Sikkerhed i RA

KOMBIT
Kommunernes it-fællesskab

Sikkerheds områder

- Behovsafklaring / Lov
- Governance
- Adgangskontrol
- Autentifikation
- Databeskyttelse
- Logning
- Tilgængelighed
- Uafviselighed

Fremgangs metodik

- I Q4 2012 -> Q1 2013 særligt fokus på systemkomplekset ifm udbud
- I Q2 2013 Review hos kommuner og leverandører
- I Q2 – Q3 2013 Færdiggørelse af kravspecifikation
- Q3 2013 Udbud

KOMBIT
Kommunernes it-fællesskab

Om modellen

Sikkerhedsmodellen

- fremlægges ikke til beslutning, men til orientering
- skal i review med kommuner og leverandører

Grundlæggende parametre for sikkerhed

- Authentifikation: Sikkerhed for at du er den du siger du er
- Authorisation: Hvad har du lov/rettighed til at gøre/se

Model udarbejdet i samarbejde med PWC, Silverbullet og IT-Crew

- Model for opbygning af Infrastruktur for adgangskontrol
- Model og krav for rettighedskontrol

Hvad skal sikres?

Confidentiality

- at oplysninger kun er tilgængelige for authoriserede brugere/systemer

Integrity

- at oplysninger ikke bliver ændret utilsigtet

Availability

- at systemer og oplysninger er tilgængelige

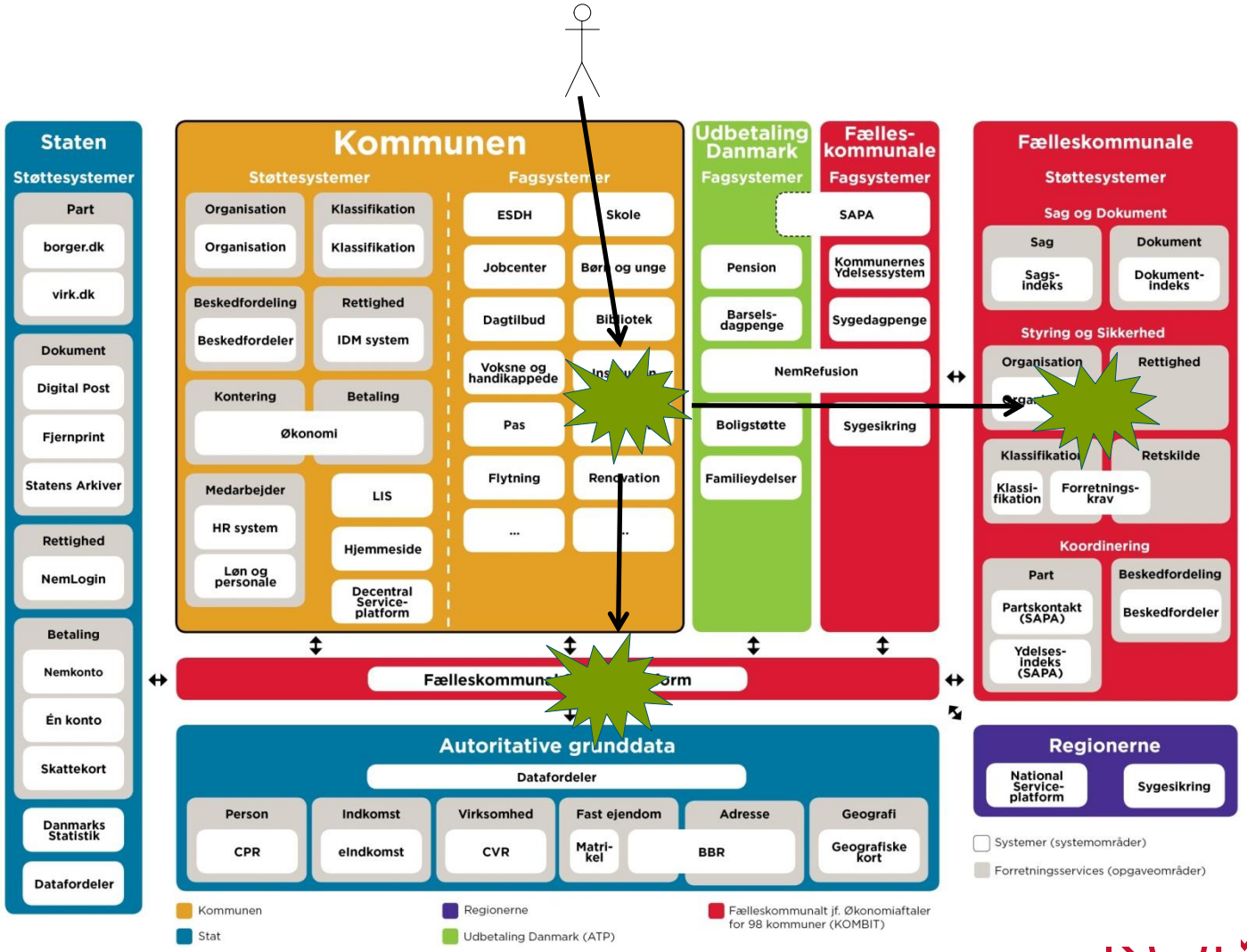
Uafviselighed

- at en bruger ikke kan afvise at have udført en handling

Hvad er udfordringerne?

- Kommunen er ansvarlig for egne opgaver og egne data jf. forvaltningsloven
- Mange personfølsomme oplysninger
- Løskoblede systemer fra forskellige leverandører
- Den samme fysiske person kan have mere end en stilling

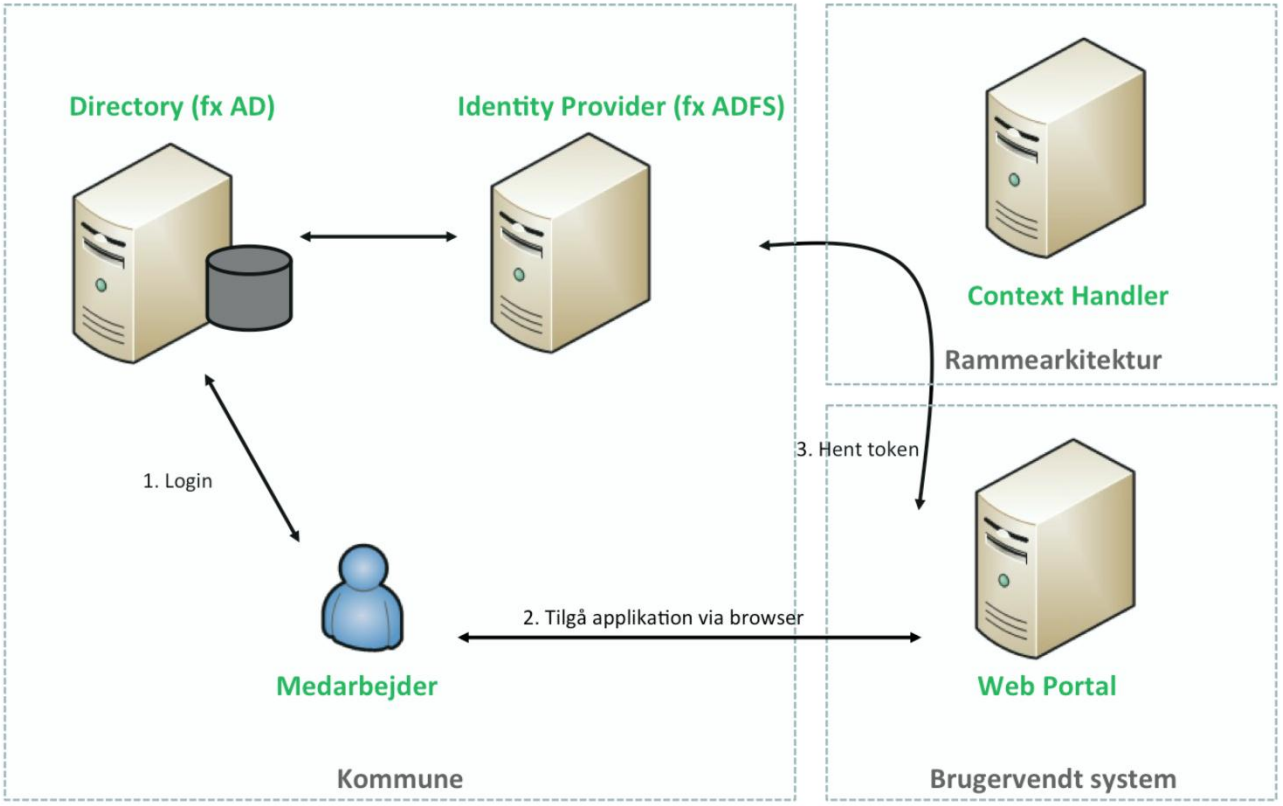
2 sikkerhedsmodeller i 1



PwC

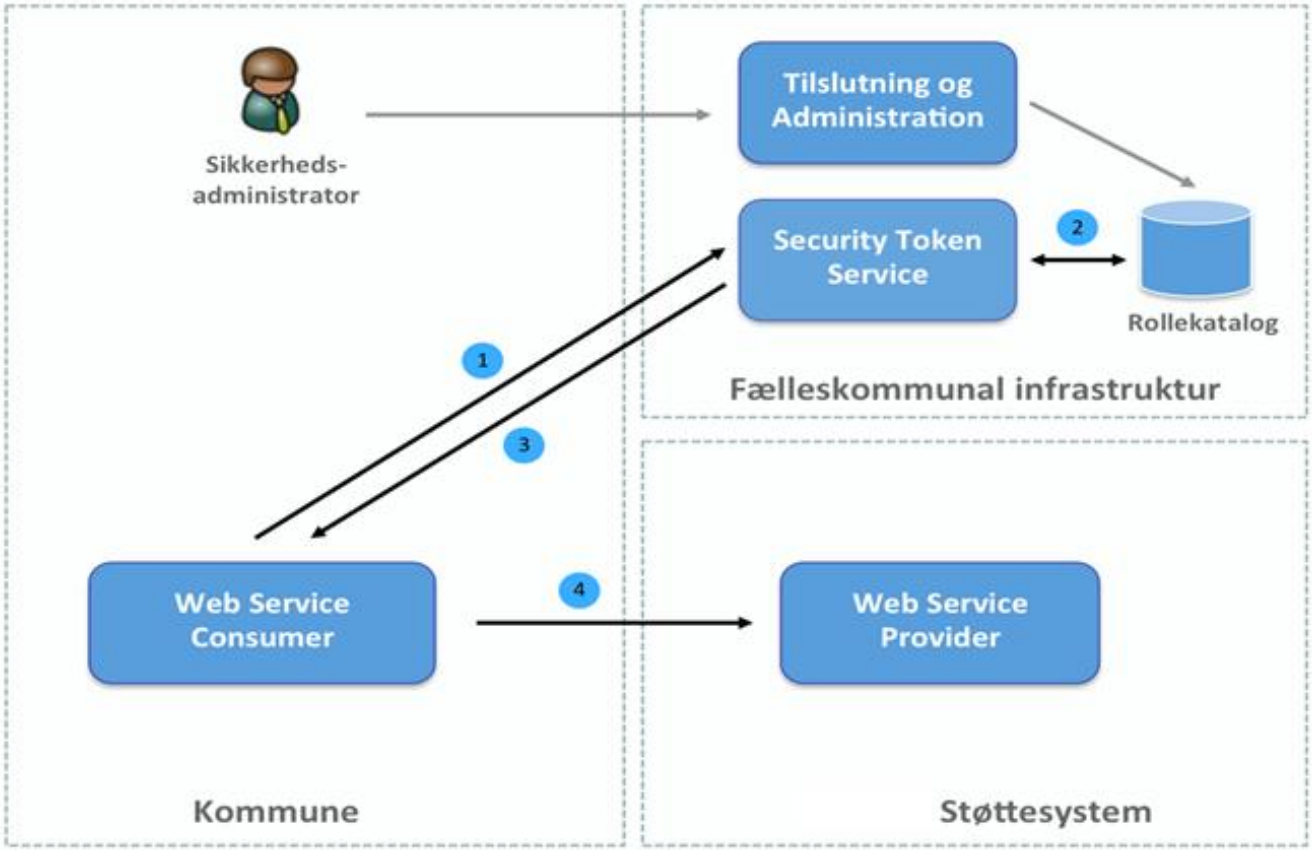
KOMBIT
Kommunernes it-fællesskab

Bruger til System



KOMBIT
Kommunernes it-fællesskab

System til System



KOMBIT
Kommunernes it-fællesskab

Tak for opmærksomheden

KOMBIT

Kommunernes it-fællesskab

Eventuelt

KOMBIT
Kommunernes it-fællesskab

Forskellige rettighedsmodeller

Støttesystemer

- Anvendersystem authoriseret til systemet (foces)
- Alene kontrol på at bruger er authentificeret (til logning)
- Anvender føderationsservice som authentifikation
- Evt. simpel rettighedskontrol på forespørgsel, eks. ud fra KL-E

Fællesudbudte systemer

- Anvender føderationsservice som authentifikation
- Anvender støttesystemer til authorisation
- Fælles roller for samtlige kommuner pr. fagområde

Systemer i øvrigt

- Anvender føderationsservice som authentifikation
- KAN anvende støttesystemer til autorisation, vurderingssag!

Behovsafklaring / Lov

- Afdækning af lovkrav
- Persondata lov
- ISO 27001/DS484
- EU-regulering – f.eks. vedrørende e-tilgængelighed
- Anbefalinger fra diverse myndigheder
- mv

- Risiko analyse
- afdækning af trusler
- prioritering af disse

- Arkitekturprincipper for sikkerhed (Opsamling af sikkerhedsområder)
- Princip
- Rationale
- Implikation

Governance

Governance-model for informationssikkerhed

- KOMBIT
- Governance-model for informationssikkerhed
- Kravstilling og indkøb
- Forvaltning

- Leverandører
- Processer for overvågning af driftsleverandører
- Governance-krav til driftsleverandører
- Governance-krav til udviklingsleverandører

- Sikkerhedsprocesser og krav for Kommuner
- Roller og ansvarsfordeling
- Styringsprocesser
- Standard for dokumentation.

Databeskyttelse

- Afklaring af klassifikationer
- Dataklassifikation
- Systemklassifikation (evt baseret på kritikalitet)

- Håndtering af databeskyttelse under:
- Lagring.
- Transport.
- Anvendelse.

Logning

- Fælles standard for logningsdata
- Krav til indholdet af logningsdata
- Tidsmæssig synkronisering på tværs af systemer for at muliggøre sammenstilling
- Krav til fælles rapporteringsformater

- Sammenstilling af logs? (Log Indeks)
- Samling af loginformationer
- Mulighed for at søge på sammenstillede logdata

- Automatiseret overvågning
- Overvågning automatiseres til at analysere brugsmønstre og alarmerer ved anormalitet.

Tilgængelighed

- Point-in-time recovery (PITR)
- Backup/Recovery – herunder PIT
- Fysisk sikkerhed, dublerede driftscentre, dubleret infrastruktur
- SLA om performance, oppetid mv.
- Overvågning, intrusion detection/prevention, beskyttelse mod denial of service (DoS)-angreb.

- Datakorruption over tid.
- Overvåge datakvalitet løbende
- Optage transaktioner og genafspille dem (når systemet er bragt tilbage i en ukorrumperet tilstand)