SDFI

FORBEDRING OG EFFEKTIVISERING AF SIKKERHED

Moderniseret Datafordeler

Dato: 18. September 2023
Version: 1.0
Forfatter: Marcus Quistgaard og René Ravn
Kontakt: mwq@netcompany.com, rra@netcompany.com

netcompany

Agenda

- Sikkerhedszoner
  - Zonerne før og efter transitionen
  - Vision om en sammenlagt zone
  - Migrering fra *as-is* til *to-be*
- Autentifikation
  - Hvordan fungerer det i dag.
  - Vision om et moderne auth flow
  - Vision om en mere granulær sikkerhedsmodel
  - Migrering fra *as-is* til *to-be*
- Brugerstyring
  - Hvordan ser det ud i dag.
  - Vision om moderne brugerstyring
  - Migrering fra *as-is* til *to-be*

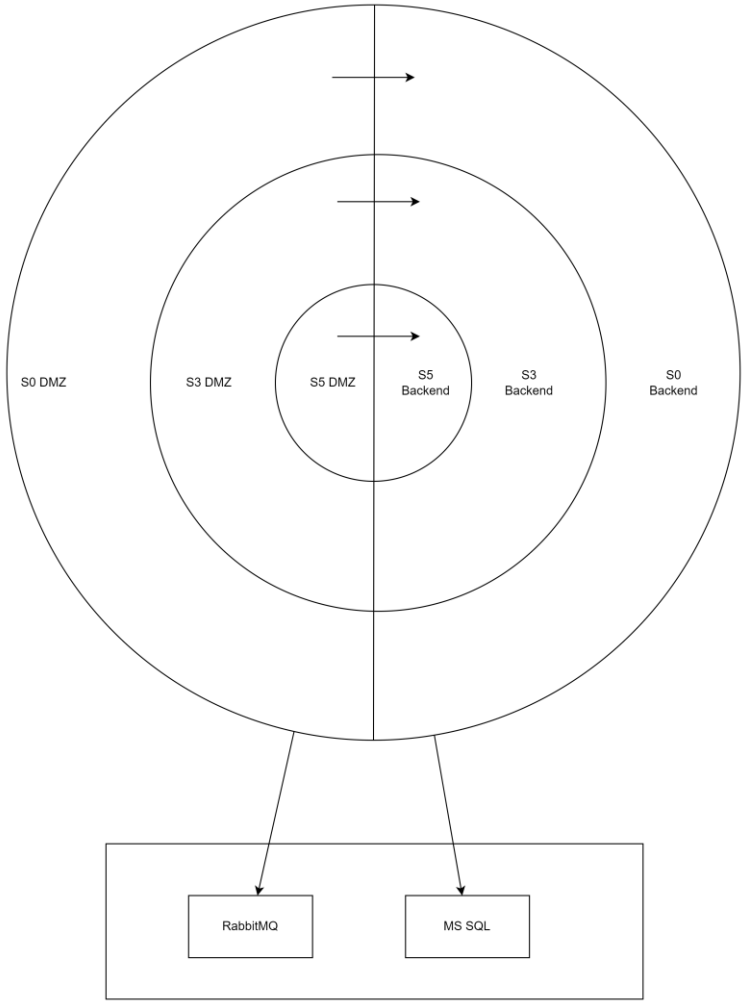
SIKKERHEDSZONER

Sikkerhedszoner

- Zone 0 og zone 5.
  - Frit tilgængelig data vs. data som kræver tilladelse.
- Indlæsning skal foregå til begge zoner.
  - Data kan være out-of-sync under indlæsning
- S0 og S5 er samme applikation med forskellige konfiguration
  - IP Whitelisting styres i firewall

Oprindeligt sikkerhedszoner

- Det oprindelige design var inddelt i 3+1 zoner.
  - Hver zone bestod af et antal dmz zoner og et antal backend zoner.
  - Kald tilladt mellem S5 -> S3,S0 og S3 -> S0 via load balancer
  - Intern trafik i zoner uden begræsninger
- Rabbit MQ anvendes til at sende beskeder mellem zoner.
- AD og AD FS anvendes på tværs og bruges som samlende brugerstyring i S0.



Sikkerhedszoner

Under transitionen er zonerne samlet til én DMZ-zone, en applikations-zone, og en database-zone.

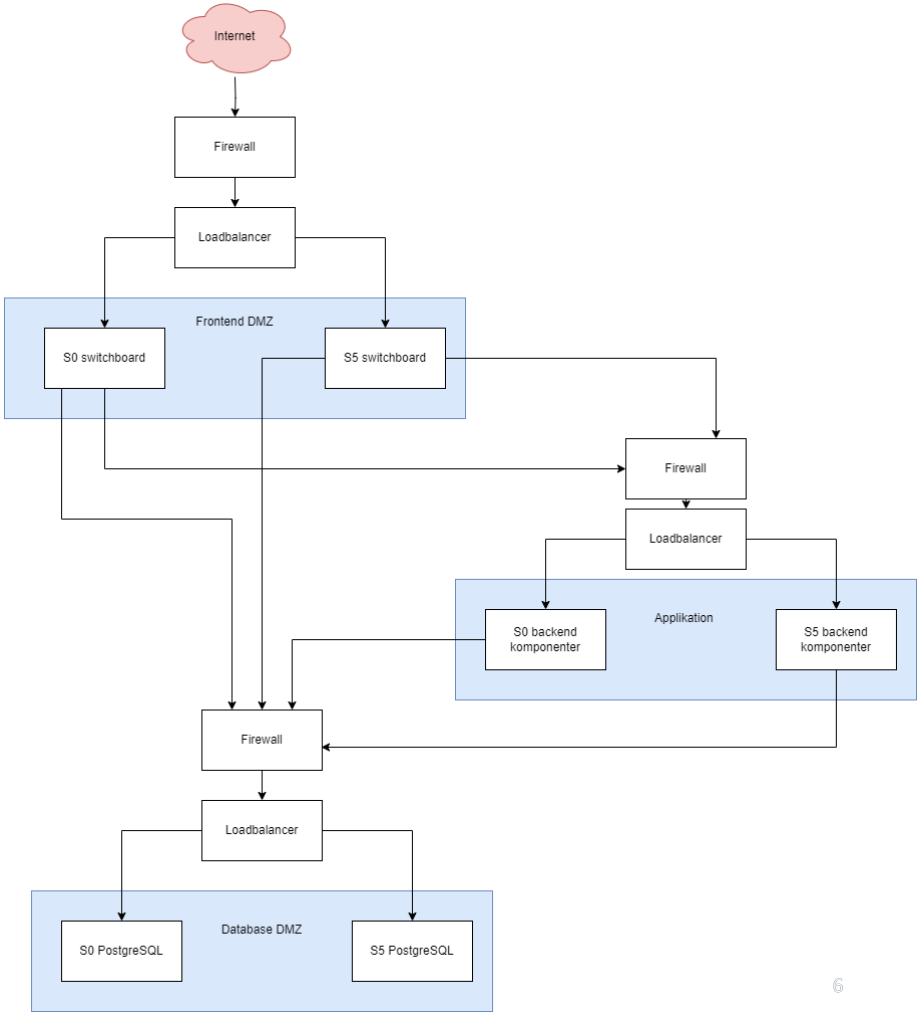
- Alle servere anvender lokale firewalls.
- Der er kontrol med hvilke komponenter kan kalde hinanden, og alt skal foregå igennem zonernes loadbalancer og firewall.
- På et netværks-zone niveau er S0 og S5 lagt sammen.

Web og Tjenestebrugere for S0 og S5 stadig samlet i ét AD

- Selvbetjeningsportal i S0 administrerer brugere i både S0 og S5.
- IP-whitelisten tilføjes for at tilgå S5.

Filudtræk afvikles altid fra S5.

- Flytter data til S0 SFTP eller S5 SFTP. Samme IP-whitelist for S5 samt ssh nøgle.



Sammenlægning af sikkerhedszoner

- Ingen opdeling i zoner fra brugernes perspektiv. Alt data skal være ”sikkert”.
- Dermed reduceres data duplikering da alt data vil ligge i samme datazone.

  Den hardware som frigives ved at fjerne zone 0, kan bruges til at håndtere den nu samlede zone.
- Hurtigere indlæsning fordi indlæsning kun skal foregå i en enkel zone.
- Det vil være en enkel applikation som kan tilgå alt data, i stedet for en S0-app og en S5-app.
- Sammenlægningen skal gå hånd i hånd med en samlet sikkerhedsmodel med mindre risiko for fejldistribution af data.

Adgangskontrol til den samlede zone

- Mulige løsninger for fremtidig adgangskontrol:

  A: IP-whitelisting sker på domæne niveau.
  For anvendere vil dette være præcis som i dag. Bagved skal de moderne tjenester kunne skelne hvilket domæne kaldet kommer fra, så adgang til "S5" data fra det "usikre" domæne ikke tillades.

  B: IP-whitelisting sker på tjenestebruger niveau.
  Muliggør ingen nye brugsmønstre for anvendere, men tillader sammenlægning af zoner uden domæne differentiering.
  Registrene vil have klarere indblik i anvenderes adgange.

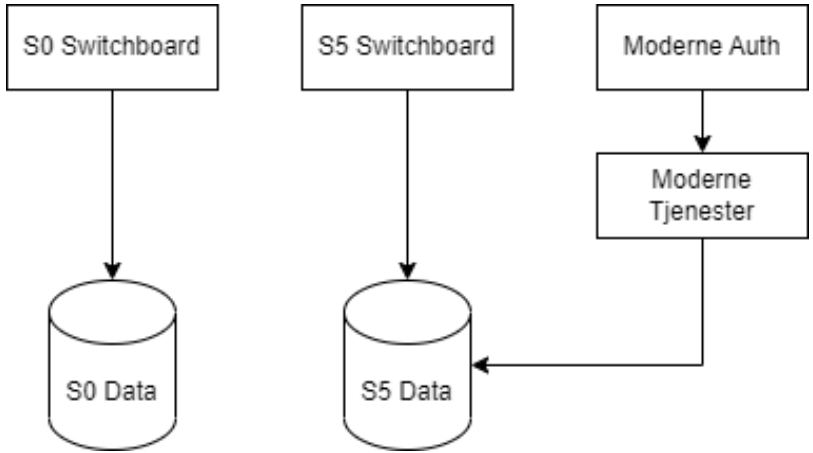
  C: IP-whitelisting afskaffes fuldstændigt.
  Hvis en anvender har fået godkendt adgang til CPR, har de denne adgang fra alle IP'er. Dette vil tillade adgang for kommunale ansatte som arbejder hjemmefra uden VPN, mobile apps, osv.

Migrering ift. sikkerhedszoner

- Hvordan undgår vi at skulle have data liggende i ”3 zoner” under paralleldriften?

  Dvs. S0, S5, og den nye samlede zone indtil det gamle bliver lukket.

- Vi ser følgende migreringsvej:
  1. S5 ”redefineres” til at være den samlede zone.
  2. Implementer moderne tjenester som gør brug af et moderne standard autentifikations flow. Tilgår udelukkende den samlede zone.
  3. S0 zonen og databaser fjernes når de gamle S0-tjenester udfases.
- Serverkapaciteten i S0 kan løbende distribueres til der hvor det er relevant.



AUTENTIFIKATIONS FLOW

Autentifikation og autorisation

Autentifikation - Hvem er brugeren i den anden ende og hvor sikker er vi på at det er den brugeren udgiver sig for at være.

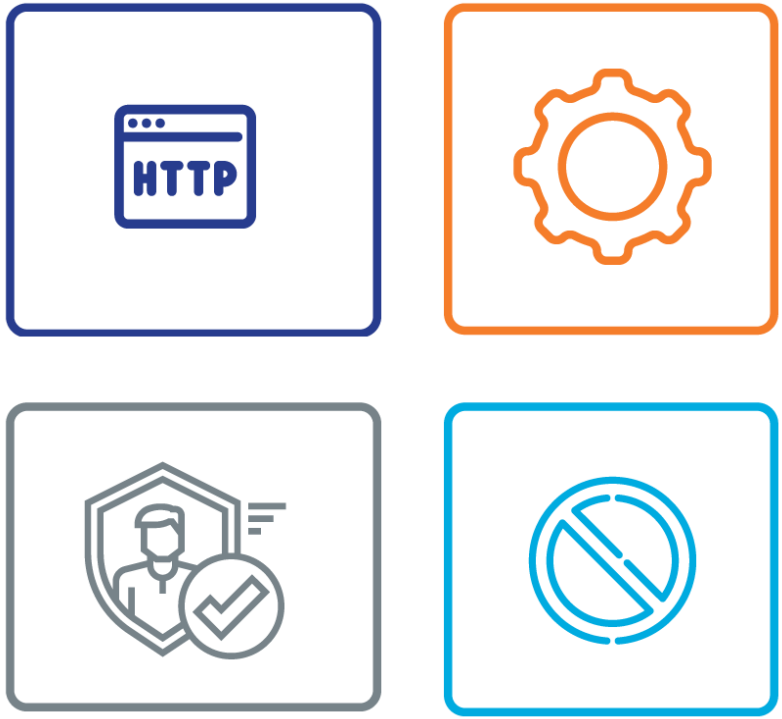
- MitID
- Brugernavn/Password
- Domæne login ala SIT.
- Google/Facebook/etc. Login

Autorisation – Givet brugerens rettigheder, må brugeren udføre den ønskede handling. Må en bruger :

- Hente oplysninger (tabeller, rækker eller felter)
- Opdatere rækker

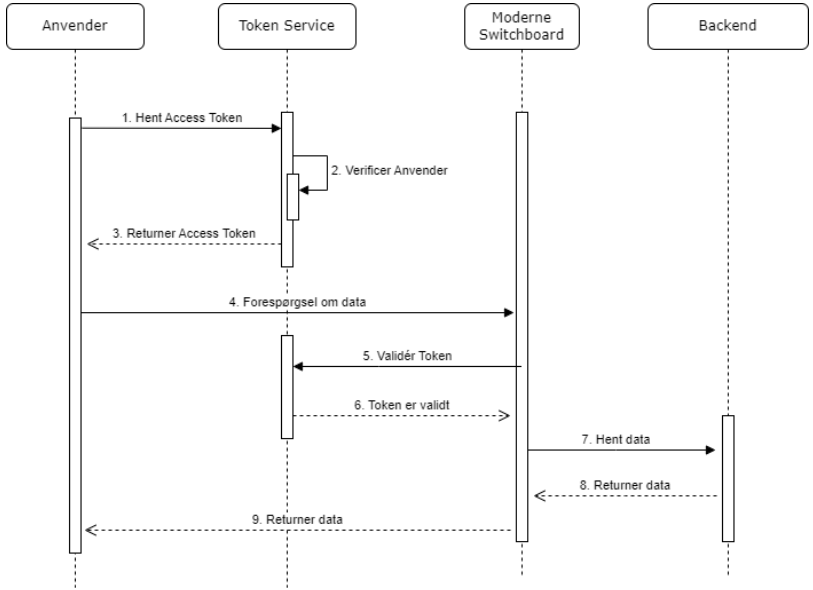
Det nuværende auth flow for tjenester

- Autentifikation er implementeret af Datafordeleren ved hjælp af et custom login flow som gør brug af standardprogrammel.
- Adgang håndhæves på tjenesteniveau.
- Auth muligheder for tjenester:
  - Anonym adgang over http og https
  - Username/password til S0 via https
  - Certifikater til S0 og S5 via https
  - *Herudover kan anvendere få et SAML2 token udstedt af ADFS via en af ovenstående auth muligheder, og så bruge det token i senere kald til alle tjenester.*
- Auth muligheder for filudtræk:
  - FTP anonym adgang til offentlige filudtræk
  - SFTP username/password til brugerdefinerede S0 filudtræk
  - SFTP SSH-nøgler til S0 og S5 filudtræk
  - HTTP anonym adgang til offentlige filudtræk



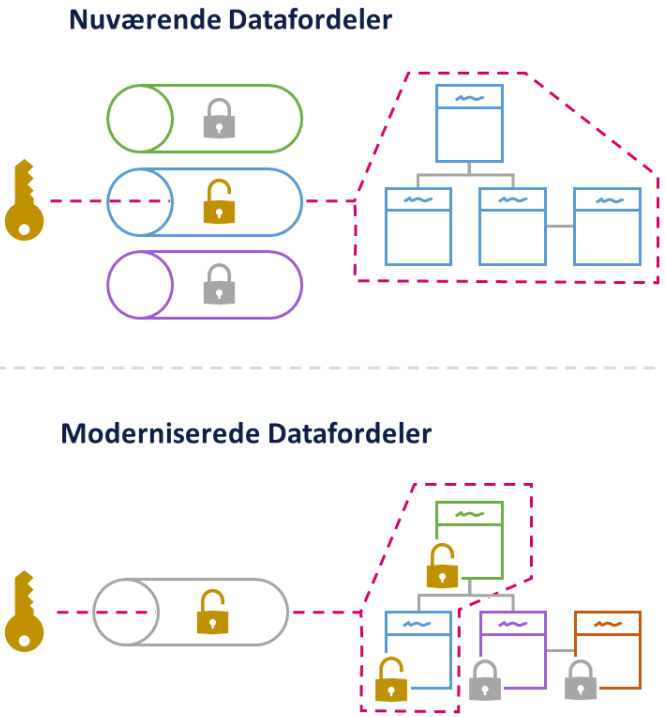
Anvendelse af Standard Autentifikation flow

- Anonym adgang skal fjernes, og https skal være påkrævet.
- Overgang til standard token-baseret adgangskontrol for samtlige anvender-vendte tjenester.
  - Standard protokol som OAuth2, OpenId og lign.
  - Ved brug af tokens kan f.eks. online kort-tjenester uddelegere adgang til deres brugere uden at give dem deres tjenestebruger password.
- Adgangsbegrænsning ved udstedelse af tokens
  - IP-whitelisting kan evt. håndhæves kun ved udstedelse af tokens, ikke ved brug.
  - Hvis krav om brug af certifikater i stedet for user/pass for brugere med adgang til sikker data skal bibeholdes kan dette evt. håndhæves ved udstedelse af et token, men derefter bruges der udelukkende tokens.
- SFTP adgang vil fortsat understøtte user/pass og ssh-keys
  - Anonym adgang til FTP fjernes



EN MERE GRANULÆR SIKKERHEDSMODEL

En mere granulær sikkerhedsmodel



- Fremadrettet vil sikkerhed foregå på enten entitet-niveau og eventuelt på felt-niveau.
- Håndhævelse af sikkerhed vil ske i de komponenter som udstiller data til anvendere.
  - *Håndhæves dermed ikke på databaseniveau*
- Går hånd i hånd med moderne opslagslogik hvor anvendere selv kan specificere hvilke felter de ønsker at modtage.
  - Anvendere som forespørger felter/entiteter de ikke har rettighed til at se, afvises inden kaldet udføres.
  - Ligeledes er fjernelse af indhold på felter som anvender ikke har adgang til ikke tilladt – CPR m.f.

Navne- og adressebeskyttelse i den granulære sikkerhedsmodel

- Ved en entitet-baseret sikkerhedsmodel vil det være oplagt at designe to CPR-Person entiter varianter som adgang kan godkendes til:
  - *Personer uden gældende navne- og adressebeskyttelser†*
  - *Personer, inklusiv dem som har gældende navne- og adressebeskyttelser*
- Ved en felt-baseret sikkerhedsmodel vil denne type begrænsning nok ikke være en del af felt-adgangen, men tilføjet som en selvstændig rettighed der kan begrænse data i besvarelsen.

† Eller som har beskyttelser men er udrejst, forsvundet, osv. jævnfør CPRs regler.

Hvordan mener I sikkerhedsmodellen skal granuleres?

Hvad synes I giver mest mening?

- Håndhævelse på felt-niveau?
- Håndhævelse på entitet-niveau?

Granulær sikkerhedsmodel fortsat

- Felt-niveau er mest fleksibel, men giver en stor adgangsmatrice, både for anvender og register.

  Herudover vil det være nødvendigt at lægge yderligere styring ovenover for at håndhæve ikke-felt-baserede begrænsninger (såsom CPR beskyttelser, og evt. GDPR krav).

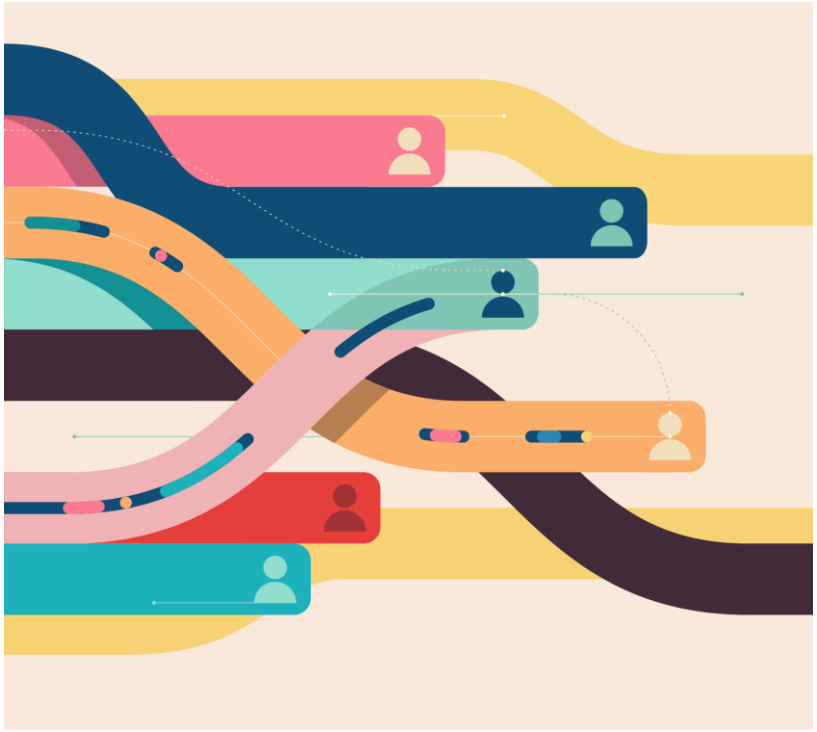
- Entitet/tabel niveau er bedre end hvad DAF kan i dag, men er ikke lige så fleksibel.

  Dermed kan alle potentielle anvender-ønsker ikke umiddelbart efterkommes.

  Hvis alle anvender-ønsker skal efterkommes kan det foretage en eksplosion af entiteter, og så ville en felt-model have været simplere i det lange løb.

	Marcus	Rene	Andreas
CPR.navn			
CPR.personnummer			
BBR.*			
DAR.*			

Migrering ift. auth flow og sikkerhedsmodel



- De moderne tjenester vil udelukkende understøtte *moderne* token authentication og bruge den nye granulære sikkerhedsmodel.
- Anvendere er dermed nødt til at blive oprettet i den nye model hvis den moderne auth hvis de vil bruge de nye tjenester.
- De gamle tjenester vil fortsat understøtte eksisterende tjenestebruger-auth indtil disse lukkes

BRUGERSTYRING

Brugerstyring i dag

- Webbrugere oprettes af anvendere/registre
- Tjenestebrugere oprettes via webbrugere
- Rettigheder
  - Adgang til services tildeles til tjenestebrugere
  - Adgang til portaler tildeles til webbrugere
- Problemer ved brugerstyring i dag:
  - Brugere kan ikke slettes, kun deaktiveres.
  - Sikkerheden omkring webbrugerne og tjenesterne er relativ lav.
  - Flere personer kan kun styre samme tjenestebrugere hvis de deler login-info.
  - Ingen notifikation om at f.eks. certifikat på tjenestebruger er ændret

Hvordan er jeres tanker om brugerstyring?

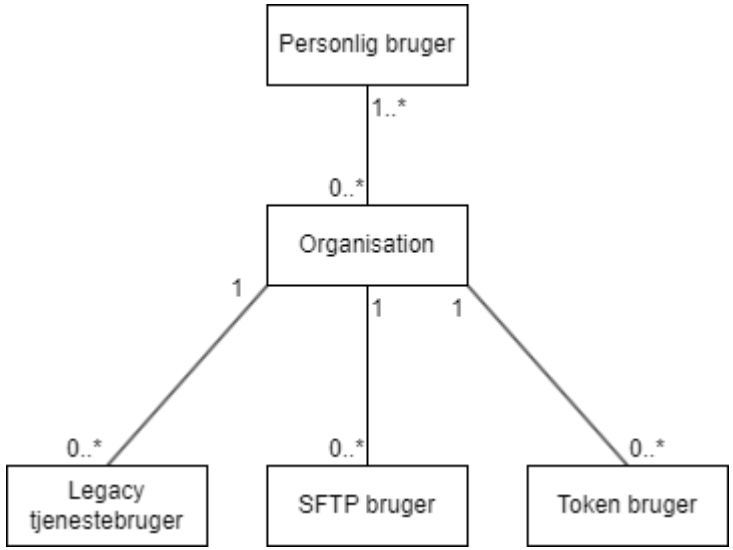
- Lad os tage 10 min i grupper af 3
  - Hvem skal have adgang
  - Hvordan skal man dele adgange for et system
  - Hvor er løsningsansvaret for hvis man mister adgang selvbetjening.

Vision om brugerstyring

- Webbrugere bliver fjernet og erstattet med en 'organisation'.

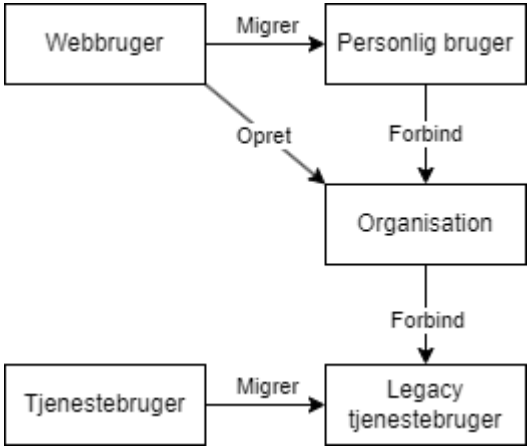
  Hvorvidt en 'organisation' f.eks. er *hele Netcompany* eller *BBR-registeret med NC som leverandør* må anvendere selv vurdere når de tager systemet i brug.

- Fremadrettet skal anvendere logge ind med en personlig bruger, som så kan få tildelt adgang til en række organisationer.
- Medlemmer af en organisation kan tilføje nye medlemmer.



Migrering ift. brugerstyring

- Migrering af *legacy tjenestebruger* til moderne tjenestebrugere skal udføres af anvenderne når de begynder at bruge de moderne tjenester.
- Legacy tjenestebrugere vil blive helt udfaset når de gamle tjenester fjernes.



Samlet opsummering

- For den moderniserede datafordeler samles alt til én zone som er offentlig tilgængelig.
- Alle endepunkter i hele løsningen beskyttes af én samlet standard fødereret autentifikationsmodel.
- Sikkerheden ensartes og testes afkoblet fra tjenesterne.
- Adgang til databærende tjenester tildeles mere granuleret end den nuværende model.
- Adgang valideres ved brug af standard programmel i de enkelte komponenter


netcompany
www.netcompany.com