i piloter.
- Der udarbejdes en samlet referencearkitektur for web tjenester (opgavebeskrivelse godkendt i det rådgivende udvalg på sundhedsområdet, RUSA)

Observationer

- Sikring af brugerens identitet overfor tjenester har hidtil haft større fokus end privatlivsbeskyttelse
- Trusselsbilledet ændres i takt med at
  - Flere data opsamles og gemmes, herunder meget følsomme data (genomdata etc.)
  - Platforme konsolideres (RKKP, SDP etc.)
  - Hackerangreb intensiveres
  - etc.

Initiativer rettet mod privatlivsbeskyttelse

- Der arbejdes i dag med forskellige former for pseudonymisering af data (dog ikke efter en fælles ramme)
- Et tidligere fællesoffentligt oplæg vedr. ”annonyme akkreditiver” ønskes undersøgt som teknologi til sikker lagring og anvendelse af personoplysninger (Proof of Concept). Oplæg er ved at blive beskrevet.
- Projekter, der vedrører privacy og Big Data følges med interesse.
- Der er ved at blive beskrevet et oplæg til initiativ under den nationale cybersikkerhedsstrategi på sundhedsområdet, der skal operationalisere kravet til Privacy-by-design og Privacy-by-default, herunder
  - revidere referencearkitektur for informationssikkerhed på sundhedsområdet
  - se på understøttende rammeværk, standarder og værktøjer.

Privatlivsbeskyttende teknologier

Teknologi	Kort beskrivelse	Eksempler	Modenhed
Standard Encryption	Kryptering baseret på gængse signerings- og krypteringsalgoritmer (DSA, RSA, 3DES, AES etc.).	Hardware Security Modules (HSM), Intel SGX	I brug utallige steder.
Anonymous Credentials	Pseudonymisering baseret på avancerede signatursystemer	Microsoft U-Prove IBM Identity Mixer	Teknologisk modent, men ikke kommercielt
Differential Privacy	Avanceret anonymisering af data	Apple, Google benytter det i visse cases.	Teknologisk modent, men med få cases i praksis.
Secure Multiparty Computation (MPC)	Beregninger på avanceret kryptering af data	Sharemind	Teknologisk modent og begyndende kommercialisering
Fully Homomorphic Encrytion	Beregninger på krypterede data (anden model)		Kun teknisk modent i version til simple beregninger

Proof of Concept:
Anonyme-, kontekstafhængige akkreditiver

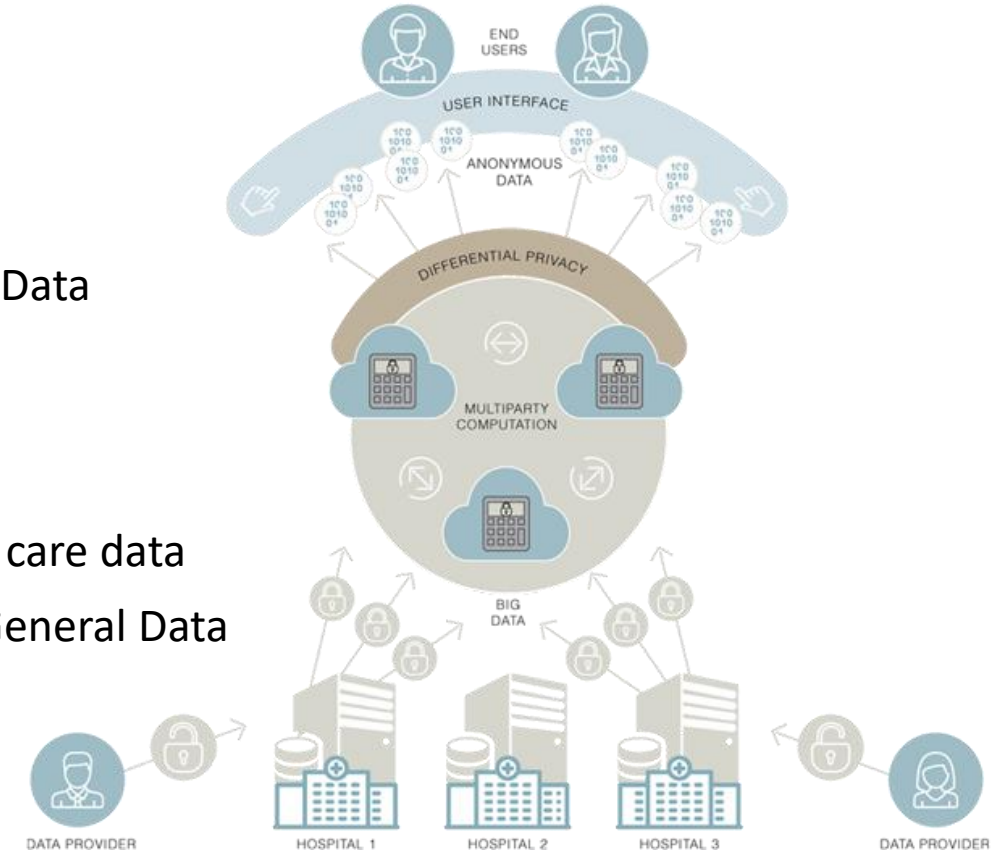
- Anvise hvordan teknologi kan tages i anvendelse for at løse privacy-udfordringer med centrale databaser/registre
- Anvise en vej fra den nuværende situation til den ønskede situation
- Anvise, hvordan ny teknologi kan integreres med eksisterende (SAML/IdP, WS-TRUST/STS, OAuth2/OIDC/AS)
- Anvise hvordan der kan mitigeres for risici vedr. leverandørafhængighed og manglende markedssupport

SUNDHEDSDATA-STYRELSEN

SODA-projektet

Scalable Oblivious Data Analytics

- EU funded project 2017-2020
  https://www.soda-project.eu/
- Privacy-preserving analytics on Big Data
- Using advanced chryptology
  - Multiparty Computation
  - Differential Privacy
- Demonstrate techniques on health care data
- Showing easier compliance to EU General Data Protection Regulation (GDPR)



SUNDHEDSDATA-STYRELSEN

Konklusioner

- Den aktuelle vurdering af trusselsbilledet sammenholdt med fælleseuropæiske krav om databeskyttelse (GDPR) nødvendiggør større fokus på privatlivsbeskyttelse
- Den nuværende fødererede sikkerhedsmodel har været under opbygning siden midt 00'erne og den udvikler sig stadig. Der er mulighed for at styrke privatlivsbeskyttelsen også indenfor det eksisterende teknologivalg.
- Den teknologiske udvikling giver løbende nye muligheder for at beskytte information og Sundhedsdatastyrelsen følger til stadighed med i udviklingen.
- Ny teknologi tages ind og bliver en del af de nationale rammer for løsninger, når teknologien har vist sig tilstrækkelig anvendelig og moden.