

# Fællesoffentlig referencearkitektur for brugerstyring

25 November 2019

**This version:**

<http://github.com/digst/trust/index.md>

**Issue Tracking:**

[GitHub](#)

**Editors:**

Digitaliseringsstyrelsen <http://arkitektur.digst.dk>

# Table of Contents

---

## Forord

## Resume (in english)

## Resume

## 1 Introduktion

- 1.1 Formål
- 1.2 Anvendelse
- 1.3 Målgruppe
- 1.4 Omfang og afgrænsning
- 1.5 Centrale begreber
  - 1.5.1 Type af entiteter
  - 1.5.2 Relationer imellem identiteter
- 1.6 Tilblivelse og styring
- 1.7 Anvendt metode, notation og signaturforklaring
- 1.8 Relation til rammearkitektur og andre referencearkitekturer
- 1.9 Læsevejledning

## 2 Strategi

- 2.1 Temaer
- 2.2 Strategiske principper
- 2.3 Vision
- 2.4 Værdiskabelse
- 2.5 Juridiske rammer
- 2.6 Sikkerhed

## 3 Forretningsarkitektur

- 3.1 Om tillidstjenester og eIDAS
- 3.2 Forretningsmæssig kontekst
- 3.3 Forretningsfunktioner
  - 3.3.1 Forretningsfunktionen udstedelse af identifikationsmidler
  - 3.3.2 Forretningsfunktionen autentifikation
  - 3.3.3 Forretningsfunktionen attributbeskrivelse
  - 3.3.4 Forretningsfunktionen udforme adgangspolitik
  - 3.3.5 Forretningsfunktionen adgangskontrol
  - 3.3.6 Forretningsfunktionen forebyggelse og kontrol
- 3.4 Tillidskæder i økosystemer
  - 3.4.1 Tillid gennem NSIS
- 3.5 Forretningsroller og aktører - og deres behov
  - 3.5.1 Personer – som borgere og som medarbejdere
  - 3.5.2 Virksomheder og myndigheder som brugerorganisationer
  - 3.5.3 Virksomheder og myndigheder som tjenesteudbydere
- 3.6 Principper???
- 3.7 Tværgående processer
  - 3.7.1 Administration af elektronisk identitet, akkreditiver og attributter
  - 3.7.2 Autentifikation
  - 3.7.3 Billetudstedelse og adgangskontrol
  - 3.7.4 Kontrol og rapportering
- 3.8 Forretningsobjekter og begreber
- 3.9 Begrebsmodel og relationer i brugerstyring

## 4 Teknisk arkitektur

- 4.1 Nødvendige applikationsservices
  - 4.1.1 Akkreditivtjeneste
  - 4.1.2 Attributbeskrivelse
  - 4.1.3 Autentifikation (genkendelse?)
  - 4.1.4 Biletudstedelse
  - 4.1.5 Adgangskontrol (men ikke autorisation?)
- 4.2 Tekniske implementering af forretningsfunktioner
  - 4.2.1 Implementering af administration af elektronisk identitet, Akkreditiver og Attributter
  - 4.2.2 Implementering af Registrering af elektronisk identitet
  - 4.2.3 Implementering af Anvendelse af brugerstyring?
- 4.3 Understøttende applikationsservices
- 4.4 Områder for standardisering

## 5 Målbillede? Implementering?

- 5.1 En målarkitektur med identitetsbrokere
- 5.2 Handleplan? Projektliggørelse?
- 5.3 Registrering af identiteter
- 5.4 Standarder for registrering af identiteter
- 5.5 Akkreditiver
- 5.6 Attributter
- 5.7 Brugerkataloger
- 5.8 Autentifikation
- 5.9 Standarder for overførsel af autentificerede brugere
- 5.10 Login-tjenester/Identitetsbrokere
- 5.11 Standarder for kommunikation mellem føderationer
- 5.12 Fælles løsning til fuldmagter

- 5.13 Brugerstyring for tjenestekonsumenter og fysiske apparater og sensorer
- 5.14 Standarder for identitetsbaserede webservices
- 5.15 Perspektivering
- 5.16 Bilag
  - 5.16.1 Ordliste
  - 5.16.2 Referenceliste
  - 5.16.3 Kilder og baggrundsmateriale
  - 5.16.4 Baggrund for valg af relationen entitet-elektronisk identitet

**Index**

Terms defined by this specification

## Forord

---

Denne referencearkitektur er udarbejdet i sammenhæng med den fællesoffentlige strategi for brugerstyring og for at understøtte implementeringen af Den fællesoffentlige digitaliseringsstrategi 2016-2020. Målet er, at referencearkitekturen skal fungere som et teknisk pejlemærke for udvikling af brugerstyringsløsninger i den offentlige sektor. Dermed har den en tæt relation til den fællesoffentlige rammearkitektur affødt af Digitaliseringsstrategiens initiativ 8.1, som indtil videre er kommet til udtryk i "En digitalt sammenhængende offentlig sektor: Hvidbog om arkitektur for digitalisering".

2017-udgaven af referencearkitekturen omfattede personer. I 2019-udgaven af referencearkitekturen er yderligere behandlet applikationer som brugere og i noget omfang ting i form af IoT - Internet of Things eller NPE – Non person entities. Brugen af føderationer og tillidstjenester og uddybet.

## Resume (in english)

---

## Resume

---

De senere års udvikling på brugerstyringsområdet i den offentlige sektor har entydigt peget i retning af føderationer baseret på tillid og fælles standarder. Der er således etableret en række føderationer i forskellige sektorer - dette gælder fx på det kommunale område (KOMBIT), på sundhedsområdet (SOSI), på miljøområdet (Miljøportalen), inden for undervisningssektoren (STIL) og fællesoffentligt (NemLog-in). Dette er samtidig i tråd med internationale tendenser herunder etablering af en EU-føderation med afsæt i eIDAS-forordningen.

Føderationer giver en lang række fordele herunder sammenhæng for brugerne, mere effektiv administration og mulighed for arbejdsdeling, hvor specialiserede tjenester (infrastruktur) varetager komplekse opgaver med håndtering af identiteter og akkreditiver for forretningstjenester, hvilket letter byrder og samtidig øger sikkerheden.

Der er til stadighed behov for, at sektorløsninger udvikles på baggrund af en fællesoffentlig referencearkitektur for brugerstyring, som udpeger fælles principper, mønstre, standarder, byggeblokke og andet. Herved kan der opnås sammenhæng, synergier og udbredelse af god praksis på tværs af hele økosystemet, og risikoen for uensigtsmæssig sub-optimering og dublering af løsninger reduceres.

Formålet med referencearkitekturen er således at skabe **rammer** for brugerstyring i den offentlige sektor - som danner grundlag for et sammenhængende økosystem med høj grad af tillid, genbrug og interoperabilitet.

Brugerstyring dækker opgaver og funktioner i forbindelse med håndtering af brugere i forhold til digitale tjenester, som overordnet kan opdeles i administrative funktioner og adgangskontrol. De administrative funktioner omfatter oprettelse, ændring og nedlæggelse af brugere i brugerstyringssystemer, udstedelse og tilknytning af akkreditiver til brugere og tilknytning af rettigheder til brugere.

Hovedaktiviteterne i **administration i brugerstyring** er følgende:

- **Registrering** af digitale identiteter og den løbende vedligeholdelse heraf.
- **Udstedelse** af akkreditiver og tilknytning af disse til digitale identiteter. Akkreditiver anvendes til at autentificere en digital identitet over for en tjeneste, som der ønskes adgang til.
- **Attributbeskrivelse** af karakteristika ved digitale identiteter, som en tjeneste kræver for at give adgang, og den løbende vedligeholdelse heraf. Det er fx rettighedsrelevante attributter i form af roller, fuldmagter, samtykker og/eller andre attributter, der udtrykker kvaliteter, som en tjeneste baserer sin adgangskontrol på.

Hovedaktiviteterne i **anvendelse af brugerstyring** er følgende:

- **Autentifikation** verificerer en identitet (tilknyttet en entitet) gennem anvendelse af et akkreditiv (identifikationsmiddel).
- **Billetudstedelse** udsteder på grundlag af en autentifikation en signeret billet (eng. security token) med det sæt attributter, som tjenesten kræver for at give adgang. I denne proces kan der evt. ske en veldefineret omveksling attributter eller berigelse med attributter fra forskellige kilder, således at tjenesten er i stand til direkte at anvende adgangsbilletten. Har brugeren ikke fået tildelt de nødvendige beskrivende attributter i det rette format, vil vedkommende ikke opnå adgang hos tjenesten.
- **Adgangskontrol** er håndhævelse af en tjeneses adgangspolitik i tjenesten (eng. policy enforcement). Det styrer, hvilke handlinger identiteten må udføre i en tjeneste, eller hvilke informationer identiteten må få adgang til på grundlag af den adgangsbillet, der er udstedt. Attributterne i adgangsbilletten er således input til adgangskontrollen.

Referencearkitekturen for brugerstyring fastlægger en række principper, der leder frem mod en fælles forretnings- og it-arkitektur for det offentlige elektroniske identiteter, akkreditiver, attributbeskrivelser, autentifikation, billetudstedelse og adgangskontrol:

Principper

*Principper med brugerbaseret fokus:*

1. Brugere oplever en sammenhængende adgangsstyring
2. Brugerstyringsløsninger udvikles med fokus på brugernes behov
3. Brugerstyringsløsninger respekterer brugernes privatliv

*Principper med teknisk fokus:*

4. Aktører indgår i føderationer baseret på tillid
5. Aktører i føderationer vurderer i deres styring af informationssikkerhed samspillet med andre aktører

6. Administration af brugere flyttes så vidt muligt ud af fagapplikationer
7. Tjenesteudbydere (den dataansvarlige) har ansvaret for at håndhæve brugernes adgange

*Principper med udviklingsfokus*

8. Brugerstyring realiseres i løst koblede komponenter
9. Tværoffentlige brugerstyringsløsninger baseres på en kerne af fælles komponenter i samspil med øvrige komponenter i infrastrukturen
10. Tværoffentlig brugerstyring etableres i overensstemmelse med internationale standarder og løsninger

Forretningsbehov og ovenstående principper peger entydigt frem mod en løst koblet, fødereret arkitektur, hvor de enkelte tjenester/tjenesteudbydere håndhæver adgang baseret på forudgående (ekstern) autentifikation og således ikke selv håndterer administration af brugere, anvendelsestyper og rettigheder.

Der er derfor valgt en token-baseret model for adgangsstyring. Denne indebærer, at brugere og systemer efter autentifikation får udstedt en signeret billet, et såkaldt *security token*, af en betroet komponent i infrastrukturen. Billetten præsenteres herefter over for den tjeneste, som leverer data eller funktionalitet, der ønskes adgang til. En billet indeholder attributter, som beskriver identitet, karakteristika samt tildelte adgangsrettigheder. Den er desuden tidsstemlet og digitalt signeret af udstederen, så den ikke kan forfalskes eller manipuleres.

Digitalisering forudsætter informationssikkerhed, og brugerstyring er et af midlerne til at håndtere risici knyttet til håndtering af digitale identiteter.

I referencearkitekturen fastlægges en række standarder for håndtering af brugere, akkreditiver og attributter. Der er behov for standarder for overførsel af data om autentificerede brugere mellem autentifikationstjenester, login-tjenester/brokere og forretningstjenester. Der er behov for standarder i forbindelse med rettighedsrelevante attributter, og der er behov for standarder for kommunikation mellem føderationer. Dette behandles i afsnit 9.6.1.

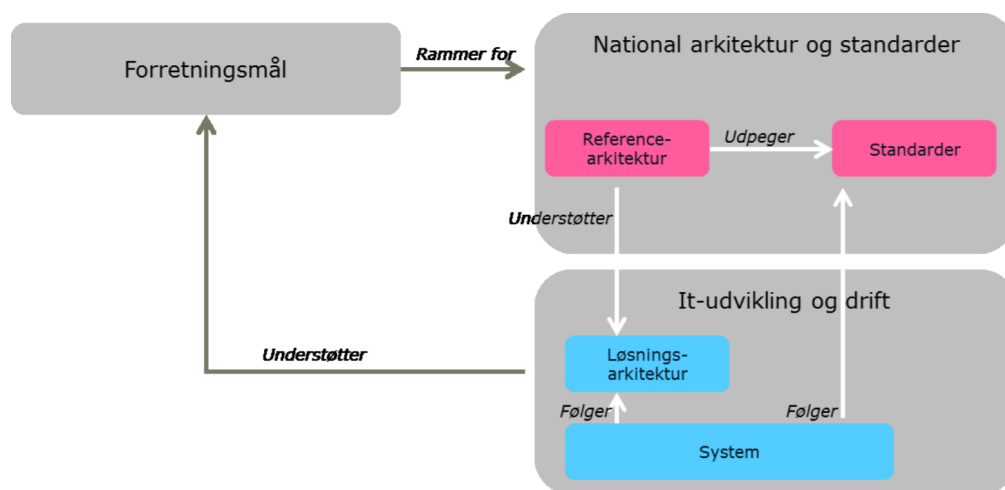
# 1. Introduktion

## 1.1. Formål

Den fællesoffentlige referencearkitektur for brugerstyring skal målrette og strukturere indsatsen for at skabe sammenhængende, effektive, sikre og brugervenlige løsninger på tværs af domæner, nationalt og transnationalt. Fokus er på det tværgående dvs. adgang til tjenester på tværs af organisationer, herunder føderationer på tværs af sikkerhedsdomæner med gensidig tillid. Referencearkitekturs formål er at skabe en arkitekturmæssig ramme for, hvordan man skal indrette løsninger, så systemer understøttet af forskellige sikkerhedsløsninger kan kommunikere med hinanden. Herved bliver løsninger enklere at etablere og drive, brugerne undgår at skulle logge på flere gange, og oplysninger om brugere skal ikke vedligeholdes flere steder.

## 1.2. Anvendelse

Referencearkitekturen skal kunne anvendes til at udpege standarder, der understøtter arkitekturen. Referencearkitekturen skal understøtte udarbejdelse af løsningsarkitektur i konkrete projekter. Referencearkitekturen anviser ikke i detaljer, hvordan myndigheder og virksomheder skal bygge løsninger, men fastlægger rammer og standarder for løsninger. Referencearkitekturen kan anvendes i sammenhæng med andre fællesoffentlige referencearkitekturer. Generelt kan en referencearkitekturs rolle illustreres med følgende figur:



Referencearkitekturs rolle

## 1.3. Målgruppe

Dette dokument har to målgrupper:

- Den ene målgruppe er strategiske beslutningstagere inden for digitalisering og it, typisk digitaliseringschefer, it-chefer, afdelings- og kontorchefer og andre med rollen som systemejer.
- Den anden målgruppe er projektledere, arkitekter og udviklere hos myndigheder, virksomheder og leverandører, der har til opgave at kravspecifilere, designe eller udvikle løsninger, hvor der indgår eller anvendes tværoffentlig brugerstyring.

## 1.4. Omfang og afgrænsning

Referencearkitekturen for brugerstyring omfatter offentlige tjenester, men referencearkitekturen kan med fordel også anvendes til ikke offentlige tjenester og til at understøtte tværgående brugerforløb med det offentlige.

Arkitekturen omfatter også rollen som leverandør af tillidstjenester - registreringstjenester, akkreditivtjenester, autentifikations-tjenester, identitetsbrokere, attributtjenester mv. Arkitekturen omfatter desuden private virksomheders mulighed for at anvende bruger- og rolledata og login-systemer.

Arkitekturen omfatter både brugeradministration og adgangskontrol, herunder det der på engelsk betegnes Credential and Identity Management (CIM), Identity Rights Management (IRM), Access Control (AC) og Identity and Access Management (IAM/IdAM).



Referencearkitekturen definerer, hvad en føderation omhandler i rammerne af brugerstyring, og den beskriver de opgaver, en føderation løser i denne ramme. Etablering af en føderation sker gennem fastlæggelse af et aftalesæt mellem føderationens deltagere.

Denne 2019-udgave af referencearkitekturen for brugerstyring er udvidet med de særlige aspekter vedrørende brugerstyring for ting, organisationer og applikationer - samlet betegnet som Non-Person Entities (NPE).

Parallelt med opdateringen af referencearkitekturen er der igangsat analyser af muligheden for en fællesoffentlig samtykkeløsning med henblik på at afdække behov og muligheder inden for dette område. Samtykkeområdet er af denne årsag kun overordnet behandlet i nærværende udgave af referencearkitekturen.

## 1.5. Centrale begreber

I referencearkitekturen anvendes nogle centrale begreber, som her beskrives for at lette læsningen.

Referencearkitekturen beskriver styring af brugeres adgang til tjenester. Brugere, her entiteter, får udstedt en identitet af en identitetsgarant. Til identiteten knyttes en række loginmidler, som identiteten kan bruge til at bevise sin identitet. Når identiteten er bevist, kan oplysninger fra identiteten, eventuelt suppleret med eksterne adgangsrättigheder, styre brugerens adgang til tjenester. I en digital sammenhæng defineres brugere som dels den entitet de virkelig er og dels den tildelte identitet, de har fået som adgang til digitale tjenester.

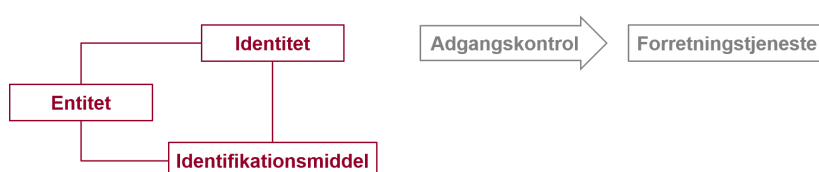


Figure 1 [Brugerstyringsbegreber]

**Entitet** Person, juridisk enhed, ting eller applikation som ønsker adgang til en tjeneste. En entitet kan have flere identiteter – for eksempel kan en fysisk person både have en privatidentitet og flere erhvervsidentiteter. Enhver entitet der skal have adgang til tjenester skal optræde som bruger med sin egen identitet.

**Identitet** Bruger repræsenteret ved et sæt af attributter der identificerer identiteten. En identitet kan være stærkere eller svagere bundet til entiteten afhængigt af den proces hvor identiteten udstedes - Identitetssikring.

**Identifikationsmiddel** som en entitet får udstedt eller registreret til brug for autentifikation. Midlet kan både være fysisk og virtuelt, og skal være under entitetens kontrol. Velkendte eksempler er brugernavn og password, NemID nøglekort, certifikater, fingeraftryk mv.

**Forretningstjeneste** løser et forretningsmæssigt behov, fx en borgerrettet selvbetjeningsløsning.

**Adgangskontrol** Håndhævelse af en tjenestes adgangspolitik. Adgangskontrollen styrer, hvilke handlinger identiteten må udføre i en tjeneste, eller hvilke informationer identiteten må få adgang til.

### 1.5.1. Type af entiteter

Entiteter ses som et subjekt, med rettigheder og pligter, eller et objekt, der kan arve rettigheder fra et subjekt.

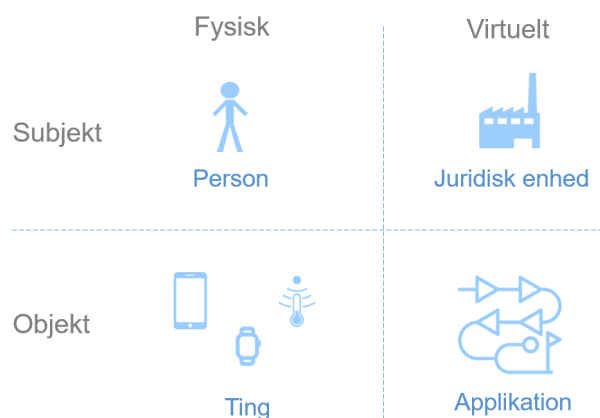


Figure 2 [Entitetsformer]

**Person** Fysisk person der kan have identiteter som borger, medarbejder eller deltage i fællesskaber, som for eksempel Facebook.

**Juridisk enhed** Organisation med adgange og rettigheder der kan delegeres til medarbejder eller applikation.

**Ting** Fysiske ting med indbygget program der kan optræde som bruger eller tjeneste. Her er programmet underlagt tingen og kan, i modsætning til en applikation, ikke optræde selvstændigt.

**Applikation** Et selvstændigt program der kan afvikles på en platform. Til forskel fra programmet i en ting, er en applikation ikke bundet til den platform det kører på. En applikation kan optræde både som bruger og tjeneste og skal have sin egen identitet med tilhørende identifikationsmidler. En automatiseringsrobot vil være en applikation og skal derfor have egen identitet og aldrig låne en personbrugers identitet. Bemærk, at automatiseringer en bruger selv afvikler efter at være logget ind på de nødvendige systemer, i brugerstyringssammenhæng ikke betragtes som en robot.

### 1.5.2. Relationer imellem identiteter

Entiteter kan have indbyrdes relationer af betydning for brugerstyring.

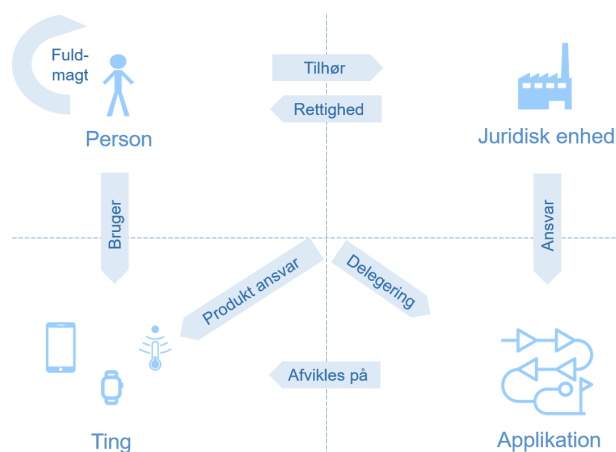


Figure 3 [Entitetsrelationer]

**Fuldmagt** der gives fra person til person. Afhængigt af fuldmagten, kan alle eller dele af en persons rettigheder videregives til den person der har fuldmagt.

**Tilhør** imellem person og juridisk enhed. Tilhøret i sig selv giver implicit en række rettigheder fra organisationen til personen. For eksempel har en borger i Danmark implicit adgang til en række tjenester som for eksempel Borger.dk og e-Boks.

**Rettighed** der eksplicit gives fra en juridisk enhed til en person. Dette kan være adgang til systemer eller steder, eller prokura til at handle på organisationens vegne.

**Bruger af** en ting. For eksempel brugeren af en mobiltelefon eller en blodtryksmåler. I begge tilfælde er det en mulighed, at tingen arver rettigheder fra brugeren.

**Produktansvar** som juridisk enhed har overfor de ting den producerer.

**Delegering** af rettigheder fra en person eller juridisk enhed til en applikation. For eksempel en automatiseringsrobot, der får delegeret rettigheder til at håndtere en givet sagsforløb.

En applikation der **afvikles på** en enhed, kan få særlige rettigheder på grund af enheden den afvikles på. < eksempel >.

Juridisk enhed der har **ansvar for** hvad en applikation gør.

Øvrige begreber uddybes i referencearkitekturens bilag A (ordliste) eller forklares undervejs.

"kun elektroniske identiteter kan anvende elektroniske tjenester".

Se Afsnit 4 og Bilag A: Ordliste

## 1.6. Tilblivelse og styring

2020-udgaven er udarbejdet i Kontor for Data og Arkitektur, Digitaliseringsstyrelsen med konsulentbistand fra ITCrew og Capgemini.

I udarbejdelsen har en arbejdsgruppe af offentlige arkitekter bidraget gennem en række af workshops. I gruppen har deltaget repræsentanter fra følgende organisationer: Kommunernes Landsforening, Danske Regioner, Styrelsen for Dataforsyning og Effektivisering, Styrelsen for It og Læring, Kystdirektoratet, Danmarks miljøportal, Udviklings og forenklingsstyrelsen, Energistyrelsen og Energinet.

2020-udgaven af referencearkitekturen godkendtes i version 2.0 i Styregruppe for Data og Arkitektur under Digitaliseringsstrategien i maj 2020. Styregruppen er herefter ejer af dokumentet, med Kontor for Data og Arkitektur som ansvarlig for vedligehold af referencearkitekturen som en del af den Fællesoffentlige, Digitale Arkitektur.

## 1.7. Anvendt metode, notation og signaturforklaring

Metodemæssigt er referencearkitekturen udarbejdet inden for rammerne af Den fællesoffentlige digitale arkitektur og følger så vidt muligt den fælles skabelon for referencearkitekturer som udarbejdet i Sekretariatet for Styregruppen for Data og Arkitektur under digitaliseringsstrategien.

I forhold til ejerskab af de elementer, der indgår i dokumentets figurer og definitioner, markerer:

- Rød tekst: At et element eller en relation ejes og defineres i denne referencearkitekturs begrebsmodel
- Blå tekst: At et element eller en relation er kendt, men ejes og defineres et andet, nærmere angivet sted, fx i andre referencearkitektur eller i lovgivning.
- Grå tekst: At et element eller en relation er identificeret, men ikke nærmere defineret i denne referencearkitektur.

## 1.8. Relation til rammearkitektur og andre referencearkitekturer

Referencearkitekturen publiceres på arkitektur.digst.dk, hvor man kan finde beslægtede dokumenter vedrørende brugerstyring, herunder relaterede standarder mv.

*[ her skal der indføres en kort beskrivelse af de øvrige referencearkitekturer ]*

## 1.9. Læsevejledning

Kapitel 1 og 2 bør læses af alle.

Kapitel 3 om den forretningsmæssige del af arkitekturen bør læses af de der skal forstå arkitekturen.

Kapitel 4 og 5 henvender sig særligt til løsningsarkitekter.

## 2. Strategi

---

### 2.1. Temaer

Det er helt centralt for realiseringen af en effektiv digitalisering, at brugerne har tillid til infrastruktur og tjenester. Hvis brugerne mister tilliden til, at en løsning giver en tilstrækkelig beskyttelse af deres persondata, vil der være risiko for, at de fravælger en given løsning og måske overgår til analog behandling eller helt fravælger en serviceydelse. Der vil derfor være forretningsmæssige fordele ved at indtænke privatlivsbeskyttelse i brugerstyringssystemer i tillæg til den rene overholdelse af lovgivningen på området. Dette kan håndteres gennem et struktureret privacy-program.

### 2.2. Strategiske principper

OECD har defineret otte basale principper for privatlivsbeskyttelse (Kan findes beskrevet hos OECD: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>):

Princippet om begrænset indsamling Princippet om datakvalitet Princippet om formålsspecificering Princippet om anvendelsesbegrænsning Princippet om datasikkerhed Princippet om åbenhed (transparens) Princippet om individets deltagelse Princippet om ansvarlighed (accountability). Løsninger bør i design, udvikling, drift og vedligehold forholde sig til ovenstående.

### 2.3. Vision

### 2.4. Værdiskabelse

### 2.5. Juridiske rammer

I maj 2018 trådte EU's forordning om persondatabeskyttelse (GDPR) i kraft. Denne stiller en række krav til persondatabeskyttelse, og en del af disse krav er dækket, hvis man følger ovenstående basale principper fra OECD. Dog er der konkrete krav i GDPR, som skal indtænkes i løsninger, herunder:

Privacy Impact Assessments Privacy-by-design og privacy-by-default Retten til at blive glemt Retten til dataportabilitet Retten til indsigt i egne data Selvom privatlivsbeskyttelse omfatter andet end informationssikkerhed, kan man med fordel indbygge sit privacy-program i eksisterende ISMS, da mange kontroller er sammenfaldende.

### 2.6. Sikkerhed


[Er det måske mere beslutning der er truffet strategisk, at vi er forpligtiget til at anvende ISO 27001? Og at vi har NSIS /madsh]

Fastlæggelse af niveau for og håndtering af informationssikkerhed skal foretages af alle offentlige organisationer og tage udgangspunkt i ISO/IEC 27001-standarden for styring af informationssikkerhed. ISO 27001 er valgt som statslig sikkerhedsstandard og har været obligatorisk at følge for statslige institutioner siden januar 2014, og kommunerne er forpligtet til at følge principperne.

Realiseringen skal ske gennem et ledelsessystem for informationssikkerhed (Information Security Management System, ISMS). Digitaliseringsstyrelsen har udarbejdet vejledninger, værktøjer og skabeloner hertil, som er placeret her: <http://www.digst.dk/Informationssikkerhed>.

Hovedindholdet i ISO/IEC 27001 er, at niveau for og håndtering af informationssikkerhed tager udgangspunkt i en risikovurdering. Organisationens ledelse fastlægger på baggrund af en risikovurdering et sikkerhedsniveau, som svarer til den forretningsmæssige betydning af de aktiver (fx informationer), som organisationen ejer, vedligeholder og har dataansvaret for, og de tjenester, som den stiller til rådighed for andre organisationer af alle typer. Organisationen skal gennemføre en afbalanceret risiko- og konsekvensvurdering under hensyntagen til de økonomiske forhold og herudfra fastlægge

retningslinjer forretningsgange og instrukser sikkerhedsforanstaltninger, som beskytter organisationen på de risikoniveauer, der er valgt. De vil ofte være forskellige, afhængigt af de konkrete informationer og tjenester.

Indenfor domænet 'brugerstyring' er det særligt relevant at beskæftige sig med risici knyttet til håndtering af digitale identiteter, rettigheder og akkreditiver. National Standard for Identiteters Sikringsniveauer (NSIS) er her et afgørende element i den samlede risikostyring, som gør det muligt at udtrykke graden af tillid til en autentificeret identitet på en tre-trinsskala:  Lav, Betydelig, Høj. NSIS kan benyttes både af brugerstyringstjenester, som leverer autentificerede identiteter, og af forretningstjenester, som aftager identiteter.

Den kommende fællesoffentlige infrastruktur for identiteter i form af MitID og NemLog-in3 bygges på NSIS, og overholdelse af NSIS standarden vil være en forudsætning for at tilslutte en forretningstjeneste, broker eller lokal IdP til NemLog-in3.

I en tværoffentlig brugerstyring er det endvidere nødvendigt at koordinere risikovurderinger og valg af niveau for og håndtering af informationssikkerheden. Dette kan ske ved at benytte et fælles trust framework som NSIS. For at alle parter kan have tillid til hinanden, ekspliciterer, harmoniserer og standardiserer et trust framework forskellige aspekter af sikkerhed, herunder politikker, sikkerhedsmæssige tiltag og fælles sprog. Harmonisering og standardisering er teoretisk set ikke en nødvendighed, men konsekvensen ved ikke at harmonisere og standardisere er, at kompleksiteten af kommunikationen mellem sikkerhedsdomæner bliver meget høj. Der skal indgås individuelle aftaler mellem parterne, og disse skal kende til hinandens politikker og arbejdsgange m.m. Et trust framework er med til at reducere denne kompleksitet.

NSIS og trust frameworks generelt giver mulighed for:

Sammenhængende løsninger på tværs af domæner og føderationer via gensidig tillid (sammenkobling af siloer). En fælles forståelse samt koordinering/governance af sikringsniveauer. Transparens gennem tydelig beskrivelse af krav til parterne og regler for deres adfærd. En flerleverandørstrategi baseret på outsourcing af funktioner med mulighed for private aktører - hvor det er ønskeligt og økonomisk fordelagtigt. Veldefineret governance gennem anmeldelse, revision og tilsyn. National Standard for Identiteters Sikringsniveauer (NSIS), der har afsæt i eIDAS-forordningen, er et dansk trust framework for identitetssikring. NSIS fastlægger som tidligere nævnt tre sikringsniveauer ("Lav", "Betydeligt" og "Høj"), som modsvarer de tilsvarende niveauer i eIDAS. Niveauerne dækker hele livscyklussen for elektroniske identiteter fra registrering til arkivering/nedlæggelse.

Når en bruger autentificerer sig mod en forretningstjeneste, vil brugerens security token (billet) indeholde information om det aktuelle sikringsniveau for autentifikationen. Forretningstjenesten kan på baggrund af dette (samt øvrige attributter om brugeren) beslutte, hvilken adgang brugeren kan få i tjenesten. Sikringsniveauet er dermed et input til adgangskontrollen i tjenesten.

### 3. Forretningsarkitektur

Brugerstyring dækker opgaver og funktioner i forbindelse med håndtering af brugere af digitale løsninger. Det er en fælles betegnelse for de foranstaltninger som sikrer, at de rette brugere får adgang til de rette it-systemer - og alle andre afvises. Brugerstyring involverer dels *administration* af brugeridentiteter (før de tilgår it-systemer), herunder registrering og udstedelse af identifikationsmidler, beskrivelse af attributter i form af egenskaber, roller, relationer mv. og dels en *'run-time'* del, når brugere tilgår it-systemer, som bl.a. involverer autentifikation og udførelse af adgangskontrol.

Figuren herunder viser de væsentligste elementer i brugerstyringsdomænet (røde kasser) og kontekst i form af blå og grå kasser.

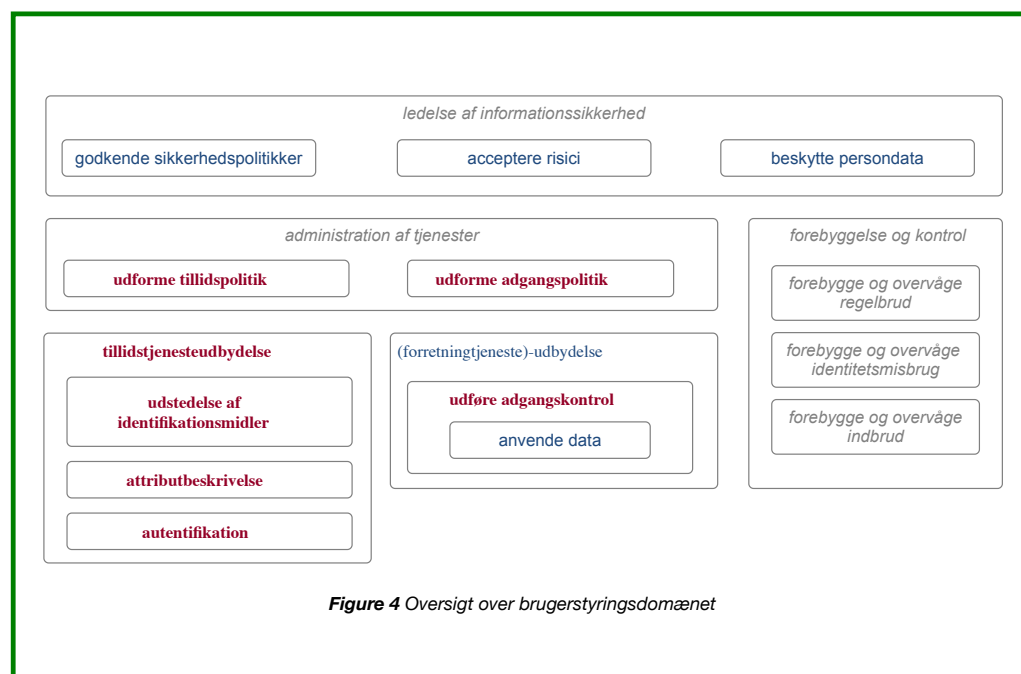


Figure 4 Oversigt over brugerstyringsdomænet

Det øverste lag i figuren omhandler governance i form af ledelse af informationssikkerhed. Det er her ledelsen i en organisation godkender sikkerhedspolitikker, og giver mandat til det sikkerhedsniveau, der skal opnås, hvordan identificerede risici håndteres, og hvordan persondata beskyttes. Her er organisationen dels underlagt lovgivning og regulering (som fx databeskyttelsesforordningen) og dels egne forretningsmæssige vurderinger af risici, risikoappetit mv.

På baggrund heraf udformes dels politikker for adgang til egne tjenester (adgangspolitikker), som beskriver kriterier og sikkerhedsniveauer for adgang, og dels politikker for anvendelse af eksterne parter i forbindelse med brugerstyring (tillidspolitikker).

Til at realisere politikkerne opereres der med en række tillidstjenester, der udfører betroede funktioner i brugerstyringen. Disse omfatter udstedelse elektroniske identifikationsmidler, som brugerne kan autentificere sig med, de omfatter beskrivelse af attributter ved brugerne (fx navn, egenskaber, roller, relationer, bemyndigelser osv.), og de omfatter endelig autentifikation af brugere. *Tillidstjenester* udfører som nævnt betroede funktioner, der understøtter forretningstjenesterne - herunder særligt den adgangskontrol, som forretningstjenesterne skal varetage, før der gives adgang til systemer og data.

I den tekniske arkitektur beskrevet i kapitel 4 beskrives en række supplerende funktioner (fx billetudstedelse, brokering, discovery), som ikke optræder på forretningsniveau.

En tjeneste og et it-system er i denne kontekst synonymt for det samme: et stykke it, der kan levere informationer og funktionaliteter. Et stykke it, der optræder som leverandør, kaldes en tjeneste eller tjenesteudbyder. Et stykke it, der optræder som den bruger, der efterspørger informationer og funktionalitet, kaldes en tjenestekonsument. Det samme stykke it kan optræde både som leverandør (være en tjeneste) og i sin udførelse af tjenesten optræde som bruger (være en tjenestekonsument) over for andre tjenester.

#### 3.1. Om tillidstjenester og eIDAS

I denne referencearkitektur anvendes betegnelsen 'tillidstjeneste' i bred forstand om en tjeneste, der udfører betroede funktioner, der understøtter brugerstyring i forretningstjenesterne. Med denne terminologi opnås et tydeligt skel til forretningstjenester, hvilket understøtter beskrivelse af eksempelvis føderationer, hvor forskellige parter leverer forskellige tjenester. Anvendelsen af termen 'tillidstjeneste' er dermed væsentligt bredere her end i eIDAS-forordningen, som regulerer nogle specifikke former for tillidstjenester (hovedsageligt) indenfor PKI-området:

- Certifikatudstedere (CA)
- Tidsstempelingsservices
- Valideringstjenester for validering af elektroniske signaturer, elektroniske segl og tidsstempler
- Tjenester til bevaring af signaturer, segl og certifikater
- Elektroniske registrerede leveringstjenester.

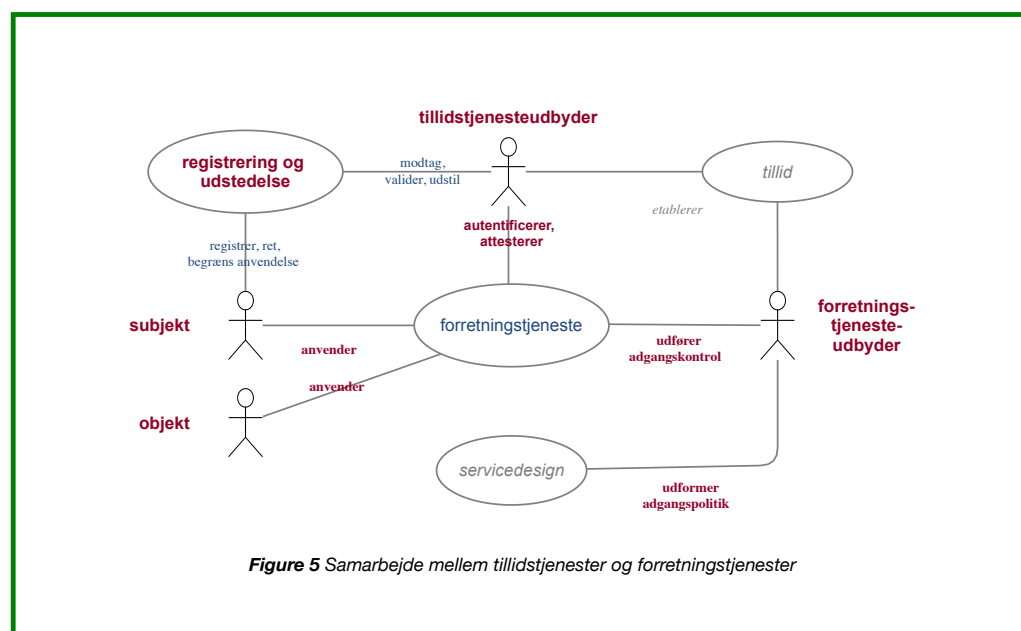
eIDAS-forordningen stiller en række krav til udbydere (PKI)-tillidstjenester, som ikke skal forveksles med tillidstjenesterne i denne referencearkitektur.

Det er endvidere vigtigt at være opmærksom på, at eIDAS-forordningen stiller krav om, at hvis en myndighed stiller en digital service til rådighed for borgerne og virksomhederne med anvendelse af en såkaldt notificeret eID-løsning, skal det være muligt at autentificere sig med notificerede eID-løsninger fra andre EU-lande med samme eller højere sikringsniveau. I kontekst af figuren ovenfor kan man sige, at eIDAS dikterer nogle elementer af visse (offentlige) tjenesters adgangspolitik, nemlig at tjenesterne skal være tilgængelige for andre EU-landes borgere og virksomheder.

### 3.2. Forretningsmæssig kontekst

Et helt centralt tema i denne referencearkitektur er, at forretningstjenester og tillidstjenester arbejder sammen om at udføre brugerstyring - såkaldt *shared use cases*. Her opfattes tillidstjenesterne ofte som noget infrastruktur, der muliggør en sikker forretningsmæssig anvendelse af et it-system. Grundlaget for samarbejdet er baseret på tillid, som gør det muligt for forretningstjenesten at uddelegere betroede funktioner til en tillidstjeneste udbudt af en tredjepart. Tilliden kan være rodfæstet i lovgivning, i standarder og rammeværk med indbygget kontrol og governance eller i aftaler (herunder databehandlaftaler). Et vigtigt eksempel er National Standard for Identiteters Sikringsniveauer (NSIS), som gennem krav og kontrol via revisionserklæringer gør det muligt at have tillid til (og kvantificere risici for) autentificerede identiteter, der er håndteret af en ekstern part (tillidstjeneste). NSIS definerer tre sikringsniveauer for en autentificeret identitet (Lav, Betydelig, Høj), og gør det dermed muligt både at klassificere tillidstjenester i forhold til disse og indrette tjenesters adgangspolitikker differentieret.

Nedenstående figur viser et funktionelt overblik med fokus på samarbejdet mellem udbydere af tillidstjenester og forretningstjenester.



I nedenstående figur er vist en shared use case med fokus på adgangskontrol:

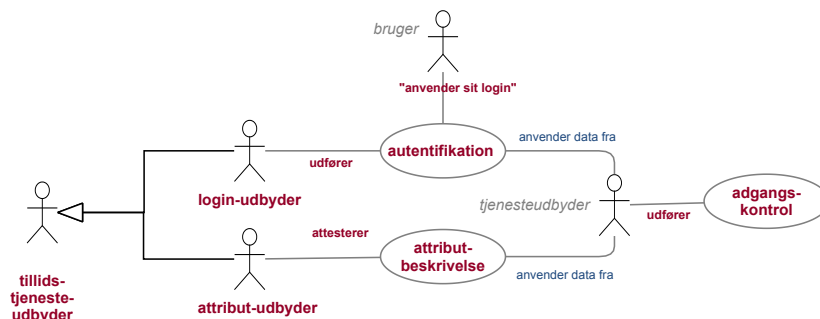


Figure 6 Samarbejde ved adgangskontrol

Bemærk at termen *attributbeskrivelse* er en væsentlig generalisering, som i praksis kan dække over en række forskellige aktiviteter, herunder:

- Administration af brugere i et brugerkatalog (fx et AD) med navn, titel, email, afdeling osv.
- Tildeling (og udstilling) af roller og fuldmagter til en brugere
- Udstilling af autoritative data der beskriver brugere som fx CPR-registret, CVR-registret, Sundhedsstyrelsens autorisationsregister mv.
- Autoritativ beskrivelse af relationer mellem brugere og andre objekter/subjekter (ansat i, forælder til, tegningsberettiget for, ejer af, værge for).

Tillidsbegrebet er vigtigt for attributter, idet de indgår som væsentligt input til beslutninger i adgangskontrollen. På engelsk bruges ofte betegnelsen *verified claims* om det forhold, at en tredjepart har verificeret en attribut. I en adgangspolitik bør man derfor forholde sig hvilke kilder til attributter (attributtjenester), der er tillid til, og i hvilken grad. I visse tilfælde kan attributter kan endda være oplyst af brugeren selv (*self-asserted claims*), hvilket kan være helt på sin plads, forudsat at dette er udtrykt i adgangspolitikken.

Bemærk at figureerne ovenfor er udtryk for abstrakte forretningsbeskrivelser, og at man i en konkret arkitektur fx kan have flere forskellige parter, som udfører fx attributbeskrivelse i et konkret scenarie. Det kan således variere betydeligt, hvilke attributter forskellige tjenester har behov for at kunne håndhæve deres adgangspolitik, samt de mekanismer attributter tilvejebringes med (fx push eller pull).

I senere kapitler vedr. den tekniske arkitektur beskrives mere konkret, hvordan attributter kan håndteres i brugerstyring. Ofte formidles de fx af sikkerhedshensyn som signerede data (*security tokens* eller *billetter* på dansk), og ofte er der tekniske komponenter (brokere), som orkestrerer indsamling og formidling af attributter fra forskellige kilder for at lette byrden for forretningstjenester. Det er således ikke ligegyldigt, hvordan forretningsfunktioner udmøntes i en teknisk arkitektur - særligt når er ønske om at opnå et økosystem der er sikkert, sammenhængende og brugervenligt.

### 3.3. Forretningsfunktioner

I dette afsnit beskrives forretningsfunktionerne i domænet i lidt større detaljer - både dem som udføres af tillidstjenester og forretningstjenester.

#### 3.3.1. Forretningsfunktionen udstedelse af identifikationsmidler

Formålet med at udstede identifikationsmidler til brugerne er, at de kan autentificere sig som en entydig identitet, når de interagerer med forretningstjenester (og evt. tillidstjenester). National Standard for Identiteters Sikringsniveau (NSIS) beskriver og stiller krav til delprocesserne under udstedelse:

- Ansøgning og registrering
- Verifikation af identitet
- Levering og aktivering af identifikationsmidler
- Suspendering, spærring og genaktivering
- Fornyelse og udskiftning.

I brugerstyring er det en forudsætning, at brugerne registreres og tildeles en identitet, som forbindes til et identifikationsmiddel. **Registreringen** af identiteten kan varetages af en underfunktion (registreringstjeneste), som også verificerer identiteten (identitetssikring). Eksempelvis agerer banker & borgerservice som registreringstjenester for NemID/MitID løsningerne. Processen for udstedelse af identifikationsmidler kan variere betydeligt i kvalitet, hvilke attributter der valideres, og scope for den efterfølgende anvendelse.



I NSIS opereres med, at identiteten kan valideres på tre forskellige sikringsniveauer (fx i forhold til om brugeren har gennemført en on-line registrering, er mødt fysisk op, har præsenteret pas/kørekort osv.). Kvaliteten af en identitetssikring betegnes ofte *Identity Assurance Level*.

Personer registrerer selv deres Facebook-identitet, hvor kun e-mail adressen verificeres, mens NemID/MitID-identiteter får valideret navn og CPR-nummer.

Efter oprettelse af den elektroniske identitet skal et **identifikationsmiddel** (fx kodeord, PIN, fingeraftryk) **tilknyttes** til identiteten. Identifikationsmidler anvendes til at autentificere identiteten i modsætning til attributter, som beskriver identiteten. En udsteder af identifikationsmidler skal dels sikre sammenhængen mellem identifikationsmidlet og identitet, og dels stå inde for identifikationsmidlets tekniske styrke (se næste afsnit). Udstederen kan knytte allerede udstedte identifikationsmidler til identiteten eller udstede et nyt identifikationsmiddel og tilknytte dette til identiteten. Styrken af identifikationsmidler er ligeledes klassificeret i NSIS og tager afsæt i bl.a. antallet af autentifikationsfaktorer, hvor resistent det er mod angreb, samt andre sikkerhedsmæssige egenskaber.

Det er centralt i denne referencearkitektur, at der opereres med en *løs* kobling mellem identiteter og identifikationsmidler. Eksempelvis kan et identifikationsmiddel benyttes til at autentificere flere forskellige identiteter (hørende til samme entitet). Et eksempel på dette i fællesoffentlig kontekst er, når samme private NemID/MitID både kan bruges til autentificere både en privatperson og en ejer (fuldt ansvarlig deltager) for en enkeltmandsvirksomhed. Brugeren skal altid i brugssituationen være oplyst om, hvilken elektronisk identitet vedkommende optræder med.

CPR-nummeret er en attribut, som desværre også historisk er brugt som identifikationsmiddel - dvs. som bevis for identitet. Denne anvendelse af CPR-nummeret er imod regler fra CPR-kontoret, men anvendes stadig i et vist omfang.

I forbindelse med registreringen eller efter denne kan identitetens karakteristika og egenskaber **beskrives i form af attributter** (fx køn, adresse, alder, et nummer i form af fx personalenummer). For medarbejderidentiteter foretages en del af registreringen typisk af en administrator udpeget af virksomhedens ledelse, hvor en central del består i at sikre relationen mellem virksomheden (som juridisk enhed) og medarbejderen (som fysisk person). For IoT-enheder kan en del af registreringen ske af brugeren eller ejeren - fx når en person tilknytter en elektronisk blodtryksmåler til sin profil på en sundhedstjeneste og giver den adgang til at indberette på denne.

### 3.3.2. Forretningsfunktionen autentifikation

Autentifikation er en proces, som genkender og verificerer en identitet (tilknyttet en entitet) gennem anvendelse af et identifikationsmiddel, der er koblet til identiteten som beskrevet ovenfor. Ved multi-faktor autentifikation forstås en autentifikationsproces, hvor det anvendte elektroniske identifikationsmiddel er baseret på flere autentifikationsfaktorer fra forskellige kategorier (noget kun brugeren ved, er, eller er i besiddelse af). Et eksempel her på findes i NemID/MitID, hvor brugerne kan logge på med en kombination af et hemmeligt kodeord og 'swipe' i en App.

Autentifikationsfunktionen varetages i nogle tilfælde af den part, der har udstedt identifikationsmidlet (fx fordi denne kender brugerens password eller en afledt værdi heraf), men kan også være separat for udstederen (fx kan man i PKI-baseret autentifikation verificere brugerens kontrol over den private nøgle op mod det tilhørende certifikat).

Styrken af en autentifikationsproces klassificeres i NSIS som AAL (Authenticator Assurance Level) og indplaceres på den sædvanlig tre-trins skala (Lav, Betydelig, Høj), og kan dermed indgå i adgangspolitikker for tjenester.

I praksis kombineres autentifikationsfunktionen ofte med attributbeskrivelse, således at den identitet, som formidles til tjeneste, er beriget med yderligere oplysninger - og den kombinerede funktion betegnes ofte som *broker* eller *identitetsbroker*. En anden vigtig egenskab ved autentifikationstjenester er, at de kan afkoble forretningstjenester fra at kende til detaljerne i validering af brugernes identifikationsmidler. I føderationer er det bærende princip, at forretningstjenester ikke må udføre autentifikation selv. Ved at delegere denne funktion til en ekstern tillidstjeneste opnås en lang række fordele som fx en mere sammenhængende, sikker og skalerbar arkitektur, hvor brugerne kan genbruge deres identifikationsmidler på tværs af forretningstjenester.

### 3.3.3. Foretningsfunktionen attributbeskrivelse

Som tidligere nævnt bruges termen *attributbeskrivelse* i denne referencearkitektur som en generalisering over 'data om brugere', som i praksis kan dække over en række forskellige aktiviteter udført af forskellige aktører, herunder:

- Administration af brugere i et brugerkatalog (fx et AD) med navn, titel, email, afdeling osv.
- Tildeling (og udstilling) af roller og fuldmagter til brugere

- Udstilling af autoritative data der beskriver brugere som fx CPR-registret, CVR-registret, Sundhedsstyrelsens autorisationsregister mv.
- Autoritativ beskrivelse af relationer mellem brugere og andre objekter/subjekter (ansat i, forælder til, tegningsberettiget for, ejer af, værge for).

Der er således både et aspekt, som vedrører administration, og et aspekt vedrørende udstilling. Førstnævnte handler fortrinsvis om datakvalitet og autoritative kilder, hvor sidstnævnte handler om at gøre attributter tilgængelige for forretningstjenesters adgangskontrol.

Traditionelt har ordet '**autorisation**' også været anvendt i brugerstyring i forskellige betydning om det at have rettigheder til en tjeneste og/eller til data i tjenesten: I denne referencearkitektur benyttes attributbeskrivelse som en bredere og mere generel term end '**autorisation**' for bedre at kunne dække den mangfoldighed af adgangspolitikker, der eksisterer.

Formålet med attributbeskrivelsen er i sidste ende at tilvejebringe grundlaget for den adgangskontrol, der udføres i en forretningstjeneste. En forretningstjeneste kan således have brug for at kende brugerens alder, køn og bopælskommune for at kunne afgøre, hvilket adgang der skal gives. Udførsel af adgangskontrol beskrives nedenfor.

#### 3.3.4. Forretningsfunktionen udforme adgangspolitik

Tjenesteudbydere bør udarbejde en adgangspolitik for deres forretningstjenester, som definerer betingelser for adgang til funktioner og data. En adgangspolitik kan fx udtrykke, at en tjeneste kun må tilgås af identiteter autentificeret på NSIS sikringsniveau Høj, som er tilknyttet et bestemt CVR-nummer, og er tildelt en bestemt rolle. Adgangspolitikker kan i praksis være formuleret mere eller mindre eksplicit (og adskilt fra implementeringen). Eksempelvis kan en borgerrettet selvbetjeningsløsning have en meget simpel politik om, at hver borger (udpeget ved CPR) får adgang til egne data. Det afgørende er, at adgangspolitikken er i overensstemmelse med ledelsens anvisninger i form af informationssikkerhedspolitik, risikovurderinger mv.

For at sikre overensstemmelse mellem adgangspolitik og den efterfølgende adgangskontrol, som håndhæver politikken, kan adgangspolitikken med fordel udtrykkes i termer af attributter, der er tilgængelige via attributbeskrivelsen. Dette er fx særligt relevant i token-baserede realiseringer, hvor adgang opnås på baggrund af attributter beskrevet i et security token. Jo mere standardiserede adgangspolitikker er på tværs af tjenester, jo lettere er det for brugere og brugerorganisationer at administrere i overensstemmelse med adgangspolitikkerne. Fællesoffentligt er visse attributter standardiseret (fx i OIOSAML profilerne), og nogle domæner har standardiseret en række attributter (dette gælder fx på sundhedsområdet).

#### !Figur 3 Adgangsrettigheder – Samspil mellem bruger og tjenesteudbyder

Adgangspolitikker kan benytte roller som basis (Role Based Access Control – RBAC), eller man kan arbejdet direkte med attributter (Attribute Based Access Control – ABAC). I begge tilfælde vil en fælles forståelse kunne udtrykkes med en klassifikation, der systematisk beskriver roller eller andre attributsæt, evt. i form af et hierarki.

#### 3.3.5. Forretningsfunktionen adgangskontrol

**Adgangskontrol** er den proces, hvor en tjenesteudbyder (på baggrund af forudgående autentifikation og attributbeskrivelse) sikrer, at der gives adgang til funktionalitet og data i overensstemmelse med adgangspolitikken. Man taler også om håndhævelse af adgangspolitikken - og nogle tekniske standarder (XACML) opererer med begrebet 'Policy Enforcement Point'. Adgangskontrollen kan endvidere benytte attributter for den aktuelle brugerkontekst (fx brugerens IP-adresse, tidspunktet på dagen, data om brugerens enhed osv.) i beslutningen om adgang.

Adgangskontrol er altid forretningstjenestens ansvar (herunder den dataansvarliges ansvar, hvis tjenesten giver adgang til personoplysninger), men dele af den kan udføres af hjælpefunktioner.

#### 3.3.6. Forretningsfunktionen forebyggelse og kontrol

Forebyggelse af svindel og kontrol med brugeridentiteter er relevant i alle systemer, både i forretningstjenester og i tillidsstjenester. Aftaler om og standarder for kontrol og audits kan være beskrevet i lovgivning, standarder (fx NSIS), vilkår, aftaler, regler i føderationers grundlag mv.

Tillidstjenester indgår typisk som en del af sikkerheden i mange forretningstjenester, og skal have ekstra fokus på kontrol og forebyggelse.

Staten har i december 2014 offentliggjort (og senere revideret) en strategi for cyber- og informationssikkerhed, som har til formål fremover at professionalisere statens arbejde med informationssikkerhed og øge samfundets robusthed mod cyberangreb. Strategien omfatter 27 konkrete initiativer, der skal bidrage til at øge informationssikkerheden og styrke beskyttelsen mod cyberangreb.

Strategien sætter fokus på udfordringerne og skaber en klar retning for den fremadrettede indsats. Truslerne på cyber- og informationssikkerhedsområdet er dog en dynamisk størrelse, og der vil derfor løbende være fokus på effekten af de 27 initiativer.

Strategien indeholder en lang række initiativer på tværs af seks indsatsområder:

1. Professionalisering og styrket it-tilsyn
2. Klare krav til leverandører
3. Styrket cybersikkerhed og mere viden på området
4. Robust infrastruktur i energisektoren og telesektoren
5. Danmark som stærk international medspiller
6. Stærk efterforskning og klar information til borgere, virksomheder og myndigheder.

Med den stadigt stigende hackeraktivitet kloden over bliver arbejdet med at sikre kvaliteten af kontrol og forebyggelse af sikkerhedsbrud mere og mere vigtigt. Det skal ske i forbindelse med den registrering, autentifikation, billetudstedelse og adgangskontrol, der er kernen i brugerstyring. Dermed er det også et emne for informationssikkerhedspolitikken og dennes udmøntning i en tværgående fællesoffentlig foderation.

Flere af de angreb mod organisationers it-infrastruktur som opleves, er rettet mod at forfalske identiteter, identifikationsmidler og adgangsbilletter, eller at give sig ud for at være den rette ihændeher af identiteter, identifikationsmidler og adgangsbilletter. Det centrale i forhold til brugerstyring er derfor hurtigt at kunne reagere ud fra den mest aktuelle viden gennem sikkerhedsforanstaltninger. Andre angreb forsøger at begrænse tilgængeligheden gennem Distributed Denial of Service-angreb mod kritiske elementer i it-infrastrukturen, herunder fællesoffentlige identitetssystemer. Center for Cybersikkerhed udsender jævnligt en opdatering af det aktuelle trusselsbillede for cyberangreb.

Til at styrke området har staten samlet kræfterne i Center for Cybersikkerhed (CFCS), og nogle private organisationer udstiller deres CERT eller CSIRT-funktion. Disse organisationer håndterer sikkerhedshændelser og arbejder på at forebygge sikkerhedshændelser:

- Netsikkerhedstjenesten i CFCS rummer statens Computer Emergency Response Team (CERT)
- NC3 er statens National Cyber Crime Center under Rigspolitiet
- DKCERT er Danmarks akademiske Computer Emergency Response Team under Danish e-Infrastructure Cooperation (DeIC), der overvåger netsikkerheden på forskningsnettet
- Finanssektoren har etableret en nordisk FinansCERT, der deler oplysninger om cybertrusler på tværs af de nordiske banker.
- Flere større virksomheder har deres eget computer security incident response team (CSIRT), et synonym for CERT.

Der stilles desuden i højere grad krav om notifikation til relevante myndigheder i forbindelse med sikkerhedshændelser. Fx skal tillidstjenesteudbydere, jf. eIDAS, notificere Digitaliseringsstyrelsen, og i medfør af persondataforordningen (GDPR), skal dataansvarlig notificere Datatilsynet ved sikkerhedshændelser. Som led i et beredskab skal man således sikre sig, at man kan informere de rette myndighed inden for fastlagte tidsrammer.

En af de forebyggende aktiviteter, en tjenesteudbyder kan udføre, er at sikre en solid logning af al aktivitet, og herefter kan en kontrol kontinuerligt monitorere for angrebsforsøg med automatiserede værktøjer suppleret med menneskelig, analytisk kapacitet. Et andet eksempel er anvendelsen af 'risk data' i MitID-løsningen, som ud fra en række data om brugerens udstyr, adfærd, geolokation, netværk og andet forsøger identificere risikofyldte transaktioner på tværs af tjenesteudbydere og brokere i infrastrukturen. Eksempelvis vil en bruger, der logger på fra to forskellige lande inden for et kort tidsrum, kunne give udslag i en høj riskoscore, som forretningstjenesten herefter kan reagere på.

Et andet væsentligt element i sikkerheden er, at alle processerne i administration og vedligeholdelse af brugerstyring implementeres. Det gælder såvel identiteters karakteristika gennem brugeres livscyklus som tjenesters adgangsbilletter, når tjenester videreudvikles. Undervejs i identiteters livscyklus sker der ændringer i registreringspraksis, i valg af anvendte identifikationsmidler og i beskrivelse af attributter, herunder roller og terminering af alle rettigheder for en bruger ved fx jobskifte, dødsfald og lign. I jo højere grad dette kan automatiseres, jo mere sikker er man på, at data ajourføres.

### 3.4. Tillidskæder i økosystemer

[TG: Jeg tænker at dette skal flyttes ned under teknikafsnit]

I et sammenhængende, skalérbart og sikkert økosystem af tillidstjenester og forretningstjenester, skal mange aktører kunne arbejde sammen i en orkestrering af de forskellige services. Med henblik på at der kan ske en sådan specialisering og arbejdsdeling, er der behov for regler og aftaler, der gør, at aktørerne kan have tillid til hi-

nanden. De aktører, som indgår i et tillidsforhold, udgør **en føderation**, som bygger bl.a. på et trust framework som fx NSIS, eIDAS eller aftaler i et domæne.

Nedenstående tegning i figur 4 illustrerer den kæde af tillid, der kan optræde mellem tillidstjenester og forretningstjenester i et komplekst scenarie. Denne kæde skal være identificeret og beskrevet i en føderation, hvor der kan være en række tillidstjenester involveret i føderationen. Man skal her være eksplicit om, hvilket sikringsniveau de enkelte tjenester opererer på, for det vil være det laveste sikringsniveau i hele kæden, der er bestemmende for det samlede sikringsniveau. For enkelhed i illustrationen er der her tegnet en føderation med kun én af hver tillidstjeneste repræsenteret.

Figur 4 Kæde af tillid i et tjenestekald

- Tjenesteudbyderen af forretningstjenesten skal have tillid til, at adgangskontrollen (engelsk: Policy Enforcement Point, PEP) kun viderestiller identiteter, hvis adgangsbillet matcher adgangspolitikken for forretningstjenesten. Tjenesteudbyderen varetager som hovedregel selv adgangskontrollen, men denne funktion kan varetages af en ekstern tjeneste.
- Adgangskontrollen bygger på tillid til, at den adgangsbillet en broker har udstedt, indeholder korrekte attributter og er sket på baggrund af en gyldig autentifikation.
- Broderen har tillid til, at autentifikationstjenesten på en sikker måde har kunnet fastslå brugerens identitet (autentificere vedkommende).
- Autentifikationstjenesten har tillid til, at udstederen af identifikationsmidlet, der har tilknyttet og udstedt identifikationsmidlet, har gjort det til de rette entiteter, nemlig de samme entiteter, som registreringstjenesten (eng: Registration Authority, RA) har identificeret og registreret identiteten på.
- I den udstrækning, som tjenesteudbyderen, adgangskontrollen, broderen eller autentifikationstjenesten anvender et eller flere attributsæt, skal disse have tillid til de attributtjenester, som de anvender.
- Attributtjenester skal have tillid til, at den der har tilknyttet og udstedt akkreditiverne, har gjort det til de rette entiteter, nemlig de samme entiteter som registreringstjenesten har identificeret og registreret identiteten på.
- Udstederen af elektroniske identifikationsmidler har tillid til de identifikationsbeviser (fx pas, kørekort) og grunddata, som udstedelsesprocessen er baseret på.
- Hele vejen gennem kæden skal der være tillid til de billetter (eng. *security token*), der udstedes af autentifikationstjenesten og beriges af brokere, og som benyttes som billet med tidsbegrænset gyldighed til en eller flere tjenester – også når adgangsbilletter omveksles ved overgang mellem sektorer.

Så længe alle tjenester i tillidskæden ligger inden for egen organisation, kan organisationens egen governance sikre tillidskæden. Når en organisation vælger at basere sig på eksterne tillidstjenester, forudsætter det, at tillid er etableret gennem et trust framework omfattende bl.a. aftaler og standarder.

I en føderation mellem en række sektorer, der hver har deres sikkerhedsdomæner, skal tilliden udvides til at omfatte komponenter som autentifikationstjenester, attributtjenester og billettjenester fra alle involverede sektorer hos alle deltagere i føderationen. Desuden er det centralt at fastlægge de kombinationer af tillidstjenester, der giver et konkret sikringsniveau, og som alle i føderationen har tillid til. Det er nødvendigt helt specifikt at beskrive den datastrøm gennem tjenesterne, der giver et bestemt sikringsniveau.

### 3.4.1. Tillid gennem NSIS

I National Standard for Identiteters Sikringsniveauer (NSIS) skal elektroniske identifikationsordninger (udstedere af identifikationsmidler) og identitetsbrokere anmeldes til Digitaliseringsstyrelsen, før de må benytte NSIS, herunder påstemple NSIS sikringsniveauer på en brugerautentifikation. Kravene til dokumentation for compliance stiger gennem sikringsniveauerne:

- På niveau Lav kan man benytte 'selvdeklarering', hvor anmelder selv indestår for opfyldelse af krav.
- På niveau Betydelig og Høj skal der vedlægges en ISAE 3000 revisionserklæring fra en uafhængig, statsautoriseret revisor. Erklæringens formål er at konkludere, hvorvidt en anmelder samlet set har etableret alle relevante kontroller og procedurer for sin løsning.

Revisionen er dermed en tillidsskabende foranstaltning, som gentages årligt, og derudover skal der afgives en ledelseserklæring første gang ved anmeldelsen.

Digitaliseringsstyrelsen gennemgår anmeldelsen og publicerer herefter denne på sin hjemmeside med angivelse af anmeldt sikringsniveau. Styrelsen er kun forpligtet til at kontrollere formalia, idet revisor skal verificere implementeringen. Digitaliseringsstyrelsen kan desuden afmelde en ID-tjeneste, som ikke lever op til kravene.

NSIS stiller ikke krav til forretningstjenesten med stiller sikringsniveauerne til rådighed for deres adgangspolitikker og -kontroller. Det anbefales at forretningstjenester på baggrund af en risikovurdering fastlægger hvilket sikringsniveau, der som minimum kræves for at få adgang til tjenesten.



### 3.5. Forretningsroller og aktører - og deres behov

Forretningsbehovene tager udgangspunkt i de udfordringer, offentlige virksomheder fremover skal være i stand til at håndtere. Scopet for referencearkitekturen for brugerrettighedsstyring er især behov vedrørende sammenhængende, effektive, sikre og brugervenlige løsninger på tværs af domæner, nationalt og transnationalt.

Forretningsbehovene er beskrevet ud fra flere synsvinkler, idet interessenterne har flere roller, som har betydning for behov:

- Behov hos personer – både som borgere og medarbejdere
- Behov hos virksomheder og myndigheder som brugerorganisationer og arbejdsgivere
- Behov hos virksomheder og myndigheder som tjenesteudbydere og som udbydere af brugerstyringstjenester

#### 3.5.1. Personer – som borgere og som medarbejdere

Borgere og medarbejdere forventer først og fremmest, at tjenester er let tilgængelige – og herunder ikke mindst at obligatoriske systemer er så smarte, som teknologien tillader.

Nogle personer har primært fokus på brugervenlighed og mindre på sikkerhed og privacy. For disse personer skal der være mulighed for at vælge så meget brugervenlighed, som hensyn til lovgivning og sikkerhed tillader. Andre personer har fokus på sikkerhed og privacy. For disse personer skal der være mulighed for løsninger, hvor personen selv har en højere grad af kontrol over, hvilke data tjenester får adgang til og indsigt i, hvilke aktiviteter deres elektroniske identiteter udfører, mulighed for anonymitet mv. Tilbud til brugerne skal dog til enhver tid bygge på en høj sikkerhed, så borgernes data ikke kompromitteres.

Et ofte udtalt brugerbehov er ønsket om at kunne anvende samme identifikationsmiddel på tværs af tjenester og sektorer - og ofte også gerne i kombination med single sign-on. Dette kan i høj grad opnås ved anvendelse af foderationsprincippet beskrevet i denne referencearkitektur. Et andet behov er, at brugerne på den ene side bør have indsigt i / kontrol over hvordan deres data flyder (herunder attributter), og på den anden side ofte har et ønske om ikke at skulle indtaste de samme oplysninger flere gange (once-only princippet).

Et eksempel på håndtering af balancen mellem brugervenlighed og privacy er, at det bliver muligt i højere grad for personer at anvende deres private identifikationsmodel i tilknytning til en erhvervsidentitet med NemLog-in3 og MitID. Dette sker med respekt for det *dobbelte frivillighedsprincip*, hvor et privat identifikationsmiddel kun anvendes i erhvervssammenhæng, hvis *både* medarbejder og virksomhed siger god for det. Begge parter kan med andre ord vælge det fra. Samtidig holdes privat- og erhvervsidentiteten fuldstændigt adskilt i overensstemmelse med tidligere beskrevne principper (kun identifikationsmidlet genbruges).

Nogle medarbejdere anvender deres akkreditiv mange gange i løbet af en arbejdsdag. For denne brugergruppe er det derfor væsentligt, at det er let og effektivt at anvende sit akkreditiv.

En del borgere har behov for at kunne give andre fuldmagt til at løse opgaver for sig. For de borgere, som afgiver og får fuldmagt, er der behov for løsninger til at administrere fuldmagter, som giver et overblik på tværs af tjenester, så brugeren ikke skal logge ind i mange tjenester for at se eller administrere fuldmagter. Det tilsvarende gælder for samtykke.

I forhold til de tekniske realiseringer har personerne behov for løsninger, der:

- Kan anvendes på forskellige typer udstyr
- Kan dække mange forskellige brugerkompetencer og behov
- Kan dække mange brugsscenarier, herunder også scenarier hvor tjenester tilgås via systemer, ting eller apps.

[Se i øvrigt også juridiske rammer. Men det er mere rettigheder end behov /madsh]

#### 3.5.2. Virksomheder og myndigheder som brugerorganisationer

Virksomheder og myndigheder har behov for nem og sikker adgang til eksterne tjenester, både web-baserede og gennem fag-applikationer. Da der er mange – og et stigende antal – eksterne tjenester, har virksomheder og myndigheder behov for at have ensartede metoder til at tilgå disse tjenester.

En situation, hvor hver tjeneste tildeler egne brugernavne, passwords eller andre identifikationsmidler, er til stor ulempe for mange virksomheder, og dette problem vil øges fremover, hvis der ikke sikres ensartede løsninger.

Mange meget små virksomheder og andre organisationer har brug for meget enkle løsninger til autentifikation og signering, og i nogle tilfælde kan brugeradministration for en stor del automatiseres og dermed ikke optræder synligt for virksomheden.

Små og mellemstore virksomheder, foreninger og anpartsselskaber med flere medarbejdere har behov for enkel brugeradministration, hvor rettigheder set med brugernes øjne administreres ét samlet sted for offentlige selvbetjeningsløsninger.

Større virksomheder har brug for forskellige løsninger, der både kan omfatte manuel indtastning, digital provisionering og eventuelt føderering. Større virksomheder har egen brugerstyring, og de kan generelt have behov for god sammenhæng mellem deres egen brugerstyring og ekstern brugerstyring.

Nogle mellemstore og større brugerorganisationer har brug for en klar adskillelse mellem borgerløsninger og medarbejderløsninger og for selv at kunne kontrollere de tekniske løsninger i sammenhæng med organisationens egen tekniske infrastruktur. De har behov for en høj grad af sammenhæng og effektivitet i administrationen af medarbejdernes elektroniske identiteter.

Der er generelt behov for en brugergrænseflade til administration, for digital provisionering og for føderede løsninger, hvor administration sker i egen brugerstyringsløsning.

Mange brugerorganisationer har behov for at få styr på deres mange forskellige eksisterende løsninger (legacy) og ønsker at arbejde frem med større ensartethed, sammenhæng og automatisering, eksempelvis automatisering ved begivenheder som ansættelse, tildeling af identitet, roller og rettigheder, organisatorisk omplacering og fratrædelse. De har desuden behov for kontrol af medarbejdernes anvendelse af elektronisk identitet på virksomhedens vegne, da det både juridisk og kommercielt kan være forpligtende for brugerorganisationen, hvad en medarbejder gør.

### 3.5.3. Virksomheder og myndigheder som tjenesteudbydere

Det er et fælles behov for tjenesteudbydere at kunne trække på modne tillidstjenester på en standardiseret måde, således at tjenesteudbydere afskærmes fra kompleksiteten i at håndtere og administrere brugeridentiteter, identifikationsmidler mv. Når man bygger en forretningstjeneste, er det ofte komplekst og ressourcekrævende selv at håndtere brugerstyring, og der er ofte en god business case i at få det som en ekstern tjeneste.

En stor del af de offentlige tjenester rummer fortrolige eller personhenførbare data, som er dækket af sikkerhedsskrav i persondatareguleringen, og som dermed skal opnå et tilstrækkeligt sikringsniveau. Flertallet af offentlige tjenester har behov for at kende borgerens CPR-nummer og i nogle tilfælde medarbejderens - dette gælder eksempelvis på sundhedsområdet. Andre offentlige tjenester har ikke samme behov / sikkerhedsskrav og kan nøjes med et lavere sikringsniveau.

Forskellige sektorer har forskelligartede behov:

- Myndigheder er omfattet af reglerne om partsrepræsentation i forvaltningsloven, og deres tjenester skal derfor understøtte anvendelse af digital fuldmagt eller alternativt etablere manuelle løsninger til partsrepræsentation.
- Tjenester i den finansielle sektor er underlagt sikkerhedsskrav samt krav om verificering af kundeidentiteter, dels i kraft lovgivning om hvidvask dels i medfør af PSD2 direktivet.
- Tjenester i spilsektoren er forpligtet ved lov til at anvende stærk autentifikation samt at kontrollere, at identiteten ikke er omfattet af spærrelisten. Tjenesterne har ikke et behov for præcis identifikation med navn.
- En virksomhed som "Den Blå Avis/DBA" har brug for at kunne garantere mod svindel, hvilket de aktuelt håndterer ved, at sælgerne og køberne kan blive NemID-valideret. DBA identificerer ikke personer med CPR, men anvender i stedet certifikatets PID, hvilket kan anses som en privacy-mæssig fordel.
- Regionerne har mange private aktører som medtjenesteudbydere.

En række tjenester har lavere sikkerhedsskrav end ovennævnte, men har stadig brug for sikker identifikation med færre oplysninger om brugeren. Det er fx ehandelstjenester, der har brug for at kende borgerens adresse eller tjenester, eller der har brug for at kende brugerens alder (fx over/under 18 år). For disse tjenester er der økonomiske fordele ved kun at kende ikke-fortrolige data, da der i så fald ikke skal anvendes ressourcer på at sikre fortrolige data. Dette er ligeledes i overensstemmelse med dataminimeringsprincippet i GDPR.

Brugerne skal kunne autentificeres på flere sikringsniveauer svarende til tjenesternes behov for sikkerhed. Tjenesteudbydere har for nogle tjenester behov for at kunne sikre, at en bruger kun får adgang til ressourcer eller data, der relaterer til den enkelte brugers aktuelle opgave. Sundhedsdomænet har eksempelvis behov for løs-

ninger, der kan sikre, at kun sundhedspersonale, der reelt har en relation til behandlingen af en patient, får adgang til patientdata (behandlerrelation).

Tjenesteudbydere har behov for kontrol med, hvem der har logget ind og udført hvilke handlinger i tjenester.

Etablerede tjenester har behov for kontinuitet (bagudkompatibilitet), idet der kan være store omkostninger ved at ændre integrationer til tværgående brugerstyringsløsninger.

### 3.6. Principper???

[Jeg vil foretrække principper spredt ud i det afsnit de hører mest til, og opsummeret i resume /madsh]

Dette afsnit formulerer rammer for de egenskaber, som løsninger inden for offentlig brugerstyring skal have. Formålet er at sikre, at de forskellige løsninger samlet set bringer brugerstyring i Danmark frem mod de mål og de gevinster, den nationale strategi for brugerstyring fastlægger. Rammerne formuleres som principper, som alle projekter og programmer skal orientere sig efter og enten følge eller forklare.

Principperne konkretiseres med beskrivelse af rationale – hvilket mål og gevinstprincippet forfølger – og implikation – en instruktion i, hvad det konkret vil sige at følge princippet. Hvis et projekt eller program mener, at det er for problematisk at følge princippet, skal projektet eller programmet forklare hvorfor, og tillige forklare hvordan man på længere sigt kan bringe løsningen inden for rammerne, som princippet angiver. [!Figur 5 Styrende principper](#)

Referencearkitekturen for brugerstyring fastlægger følgende principper for at styre frem mod en fælles forretnings- og it-arkitektur for det offentlige elektroniske identiteter, autentifikation og adgangskontrol. Som overordnet ramme for disse principper ligger de ti tværoffentlige overordnede principper for forretnings- og it-arkitektur(<http://arkitekturguiden.digitaliser.dk/principper/10-overordnede-principper>), og hvad der står heri gentages ikke. Det skal her bemærkes, at disse principper opdateres som følge af arbejdet med hvidbogen for den fællesoffentlige rammearkitektur, hvilket kan give anledning til ændringer i kommende udgaver af denne referencearkitektur.

*Principper med brugersfokus:*

1. Brugere oplever en sammenhængende adgangsstyring
2. Brugerstyringsløsninger udvikles med fokus på brugernes behov
3. Brugerstyringsløsninger respekterer brugernes privatliv

*Principper med teknisk fokus:*

4. Aktører indgår i føderationer baseret på tillid
5. Aktører i føderationer vurderer i deres styring af informationssikkerhed samspillet med andre aktører
6. Administration af brugere flyttes så vidt muligt ud af fagapplikationer
7. Tjenesteudbyder (den dataansvarlige) har ansvaret for at håndhæve brugernes adgange

*Principper med udviklingsfokus*

8. Brugerstyring realiseres i løst koblede komponenter
9. Tværoffentlige brugerstyringsløsninger baseres på en kerne af fælles komponenter i samspil med øvrige komponenter i infrastrukturen
10. Tværoffentlig brugerstyring etableres i overensstemmelse med internationale standarder og løsninger

#### **Princip 1: Brugere oplever en sammenhængende adgangsstyring**

Brugere vil i deres dialoger med offentlige myndigheder skulle betjene sig af en række forskellige tjenester. Disse tjenester skal opleves sammenhængende, uanset hvor mange tjenester eller myndigheder der er involveret.

*Rationale*

- Borgere og virksomheder vil opleve en bedre og mere gnidningsfri løsning af deres opgaver, der kræver forretningsprocesser på tværs af organisationer og sektorer. Dette vil medvirke til at fjerne en væsentlig barriere for udviklingen mod fuld digitalisering, så digitale tjenester fungerer nemt og effektivt, uanset hvilken situation man er i.
- For udviklings- og supportfunktioner betyder det, at de vil få mere tilfredsebrugere og fx færre supporthenvendelser fra brugere, der ikke kan finde ud af at logge på.

*Implikationer*

- Brugere skal, hvor det er relevant, kunne afgive samtykke til, at deres oplysninger anvendes til angivne formål, og at oplysningerne er grundlag for handlinger inden for en føderation i forbindelse med brugerstyring.
- Brugere skal kunne delegerede fuldmagt til andre elektroniske identiteter og have et samlet overblik over afgivne og modtagne fuldmagter på tværs af tjenester.
- Brugere skal opleve en sammenhæng mellem autentifikation og evt. senere signering.
- Brugere skal opleve en sammenhængende administration af oprettelse af brugere, administration af fuldmagter og administration af rettigheder.
- Brugere skal i videst muligt omfang have brugergrænseflader, hvor krav til sikkerhed og privacy forenes med krav om brugervenlighed.
- Brugere skal tilbydes Single Sign-On i brugerforløb, der krydser flere tjenester.

*! Princippet om sammenhængende adgangsstyring for brugere SKAL efterkommes i fællesoffentlige løsninger, herunder det fællesoffentlige eID og NemLog-in samt af tjenester, der anvender disse. For øvrige BØR princippet efterkommes.*

### **Princip 2: Brugerstyringsløsninger udvikles med fokus på brugernes behov**

Brugerstyringsløsninger anvendes af mange forskellige borgere, medarbejdere, virksomheder og myndigheder som brugerorganisationer og tjenesteudbydere. Disse brugere har meget forskelligartede behov afhængig af brugssituationen, det anvendte udstyr, virksomhedens karakter, størrelse og sikkerhedsbehov. Brugerstyringsløsningerne udvikles med henblik på at dække de forskellige brugeres behov.

#### *Rationale*

- Måltrettet dækning af forskellige behov øger brugertilfredshed og effektivitet.
- Innovation fordrer plads til forskellighed (inden for en veldefineret ramme).
- Brugere og tjenesteudbydere ønsker både lette løsninger, billige løsninger og sikre løsninger. At tilbyde løsninger måltrettet forskellige brugergrupperes behov bidrager til at dialogen med det offentlige bliver nem og effektiv.

#### *Implikationer*

- Standarder og komponenter skal være så fleksible, at de kan anvendes til differentierede, målrettede løsninger, fx også mobile løsninger.
- Løsninger skal stadig overholde referencearkitekturen for brugerstyring, dvs. respektere strukturen af tjenester og standarder for overførsel af informationer mellem tjenester.

*! Princippet om fokus på brugernes behov SKAL efterkommes i fællesoffentlige løsninger, herunder det fællesoffentlige eID og NemLog-in. Princippet BØR efterkommes af tværoffentlige brugerstyringsløsninger. Princippet BØR efterkommes af brugerrettede tjenester, der anvender ovenstående brugerstyringsløsninger. For øvrige KAN princippet efterkommes.*

### **Princip 3: Brugerstyringsløsninger respekterer brugernes privatliv**

Fællesoffentlig brugerstyring indebærer, at information om brugere lagres og udveksles mellem registrerings-tjenester, autentifikationstjenester, attributtjenester, identitetsbrokere og tjenester. Brugerstyringsløsninger skal beskytte information om brugere (fortrolighed) og indhente og udveksle så lidt information som muligt (Data Minimisation).

#### *Rationale*

- Persondataloven og EU-forordningen om beskyttelse af personoplysninger (GDPR) stiller en række krav til beskyttelse af borgernes privatliv (privacy).
- Brugernes privatliv respekteres ved, at brugere kan se, hvad data bruges til (transparens), og ved at brugere skal kunne træffe valg (samtykke). Dette understøtter, at personoplysninger kun videregives efter "Data Minimisation"-princippet.
- Transparens styrker brugernes tillid til offentlige digitale tjenester.

#### *Implikationer*

- Registreringstjenester, autentifikationstjenester, attributtjenester og identitetsbrokere skal ikke registrere og videregive overflødige informationer om brugere.
- Danske offentlige tjenester må fortsat bruge CPR-nummeret, men skal overveje kun at anvende det, hvor det er nødvendigt.
- Det skal være tydeligt for brugeren, hvad oplysningerne anvendes til.



- En brugerstyringstjeneste bør vælge at give borgeren adgang til at se alle informationer og opdatere alle eller nogle af de informationer, som tjenesten vedligeholder om brugeren.
- Brugeren bør have adgang til at få rettet unøjagtige eller fejlagtige persondata, hvis der ikke er mulighed for selv at rette data.

*! Princippet om respekt for brugernes privatliv SKAL efterkommes i fællesoffentlige løsninger, herunder det fællesoffentlige eID og NemLog-in. For øvrige SKAL princippet efterkommes.*

**Princip 4: Aktører indgår i føderationer baseret på tillid og aftaler** [Måske et nyt princip 2: Føderation /madsh]

Aktørerne bør overholde en række fælles standarder for identiteter, fælles sikkerhedspolitikker og aftaler, og tilbyde servicekald på tværs af føderationernes grænser, således at aktører i forskellige organisationer kan indgå i føderationer. I denne sammenhæng omfatter aktører både myndigheder og virksomheder i rollerne som brugerorganisationer, tjenesteudbydere og udbydere af brugerstyringstjenester. Aktører kan også omfatte private tjenesteudbydere og brugerstyringstjenesteudbydere, såfremt de ansvarlige for føderationen vælger dette.

*Rationale*

- Gennem etablering af føderationer vil man over en årrække kunne fjerne nogle stærke sikkerheds- og teknologiske barrierer for udnyttelse af digitalisering.
- Den fødererede model muliggør, at brugeradministrationen (oprettelse og nedlæggelse af brugere samt tildeling af attributter) udføres lokalt i organisationens egen brugerstyringsløsning (fx Active Directory eller anden Identity Management-løsning). Herved kan organisationer af en vis størrelse og modenhed vælge en løsning, så de undgår dobbelt vedligehold af de samme brugere, og administrationen sker tættest på brugerne med størst viden om deres jobfunktioner og med størst sikkerhed for korrekthed og hurtig respons på ændringer.
- En fødereret model gør det muligt for private aktører at indgå i eller i samspil med offentlige føderationer, såfremt dette vælges af føderationen.

*Implikationer*

- En føderation definerer klart og entydigt såvel rammer som indhold af de former for elektroniske identiteter, autentifikationer og adgangskontroller, som en gensidig tillid baseres herpå. Det gælder både teknisk og organisatorisk.
- For føderationen defineres en styringsmodel (governance) for, hvorledes føderationens rammer og indhold vedligeholdes, og for kvalitetskrav til og ansvarsforpligtigelser hos de organisationers brugerstyringsadministration, som indgår i føderationen.
- Der udarbejdes et trust framework med evt. akkreditering og certificering baseret på en risikovurdering.
- Der udøves kontrol og defineres sanktionsmuligheder.

*! Princippet om føderationer baseret på tillid og aftaler BØR efterkommes i fællesoffentlige løsninger, herunder det fællesoffentlige eID og NemLog-in og i tværoffentlige brugerstyringsløsninger. Princippet BØR efterkommes i tjenester, der anvender disse. For øvrige KAN princippet efterkommes.*

**Princip 5: Aktører i føderationer vurderer i deres styring af informationssikkerhed samspillet med andre aktører**

I brugerstyring, hvor opgaverne løses af forskellige aktører i føderationer, og som bygger på en kæde af tillid og aftaler mellem parterne, er sikkerheden afhængig af den enkelte aktørs interne sikkerhed samt af sikkerheden i samspillet mellem aktører.

*Rationale*

- Der er klare regler for den enkelte aktørs ansvar for sikkerheden, og tilsynet hermed varetages af overliggende myndigheder og revision (fx Rigsrevisionen).
- Der er behov for præcisering af, hvilket ansvar for den enkelte aktør der følger af, at denne aktør er afhængig af og påvirker sikkerheden hos andre aktører.
- Der er behov for vurdering af samspillet mellem aktørerne i føderationer, fx for hvordan sikkerhedsrisici og -hændelser skal formidles til andre aktører i føderationer.

*Implikationer*

- De risici, der beror på arbejdsdeling mellem aktørerne, skal håndteres ved, at hver enkelt aktør skal vurdere samspillet med andre aktører i sin sikkerhedsmæssige risikovurdering i henhold til fx ISO/IEC 27001.
- Aktører i føderationer skal i relevant omfang informere andre aktører i føderationen om risikovurderinger og sikkerhedshændelser.

*! Princippet om styring af informationssikkerhed i føderationer er en følge af ISO/IEC 27001, ISO/IEC 27005, EU's General Data Protection Regulation (GDPR) og den danske persondatalov og SKAL efterkommes i fællesoffentlige løsninger, i tværoffentlige brugerstyringstjenester og i tjenester, der anvender disse, samt i andre offentlige løsninger.*

**Princip 6: Administration af brugere flyttes så vidt muligt ud af fagapplikationer** [Måske et nyt princip 1 /madsh]

Historisk har fagapplikationer, der anvendes på tværs, selv forvaltet brugeres identiteter, akkreditiver og attributter med det resultat, at den samme bruger har mange forskellige elektroniske identiteter og akkreditiver, og at disse identiteter ikke kan anvendes på tværs af tjenester. Fagapplikationerne skal i stedet kunne indgå i føderationer på tværs af organisationsenheder og myndigheder - og agere som konsument af identitet leveret af andre.

*Rationale*

- Det giver mindre overlap, sub-optimering og dublering af løsninger, hvilket sparer penge ved udvikling og drift af applikationerne og resulterer i mere effektive løsninger.
- Brugeradministrationen effektiviseres, idet brugerne ikke skal vedligeholdes mange forskellige steder.
- Muliggør adgangsstyring på tværs af løsninger i de forskellige domæner.
- Sikkerheden øges, idet erfaringen er, at brugere der forlader en organisation, sjældent får ændret status rettidigt og derfor bliver til en sårbarhed for den organisation, vedkommende forlader. Et arbejdsophør kan automatisk udløse, at identiteten bliver suspenderet eller spærret, og at alle rettigheder bliver blokeret for denne identitet.

*Implikationer*

- Brugernes identiteter, akkreditiver og attributter administreres ikke i de enkelte fagapplikationer. Information om identiteter og attributter leveres i stedet til applikationen af identitetsbrokere i en adgangsbillet.
- Der skal etableres fællesoffentlige føderationer baseret på valg af fælles politikker, regler og obligatoriske standarder inden for et område, hvor dette giver gevinster.

*! Princippet om administration af brugere uden for fagapplikationer BØR efterkommes i fællesoffentlige løsninger, herunder Digital Post, i tværoffentlige brugerstyringstjenester og i tjenester, der anvender disse. For øvrige KAN princippet efterkommes.*

**Princip 7: Tjenesteudbyder (den dataansvarlige) har ansvaret for at håndhæve brugernes adgange** [Hvem kunne det ellers være? NATO som anti-pattern? Følger princippet af GDPR? /madsh]

De fælles elementer i brugerstyring forsyner en elektronisk identitet med attributter, der fremsendes til den tjeneste, som brugeren vil have adgang til. Det er tjenesteudbyder, der har ansvaret for at håndhæve brugeres adgange til tjenesten på grundlag af information fra en identitetsbroker (og eventuelt supplerende lokale attributter). Tjenesteudbyder har ansvaret for ud fra sin adgangspolitik at afgøre, om brugeren får adgang.

*Rationale*

- Det er hos tjenesteudbyder, at viden om konsekvenserne af at give adgang kan findes, og det er derfor tjenesteudbyder, der har ansvaret for at afgøre, om der gives adgang.
- Det juridiske ansvar for at håndhæve adgangen til tjenesten ligger hos dens ejer (den dataansvarlige, jf. fx persondataloven).

*Implikationer*

- Funktioner til styring af adgangskontrol skal bygges i sammenhæng med tjenesterne.
- Der kan inden for sikkerhedsdomæner være en gevinst i at vedligeholde fælles adgangspolitikker og i sammenhæng hermed et sæt fælles attributter på tværs af aktører og tjenester i sikkerhedsdomænet.

*! Princippet om tjenesteudbyderes håndhævelse af brugeres adgang er en følge af krav i persondataloven om dataansvar, og derfor SKAL det efterkommes af alle med dataansvar for fagapplikationer med persondata. Det BØR efterkommes af alle med dataansvar for fagapplikationer uden persondata.*

**Princip 8: Brugerstyring realiseres i løst koblede komponenter**

Stadig flere løsninger for administration af elektroniske identiteter, autentifikation og adgangskontrol er præget af stigende arbejdsdeling og opdeling i løst koblede komponenter, der kan kombineres efter behov. De nødvendige aktiviteter omkring identitet og adgangsstyring skal logisk opdeles i udstedelse af akkreditiver, autentifikation af en given identitet, adgangskontrol, vedligeholdelse af attributter og vedligeholdelse af brugeres identiteter og adgange. På sigt vil vi sandsynligvis se en yderligere opdeling.

*Rationale*

- Løst koblede, sammensatte komponenter og standarder for informationsoverførsler mellem de definerede rammer, som leverandører kan agere i. Dette giver større fleksibilitet og bedre udnyttelse af udvikling og innovation i markedet, og aktørerne kan udnytte og udfolde det løsningsrum, som rammerne giver.
- En åben og modulær arkitektur giver mulighed for at udskifte/varierte deløsninger, integrere nye teknologier og implementere ændrede regler og politikker. Dette leder til større agilitet og ændringsparathed.
- En opdeling i komponenter skal reducere den samlede kompleksitet af den fællesoffentlige brugerstyring.

*Implikationer*

- En anvendelse af referencearkitekturen skal definere et overordnet sæt tjenester eller byggeblokke for brugerstyring og et antal områder for fællesoffentlige standarder for, hvordan disse udveksler adgangsbilletter og attributter. Enhver løsning inden for brugerstyring skal tage udgangspunkt i disse tjenester og skal overholde disse standarder.
- Anvendelse af åbne, løst koblede komponenter håndteret af flere aktører forudsætter, at der er tillid mellem parterne, jf. 4.4.
- Åbne, løst koblede komponenter implementeres, så brugerne får en sammenhængende brugeroplevelse.
- Standarderne for informationsoverførsler mellem de løst koblede komponenter tager udgangspunkt i internationalt anerkendte standarder inden for EU eller globalt.

*! Princippet om løst koblede brugerstyringskomponenter SKAL efterkommes i fællesoffentlige løsninger, herunder fællesoffentlige eID og NemLog-in. Princippet BØR efterkommes af tværoffentlige brugerstyringsløsninger. For øvrige KAN princippet efterkommes.*

**Princip 9: Tværoffentlige brugerstyringsløsninger baseres på en kerne af fælles komponenter i samspil med øvrige komponenter i infrastrukturen**

I opbygningen af en digital infrastruktur har det offentlige gentagne gange opnået gode resultater ved at gå sammen om at opbygge en fælles kerne, som fungerer i samspil med øvrige komponenter. Det gælder fx NemID, NemLog-in og Datafordeleren der er fællesoffentlige, men det kan også gælde komponenter udviklet i en speciel kontekst som fx WAYF eller UNI-Login der indgår i et samspil på tværs.

*Rationale*

- Infrastrukturløsninger kræver store investeringer og kan som oftest kun opbygges ved at flere parter går sammen.
- Der er besparelser ved at opbygge en kerne i fællesskab, som alle kan anvende, i stedet for at der udvikles flere komponenter, som delvist dækker samme opgaver.
- En fælles kerne af infrastruktur og principper giver et operationelt grundlag for at opbygge løsninger med den målsatte sammenhæng og kvalitet.

*Implikationer*

- Ambitioner og omfang af den fælles kerne skal aftales mellem de centrale parter.
- Der er løbende behov for at tage stilling til balancen mellem den fælles kerne og de decentrale elementer.

*! Princippet om brugerstyring baseret på fælles kerne i samspil med decentrale komponenter SKAL efterkommes af alle fællesoffentlige løsninger. For de øvrige løsninger BØR princippet efterkommes.*

**Princip 10: Tværoffentlig brugerstyring etableres i overensstemmelse med internationale standarder og løsninger**

Tværoffentlig brugerstyring indgår i et samspil med det internationale på flere måder. Flertallet af tekniske løsninger er udviklet i udlandet, og arkitekturer og standarder er udviklet i internationale samarbejder. Dansk brugerstyring på tværs skal så vidt muligt lægge sig tæt op ad den internationale udvikling, dog med en konkret vurdering af, hvorvidt denne udvikling passer i en dansk sammenhæng

*Rationale*

- Anvendelse af standarder og løsninger med internationalt scope betyder bedre og billigere løsninger, der kan indgå i sammenhæng.
- Lokale brugerstyringsløsninger anvender generelt internationale produkter, der efterlever internationale standarder, og internationalt baserede løsninger og standarder vil derfor lette samspillet mellem det lokale og det tværgående.
- Fælles åbne standarder sikrer interoperabilitet.

- Der er generelt bedre adgang til leverandører og kompetencer på markedet, når løsningerne baserer sig på anerkendte og udbredte standarder.
- Ved at basere sig på standarder, som andre også anvender, øges 'beredskabet' omkring eventuelle problemer der skulle opstå med standarderne, f.eks. hvis der bliver fundet sikkerhedshuller.

#### Implikationer

- Det skal altid undersøges, hvilke internationale standarder det er muligt at anvende, evt. med dansk profilering.
- Danske profileringer bør begrænses til at dække forhold i økosystemet, som er specifikt danske, og som ikke kan ændres til at følge internationale standarder (fx CPR-data).

*! Princippet om brugerstyring i overensstemmelse med internationale standarder og løsninger BØR efterkommes i fællesoffentlige løsninger, i tværoffentlige brugerstyringsløsninger og i tjenester, der anvender disse. For øvrige KAN princippet efterkommes*

### 3.7. Tværgående processer

I dette afsnit vises med nogle få eksempler, hvordan byggeblokkenes interfaces kan benyttes til understøttelse af forskellige typiske brugssituationer. Brugssituationerne beskrives ved hjælp af arbejdsgange. [Jeg tror vi skal helt over i BPMN diagrammer /madsh]

De aktiviteter, der er skitseret i arbejdsgangene, er eksempler. Der kan være flere eller færre aktiviteter, og rækkefølgen af disse kan i nogle tilfælde være en anden. Det er arbejdsgangene i den enkelte myndighed, der afgør, hvilke konkrete aktiviteter en given arbejdsgang består af i praksis.

I de efterfølgende eksempler på arbejdsgange opererer hver aktør (myndighed, leverandør af brugerstyringstjenester) i sin egen svømmebane. De forskellige tjenester har desuden fået hver deres bane, hvor brugen af de forskellige interfaces vises. For overskuelighedens skyld er aktiviteterernes brug af disse interfaces vist som en direkte anvendelse af disse fra aktiviteterne. I praksis vil dette ofte ske gennem forskellige tjenester, men da disse er mangfoldige og uden for denne referencearkitekturs scope, er oversigten over arbejdsgange simplificeret ved, at disse tjenester ikke vises i de følgende eksempler, jf. nedenstående figur.

#### !Figur 11 Model til brug for brugerstyringstjenester i processer

*! Den tekniske opbygning af brugerstyring med opdeling i klart adskilte delprocesser og arbejdsdeling mellem aktørerne i administrative processer og autentifikation, billetudstedelse og adgangskontrol samt kontrol og rapportering BØR efterkommes i fællesoffentlige løsninger, i tværoffentlige brugerstyringsløsninger og i tjenester, der anvender disse. Dette afsnit KAN efterkommes af løsninger i offentlige sektorer.*

#### 3.7.1. Administration af elektronisk identitet, akkreditiver og attributter

Processer i forbindelse med administration af identiteter, akkreditiver og attributter kan gennemføres på forskellige måder og med forskellig sikkerhed for sammenhæng mellem elektronisk identitet og en fysisk person eller anden entitet. Kravene på forskellige sikringsniveauer (Levels of Assurance) beskrives normalt i et trust framework som NSIS, således at modtageren af en identitet kan matche dette mod deres risikoniveauer.

De administrative processer kan gennemføres i et samlet forløb (som det beskrives her) eller i flere adskilte forløb. Enkelte processer kan gentages, fx kan brugeren få tilknyttet flere akkreditiver (fx et nyt smartcard) og flere attributter på et senere tidspunkt.

**Registrering af elektronisk identitet** kan på lave sikringsniveauer ske ved, at en person registrerer sig selv – og med data, der er valgt af personen selv eller med de officielle data som navn og adresse fra CPR. Der er et tilsvarende behov for registrering af organisationer og ting.

En myndighed kan registrere personen, verificere personens identitet (eng. *identity proofing*) og angive styrken af registreringen (NSIS IAL), fx om registreringen er sket på grundlag af fysisk fremmøde eller på anden måde.

En arbejdsgiver kan registrere sine medarbejdere i egne brugerstyringssystemer eller i eksterne brugerstyringssystemer fx i det NemLog-in og Miljøportalen. Det kan ske manuelt eller ved overførsel fra arbejdsgivers eget brugerstyringssystem til det eksterne system.

En arbejdsgiver kan også registrere en tilknytning mellem sin virksomhed og en given identitet, fx ved at en person med en given identitet må udføre handlinger i virksomhedens systemer eller for virksomheden.

For de mange virksomheder, der er personligt ejede, kan tilknytningen mellem virksomhed og en given identitet ske automatisk på grundlag af registreringer i CVR-registret (fx at en person er fuldt ansvarlig deltager eller kan

tegne alene for en given virksomhed).

**Attributbeskrivelsen** er her beskrevet meget forenklet. Attributter for en identitet kan hentes fra eksterne kilder i forbindelse med registreringen (fx CPR-oplysninger), kan registreres i forbindelse med registreringen, kan registreres i brugerstyringssystemer eller i andre systemer. Attributter kan på samme måde som en identitet have forskellige kvalitetsniveauer, der bl.a. afhænger af de processer, der er anvendt under registreringen.

#### [!Figur 12 Registrer identitet](#)

Processen for registrering af en elektronisk identitet foregår forenklet set gennem følgende trin:

- En bruger anmoder om en identitet.
- Registreringstjenesten verificerer identiteten fx med hjælp fra grunddata samt beviser leveret af ansøgeren (fx pas og kørekort). Disse grunddata kan desuden indgå i trinnet Registrer attributter.
- I akkreditivtjenesten kan der tilknyttes allerede anskaffede akkreditiver, eller der kan udstedes og tilknyttes nye akkreditiver. Akkreditiver kan bestå af både digitalt information, som en nøgleapp, og fysisk information, som fx et nøglekort.
- Aktøren registrerer de attributter, der er krævet/ønsket.
- Resultatet vises for brugeren.

En attribut kan være niveauet af registreringskvalitet (IAL) og akkreditivets kvalitet (AAL) som beskrevet i NSIS eller eIDAS, der begge har en model for fastlæggelse af niveauer af registreringskvalitet for en identitet.

### 3.7.2. Autentifikation

Når en bruger anmoder om adgang til en tjeneste, der kræver et eller flere attributsæt for at give adgang, aktiveres de ovenfor beskrevne tjenester i en proces, der typisk forløber, som illustreret i følgende figur:

#### [!Figur 13 Autentifikation](#)

Processer i forbindelse med autentifikation kan gennemføres på forskellige måder og med forskellig sikkerhed for sammenhæng mellem elektronisk identitet og de udstedte akkreditiver (sikringsniveauer).

Typisk skelnes der mellem, hvor stærke akkreditiver der anvendes, styrken af autentifikationsprotokollen samt hvilke kontroller der er tilknyttet selve autentifikationsprocessen. Login med et akkreditiv (1-faktor login) er fx på lavere sikringsniveau end 2-faktor login. Login via en protokol, som er robust over for fx replay-angreb, er stærkere end login via protokoller, som ikke kan sikre mod denne type angreb.

Autentifikationen kan som beskrevet ske ved, at tjenesten henvender sig direkte til autentifikationstjenesten, men der kan også indgå flere aktører i processen, som når både en broker (NemLog-in) og en autentifikationstjeneste indgår.

1. Brugeren tilgår (anmoder om adgang til) forretningstjenesten.
2. Forretningstjenesten anmoder evt. brugeren om at vælge, hvilken broker eller autentifikationstjeneste brugeren ønsker at benytte (fx NemLog-in, WAYF, KOMBIT).
3. Forretningstjenesten anmoder broderen autentifikationstjenesten om en adgangsbillet (en token) til brug for login.
4. Autentifikationstjenesten beder brugeren om at autentificere sig via sine akkreditiver.
5. Brugeren autentificerer sig over for autentifikationstjenesten.
6. Autentifikationstjenesten/broderen validerer brugerlogin.
7. Autentifikationstjenesten/broderen udsteder en signeret billet til tjenesten med brugerens identitet og eventuelle attributter.
8. Forretningstjenesten kontrollerer den udstedte billet og etablerer evt. en session med brugeren.
9. Brugeren kan anvende forretningstjenesten underlagt dennes adgangskontrol.

Forløbet i denne proces varierer afhængigt af brugertype og situation. I figuren herover starter processen i forretningstjenesten, som re-dirigerer til autentifikationstjenesten. Hvis brugeren allerede har en session med autentifikationstjenesten, sker der ikke nødvendigvis fornyet login, men der udstedes en adgangsbillet til den ny forretningstjeneste.

Ovenstående dækker både processer, hvor brugeren tilgår tjenesten i en browser, app eller rig applikation. Der vil dog være forskelle i de tekniske implementeringer.

### 3.7.3. Billetudstedelse og adgangskontrol

I denne proces kræver tjenestens adgangspolitik, at adgangsbilletten indeholder bestemte attributter. Processerne i forbindelse med Billetudstedelse og Adgangskontrol tager derfor udgangspunkt i, at der er oprettet en identitet, som har fået tilknyttet attributter, der matcher forretningstjenestens adgangspolitik, og at identiteten endvidere kan autentificere sig på det sikringsniveau, som tjenesten kræver. Efter autentifikation skal identiteten derfor have udtrykt disse attributter og aktuelle sikringsniveau i den adgangsbillet, som forretningstjenesten modtager.

Arbejdsdelingen mellem de forskellige aktører kan også være forskellig, hvilket kan have betydning for, hvor attributter (fx rolle) hentes fra, og om fx adgangspolitikker håndteres af rettighedstjenester eller forretningstjenesten selv. Det kan også have betydning for, hvor aktørerne administrerer attributter.

#### !Figur 14 Billetudstedelse og adgangskontrol via en broker

1. En person anmoder om at anvende en tjeneste hos en tjenesteudbyder.
2. Tjenesten beder derfor en Billetudstedelse (identitetsbroker) om en signeret billet. Identitetsbrokern tager sig af at sikre gennemførelse af autentifikation, indhente alle nødvendige attributter og udsteder adgangsbilletten.
3. Autentifikationstjenesten verificerer brugerens akkreditiv gennem en autentifikationsproces. Kun hvis dette er gyldigt, fortsættes, ellers afvises personen.
4. Autentifikationstjenesten udsteder herefter en adgangsbillet til identitetsbrokern med de attributter for identiteten, som tjenesten kræver inkl. angivelse af aktuelt sikringsniveau.
5. En eller flere grunddatatjenester leverer de fornødne attributter knyttet til identiteten.
6. En eller flere attributtjenester leverer attributter knyttet til identiteten.
7. Brokern beriger adgangsbilletten med attributter og udsteder denne til forretningstjenesten.
8. Denne forretningstjeneste etablerer en session, som personen kan agere i med disse rettigheder og attributter.
9. Forretningstjenesten håndhæver adgangspolitikken i personens anvendelse af forretningstjenesten.
10. Brugeren anvender forretningstjenesten.

#### 3.7.4. Kontrol og rapportering

I eksemplet om Billetudstedelse og Adgangskontrol ovenfor skal alle brugerstyringstjenesterne for hver aktivitet logge resultatet af aktiviteten som adgangshændelser. Hvis man i brugerstyringstjenesterne konstaterer et sikkerhedsbrud, logges det som en sikkerhedshændelse, og denne forsynes med tilstrækkelige metadata til, at de tjenester der overvåger sikkerhedsbrud, kan anvende informationen og agere på den.

Sikkerhedsfunktionen hos udbydere af brugerstyringstjenester og forretningstjenester bør med passende mellemrum undersøge loggen af adgangshændelser for spor af forsøg på sikkerhedsbrud som led i forebyggelse af sikkerhedsbrud, fx gennem datamining-teknikker, herunder maskinlæring. Derigennem kan indbrudsforsøg afdækkes, og sikkerhedsforanstaltninger foretages og forebygges. Dette rapporteres også som en type sikkerhedshændelse til føderationen og til sikkerhedstjenester i føderationen. Samme sted kan tjenesteudbyderens sikkerhedsfunktion og udbydere af brugerstyringstjenester hente de seneste erfaringer med sikkerhedshændelser eller spor af sikkerhedshændelser og anvende dette i deres forebyggende arbejde.

#### 3.8. Forretningsobjekter og begreber

I dette afsnit beskrives en terminologi og begrebsmodel for brugerstyring. Begrebsmodellen er på et generelt og overordnet konceptuelt niveau. Dvs. at den ikke er bundet til en bestemt type person, organisation, anvendelse eller implementering. Begrebsmodellen kan således danne udgangspunkt for flere forskellige implementeringer

*! Begrebsmodellen SKAL anvendes i fællesoffentlige løsninger, i løsninger, der kommunikerer mellem offentlige sektorer, og i tjenester, der anvender fællesoffentlige løsninger. Begrebsmodellen KAN efterkommes af løsninger i offentlige sektorer. Bruger man andre termer for begreberne inden for sin egen sektor, SKAL man kunne oversætte eller transformere disse entydigt til de autoritative termer, når man kommunikerer verbalt eller digitalt på tværs af offentlige sektorer. Dette vil sikre bedre forståelse og kommunikation mellem forskellige sektorer om brugerstyring uden at fratage dem retten til at beholde egne velfungerende termer.*

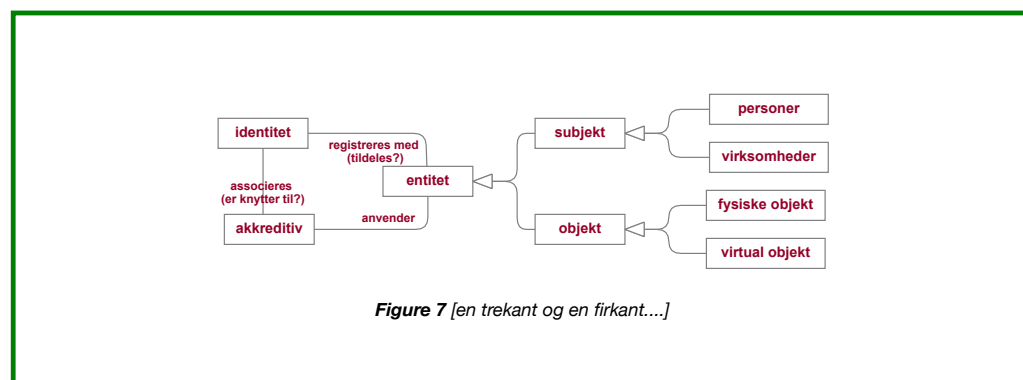


I denne liste gives kun definitioner for de begreber, som referencearkitekturen for brugerstyring autoritativt definerer, og som er markeret på figur 6 (nedenfor) med røde rammer.

| *Begreb* | Definition | Eksempler | --- | --- | --- | | Entitet | Noget værende, der kan have en identitet. | En person (borger, medarbejder), organisation (myndighed, virksomhed, forening), ting (sensor, apparat) eller tjeneste (system, app, applikation, paskontor). | | Identitet | En digital persona repræsenteret ved et sæt af attributter. En entitet kan have mere end en identitet. | Den repræsentation i et sæt attributter, som man giver en entitet gennem brugerstyring, er målrettet de tjenester, som entiteten skal have adgang til. | | Akkreditiv | Et elektronisk eller fysisk objekt/genstand, der kan anvendes til at gennemføre en autentifikation af en identitet. Også benævnt elektronisk identifikationsmiddel. | Et akkreditiv kan være et brugernavn, et brugernavn og password, en PIN-kode, et SmartCard, et certifikat, et (hardware) token, et fingeraftryk, et pas osv. Akkreditivet udstedes af en akkreditivtjeneste på baggrund af den foregående registrering af et eID. Akkreditivet kan også karakteriseres ved sikringsniveauer. | | Attribut | Karakteristika eller egenskaber ved en entitet. På engelsk betegnes attributter som *claims*. | Navn, adresse, køn, alder, UUID, PID, CPR-nummer, CVR-nummer, EAN nummer, Serienummer, URL, titel, uddannelse, kompetencer, ansvarsområde, specifik funktion, rolle, specifik kvalitet, specifik information osv. Når man vil tilgå en tjeneste, samler man de attributter tilhørende den elektroniske identitet, som tjenestens adgangspolitik kræver for at give adgang, og udsteder en adgangsbillet. Attributter kan vedligeholdes i kataloger som fx LDAP og AD. De kan også vedligeholdes af en attributtjeneste eller tildeles af en akkreditivtjeneste, samtidig med at der udstedes et akkreditiv. | | Adgangsbillet | Et elektronisk objekt, der beskriver attributter vedr. en identitet og er udstedt af en betroet tjeneste (identitetsbroker eller login-tjeneste). En adgangsbillet betegnes på engelsk som *security token*. | For at opfylde adgangspolitikken for en tjeneste, skal der indhentes en eller flere adgangsbilletter hos brugerstyringstjenester, som tjenesten har tillid til. Dette foretages af en billettjeneste, der kan være en simpel funktion til håndtering af et login, der håndteres af autentifikationstjenesten, eller billetudstedelsen kan foretages af en identitetsbroker. Denne kan, baseret på en autentifikationstjenestes verificering af et akkreditiv, indsamle attributter fra flere attributtjenester, og identitetsbrokern kan også omveksle attributter med samme betydning og sikringsniveau fra et protokolformat til et andet. Eksempelvis kan en borger få en SAML assertion (token) udstedt hos NemLog-in, der indeholder brugerens CPR-nummer, hvorefter borgeren kan få adgang til eksempelvis SKAT's Tast Selv Borger-løsning. Her virker NemLog-in som en identitetsbroker. Et andet eksempel er en Kerberos Server, der udsteder "tickets", som giver brugere adgang til servere i et sikkerhedsdomæne (fx Active Directory). | | Adgangspolitik | En adgangspolitik beskriver betingelserne for at udføre en eller flere funktioner eller give adgang til alle informationer (data) eller en afgrænset mængde af informationer (data) i en tjeneste. | En adgangspolitik for en tjeneste fastlægges af tjenesteudbyder, baseret på tjenesteudbyderens informationssikkerhedspolitik. En adgangspolitik har to repræsentationer: -En repræsentation i almindelig tekst beregnet på personer, der informerer om, hvilke attributter en identitet skal møde op med for at kunne få adgang til hvilke funktioner og informationer. -En repræsentation i struktureret format, der kan læses maskinelt af en tjeneste, der undersøger betingelserne til at få adgang til funktioner og informationer. Når en identitet møder op med en adgangsbillet, anvendes adgangspolitikken til at afgøre, om en identitet må udføre en specifik handling på et objekt, herunder hvilke specifikke data entiteten må få adgang til. Hvis ikke identitetens adgangsbillet indeholder attributter, der modsvarer, hvad adgangspolitikken kræver, giver adgangskontrollen ikke adgang. |

Der henvises i øvrigt til NSIS for en mere detaljeret gennemgang af begreber relateret til brugerstyring.

### 3.9. Begrebsmodel og relationer i brugerstyring



Begrebsmodellen illustrerer begrebernes relationer til hinanden. De røde begreber er referencearkitekturs kernebegreber og defineres af denne. De anvendes til at identificere og beskrive de centrale tjenester og roller, som er relevante i referencearkitekturen. De blå begreber er i princippet eksterne i forhold til referencearkitekturen. De er med som (udvalgte eksempler på) støttebegreber, der viser kontekst, relaterer til kernebegreberne og kan bruges til at pege på væsentlige støttetjenester. [!Figur 6. Begrebsmodel for brugerstyring](#) [Den er vist helt gal... De skal ikke beskrives som en relation i en begrebsmodel, men som en aktivitet i en process]

| Relation | Definition | --- | --- | | En entitet registres med en eller flere identiteter. | En identitet fastlægges og valideres af en registreringstjeneste | | En entitet får tildelt et eller flere akkreditiver knyttet til identiteter. | En akkreditivtjeneste udstyrer entiteten med fysiske eller digitale objekter (pas, kørekort, brugernavn-kodeord, Ne-

mID), der kan autentificere identiteten over for den tjeneste, der forestår autentifikationen. | | En identitet kan associeres med (knyttes til) flere akkreditiver, og et akkreditiv kan associeres med flere identiteter. | Ved at koble identitet og akkreditiver løst kan identiteten være vedvarende over tid med mulighed for at skifte akkreditiv. Det giver også mulighed for, at brugeren kan indrullere flere akkreditiver som supplement til et udleveret akkreditiv (fx indrullere fingeraftryk). | | En identitet associeres med en eller flere attributter (claims) og en attribut kan associeres med flere identiteter. | En identitet tilknyttes attributter, der karakteriserer den specifikke identitet, til brug for en tjeneses vurdering af, om tjenesten kan give denne identitet adgang. Et givet antal attributter hos en identitet skal matche adgangspolitikken hos tjenesten, for at tjenesten giver identiteten adgang. | | En adgangsbillet indeholder et eller flere sæt attributter. | En anmodning om adgang behandles af login-tjeneste eller identitetsbroker, som udsteder en adgangsbillet med en eller flere attributter, der beskriver identiteten. | | En adgangsbillet matches med en adgangspolitik. | Adgang gives af en tjeneste på grundlag af de attributter, der fremgår af adgangsbilletten, samt et tillidsforhold til den tjeneste, som har udstedt billetten. Adgangskontrollen følger tjenesteudbyderens vedtagne adgangspolitik for den pågældende tjeneste. | | En tjeneste har en adgangspolitik. | En tjenesteudbyders tjeneste stiller funktionalitet og informationer (data) til rådighed, som er underlagt en adgangspolitik, der specificerer, hvilke attributter identiteten skal demonstrere for at få adgang til specifikke funktioner og informationer. Denne adgangspolitik fastlægger niveauet for funktionaliteters og informationers (datas) tilgængelighed og beskyttelse, herunder de sikringsniveau for identitet og akkreditiver, som tjenesten accepterer, og den kvalitet i attributter den forventer. |

Afsnit 12: Bilag C giver en begrundelse for valget af denne begrebsmodel



Brugerstyring foregår i en kontekst, og for referencearkitekturen er der dele af denne kontekst, som det er særlig vigtigt at være opmærksom på. Den ene er informationssikkerhedspolitikken og registrering af sikkerhedshændelser, mens den anden er, hvilke konkrete former som identiteter i en brugerstyring optræder med. Kontekstens begreber er markeret med blått og vil være defineret i andre referencearkitekturer eller standarder.

#### !Figur 7. Konteksten for begrebsmodellen for brugerstyring

For denne kontekst beskrives relationerne til begrebsmodellen for brugerstyring.

| Relation | Definition | |---| | En entitet kan være en person, en organisation, en ting eller en tjeneste. | Siden er der udviklet en dansk standard for fysiske personer, juridiske enheder og erhvervsidentiteter (se NSIS), der bygger på eIDAS, og identiteter efter eIDAS skal overholdes af alle EU-lande. Dette rammeværk er endnu ikke udviklet for ting eller tjenester. En tjeneste, der optræder som entitet, kaldes en tjenstekonsument. | | En informationssikkerhedspolitik påvirker identitet og dens tilhørende akkreditiver og attributter. | Politikens retningslinjer, forretningsgange og instrukser og sikkerhedsforanstaltninger påtrykkes den konkrete specifikation af identitet, akkreditiv og attributter, således at sikkerhedshændelser forebygges. | | En informationssikkerhedspolitik påvirker hvilken adgangspolitik, der kan lægges for en tjeneste. | Det er gennem anvendelse af informationssikkerhedspolitikken og tilhørende risikovurderinger, at en adgangspolitik kan fastlægges. En risikovurdering kan fx klarlægge, hvilket NSIS sikringsniveau, der kræves for en autentificeret bruger for at få adgang. | | Log af sikkerhedshændelser foretages hver gang, der forsøges at forfalske autentifikation eller omgå adgangskontrol. | Alle begrebers repræsentationer i data fra og med identitet til og med tjeneste kan blive kompromitteret. En log registrerer alle trin i behandling af en identitets anmodning om en adgang. | | Flere logs knyttes til et spor af en sikkerhedshændelse | Gennem statistisk og algoritmisk behandling findes mønstre i logs af sikkerhedshændelser, der giver et spor. | | En sikkerhedshændelse kan ske ved angreb på eller forvanskning af identitet, akkreditiv, attributsæt, adgangsbillet eller adgangskontrol. | Alle muligheder udnyttes af fjendtlighedsindede. Overvåges og håndteres af organisationers Cyber Emergency Response Team (CERT), som for staten er placeret i Center for Cybersikkerhed. | | En sikkerhedshændelse knyttes til en sikkerhedstype. | En gruppering af sikkerhedshændelser |



## 4. Teknisk arkitektur

I dette afsnit beskrives de byggeblokke, der skal være til stede for at kunne realisere de løsninger, der lægges op til med referencearkitekturen. Referencearkitekturen begrænser sig til at definere de tjenester, som forvalter referencearkitekturens begreber. Disse tjenester er markeret med røde rammer nedenfor

De forretningsbehov der er beskrevet i afsnit **Fejl! Henvisningskilde ikke fundet.**, og ovenstående principper peger entydigt frem mod en løst koblet, fødereret arkitektur. Her vil de enkelte tjenester/tjenesteudbydere håndhæve adgang baseret på forudgående (ekstern) registrering, attributbeskrivelse, autentifikation og billetudstedelse. Således vil de ikke selv skulle håndtere en registreringstjeneste, en attributtjeneste, en autentifikationstjeneste og en billettjeneste. Der er derfor valgt en token-baseret model for adgangsstyring.

[Måske er der en princip mere her... Token baseret? /madsh]

Denne indebærer, at en autentificeret identitet får udstedt en adgangsbillet (et såkaldt Security Token) af en betroet komponent i infrastrukturen, der fx kan være en autentifikationstjeneste eller identitetsbroker. Adgangsbilletten præsenteres herefter over for den tjeneste, som leverer data eller funktionalitet, der ønskes adgang til. En adgangsbillet indeholder information om identitetens karakteristika og egenskaber i form af attributter og skal være digitalt signeret af den betroede udsteder, så den ikke kan forfalskes eller manipuleres. Valget af den token-baserede fødererede model er i tråd med alle nyere løsninger og planlagte initiativer i de forskellige sektorer i Danmark såvel som internationalt. Fællesoffentlige løsninger inden for brugerstyring er baseret på en model og standarder, der understøtter den, herunder OIOSAML-standard. Således benytter eksempelvis NemLog-in, grunddataprogrammet, Borger.dk, Virk.dk, Danmarks miljøportal, den fælleskommunale rammearkitektur og sundhedsområdet alle en token-baseret model.

*! Opbygning af brugerstyring med byggeblokkene Registrering af elektronisk identitet, Akkreditivtilknytning, Attributbeskrivelse, Autentifikation, Billetudstedelse og Adgangskontrol BØR efterkommes i fællesoffentlige løsninger, i tværoffentlige brugerstyringsløsninger og i tjenester, der anvender disse. Dette afsnit KAN efterkommes af andre løsninger i offentlige sektorer.*



### !Figur 10. Byggeblokke i konteksten for brugerstyring

Byggeblokke i konteksten for brugerstyring er genstand for andre referencearkitekturer og standarder, så vi henviser til disse beskrivelser:

- *Informationssikkerhedspolitik* er beskrevet i ISO/IEC 27001, og der er vejledninger på Digitaliseringsstyrelsens hjemmeside.
- *Kontrol og forebyggelse* koordineres af Center for Cybersikkerhed, der udgiver vejledninger og jævnligt opdaterer trusselsbilleder.
- *Organisation*: OIO Organisation er den fællesoffentlige standard for Organisation. Denne forventes revideret som led i digitaliseringsstrategien 2017-2020.
- *Person*: Her er CPR-version 1.1.0 den seneste fællesoffentlige standard.

[Se anvendelse af blå og røde byggeblokke i 'deling af data og dokumenter']

### 4.1. Nødvendige applikationsservices

#### 4.1.1. Akkreditivtjeneste

[Er det en specialisering af 'registrering' /madsh] Gennem byggeblokken "Akkreditivtjeneste" skabes en relation mellem en identitet og et akkreditiv, som garanterer nogle centrale karakteristika ved denne identitet, som udstederen af akkreditiver står inde for.

Det mest simple og udbredte akkreditiv er et kodeord knyttet til et navn, der repræsenterer identiteten. Et andet eksempel er NemID og den kommende MitID løsning.

Akkreditivtjenesten skaber i nogle tilfælde alene en tilknytning mellem en repræsentation af en identitet og et allerede eksisterende akkreditiv, mens der i andre tilfælde udstedes et nyt akkreditiv, som knyttes til identiteten. Nogle akkreditivtjenester tilføjer også flere beskrivende attributter til identiteten.

Akkreditivtjenesten har et vedligeholdelsesansvar for akkreditivets livscyklus, idet akkreditiver kan have en tidsbegrænset varighed og kan blive kompromitteret. NSIS standarden stiller en række til håndtering og udstedelse

af akkreditiver møntet på de forskellige faser af akkreditivets livscyklus.

#### 4.1.2. Attributbeskrivelse

[Er det en specialisering af 'registrering' /madsh] I forbindelse med registrering og oprettelse af den elektroniske identitet vil der typisk blive registreret en række beskrivende attributter. Attributterne beskriver identiteten, f.eks. med identifikatorer (UUID, CPR eller brugernavn), navne, højde, øjenfarve eller andet. Der kan dog også registreres andre typer attributter, der i sidste ende kan være adgangsgivende ift. tjenester, f.eks. den eller de arbejdsfunktioner, som ledelsen i en virksomhed ønsker at personen skal kunne optræde i, eller attributter vedrørende roller, bemyndigelser eller andet. Tilknytning af attributter til en elektronisk identitet kaldes i denne referencearkitektur for *attributbeskrivelse*.

Der kan være mange, der knytter attributter til identiteter. Nogle vil, som ovenfor nævnt, typisk blive tilknyttet i forbindelse med registrering og oprettelse af den elektroniske identitet, mens andre kan komme til i senere processer, hvor f.eks. brugeradministratorer tildeler 'roller', vedligeholder eksisterende attributter eller tilføjer nye attributter.

Indgår man i en føderation, kan der fastlægges attributter, som er særlig vigtige for samspil mellem føderationens deltagere, og derfor tildeles af en attributtjeneste anerkendt inden for føderationen. Det samme kan gælde, hvis man ønsker, at roller skal håndteres ens på tværs af en føderations deltagere. Inden for sundhedsområdet er det fx vigtigt, at visse roller – og dermed attributter – håndteres ens på tværs af sundhedsaktører, der skal samarbejde om behandlingen af patienter.

Enheder, der leverer attributbeskrivelser, skal vælges og håndteres med en omhu, der afspejler det sikringsniveau, som man ønsker, at attributterne skal matche. På sundhedsområdet er det meget veldefineret, hvilken myndighed der må koble en persons identitet til forskellige autorisationer til at udføre sygepleje og lægebehandling. I andre sammenhænge kan man lade en virksomhed beskrive de roller, som man som samarbejdspartner kan optræde i.

#### 4.1.3. Autentifikation (genkendelse?)

[Er det en specialisering af 'opslag'? /madsh]

Byggeblokken "Autentifikation" er den tjeneste, der validerer en identitet på baggrund af et akkreditiv. Autentifikation er baseret på brug af akkreditiver som fx kodeord (noget kun brugeren ved), et token (noget kun brugeren har) eller biometri (noget kun brugeren er eller gør). Tjenesten kan desuden levere identitetsattributter samt information om validiteten af identiteten til tjenesten Billetudstedelse, der danner adgangsbilletter (*security tokens*) med tidsbegrænset gyldighed til en eller flere tjenester. I en føderation er det adgangsbilletten, der giver adgang til tjenesten – ikke det akkreditiv, som er udstedt til bruger/serviceaftager, da dette typisk er usynligt for tjenesten grundet den arkitekturmæssige afkobling.

Før tjenesteudbyderen giver adgang til en bruger, anvender tjenesteudbyderen en autentifikationstjeneste til at validere identiteten. Tjenesteudbyderen kan anvende autentifikationstjenesten direkte eller gennem tjenesten "Billetudstedelse", som beskrives i næste afsnit.

Autentifikationen bygger på tillid til, at den akkreditivtjeneste, der har tilknyttet og udstedt akkreditiverne, har gjort dette til de rette entiteter, nemlig de samme entiteter som registreringstjeneste har identificeret og registreret identiteten på.

#### 4.1.4. Billetudstedelse

[Er det i det måske omvekslingen der skal i fokus? /madsh]

Byggeblokken "Billetudstedelse" er den del af brugerstyringen, som udsteder adgangsbilletter (eng: *security tokens*) til tjenester på grundlag af en autentifikation, og tilføjer attributter, der beskriver identiteten, samt anden relevant information som fx tidspunkt for autentifikation, NSIS sikringsniveau for autentifikationen mm. Attributterne udtrykker kendetegn, roller eller andre typer af attributter som en relation ("repræsenterer og er under instruks af CVR", "arbejder på vegne af læge X"), eller attributter, der udtaler sig mere specifikt om identitetens funktion ("arbejdsfunktion", "rolle").

Attributter kan stamme fra en autentifikationstjenesten, fra attributtjenester eller fra egne brugerstyringssystemer. Byggeblokken kan desuden tilbyde, at de udstedte adgangsbilletter leveres i flere standardformater. Byggeblokken kan varetages af en broker, der dels kan indsamle attributter fra forskellige attributtjenester, dels kan omvexle attributformater, hvis en tjeneste kræver et bestemt format for adgangsbilletten.

I en føderation bygger tjenesten Billetudstedelse på tillid til føderationens registreringstjenester, akkreditivudstedere og attributtjenester. Endvidere kan brokere omvexle og berige tokens fra andre brokere og dermed danne en *tillidskæde*. Autentifikationstjenestens tjek af akkreditivet sikrer, at det er den rette brugeridentitet, som udtrykkes i billetten. Den billet, som Billetudstedelse udsteder, skal indeholde det eller de attributter for

denne konkrete identitet, som kræves af tjenestens adgangskontrol, før der kan opnås adgang. Det er dermed en fordel for broderen at kende til tjenestens krav til attributter, hvilket ofte løses ved, at det ønskede attributsæt registreres, når tjenesten tilsluttes broderen.

#### 4.1.5. Adgangskontrol (men ikke autorisation?)

Tjenesteudbyderen er den, der forvalter det juridiske ansvar for adgangen til de informationer og funktioner, som tjenesteudbyderen udstiller - som hovedregel i rollen som *dataansvarlig*.

Det sker på grundlag af:

- Adgangspolitikken for tjenesten.
- Adgangskontrollen, som er håndhævelsen af adgangspolitikker, når en bruger anmoder om adgang.

Tjenesteudbyderen fastlægger en **adgangspolitik** på grundlag af sin sikkerhedspolitik med klassifikationer af sine informationer og funktioner på følgende parametre:

- *Fortrolighed*, at kun autoriserede personer har ret til at tilgå informationerne, og informationerne skal kun være tilgængelige for autoriserede personer.
- *Integritet (pålidelighed)*, at data er komplette, korrekte og opdaterede.
- *Tilgængelighed*, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

Tjenesteudbyderen skal ud fra sin adgangspolitik og en risikovurdering fastlægge, hvilke sikringsniveauer og attributsæt, der giver adgang til hvilke informationer og funktioner. Disse kan være udmøntet i et struktureret format, der kan læses maskinelt af en funktion, der undersøger betingelserne til at få adgang til tjenestens funktioner og informationer.

Beskrivelsen af adgangspolitikken er desuden grundlaget for brugerens eller brugerorganisationens administration af brugerens rettighedsrelevante attributter. Tjenesteudbydere og brugere/brugerorganisationer skal derfor have fælles forståelse af adgangspolitikken - herunder fx hvad konsekvensen af at tildele en bruger en bestemt rolle er. I en standard som WS-SecurityPolicy er der specificeret et sprog for at udtrykke en adgangspolitik. Dette giver en Billetudsteder mulighed for maskinelt at spørge tjenesten, hvilken adgangspolitik der skal opfyldes, for at få adgang til en bestemt funktion eller bestemte informationer. En mere simpel logik findes i SAML standarden, hvor en tjenestes behov for attributter kan udtrykkes i en såkaldt metadatafil.

Den løbende vedligeholdelse af den adgangspolitik, en given tjeneste kræver, er omfattende, idet den skal realiseres for enhver tjeneste, som tjenesteudbyder stiller til rådighed for brugere. Det samme gælder, hvilke akkreditiver og attributter der giver adgangsrettigheder til hvilke informationer og funktioner. De arbejdsprocesser, der foretager al denne vedligeholdelse, er i sin manuelle implementering meget ressourcekrævende. Der er derfor klare gevinster at hente gennem automatisering af administration i form af sparede manuelle ressourcer og sikring af, at personer der forlader organisationen, eller organisationer der forlader føderationen, også meldes ud.

En udbredt model for adgangsrettigheder er rollebaseret adgangskontrol (RBAC), hvor brugerorganisationen kan anvende egne organisatoriske roller i forbindelse med adgangskontrol. I de seneste år har en ny model, attributbaseret adgangskontrol (ABAC), vundet frem, hvor en regelmotor kan agere ud fra de attributværdier, en tjeneste præsenteres for gennem adgangsbilletten. RBAC kan opfattes som en delmængde af ABAC, idet roller kan udtrykkes som attributter.

I **Adgangskontrol** kontrolleres de attributter, som er indeholdt i den adgangsbillet, som brugeren medbringer fra Autentifikation og Billetudstedelse. Dette attributsæt skal matche den definerede adgangspolitik for tjenesten for de funktioner og informationer, der ønskes adgang til. Ellers afvises det at give identiteten adgang. I tilfælde af at der er etableret Single Sign-On funktionalitet, kan dette sæt af attributter (efter den initiale validering) repræsenteres af en session cookie eller en OAuth access token, der er udvekslet til at holde sessionen åben i en bestemt tidsperiode.

Adgangskontrollen påhviler tjenesteudbyder. Dele af den kan løses af en fælles byggeblok i referencearkitekturen.

## 4.2. Tekniske implementering af forretningsfunktioner

### 4.2.1. Implementering af administration af elektronisk identitet, Akkreditiver og Attributter

Følgende figur illustrerer de løst koblede byggeblokke for administration i brugerstyring, der udgør de centrale byggeblokke i den samlede arkitektur:

!Figur 8 Byggeblokke for administration i referencearkitekturen

Byggeblokkene "Registrering", og "Akkreditivtjeneste" er de tjenester, der registrerer identiteter, og de akkreditiver som anvendes til at validere identiteter. Attributter som beskriver identiteten, kan vedligeholdes af attributtjenester. Tabel 1 giver som overblik nogle eksempler.

Tabel 2. Eksempler på identifikatorer, akkreditiver og attributter for entiteter

|| | Attributter || | |-----|-----|-----|-----|  
-----| | **Entitet** | **Akkreditiv** | *Baseret på tal* | *Baseret på navne* | *Baseret på klassifikationer* | Person | Kodeord,  
nøglekort, nøglefil, fingeraftryk, irisscanning | CPR-nr., administrativt CPR-nr. | Brugernavn, vanlig-navn, køn,  
alder, UNI\*Login | Specialkonsulent, leder, administrator, kompetence, uddannelse, certificering. | | Organisation  
| Nøglefil | CVR-nr., EAN, SEEnr. | Vanlig-navn, logi, branchekode | Leverandør, rådgiver, kontrollant, certificering | |  
Ting | Nøglefil, token | Serienummer, URL, Typenummer | Funktion, RDF, OWL | Sensortype, triggertype, certifi-  
cering | | Tjenestekonsument | Nøglefil (p.t. FOCES) | P-nummer | RDF, OWL, funktionsnavn | FORM, opmærkn-  
ing, funktionstype |

Implementering af disse byggeblokke målrettes det eller de sikringsniveauer, som informationssikkerhedspolitikken har fastlagt. Det udtrykkes fx af forskellen i processen for at opnå et NemID eller et virksomhedscertifikat i forhold til at opnå et brugernavn-kodeord til at tilgå sin virksomheds informationer. Grundet tradition logger de fleste medarbejdere på deres organisations lokale netværk blot med brugernavn-kodeord, men påtvinges så at skifte dette ofte, fx med tre måneders mellemrum.

Jo stærkere garanti for akkreditiv og attributter, som et valgt sikringsniveau kræver, jo stærkere skal kontrolfunktionerne omkring registreringen være.

Brugerstyringstjenesterne kan varetages af samme organisation, men kan i en tværgående føderation varetages af forskellige organisationer. Opdelingen kædes sammen med fællesoffentlige standardprotokoller for informationsudveksling. Da de forskellige standardsystemer, som anvendes af myndigheder og virksomheder, ikke nødvendigvis har de fælles protokolstandarder indbygget, kan dette løses af en broker, der foretager protokolkonvertering.

En særlig opmærksomhed skal gives vedligeholdelse af identiteters attributter gennem hele deres livscyklus. Denne livscyklus indeholder ændringer i registreringspraksis, i valg af anvendte akkreditiver og i beskrivelse af attributter, herunder roller og terminering af alle rettigheder for en identitet ved fx jobskifte, dødsfald, konkurs, udskiftning, ændring eller nedlæggelse af tjeneste og lign.

Det gentages her, at denne referencearkitektur anvender følgende termer i stedet for termen autorisation med henblik på at opnå den størst mulige præcision:

- Administration af en identitets rettigheder gennem associering af attributter.
- Udstedelse af adgangsbillet med identitet, roller, dataafgrænsninger og andre attributter betegnes med *billetudstedelse*.
- Fastlæggelse af adgangspolitikker og adgangsrettigheder betegnes *adgangspolitik*.
- Håndhævelse af adgangsrettigheder kaldes *adgangskontrol*.

#### 4.2.2. Implementering af Registrering af elektronisk identitet

Byggeblokken "Registreringstjeneste" har til opgave at foretage en tilknytning mellem en entitet og en identitet og udføre dette efter National Standard for Identiteters Sikringsniveauer (NSIS). NSIS fastlægger tre veldefinerede sikringsniveauer, som en tjenestes adgangskontrol kan tage udgangspunkt i, når de præsenteres for en autentificeret identitet. En entitet kan knyttes til flere identiteter.

En registreringstjeneste har ansvar for ikke blot at registrere identiteter første gang, men også for at vedligeholde en identitetsregistrering i hele dets livscyklus. Dette inkluderer nedlæggelse af identiteten, hvis identiteten ophører med at eksistere fx ved dødsfald eller konkurs.

#### 4.2.3. Implementering af Anvendelse af brugerstyring?

Følgende figur illustrerer de løst koblede byggeblokke for *anvendelse* af brugerstyring, der udgør de centrale byggeblokke i den samlede arkitektur:

!Figur 9. Byggeblokke for referencearkitekturens brugerstyring i anvendelse

### 4.3. Understøttende applikationsservices

[Mon ikke der er noget at hente i 'deling af data og dokumenter' fx dataservice... log... /madsh]

#### 4.4. Områder for standardisering

Referencearkitekturen peger på, hvilke områder der skal være standarder for, at referencearkitekturen fungerer.

I afsnit 0 er beskrivelse af standarder på de udpegede områder. En detaljeret oversigt over obligatoriske og anbefalede standarder skal vedligeholdes på arkitekturguiden.digitaliser.dk

[!Figur 20 Områder for standarder for brugerstyring](#) Note til figur: Pilene angiver områder for standarder

Der skal være **standarder for registrering af brugere, akkreditiver og attributter**. Disse standarder skal dække registreringskvaliteten (eIDAS, National Standard for Identiteters Sikringsniveau (NSIS), ISO29115, Kantara Identity Assurance Framework).

Der skal være **standarder for overførsel af data om autentificerede brugere** mellem autentifikationstjenester, login-tjenester/brokere og tjenester (her bruges i dag fx OIOSAML standarden mellem NemLog-in og tjenester).

Der er behov for **standarder i forbindelse med rettigheder og attributter**. Det drejer sig dels om standarder til at kommunikere med attributtjenester (SAML, OpenID Connect), dels at kommunikere mellem attributtjenester og forretningstjenester (fx XACML). Et andet aspekt er standarder for at indhente brugernes samtykke, når dette indgår i adgangsbeslutninger – her er UMA og OAuth muligheder.

Der er behov for **standarder for kommunikation mellem føderationer**. Disse skal identificeres og fastlægges i arbejdet med implementering af referencearkitekturen. Arbejdet i EU-regi (STORK og eIDAS) er baseret på SAML2-profiler.

[!Figur 21 Kommunikation mellem føderationer](#)



Figuren herunder viser interoperabilitet for brugerrettighedsstyring iht. referencemodellen for interoperabilitet, som den er beskrevet i hvidbogen for fællesoffentlig rammearkitektur.

I takt med videreudvikling og konsolidering af området, kan denne figur opdateres og udstilles som en del dokumentationen af den fællesoffentlige rammearkitektur:

[!Figur 22 Interoperabilitet for brugerstyring](#)



## 5. Målbillede? Implementering?

[Det var et afsnit vi undlod i 'deling af data og dokumenter' /madsh]

Dette afsnit beskriver det systemtekniske målbillede, de væsentligste komponenter og standarder.

Det er kendetegnende for brugerstyringsområdet, at området er veludbygget med en lang række føderationer, tekniske løsninger og standarder. Dette giver samtidig en udfordring med at sikre interoperabilitet på tværs af sektorer og domæner, idet nuværende praksis til en vis grad er opstået gennem decentralt knopskydning og lokal profilering af fælles standarder.

Der er derfor i forbindelse med referencearkitekturen behov for at etablere nye tekniske løsninger på få, begrænsede områder, idet de enkelte komponenter i målbilledet stort set er til stede. Der er fx behov for at etablere føderationer og forbedre samspillet mellem føderationer.

Der forventes desuden en fortsat øget specialisering af funktioner i økosystemet, hvilket kan føre til udvikling af nye standarder, til kommunikationen mellem komponenter samt løbende tilpasning af eksisterende standarder.



*! Den tekniske målarkitektur BØR efterkommes i fællesoffentlige løsninger, i løsninger, der kommunikerer mellem offentlige sektorer, og i tjenester, der anvender fællesoffentlige løsninger. Den tekniske målarkitektur KAN efterkommes af løsninger i offentlige sektorer.*

Det systemtekniske målbillede viser, hvor validering af og data om brugere og andre identiteter stilles til rådighed af brugerstyringstjenesterne til forretningsformål, ligesom de kan indgå i samspil med andre infrastrukturtjenester.

### !Figur 15 Brugerstyringstjenester i logisk sammenhæng

Brugerstyringstjenesterne skal gøre det muligt for forretningssystemerne at anvende og opdatere data om brugere til de mange forskellige formål, der er beskrevet ovenfor.

Brugerstyringstjenesterne kan indgå både i den enkelte organisations infrastruktur og i den nationale infrastruktur, hvor brugerstyringstjenesterne kan anvende fx tjenester for Klassifikation og Organisation, og hvor andre infrastrukturtjenester kan anvende brugerstyringstjenesterne.

Det systemtekniske målbillede tager udgangspunkt i, at der implementeres snitflader baseret på åbne standarder i de enkelte brugerstyringssystemer og i de øvrige systemer, der skal anvende brugerstyringstjenester.

### 5.1. En målarkitektur med identitetsbrokere

*! Arkitektur med identitetsbrokere SKAL efterkommes i fællesoffentlige løsninger, mens øvrige løsninger i offentlige sektorer BØR efterkomme ovenstående.*

En login-tjeneste er en brugerstyringstjeneste, der foretager autentifikation af brugere på vegne af forretningstjenester eller billetudstedere. Autentifikationen består som regel i at verificere et akkreditiv evt. ved at kontakte en akkreditivudsteder, men man kan også omveksle billetter, udstedt af andre login-tjenester (brokering). Ud over autentifikation kan login-tjenesten indhente yderligere information om brugeren hos attributtjenester, som indlejres i en billet, udstedt til forretningstjenesten. En login-tjeneste kan evt. også danne en session med brugeren med henblik på at etablere Single Sign-On.

En login-tjeneste kaldes også for en identitetsbroker. Ved at anvende en identitetsbroker opnår forretningstjenesten en løs kobling til brugerens akkreditiver og hermed autentifikationstjenester. Forretningstjenesten skal blot forholde sig til, hvem brugeren er, og hvilke andre attributter (fx rettigheder) der står i billetten, samt sikringsniveauet for autentifikationen (jf. NSIS), men ikke hvordan brugeren er logget ind og med hvilke akkreditiver. Dette betyder eksempelvis, at man kan indføre nye typer akkreditiver eller nye snitflader til autentifikationstjenester uden at påvirke forretningstjenesterne. Et eksempel på dette var indførslen af NemID Javascript-løsningen i 2014. Her skiftede NemLog-in fra Java-implementeringen af NemID til JavaScript-implementeringen, og med ét slag var de over 200 offentlige tjenester tilsluttet NemLog-in overgået til den nye teknologi – uden at ændre én linje kode selv.

*! Identitetsbrokere BØR kommunikere sikringsniveauet (eng: Level of Assurance) for autentifikation ved at indlejre en attribut i billetten, som angiver dette (hvor niveauet typisk er defineret i et trust framework som fx National Standard for Identiteters Sikringsniveau (NSIS)). Dette gælder for fællesoffentlige løsninger og tværoffentlige brugerstyringsløsninger.*

Et andet væsentligt aspekt af den løse kobling er, at forretningsapplikationen ikke hårdkodes til at hente oplysninger om identiteter bestemte steder, men i stedet får dem leveret af infrastrukturen gennem den udstedte billet. Herved har man frihed til at ændre i placeringen af attributter, uden at forretningstjenesterne påvirkes.

#### [!Figur 16: Broker-baseret arkitekturmodel](#)

Denne model svarer til "four corner"-modellen for betalingskortinfrastrukturen, som vist på Figur 17 Arkitektur til betalingskortinfrastruktur, hvor kortholderen (svarende til identiteten) forbindes til betalingsmodtager (svarende til tjenesteudbyder) gennem kortudsteder (svarende til registreringstjeneste og akkreditivudsteder) og kortindløser (svarende til broker). Modellen har vist sig meget skalerbar i praksis, både i forhold til antallet af aktører og i forhold til transaktioner.

#### [!Figur 17 Arkitektur til betalingskortinfrastruktur](#)

For langt hovedparten af offentlige tjenesteudbydere anvendes denne model, som nævnt, allerede med NemLog-in som identitetsbroker. Ligeledes fungerer sundhedsområdets SOSI STS som identitetsbroker.

Denne arkitekturmodel understøtter, at der er flere autentifikationstjenester, bl.a. som følge af eIDAS-forordningens krav om gensidig anerkendelse af elektroniske identiteter på tværs af EU-landegrænser. STORK2-projektets arkitektur kan umiddelbart implementeres ved at indarbejde funktionalitet hos en broker til at modtage eID fra andre EU-medlemsstater – en såkaldt eID-gateway. I Danmark er NemLog-in og danske eID gateway eksempler på identitetsbrokere, som benyttes mod alle offentlige nationale selvbetjeningsløsninger med behov for sikker identifikation, herunder løsninger på portalene borger.dk, virk.dk og sundhed.dk. NemLog-in understøtter p.t. kun NemID som akkreditiv. Som andre eksempler kan nævnes Uni\*Login, WAYF og ContextHandleren, som implementeres i regi af den fælleskommunale infrastruktur.

Hvis en broker eller login-tjeneste understøtter flere forskellige autentifikationsmekanismer, KAN der være et element af brugerinteraktion, hvor brugeren vælger login-mekanisme. Et eksempel på dette findes i WAYF-løsningen og i KOMBIT's føderation, hvor brugeren normalt skal vælge, hvilken organisation han/hun tilhører for efterfølgende at autentificere mod dennes login-tjeneste, inden brokern omveksler billetten til forretningstjenesten.

Arkitekturmodellen betyder – som for betalingskort – at brugerne kan anvende flere forskellige akkreditiver fra flere registreringstjenester, og hver identitet kan have tilknyttet forskellige akkreditiver fra forskellige akkreditivudstedere. For tjenesterne betyder det, at de kun skal have forbindelse til en identitetsbroker, som så håndterer forbindelsen til forskellige registreringstjenester og akkreditivudstedere. Tjenesteudbyder behøver således ikke have kendskab til de enkelte registreringstjenester og akkreditivudstedere, men skal blot definere en politik for et ønsket veldefineret sikringsniveau.

Anvendelse af en broker-baseret arkitektur åbner desuden mulighed for, at tjenesteudbydere kan få mere relevante og branchespecifikke attributter for den konkrete kontekst, uden at registreringstjenester og akkreditivudstedere skal akkumulere en lang række informationer om brugerne. Dette kendes allerede i dag fra sundhedssektoren, hvor SOSI STS'erne fungerer som brokere og tilfører information om brugerne fra eksempelvis Sundhedsstyrelsens autorisationsregister.

Det er langt fra altid, at en rettighedstjeneste eller tjenesteudbyder har brug for entydigt at kende identifikation af brugeren/serviceaftageren for at kunne afgøre dennes adgang til en service. Ved et køb af billet til bus eller tog er der, som tidligere nævnt, et behov for at levere et bevis for betaling, men ikke nødvendigvis for kundens identitet. Et andet eksempel er løsninger, der blot har brug for at vide, om brugeren er myndig (alder>18) eller vedkommendes bopælskommune. Her BØR login-tjenesten/identitetsbrokern nøjes med at sende relevante attributter videre til tjenesten og ikke data, der afslører brugerens identitet. Dette princip kaldes ofte for "minimal disclosure" (dataminimeringsprincippet) og er altså et udtryk for, at man af hensyn til brugerens privatliv sender den minimale mængde af information, som tjenesten har behov for. Som eksempel på denne tendens benytter OIOSAML 3.0 profilen som udgangspunkt et tjenesteudbyderspecifikt UUID som *identifier* for brugeren i den udstedte billet for at forebygge muligheden for, at en bruger kan spores på tværs af tjenester. For tjenester, der har lovhjemmel og relevant behov, kan der dog stadig leveres en CPR-attribut i en OIOSAML 3.0 Assertion.

I forhold til en infrastruktur med flere registreringstjenester og akkreditivudstedere vil anvendelse af identitetsbrokere skjule kompleksiteten for den enkelte tjenesteudbyder. Anvendelse af en broker vil således minimere påvirkning af tjenesteudbyder ved ændringer i form af teknologiskift hos de eksisterende autentifikationstjenester og etablering af nye autentifikationstjenester.

Samtidig vil en tjenesteudbyder have mulighed for at indgå aftale med flere brokere med henblik på at sikre størst mulig opptid.



Det skal bemærkes, at en registreringstjeneste eller akkreditivudsteder kan operere som identitetsbroker, lige som en større tjenesteudbyder kan etablere egen broker-funktion. Endvidere kan brokere forbinde sig til andre brokere.

#### !Figur 18 Arkitektur med flere registreringstjenester, en akkreditivudsteder og brokere

En brokerbaseret arkitektur kan indføres fleksibelt og gradvist, hvor tjenesteudbydere kan vælge at understøtte login og signering som en integreret del af egen tjeneste eller benytte en ekstern identitetsbroker. Introduktion af brokere kan baseres på frivillighed og med tiltag, der fremmer overgang til brug af brokere, herunder markedsføring af akkrediterings-/mærkningsordning af brokere. Alternativt kan der stilles krav om, at der benyttes en godkendt broker – fx indeholder National Standard for Identiteters Sikringsniveau (NSIS) krav til identitetsbrokere på forskellige sikringsniveauer. Ved brug af MitID løsningen som afløser NemID bliver det obligatorisk at anvende en broker, idet den enkelte tjenesteudbyder ikke selv får lov at integrere direkte med MitID-kernen.



Referencearkitekturen beskriver en løst koblet arkitektur, hvor mange forskellige aktører og løsninger skal arbejde sammen om en effektiv og sikker brugerstyring. Dette indebærer en lang række fordele i forhold til fleksibilitet, arbejdsdeling mv., men gør det også mere kompliceret at få et overblik over det samlede sikkerhedsniveau. Som tidligere beskrevet, vil den enkelte tjenesteudbyder være afhængig af en række brugerstyringstjenester (fx udstedere af akkreditiver, logintjenester, identitetsbrokere, attributtjenester osv.). Et sikkerhedsbrud i én brugerstyringstjeneste eller forretningstjeneste kan i værste fald påvirke mange tjenester. Det gælder både i forhold til fortrolighed, integritet og tilgængelighed. Dette er et udtryk for det velkendte princip om, at en kæde ikke er stærkere end det svageste led. Omvendt kan man ved at bygge nogle fælles brugerstyringstjenester opnå en kritisk masse i udviklingen, og derved bygge dem stærkere end en enkelt udbyder af en forretningstjeneste selv har ressourcer eller viden til at etablere. I NSIS standarden håndteres tillidskæder ved, at det er det svageste led i kæden, som definerer det samlede sikringsniveau. En broker på sikringsniveau NSIS Betydelig kan fx ikke formidle autentifikationer på sikringsniveau NSIS Høj, selvom brugeren måtte kunne autentificere sig på niveau Høj.

#### !Figur 19 Sikkerhedskæder i fødereret brugerstyring

I en løst koblet og distribueret arkitektur er det derfor nødvendigt med fælles rammer for sikkerhed, der definerer roller og ansvar for de forskellige komponenter. Disse spilleregler er grundlaget for tilliden mellem parterne i arkitekturen og sikrer, at der ikke falder noget mellem to stole.

For *brugerstyringstjenester* som fx registreringstjenester, akkreditivudstedere, logintjenester/identitetsbrokere opstiller National Standard for Identiteters Sikringsniveau (NSIS) rammeværket en række sikkerhedskrav, knyttet til forskellige sikringsniveauer. Disse definerer et mål for kvaliteten af disse tjenester og har tilknyttet en række forskellige sikkerhedskrav samt krav til revision. For de løsninger, som udbydes fællesoffentligt (herunder NemID/MitID og NemLogin), fører Digitaliseringsstyrelsen endvidere et løbende tilsyn med leverandørerne og følger op på løsningernes sikkerhedsniveau.

For *forretningstjenester* er det udgangspunktet, at myndighederne ud fra en risikovurdering selv skal beslutte deres sikkerhedsniveau, hvilket også ligger i rollen som dataansvarlig i persondataloven. En sådan risikovurdering kan med fordel tage udgangspunkt i metodikken, defineret i ISO/IEC 27005, og styringen af informationssikkerhed kan med fordel tage afsæt i ISO/IEC 27001-standarden. Behandler forretningstjenesten personoplysninger og indebærer behandlingen sandsynligvis en høj risiko for fysiske personers rettigheder og frihedsrettigheder, er der tillige behov for gennemførelse af en konsekvensanalyse vedrørende databeskyttelse (også kaldet *Privacy Impact Assessment*, PIA). Databeskyttelsesforordningen fra EU (GDPR) stiller krav til indholdet af en sådan vurdering (Artikel 35), samt hvornår Datatilsynet skal konsulteres. En skabelon til formålet kan findes på Digitaliseringsstyrelsens hjemmeside (<http://www.digst.dk/informationssikkerhed/Konsekvensvurdering-for-privatlivet>). En sådan konsekvensanalyse kan identificere behov for yderligere sikkerhedsforanstaltninger, der skal implementeres i tjenesten.

Både risikovurdering og PIA kan afdække krav til sikringsniveauet for de brugerstyringstjenester, som forretningstjenester benytter sig af – fx at brugerne skal autentificeres i henhold til et bestemt sikringsniveau i henhold til NSIS-standarden.

Derudover kan der i en fødereret infrastruktur være behov for at have fokus særligt på tværgående aspekter, hvor kompromittering af én tjeneste kan påvirke sikkerheden i en anden tjeneste:

- Når tjenester udstiller attributter eller andre stamdata, som bruges af andre tjenester til at træffe beslutning om afgørelser eller adgange, er det essentielt at afklare afhængigheder og forudsætninger. Et eksempel kunne være, at sårbarheder i et kildesystem kunne udnyttes til at få adgang til andre systemer (fx at falske data, plantet i et pasregister, udnyttes til at skaffe en identitet i en anden persons navn). Her er det relevant at foretage en tværgående risikovurdering og på forhånd klarlægge kvalitetskrav til de data, der anvendes, således at integriteten af de samlede processer bevares.



- Ved servicekald mellem tjenester, der indgår i en samlet forretningsproces, kan der være behov for at etablere og udveksle korrelations-ID'er, således at det bliver muligt ved brug af logfiler at efterforske hændelsesforløb på tværs af tjenester. Hvis hver tjeneste kun ser en lille delmængde af et hændelsesforløb, kan det være vanskeligt at opdage svindel.
- Hvis en tjeneste er afhængig af en anden tjeneste for kunne fungere, kan manglende tilgængelighed, fx som følge af DDoS-angreb, give kaskadeeffekter på tværs af infrastrukturen.
- Hvis sikkerheden i en tjeneste er afhængig af kontrolmiljøet på slutbrugerens enhed (fx en mobil enhed), kan der være særlige afhængigheder til den part, der udleverer/kontroller slutbrugerenhederne.
- Hvis en tjenesteudbyder undlader at implementere logout i tjenesten, betyder det, at en person med adgang til en brugers udstyr kan udnytte en session til at tilgå denne eller en anden tjeneste og fx få adgang til eller ændre data i tjenester og i registreringer vedrørende personen.

*! Der er følgende krav til fællesoffentlige brugerstyringstjenester og forretningstjenester i den fællesoffentlige federation. Dette er begrundet i konteksten for brugerstyring: ISO/IEC 27001, ISO/IEC 27005, EU's General Data Protection Regulation (GDPR) og den danske persondatalov:*

- Tjenesteudbyder SKAL styre sikkerheden i egen tjeneste i forhold til fortrolighed, integritet og tilgængelighed.
- Tjenesteudbyder SKAL sikre, at udveksling af data (indgående og udgående) sker med tilstrækkelig sikkerhed.
- Tjenesteudbyder SKAL gennemføre risikovurderinger af, hvordan tjenestens placering i føderationen påvirker tjenestens sikkerhed – og hvordan tjenesten påvirker andre tjenesters sikkerhed og gennemføre de nødvendige tiltag.
- Tjenesteudbyder SKAL i relevant omfang informere andre aktører i føderationen om risikovurderinger og sikkerhedshændelser. Ovenstående regler SKAL følges af brugerstyringstjenester og forretningstjenester i andre føderationer.

## 5.2. Handleplan? Projektliggørelse?

### 5.3. Registrering af identiteter

Som tidligere beskrevet kan processer i forbindelse med at registrere identitet gennemføres på forskellige måder og med forskellig sikkerhed for sammenhæng mellem elektronisk identitet og en fysisk person eller anden entitet. Kravene på forskellige sikringsniveauer (*Levels of Assurance*) beskrives i et "trust framework", således at modtageren af en identitet kan matche dette mod deres risikoniveauer.

### 5.4. Standarder for registrering af identiteter

Der findes en lang række forskellige og ukoordinerede mekanismer til registrering og navngivning af elektroniske identiteter. Hvis behovet for en mere sammenhængende infrastruktur skal understøttes, skal der ske en højere grad af standardisering under hensyntagen til privatlivsbeskyttelse.

I referencearkitekturen for fællesoffentlig brugerstyring er National Standard for Identiteters Sikringsniveau (NSIS) standarden fra Digitaliseringsstyrelsen den fælles referenceramme, der beskriver krav til de forskellige sikringsniveauer. Det skal bidrage til at sikre, at identiteterne er registreret med så høj kvalitet, at risiko for misbrug af identiteter (herunder identitetstyveri) mindskes.

*! Brug af National Standard for Identiteters Sikringsniveau (NSIS) SKAL efterkommes i fællesoffentlige løsninger og løsninger, der kommunikerer mellem offentlige sektorer, og BØR efterkommes af løsninger i offentlige sektorer. En identitetsløsning BØR fastlægge et krævet NSIS-sikringsniveau "Begrænset", "Lav", "Betydelig" eller "Høj" i forhold til anvendte akkreditiver og den samlede livscyklus. Dette muliggør en lettere integration mellem systemer, idet sikringsniveauer er umiddelbart sammenlignelige.*

Der vurderes ikke behov for yderligere rammesætning om registreringsprocesser. Tværtimod er det hensigten i NSIS at åbne for et marked, hvor innovation og kreative løsninger kan opstå, blot de opfylder krav til de sikringsniveauer, de påberåber sig, og at udbyderne af brugerstyringstjenester påtager sig det ansvar, der er defineret i NSIS.

Der arbejdes fællesoffentligt med, hvordan der i praksis kan opnås de sikringsniveauer for registrering, som indgår i NSIS. Det sker i arbejdet med valide identiteter.

*! Ved udstedelse af certifikater BØR semantik fra ETSI EN 319 412-1 anvendes, og det skal overvejes, om navngivning af brugere med fordel KAN genbruge denne semantik, også uden for en certifikatkontekst. Dette gælder særligt i de situationer, hvor brugere skal kunne tilbydes certifikater til signering, hvorved navngivning er ens for en indledende autentifikation og den efterfølgende signering. Dansk Standard DS 844 er en alternativ standard for navngivning i certifikater. Denne SKAL FORLADES i nye løsninger, da den ikke i tilstrækkelig grad er fremtidssikret i en international sammenhæng.*

## 5.5. Akkreditiver

Det væsentligste arkitekturprincip for akkreditiver er, at de er beskrevet på et sikringsniveau i henhold til National Standard for Identiteters Sikringsniveau (NSIS), og at de ikke er tæt bundet til brug i én forretningstjeneste, men gennem en interoperabel sikkerhedsinfrastruktur, som principielt kan anvendes på tværs af alle tjenester. Sagt på en anden måde: Integrationen mellem en forretningstjeneste og et akkreditiv BØR ske via en mellemliggende logintjeneste/identitetsbroker for løsninger, der kommunikerer mellem offentlige sektorer.

De ovennævnte arkitekturprincipper sikrer en løs kobling og fleksibilitet, der muliggør innovation som fx ibrugtagning af biometriske akkreditiver, uden at alle forretningstjenesterne skal skrives om. Desuden opnås en hensigtsmæssig arbejdsdeling, hvor den enkelte forretningstjeneste ikke behøver specialistviden om identitetssikring og sikker håndtering af akkreditiver.

I referencearkitekturen er det centrale, at flere registreringstjenester og akkreditivudstedere, leveret af både offentlige og private aktører, kan sameksistere i det digitale økosystem, og at forretningstjenester ikke bør være tæt forbundet til en bestemt registreringstjeneste og en bestemt akkreditivudsteder, men kan acceptere adgang for brugere, uanset hvem der har registreret identiteten eller udstedt et akkreditiv. En forretningstjeneste skal således primært forholde sig til, om identiteten er autentificeret på det krævede sikringsniveau, om udstederen af adgangsbilletten er en kendt brugerstyringstjeneste på dette niveau (som led i NSIS vil Digitaliseringsstyrelsen publicere anmeldte tillidstjenester på sin hjemmeside.) og inden for den aktuelle føderation, samt at brugeren i øvrigt opfylder adgangskravene (fx er tildelt adgangsgivende roller til tjenesten).

*! Af hensyn til forsyningsikkerheden og grundlaget for digitaliseringen SKAL det offentlige etablere mindst en generel registreringstjeneste og en generel akkreditivudsteder i økosystemet – samtidig med at der er åbnet for alternative løsninger.*

Med National Standard for Identiteters Sikringsniveau (NSIS) som tillidsramme og med eksistensen af standarder for attributter og protokoller vurderes det, at rammebetingelserne herfor er til stede.

Der findes dog huller i landskabet af registreringstjenester og akkreditivtjenester – særligt for børn og unge under 13/15 år, som p.t. ikke har nogen sikre id-løsninger (på NSIS sikringsniveau Betydelig). Der findes et initiativ i Digitaliseringsstrategien, som skal analysere mulighederne for sikre id-løsninger til børn. I forbindelse med implementering af en kommende løsning vil det være relevant, at denne udstilles gennem NemLog-in, UNI-Login eller andre identitetsbrokere.

*! Understøttelse af notificerede eID-løsninger fra andre EU-lande SKAL ske gennem national eID-Gateway, der stilles til rådighed af Digitaliseringsstyrelsen. Løsninger, der skal servicere andre EU-borgere, SKAL afsøge muligheden for at anvende eID-Gateway'en til dette formål.*

## 5.6. Attributter

Som tidligere nævnt, spiller attributter en vigtig rolle i brugerstyringen, dels som grundlag for beskrivelse af brugerne og deres kontekst, dels som grundlag for håndhævelse af adgangskontrol.

Nedenfor er givet eksempler på forskellige, vigtige kategorier af såvel identitetsattributter som beskrivende attributter:

- Identitetsattributter, der er specifikke karakteristika ved den identiteten (fx navn, adresse, CPR-nummer).
- Andre attributter om identiteten (fødselsdag, øjenfarve, biometri).
- Tildelte/udstedte identifikationsnumre/registreringsnøgler (fx UUID, CVR-nummer, PID-, RID- eller FID-numre) eller tjenestespecifikke pseudonymer.
- Attributter, der beskriver relationer (repræsenterer virksomhed xyz).
- Rettighedsrelevante attributter (roller, rettigheder eller indhold af dataafgrænsninger, autorisation af læge/sygeplejerske/o.m.a for sundhedsprofessionelle).
- Kontekstafhængige attributter for en autentifikation (IP-adresse, devicetype, tidspunkt for login).
- Fuldmagter eller samtykker udtrykt som attributter.

Nogle attributter fastlægges i forbindelse med den indledende identitetsregistrering, mens andre etableres på andre tidspunkter af andre end en registreringstjeneste – eksempelvis i forbindelse med, at en brugeradministrator tildeler rettigheder, eller en attributtjeneste gør det på vegne af en føderation.

Der er vigtigt, at den fulde livscyklus for attributter håndteres, idet de kan ændre sig over tid. Det skal med andre ord være muligt dynamisk at tilføje attributter eller ændre deres værdier. Historisk har det eksempelvis vist sig problematisk at anvende X.509-certifikater til attributformidling, fordi et certifikat ikke kan ændres – og derfor skal der udstedes et nyt, hvis de underliggende attributter ændres.

I forbindelse med adgangskontrol af attributter i forretningstjenester er det vigtigt at forholde sig til attributternes kvalitet. Dette gælder særligt, når attributter anvendes som grundlag for beslutninger om adgang til følsomme data. I dag er der kun fælles rammer for visse attributters kvalitet – fx CPR-nummeret, CVR-numre eller de identitetsattributter, der håndteres gennem sikringsniveauerne i National Standard for Identitets Sikringsniveau (NSIS). Da mange attributter sædvanligvis er stabile over tid, er det ofte tilstrækkeligt at kende kvaliteten af attributter ved en tjenestes etablering og ved dialog med attributtjenesten at sikre sig, at der informeres ved ændringer i kvaliteten.

*! Attributtjenester BØR udstille deklaration af kvaliteten af attributter, således at tjenester, der anvender attributter, har den nødvendige information om kvalitet.*

*Fællesoffentlige brugerstyringstjenester og forretningstjenester i fællesoffentlige føderationer, der anvender attributter, SKAL vurdere, om kvaliteten af attributter svarer til tjenestens behov.*

I det fremadrettede arbejde med fællesoffentlig brugerstyring er der behov for at analysere videre i forhold til, på hvilke områder der er behov for fælles standarder for attributters kvalitet. Attributter defineres ofte inden for en bestemt sektor, men der kunne fællesoffentligt godt være mening i at specificere fælles mekanismer til at udtrykke og formidle kvalitetsinformation, så dette kan udveksles på en interoperabel måde.

Forskellige forretningstjenester har behov for at *modtage* bestemte attributter for at kunne fungere, mens forskellige login-tjenester/identitetsbrokere og attributtjenester kan *levere* forskellige sæt af attributter for bestemte identiteter. Disse sæt af attributter kan beskrives eksplicit som en del af snitfladen, så sikkerhedsinfrastrukturen kan foretage en automatisk orkestrering.

Eksempelvis kan en identitetsbroker evaluere tjenestens attributbehov og herefter kontakte et antal andre login-tjenester/identitetsbrokere og supplerende attributtjenester, som tilsammen kan levere de ønskede attributter, hvorefter brokern udsteder en samlet adgangsbillet mod tjenesten med foreningsmængden af attributter.

I den nuværende fællesoffentlige brugerstyringsinfrastruktur er der en begrænset dynamik i orkestreringen af attributter, og det er fx ikke direkte muligt at tilkoble en ny ekstern attributtjeneste til NemLog-in (kræver udvikling). Det kan derfor i det videre arbejde være relevant at se på mulighederne for en mere dynamisk håndtering af attributter, som følger ovennævnte arkitekturprincipper. Desuden kan det være relevant at give personbrugerne transparens og medejerskab for deres attributter, fx ved at etablere en brugerprofilside på NemLog-in eller borger.dk, hvor brugerne kan se (og for visse indtaste/rette) attributter samt styre præferencer for deling af attributter mellem tjenester.

Endelig er der en fællesoffentlig udfordring i håndtering af CPR-nummerattributten. Mange forretningstjenester har en hård binding til dennes nuværende form, hvilket gør det vanskeligt at skifte den ud, grundet det kommende udløb af numre. I den forbindelse definerer OIOSAML 3.0 profilen i stedet brug af CPR UUID'er, således at tjenester kan påbegynde migrering til disse.

*! Nye forretningstjenester (og moderniseringer af eksisterende) tjenester, der anvender fællesoffentlige løsninger, BØR benytte et design, hvor CPR-nummeret kan skifte form, uden at tjenestens forretningslogik bryder sammen.*

## 5.7. Brugerkataloger

Et brugerkatalog indeholder informationer om et sæt af brugeridentiteter (evt. både personbrugere og tjenestekonsumenter), typisk i form af attributter og i mange tilfælde også information til brug for validering af akkreditiver for en brugerkonto. Et velkendt eksempel er *LDAP Directories* (som fx Active Directory), der både udstiller services til brugerautentifikation, til at hente attributter, og som har en veldefineret administrationsstruktur.

Brugerkataloger etableres i mange kontekster som fx:

- Et brugerkatalog til en bestemt applikation (applikationens brugerdatabase).
- Et brugerkatalog for en organisation eller virksomhed.
- Brugerkataloger knyttet til et bestemt domæne (fx som i UNI•Login).
- Fællesoffentlige brugerkataloger (fx brugerdatabase i NemLogin).

Traditionelt har *enterprise directories* været en del af centralnervesystemet i større virksomheders systeminfrastrukturer, og i de senere år er der opstået en stigende tendens til at etablere brugerkataloger i skyen med henblik på at understøtte økosystemet af cloud-applikationer.

I referencearkitekturen indgår brugerkataloger ikke som selvstændige tjenester, men de udstilles gennem veldefinerede snitflader som logintjenester/identitetsbrokere eller attributtjenester med henblik på at etablere den ønskede løse kobling. Brugerkataloger opfattes med andre ord som en privat implementering af disse typer af tjenester, og der bør ikke i udgangspunktet skabes tætte koblinger til brugerkataloger gennem brug af deres leverandørspecifikke snitflader. En tydelig tendens mod den mere løst koblede model kan observeres med Active Directory, hvor man for år tilbage ofte koblede organisationer sammen via proprietære mekanismer, der kunne forbinde AD'er. I dag anvendes i langt højere grad *Federation Services*, hvor sammenkoblingen sker via föderationsprotokoller som SAML, OpenID Connect mv.

Referencearkitekturen kommer ikke med specifikke anbefalinger til, hvilke brugerkataloger der skal etableres – men fokuserer hovedsageligt på, hvordan de udstilles. Behov for brugerkataloger vil således i høj grad afhænge af lokale forhold, herunder behov for organiseringen af brugeradministration.

Som en god praksis (og som det fremgår af Princip: Administration af brugere flyttes så vidt muligt ud af fagapplikationer) bør brugere i en organisation i udgangspunktet oprettes i så få brugerkataloger som muligt med henblik på at effektivisere brugeradministrationen og sikre et centralt overblik. Dette gælder løsninger, der finansieres og fungerer inden for den offentlige sektor.

Som eksempel på mitigerende af problemstillingen med mange, adskilte brugerkataloger (siloer), etablerer mange organisationer såkaldte Identity Management-løsninger, som kan skabe sammenhæng mellem mange brugerkataloger gennem processer, teknisk provisionering og adapters. Herved kan man oprette, administrere og nedlægge brugere centralt og automatisk få de nødvendige opdateringer kommunikeret til applikationer og infrastruktur. Dette er dog i mange sammenhænge udtryk for applikationernes manglende modenhed inden for brugerstyring (de fastholder et lokalt brugerkatalog som deres eneste verdensbillede), og løsningen med provisionering og applikationsspecifikke adapters fastholder den tætte binding frem for at løse det underliggende problem og skabe en åben, løst koblet arkitektur.

I den fællesoffentlige brugerstyring findes et centralt brugerkatalog for virksomheder i form af NemLog-in/Brugeradministration, der i Nemlog-in3 erstattes med en samlet komponent til erhvervsidentitetsadministration (EIA). Hensigten med dette er at garantere danske virksomheder adgang til mindst et brugerkatalog, da særligt mindre virksomheder ikke kan forventes selv at kunne etablere en sådan infrastruktur. Med NemLog-in3 får større virksomheder kan vælge at bruge deres eget lokale brugerkatalog, også i forbindelse med administration af adgang til offentlige løsninger.

## 5.8. Autentifikation

Autentifikation er de processer, hvor en bruger anvender sine akkreditiver, og hvor en autentifikationstjeneste (ved login) dels garanterer, at de fremviste akkreditiver tilhører den identitet, de er udstedt til, dels kontrollerer, hvilke sikringsniveauer registrering og akkreditivudstedelse er kendetegnet ved. Det aktuelle sikringsniveau er altid det laveste af de to konstaterede sikringsniveauer.

Det centrale i referencearkitekturen i forhold til autentifikation er dels at fastlægge standarder for overførsel af autentificerede identiteter til tjenesteudbydere og mellem autentifikationstjenester, login-tjenester/brokere og forretningstjenester, dels at autentifikationen kan være en del af en login-tjeneste/identitetsbroker.

## 5.9. Standarder for overførsel af autentificerede brugere

! I dag anvender NemID XMLDSig i forbindelse med autentifikation, hvor særligt det indlejede OCES-certifikat er kilde til attributter om brugeren. XMLDSig BØR FORLADES fremadrettet og ikke danne grundlag for en fodereret løsning, idet der findes protokoller, der i højere grad er velegnede til dette formål.

NemLog-in anvender den fællesoffentlige OIOSAML-profil af SAML 2.0- standarden til overførsel af data om autentificerede brugere til tjenesteudbydere, som er tilsluttet NemLog-in. Til brug i NemLog-in3 er profilen moderniseret til versio 3.0. Profilen understøtter scenariet, hvor en personbruger via en browser logger på en webapplikation. Til repræsentation af roller og rettigheder i SAML Assertions benyttes søsterprofilen OIO Basic Privilege Profile. Ud over NemLog-in er OIOSAML og OIO Basic Privilege Profile grundlaget for en række løsninger i specifikke domæner som fx systemerne til adgangsstyring i den fælleskommunale rammearkitektur. Hensigten med OIOSAML er at sikre interoperabilitet gennem fastlåsning af visse valg i SAML – men samtidig åbne for, at specifikke sektorer kan definere deres egne underprofiler ved fx at definere domænespecifikke attributter.

*! OIOSAML og OIO Basic Privilege Profile har status af anbefalede fællesoffentlige standarder og BØR som minimum følges, når der er behov for håndtering af eksterne brugere i webapplikationer. Dette gælder for fællesoffentlige løsninger og tjenester, der anvender fællesoffentlige løsninger.*

Der er tale om modne standarder med en stor udbredelse i den offentlige sektor. Her kan det bemærkes, at OIOSAML specificerer udvekslingsmekanismen (protokollen), men er åben for tilføjelse af sektorspecifikke attributter. Et eksempel på dette er sundhedsområdets underprofiler.

Som supplement til OIOSAML findes OpenID Connect-standarden samt OAuth 2.0, der begge er internationale, åbne standarder med en vis markedsudbredelse. OpenID Connect kan løse de samme use cases som SAML 2.0, men benytter mere moderne teknologier, som bl.a. er velegnede i forbindelse med apps på mobile enheder. Der findes få fællesoffentlige profiler af OpenID Connect og OAuth 2.0 - bl.a. OIO IDWS REST profilen. Det skal endvidere bemærkes, at en brugerauthentifikation i disse standarder kan anvende SAML, så derfor kan eksisterende løsninger sameksistere (indpakkes i) de nye standarder. OpenID Connect har status af kommende standard, som på sigt forventes at supplere eller tage over efter SAML.

*! For fællesoffentlig infrastruktur BØR standarden OpenID Connect på kort til mellemlangt sigt tilbydes som et supplement til SAML 2.0 services, således at de forretningstjenester, der har behov for det, kan udnytte de nye muligheder – men uden at alle tvinges til det.*

Indtil der er etableret fællesoffentlige profiler af OpenID Connect, er der dog en vis risiko for, at forskellige parter implementeringer ikke vil være interoperable eller have samme sikkerhedsniveau, hvilket kan give udfordringer i tværgående sammenhænge. OpenID Connect er en profil af OAuth 2.0, og denne profil *anbefales* i stedet for brug af den rene OAuth 2.0-standard, da OpenID Connect i højere grad er kompatibel med referencearkitekturens principper om føderering.

Herudover kan det nævnes, at Microsoft og IBM har udviklet hhv. UProve og IdentityMixer, som er protokoller med særlige privacy-egenskaber. Anvendelse af disse teknologier er beskrevet i diskussionspapiret "Nye Digitale Sikkerhedsmodeller" (<https://digitaliser.dk/resource/781482>) fra IT- og Telestyrelsen som et alternativt og innovativt bud på, hvordan en sikkerhedsarkitektur kan designes. Ingen af disse teknologier har endnu vundet markedsudbredelse (ikke engang i de respektive leverandørers egne produkter), og de BØR derfor endnu IKKE anvendes til andet end specialsituationer, som ikke kan løses med andre mere mainstream teknologier.

Kantara har defineret en protokol for administration af rettigheder kaldet User Managed Access (UMA). Denne har støtte fra en lang række internationale aktører (bl.a. Google), men har endnu ikke vundet markedsudbredelse. Ud fra en modenhedsbetragtning er UMA endnu ikke en anbefalet standard, men blot en kommende standard, som bør følges tæt i den fællesoffentlige brugerstyring. I givet fald er UMA interessant som en model for at give slutbrugerne kontrol med adgangen til deres ressourcer, og den bør derfor i de kommende år overvejes i forbindelse med løsninger til fuldmagter og samtykker.

## 5.10. Login-tjenester/Identitetsbrokere

En login-tjeneste/identitetsbroker er en tjeneste, der på vegne af forretningstjenester foretager en eller flere brugerstyringstjenester:

- Autentifikationen gennem at verificere et akkreditiv evt. ved at kontakte en akkreditivudsteder og herfra modtage en adgangsbillet.
- Omveksle adgangsbilletter, udstedt af andre login-tjenester/identitetsbrokere.
- Indhente yderligere information om brugeren hos attributtjenester og berige adgangsbilletten.
- Evt. danne en session med brugeren med henblik på at etablere Single Sign-On (SSO).

Der er en række udfordringer, der skal håndteres i forbindelse med anvendelse af identitetsbrokere.

I forhold til en model, hvor tjenesteudbydere er koblet direkte til registreringstjenester og akkreditivudstedere, er der med introduktion af brokern endnu en part, der kan påvirke den samlede opetid for tjenesteudbyderen i negativ retning. Den enkelte tjenesteudbyder kan mitigere risikoen ved at indgå aftale med flere brokere, som illustreret for tjenesteudbyder B i Figur 18 Arkitektur med flere registreringstjenester, en akkreditivudsteder og brokere.

Der skal etableres en forretningsmodel, der understøtter anvendelse af brokerfunktion. Forretningsmodellen skal gerne gøre det fordelagtigt for registreringstjenester, akkreditivudstedere og brokere at indgå aftaler og skal desuden minimere risikoen for udnyttelse af en dominerende stilling på markedet for hhv. registreringstjenester, akkreditivudstedere og brokere. National Standard for Identitets Sikringsniveau (NSIS) rammeværket indeholder, som nævnt, krav til sikkerhed og revision for identitetsbrokere, der kan regulere de sikkerhedsmæssige aspekter.

*! For at opnå en sikker og omkostningseffektiv integration for tjenesteudbydere og for at understøtte konkurrencen på markedet SKAL en identitetsbroker som minimum udstille en eller flere veldefinerede, åbne og standardiserede interfaces til tjenesteudbydere. Dette kan typisk være et SAML2 (som kendes fra NemLog-in) og/eller OpenID Connect.*

*Tilsvarende SKAL der stilles veldefinerede interfaces til rådighed for digital signering*

I den tværoffentlige brugerstyringsinfrastruktur er der fortsat behov for en identitetsbroker. Denne opgave løses i dag af NemLog-in, som er implementeret for det offentlige af Digitaliseringsstyrelsen.

*! Der SKAL fortsat være en broker som NemLog-in i den fællesoffentlige brugerstyringsinfrastruktur.*

I andre sektorer er der tilsvarende brokere. Det er fx SOSI STS'er i sundhedssektoren, og WAYF i uddannelses- og forskningssektoren. For andre sektorer er bestemmelserne om brokere vejledende.

### 5.11. Standarder for kommunikation mellem føderationer

Ved kommunikation mellem føderationer (interføderation) benyttes normalt de samme standarder/protokoller som inden for et domæne (fx SAML eller WS Trust), og der vurderes generelt ikke at være væsentlige behov for yderligere standardisering på området. Som eksempel kan nævnes, at EU-føderationen i regi af eIDAS baseres på en SAML-profil.

De primære udfordringer ved interføderation opstår, når hvert domæne har etableret egne domænespecifikke attributter, domænepolitikker eller har egne sikringsniveauer, der ikke er kompatible. Her kan NSIS (og eIDAS) løse udfordringen med fælles sikringsniveauer, mens der ikke findes generelle standarder for oversættelse mellem domæners attributter og politikker. Et første skridt i den retning kunne være at etablere fælles vokabularer (fx i stil med OIO Organisation og *ISA Core Vocabularies* ([http://ec.europa.eu/isa/ready-to-use-solutions/core-vocabularies\\_en.htm](http://ec.europa.eu/isa/ready-to-use-solutions/core-vocabularies_en.htm)) som findes i EU-regi). Dette arbejde har dog mere karakter af datastandardisering og semantiske modeller og vurderes ikke nødvendigvis som hjemmehørende under brugerstyringsarbejdet.

### 5.12. Fælles løsning til fuldmagter

En fælles løsning til digitale fuldmagter gør det muligt for borgere og virksomheder at lade en repræsentant agere på deres vegne i en onlinetjeneste. Dette muliggør både at yde god digital service, som tager hensyn til it-svage borgere, og samtidig at fx forvaltningslovens krav til partsrepræsentation kan opfyldes.

Hovedfunktionerne i en digital fuldmagtsløsning er:

- Funktionalitet til digital afgivelse af fuldmagt gennem et selvbetjeningsforløb (inkl. udpegning af modtager, indhold af fuldmagt, gyldighedsperiode og signering af fuldmagt).
- Funktionalitet til at få overblik over afgivne og modtagne fuldmagter.
- Funktionalitet til at tilbagekalde en fuldmagt.
- Funktionalitet for en tjeneste til at definere de "fuldmagtspakker", som beskriver indholdet af de fuldmagter, der kan afgives til tjenesten (fx roller til tjenesten).
- Funktionalitet til, at en betroet medarbejder kan indtaste en fuldmagt på vegne af en (it-svag) borger – fx på baggrund af en underskrevet papirblanket.
- Integration med identitetsbrokere, så fuldmagter kan indlejres i udstedte adgangsbilletter til tjenester.
- API'er for tjenester til at batch-hente fuldmagter.

En fællesoffentlig løsning er i dag etableret i regi af NemLog-in, kaldet 'Digital Fuldmagt'. Løsningen findes i to forskellige varianter, der er målrettet til forskellige brugssituationer:

- En løsning til Erhvervsfuldmagt i NemLog-in/Brugeradministration (FBRS).
- En løsning til Borgerfuldmagt (selvstændig brugergrænseflade).

For begge løsningers vedkommende vil afgivelse af en fuldmagt resultere i, at adgangsbilletten tilhørende identiteten for repræsentanten markeres, at der er delegeret en rettighed (privilegie) fra fuldmagtsgiver. Digitale fuldmagter udmøntes med andre ord som en delegering af rettigheder til en tjeneste, udtrykt som attributter i en adgangsbillet – og dermed benytter de grundlæggende byggeblokke, der allerede findes i arkitekturen. Herved er det væsentligt lettere for tjenester at tage fuldmagtsfunktionaliteten i brug, idet eksisterende grænseflader og integrationer med NemLog-in genanvendes. Konkret består disse i OIOSAML profilen, og delegeringen udtrykkes via OIO Basic Privilege Profile.

I den nuværende løsning vil en fuldmagt bestå i en delegering af en statisk rolle i en tjeneste, som fx kunne være "se sag", "indsend ansøgning", "ansøg om tilskud" etc. Der er p.t. ikke mulighed for at udtrykke dataafgræn-

sninger i kombination med rollen, hvilket kunne udtrykke mere finkornede og præcise fuldmagter (fx "se sagsnr. AZ-7291"). Fuldmagtsløsningen skal med andre ord også respektere dataafgrænsninger, som beskrevet i afsnittet om adgangskontrol. Dette er dog et identificeret videreudviklingsønske, som forventes at blive realiseret.

Endelig kan det nævnes, at den nuværende fuldmagtsløsning i regi af NemLog-in hidtil har været frivillig at anvende for offentlige tjenester. Denne referencearkitektur skærper dette til et "bør".

! I henhold til arkitekturprincipperne om at genbruge løsninger og anvende fælles standarder BØR fuldmagtsløsningen anvendes for borgerrettede løsninger, der finansieres og fungerer inden for den offentlige sektor.

Dette sikrer genbrug, strømning af infrastrukturen og ensartet brugeroplevelse og giver borgere og virksomheder mulighed for at få en central indgang til alle deres fuldmagter på tværs af tjenester. Dette vil formentlig indebære, at NemLog-in's fuldmagtsløsning videreudvikles funktionelt, så behov i langt de fleste sektorer og løsninger kan understøttes.

### 5.13. Brugerstyring for tjenestekonsumenter og fysiske apparater og sensorer

Hovedparten af ovenstående beskrivelser adresserer brugerstyring for personbrugere, dvs. fysiske personer eller fysiske personer associeret med en juridisk person. Dette område har været første bastion i arbejdet med fællesoffentlig brugerstyring, men der er i stigende grad behov for at løse de samme udfordringer i forbindelse med systembrugere – altså identiteter, der repræsenterer et it-system, der fx optræder som tjenestekonsument, og som tilhører en organisation eller en person.

Eksempler på dette kan være server-til-server kommunikation mellem myndigheder, apps eller rige klienter, der kalder et API på vegne af en bruger (fx tilgår brugerens profil og data), softwarebotter, telemedicinsk udstyr installeret i en patients hjem, der indrapporterer måleværdier, eller fjernstyring af kontrolenheder i energisektoren.

Dette område er karakteriseret ved en stor diversitet i behov og muligheder – og mangel på fælles standarder og løsninger på tværs. Der eksisterer således standarder og løsninger inden for specifikke områder, men ikke nogen universelle, der dækker bredt. Som eksempel kan nævnes, at National Standard for Identiteters Sikringsniveau (NSIS) standarden ud fra betragtninger om lav modenhed på området eksplicit har fravalgt at behandle identiteter for systemer og enheder og alene fokusere på personbrugere. Nedenfor gives et overblik over de væsentligste løsninger og standarder, og der peges på områder, der bør arbejdes videre med i den videre proces.

Den klassiske tilgang for sikring af systemkommunikation har været at sikre punkt-til-punkt forbindelser med X.509-certifikater, passwords, SSH-nøgler etc. afhængigt af den valgte kommunikationsprotokol. Det er eksempelvis muligt i den nuværende fællesoffentlige identitetsinfrastruktur at få udstedt OCES-funktionseller virksomheds-certifikater og benytte dem til system-til-system kommunikation ved at udveksle den offentlige nøgle med modparten. Dette giver en simpel og isoleret løsning for en konkret integration, men kan i større infrastrukturer hurtigt lede til et ustruktureret og u håndterbart virvar af punkt-til-punkt sikringer, som ingen har overblik over, og som er usammenhængende og ufleksibelt i forhold til ændringer i infrastrukturen. Uden videre tiltag og en fælles arkitektur er der derfor stor risiko for fragmentering og mangel på sammenhæng og interoperabilitet.

### 5.14. Standarder for identitetsbaserede webservices

Der er fællesoffentligt specificeret en række standarder, omhandlende *identitetsbaserede webservices*. Disse standarder kan eksempelvis benyttes, når en tjenestekonsument skal anmode om et *security token* på vegne af en bruger, som herefter benyttes til at autorisere et kald til en webservice i et andet domæne. Et eksempel kan være, at en bruger logger ind på en webportal, som herefter har brug for at hente data om brugeren hos en anden tjenesteudbyder.

!

Profilerne for identitetsbaserede webservices(<https://digitaliser.dk/resource/526486>) består af:

- OIO WS-Trust Profile (profil til at anmode om Security Token).
- OIO WS-Trust Deployment Profile (profil til at anmode om Security Token).
- OIO Profile for Identity Tokens (profil for token udformning i webservice-kald).
- OIO Bootstrap Token Profile (profil for veksling af Web SSO session til token ifm. systemkald).
- Liberty Basic SOAP Binding (profil af WS-Security til sikring af SOAP-baserede webservice-kald med SAML Token).
- OIO IDWS Rest Profile (profil til sikring af REST-baserede webservice-kald med SAML Token).

For disse standarder gælder, at de BØR følges ved etablering af system-til-system kommunikation, hvor kaldet sikres med en adgangsbillet (et *security token*) i henhold til denne referencearkitekturs principper, frem for en punkt-til-punkt integration. Dette gælder for fællesoffentlige løsninger og løsninger, der kommunikerer mellem offentlige sektorer.

Disse profiler er endvidere suppleret med open sourcereferenceimplementeringer i Java og .Net for at lette udbredelsen.

Profilerne er i dag implementeret i NemLog-in gennem udstilling af en Security Token Service. Underprofiler af disse er endvidere specificeret inden for sundhedsdomænet samt den fælleskommunale rammearkitektur.

Sundhedsområdet benytter samme arkitekturprincipper og har defineret egne SAML-baserede standarder, suppleret med egne STS'er deployet i domænet. Det overordnede princip i OIO IDWS-modellen er at anvende en fødereret og token-baseret model for systemer på samme måde som for personbrugere. En Security Token Service udfylder samme rolle for systemer som en SAML Identity Provider udfylder for personer (autentifikation og udstedelse af adgangsbillet). Endvidere kan man med identitetsbaserede webservices opnå, at et system (fx server eller rig klient) kan agere på vegne af en person, der er logget ind på systemet. Dette er fx relevant, når en bruger logger ind på en portal, som herefter har brug for at kontakte en tredje tjeneste for at tilgå brugerens data.

I grunddataprogrammet har man valgt en fælles, tværgående sikkerhedsmodel, baseret på udstedelse af Security Tokens for de services, der muliggør opdatering af registre. Dette giver en struktureret model på tværs af programmet frem for et virvar af punkt-til-punkt integrationer, baseret på certifikater. Modellen er baseret på, at myndighederne registrerer deres opdateringsservices i NemLog-in med tilhørende roller, og at såkaldte systembrugerklinter kan blive tildelt rettigheder til disse services. Efter tildelingen kan en systembrugerklinter anmode NemLog-in's STS om en adgangsbillet til en service, hvor rollerne så vil fremgå af adgangsbilletten.

*! Kommunikation til/fra webservices med følsomt indhold, der ønskes sikret med Security Tokens, BØR baseres på profilerne Liberty Basic SOAP Binding (dennes efterfølger OIO IDWS SOAP Binding) eller OIO IDWS Rest Profile ved ekstern kommunikation over internettet.*

På mobile enheder er der ofte behov for at kunne autorisere en app til at kunne agere på brugerens vegne. Der findes endnu ingen fællesoffentlige standarder på dette område, men der tegner sig alligevel en række mønstre og best practices, baseret på anvendelse af OAuth 2.0 samt OpenID Connect standarderne. Det grundlæggende princip i disse er, at brugeren via en mobil browser sendes til en autorisationsserver, hvor brugeren logger ind og bekræfter, at app'en må tilgå brugerens data og ressourcer. Herefter udstedes en adgangsbillet til app'en, som herefter kan anvendes til at autorisere kald til webservices - og såvel app'ens identitet som akkreditiv er adskilt fra brugerens. Her skal bemærkes, at brugerautentifikationen (indlejret i OAuth eller OpenID Connect) sagtens kan være baseret på SAML2.0, hvorfor den eksisterende infrastruktur kan genanvendes. Digitaliseringsstyrelsen har i 2011 udgivet en vejledning til OAuth 2.0 (<https://digitaliser.dk/resource/1246357>), der viser hvordan standarden kan anvendes. Det ventes endvidere, at der i videreudviklingen af NemLog-in vil blive etableret bedre understøttelse af mobile enheder via andre protokoller end SAML.

Et eksempel på, hvordan et udbredt mønster for autorisering af en app med OpenID Connect kunne se ud i en fællesoffentlig kontekst, er illustreret nedenfor i Figur :

[!Figur 23: Eksempel på autorisering af en mobil app via OpenID Connect med en indlejret SAMLbrugerautentikation](#)

Der er identificeret følgende emner til det videre arbejde med fællesoffentlig brugerstyring, hvor identiteten er en tjenestekonsument eller et fysisk apparat eller sensor:

- Fællesoffentlige profiler af nye standarder som OAuth 2.0/OpenID Connect og -mønstre for håndtering af apps via disse.
- Understøttelse af nye profiler via services i infrastrukturen (primært NemLog-in).
- Etablering af brugergrænseflade for brugerne, der giver overblik over, hvilke apps de har autoriseret til hvad (inkl. mulighed for at tilbagetrække autorisation).
- Videre analyser i forhold til Internet of Things, herunder om app-modeller kan bruges, eller der skal udvikles separate løsninger for disse enheder.
- Videre analyser i forhold til anvendelse af den nuværende PKI-infrastruktur for IoT (herunder FOCES/VO-CES-certifikater i særlige profiler, målrettet specifikke sektorer).

Det skal bemærkes, at visse sektorer har helt specielle krav, der bedst opfyldes med højere grad af decentralisering. Elsektoren baserer eksempelvis den kommende sikring og brugerstyring af enheder på standarderne IEC 61850 og IEC 62351, der anvender punkt-til-punkt forbindelse ved brug af X.509v3. Det kan med rimelighed antages, at resten af forsyningssektoren vil kunne anvende samme model som elsektoren.



## 5.15. Perspektivering

## 5.16. Bilag

### 5.16.1. Ordliste

Nedenstående liste forklarer betydningen af de væsentligste ord og begreber, der indgår i den tværoffentlige referencearkitektur for brugerstyring.

Ord, der er markeret med *kursiv*, er ord, hvor definitionen kan findes på ordlisten. || | Brugerrolle | Rolle der udgøres af en eller flere *adgangsrettigheder* til et eller flere it-systemer, som en bloc tildeles til en bruger. Brugerroller anvendes til at afgøre, hvilke handlinger en bruger må udføre i et it-system. Brugerrollen fastlægger de *adgangsrettigheder*, som brugeren er tildelt. Brugere tilknyttes til roller og opnår *adgangsrettigheder* ved at være rolleindehaver. Brugerroller er grupperinger af *adgangsrettigheder*. Der er ikke nødvendigvis sammenfald mellem brugerroller og brugerens profession, stillingsbetegnelse mv. | IT- & Telestyrelsen, Begrebsmodel til brugerstyring || Brugerrollerestriktion | En begrænsning som specificerer, hvad en *brugerrolle* må bruges på. Et typisk eksempel er en såkaldt *dataafgrænsning*, som angiver hvilke dataobjekter (fx sager) som en given rolle må anvendes på (fx rollen *læs sag* afgrænset til sag med nummeret xyz'). I RBAC samt OIO Basic Privilege Profile benævnes dette for en *constraint*. | IT- & Telestyrelsen, Begrebsmodel til brugerstyring || Brugerrolletildeling | Angivelse af de *brugerroller* som en bruger er tildelt evt. med tilhørende *brugerrollerestriktioner*. Brugerrolletildeling anvendes til at definere en brugers *brugerroller* med de begrænsninger (*brugerrollerestriktioner*), der måtte være i forhold til anvendelsen af brugerrollen. I OIO Basic Privilege Profile anvises hvordan brugerens roller kan udtrykkes i et en SAML Assertion. | IT- & Telestyrelsen, Begrebsmodel til brugerstyring || Brugerstyring | Brugerstyring anvendes bredt i denne tværoffentlige strategi og referencearkitektur for brugerstyring. Betegnelsen omfatter både *adgangskontrol* og administration af identiteter, akkreditiver, attributter og *adgangsrettigheder*, herunder det der på engelsk betegnes Credential and Identity Management (CIM), Identity Rights Management (IRM), Access Control (AC) og Identity and Access Management (IAM/IdAM). Brugerstyring dækker således opgaver i forbindelse med *indrullering*, *autentificering*, *autorisation*, *billetudstedelse*, *adgangskontrol* osv. || | Certificate Authority (CA) | En betroet enhed, der udsteder *certifikater* til identificerede og registrerede parter (se også *registreringsmyndighed*). Opgaverne og ansvarsområderne tilhørende en CA er opdelt i Identity Proofing Service (IPS) og *Credential Management Service (CMS)*. || | Certifikat | En elektronisk attest, som angiver certifikatindehaverens offentlige nøgle sammen med supplerende information, og som entydigt knytter den offentlige nøgle til identifikation af certifikatindehaveren. Et certifikat skal signeres af et certificeringscenter (CA), som derved bekræfter certifikatets gyldighed. | OCES certifikatpolitikker || | Certifikatudbyder, Certifikatudsteder, Certificeringscenter | En fysisk eller juridisk person, der er bemyndiget til at generere, udstede og administrere *certifikater* (jf. *identitetsudbydere*). Se også *Certificate Authority*. | OCES certifikatpolitikker || | Claim | Synonym for attribut. || | Credential | Synonym for *Akkreditiv*. || | Credential Management Service | Service der varetager udstedelse og vedligeholdelse af akkreditiver gennem hele deres livscyklus. | Fællesoffentlig eID i regionerne - Definition af begreber og termer || | Credential Service Provider (CSR) | Se Udsteder af akkreditiv. || | Delegering | Omhandler personers adgang til at benytte medhjælp, dvs. under ansvar og efter instruktion og under tilsynspligt uddelegere nogle af den uddelegerendes rettigheder. Karakteristisk for delegering er, at der er tale om en person, der instruerer en anden i at handle på sine vegne. Med delegeringen kan der følge en pligt til at instruere og kontrollere. Der stilles derfor krav om, at man skal kunne se, hvem der handler på hvis vegne ved centrale opslag. | Fællesoffentlig eID i regionerne - Definition af begreber og termer || | Digital identitet | En digital persona repræsenteret (entydigt) ved et sæt af attributter. En entitet kan have mere end en identitet. | Informationsordbogen || | Digital Signatur | Anvendes om første generation af offentlige *certifikater* til elektronisk service (OCES). Et matematisk skema til at bevise autenticiteten af en digital besked eller dokument. Digitale signaturer dannes ved brug af asymmetrisk kryptering og hashfunktioner. Anvendes ikke synonymt med eSignatur. | Informationsordbogen || | eIDAS | Electronic identification and trust services. EU-forordningen om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner. | eIDAS || | Elektronisk Identitet | Se *Digital Identitet*. || | Elektronisk signatur | Data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre data i elektronisk form, og som anvendes af underskriveren til at skrive under med. | EU 910/2014 Fællesoffentlig eID i regionerne - Definition af begreber og termer || | Elektronisk identifikationsmiddel | Et elektronisk eller fysisk objekt/genstand, der kan anvendes til at gennemføre en autentifikation af en identitet. Eksempler kan være brugernavn/kodeord, et NemID nøglekort, et certifikat med tilhørende privat nøgle, et SAML token etc. Betegnes også for Akkreditiv. | National Standard for Identiteters Sikringsniveauer (NSIS) || | Elektronisk signaturgenereringssystem | Konfigureret software eller hardware, der bruges til at generere en elektronisk signatur. | EU 910/2014 Fællesoffentlig eID i regionerne - Definition af begreber og termer || | ID-tjeneste | En betroet tjeneste, som leverer en eller flere af de processer, som er underlagt krav i (NSIS). Dette kan fx være identitetssikring, udstedelse af elektroniske identifikationsmidler eller drift af en broker. Bemærk, at eIDAS reguleringen bruger det komplementerende begreb "tillidstjeneste" om tjenester involveret i udstedelse af digitale signaturer/certifikater, validering af certifikaters gyldighed og tidsstempling. Der er intet overlap mellem ID-tjenester i NSIS og tillidstjenester i eIDAS - det er således helt komplementære begreber. | National Standard for Identiteters Sikringsniveauer (NSIS) || | Entitet | En fysisk person eller juridisk enhed, som ønsker adgang til en on-line tjeneste gennem autentifikation med elektroniske identifikationsmidler. En entitet kan have flere elektroniske iden-

titeter – fx kan en fysisk person både have en privatidentitet og flere erhvervsidentiteter. En entitet er noget værende, og kan også være en ting, sensor, app, apparat eller softwarerobot. | National Standard for Identiteters Sikringsniveauer (NSIS) | | eSignatur | eSignatur defineres som data i elektronisk form, der er logisk forbundet med andre elektroniske data, som autentificerer den, der signerer. En "avanceret" signatur er en eSignatur, der kan identificere den, som signerer. Anvendes primært om begrebet elektronisk underskrift og i begrænset omfang om en specifik elektronisk underskrift. \*

### 5.16.2. Referenceliste

California - Identity and Access Management (IdAM) Reference Architecture (RA), 2014

<http://ocio.ca.gov/ea/docs/Identity-and-Access-Management-IdAM-V1.pdf>

Datatilsynet, Flere faktorer i login

[http://www.datatilsynet.dk/fileadmin/user\\_upload/dokumenter/Publikationer/ST1.pdf](http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/ST1.pdf)

eIDAS, EU-forordningen om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner

<http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond>

EU 910/2014. Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester <http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32014R0910>

Fællesoffentlige brugerstyringsløsninger – En analyse af sikkerhedsstandarder og -løsninger [http://www.google.dk/url?](http://www.google.dk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.kl.dk%2FImageVaultFiles%2Fid_67589%2Fcf_202%2FBilag_5_-_Udkast_til_rapporten_F-llesoffentlige_br.PDF&ei=LsevVM3yN4iGzAPtLwDA&usq=AFQjCNFV8hOc84wYml5TG5GfHYAv0BvbAw&bvm=bv.83339334,d.bGQ)

[sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.kl.dk%2FImageVaultFiles%2Fid\\_67589%2Fcf\\_202%2FBilag\\_5\\_-\\_Udkast\\_til\\_rapporten\\_F-llesoffentlige\\_br.PDF&ei=LsevVM3yN4iGzAPtLwDA&usq=AFQjCNFV8hOc84wYml5TG5GfHYAv0BvbAw&bvm=bv.83339334,d.bGQ](http://www.kl.dk%2FImageVaultFiles%2Fid_67589%2Fcf_202%2FBilag_5_-_Udkast_til_rapporten_F-llesoffentlige_br.PDF&ei=LsevVM3yN4iGzAPtLwDA&usq=AFQjCNFV8hOc84wYml5TG5GfHYAv0BvbAw&bvm=bv.83339334,d.bGQ)

Fællesoffentlig eID i regionerne - Definition af begreber og termer

<http://lionel.lakeside.dk/twiki/bin/view/Main/EIDBegrebsListe>

Informationsordbogen [www.informationsordbogen.dk](http://www.informationsordbogen.dk)

ISO/IEC 24760, A framework for identity management [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=57914](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57914)

IT- & Telestyrelsen, Begrebsmodel til brugerstyring, Version 1.1, 2010 [http://www.digst.dk/~media/Files/Nem-Login/Begrebsmodel\\_til\\_brugerstyring\\_-\\_Version\\_1\\_11.ashx](http://www.digst.dk/~media/Files/Nem-Login/Begrebsmodel_til_brugerstyring_-_Version_1_11.ashx)

Kantara, Identity Relationship Management <https://kantarainitiative.org/irmpillars/>

Lakeside, Region Midtjylland, Digital identitet – vigtige begreber og processer, 2014 *Grundlaget for eID i regionerne – Bilag 7: Digital identitet – vigtige begreber og processer*

National Standard for Identiteters Sikringsniveauer (NSIS) Forventes publiceret primo 2017

Network Working Group, Request for Comments 2828 <http://www.ietf.org/rfc/rfc2828.txt>

NIST, Electronic Authentication Guideline <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

OCES-certifikatpolitikker [https://www.nemid.nu/dk-da/digital\\_signatur/oces-standarden/oces-certifikatpolitikker/](https://www.nemid.nu/dk-da/digital_signatur/oces-standarden/oces-certifikatpolitikker/)

W3C, Web Services Architecture, Working Group Note, 11 February 2004 <http://www.w3.org/TR/ws-arch/>

### 5.16.3. Kilder og baggrundsmateriale

Nedenstående liste viser det baggrundsmateriale, der indgår i udarbejdelsen af den tværoffentlige referencearkitektur for identitets- og rettighedsstyring.

| Kilde | Materiale | -----|-----|

-----| California, Department of Technology | Identity and Access Management (IdAM) Reference Architecture (RA) 02-01-2014 <http://ocio.ca.gov/ea/docs/Identity-and-Access-Management-IdAM-V1.pdf> | | Digitaliseringsstyrelsen | CIDR – borger.dk <http://digitaliser.dk/group/2289910> | | Digitaliseringsstyrelsen | Digitaliseringsstyrelsens anbefalinger for brug af standarder for identitetsog rettighedsstyring som f.eks. OIO Web SSO Profile 2.0.6 (også kendt som OIOSAML 2.0) <http://www.digst.dk/Arkitektur-og-standarder/Standardisering/Standarderfor-serviceorienteret-infrastruktur/Standarder-og-anbefalinger-forbruger>

styring | | Digitaliseringsstyrelsen | Forslag til fælles sikkerhedsmodel for Grunddataprogrammet - 2014-06-19 | | Digitaliseringsstyrelsen | Fuldmagtsrapport 2012. Fuldmagt, partsrepræsentation og samtykke. Behov og løsningsmuligheder, Rambøll for Digitaliseringsstyrelsen 2012 | | Digitaliseringsstyrelsen | National Standard for Identitetens Sikringsniveauer (NSIS) Forventes publiceret primo 2017 | | Digitaliseringsstyrelsen | Persongrunddata-rapporten | | eIDAS | European Commission, Electronic identification and trust services <http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond> | | Initiativ 3.4 i den Nationale Strategi for Digitalisering af Sundhedsvæsenet 2013 – 2017 | Fællesoffentlige brugerstyringsløsninger – En analyse af sikkerhedsstandarder og -løsninger | | IT- & Telestyrelsen | Den fællesoffentlige begrebsmodel til brugerstyring, der er udgivet af ITog Telestyrelsen. [http://www.digst.dk/Loesninger-oginfrastruktur/NemLogin/~media/Files/NemLogin/Begrebsmodel\\_til-brugerstyring\\_-\\_Version\\_1\\_11.ashx](http://www.digst.dk/Loesninger-oginfrastruktur/NemLogin/~media/Files/NemLogin/Begrebsmodel_til-brugerstyring_-_Version_1_11.ashx) | | IT- & Telestyrelsen | Nye digitale sikkerhedsmodeller- et oplæg til diskussion. Januar 2011 | | Kantara | Kantara Initiative accelerates identity services markets by developing innovations and programs to support trusted on-line transactions. The membership of Kantara Initiative includes international communities, industry, research & education, and government stakeholders. <http://kantarainitiative.org> | | KOMBIT | Adgangsstyring i Rammearkitekturen - 22-03-2013 (kravspecifikation) | | KOMBIT | Introduktion til Adgangsstyring <https://sharekomm.kombit.dk/P024/Delte%20dokumenter/Introduktion%20til%20Adgangsstyring.pdf> | | Miljøportalen | Analyse af anvendelse af NemLog-in som brugerstyringsløsning??? | | National Sundheds-it | Referencearkitektur for Informationssikkerhed, september 2013 <http://www.ssi.dk/Sundhedsdataogit/National%20Sundhedsit/~media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/NationalSundhedsit/Standardisering/Referencearkitektur%20for%20informationssikkerhed%20v%20%201%200%20nyt%20layout.ashx> | | NIST | Electronic Authentication Guideline <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf> | | Thomas Gundel | Fællesoffentlig brugerstyring - arkitekturtegninger 30-10-2013 | | Thomas Gundel | Fællesoffentligt Trust Framework - Indledende overvejelser | | Uni-login | UNI•Login Adgangskontrol <http://www.stil.dk/~media/UNIC/Files/Publikationer/Tekniske%20vejledninger/uni-login-adgangskontrol.pdf> | | US Army | Identity and Access Management (IdAM) Reference Architecture (RA) - 07- 05-2014 [http://ciog6.army.mil/Portals/1/Architecture/2014/20140507-US\\_Army\\_IdAM\\_Reference\\_Architecture\\_V3-0.pdf](http://ciog6.army.mil/Portals/1/Architecture/2014/20140507-US_Army_IdAM_Reference_Architecture_V3-0.pdf) | | WAYF | Introducing transparency in hub-and-spoke federation architectures using SAML2 authentication request scoping elements [http://www.wayf.dk/wayfweb/artikler\\_og\\_notater\\_attchmt/2010\\_09\\_01\\_TNC\\_article\\_SAML2-scoping.pdf](http://www.wayf.dk/wayfweb/artikler_og_notater_attchmt/2010_09_01_TNC_article_SAML2-scoping.pdf) | | Økonomistyrelsen | Anbefalinger til retningslinjer for tværoffentlig brugerstyring – roadmap og koncept 1.0

#### 5.16.4. Baggrund for valg af relationen entitet-elektronisk identitet

**Om relationen entitet – elektronisk identitet** De grundlæggende begreber i brugerstyring bygger på eIDAS-forordningen inkl. gennemførselsforordning (EU) 2015/1502 og National Standard for Identitetens Sikringsniveau (NSIS), som er en dansk konkretisering af forordningen.

I disse defineres følgende begreber:

- »Entitet«: Et subjekt/en bruger, som skal have adgang til en tjeneste.
- »[Elektronisk] Identitet«: En digital persona, repræsenteret ved et sæt af attributter, forkortes eID.
- »Elektronisk identifikationsmiddel«: Et elektronisk eller en fysisk objekt/genstand, der kan anvendes til at gennemføre en autentificering af en identitet. "Elektronisk identifikationsmiddel" kaldes herefter "akkreditiv".

Det betyder, at de fleste personer i dag har en række elektroniske identiteter:

- NemID-borger med attributter som PID og navn
- Identitet hos arbejdsgiver, typisk med akkreditiverne brugernavn og kodeord og attributter som navn, organisatorisk enhed
- Identitet hos Uni•Login
- Identitet hos Facebook
- Identitet hos Google
- Identitet hos en række andre tjenester.

#### !Figur 24. De tre grundlæggende begreber i identitet

Der er mange tiltag for at reducere antallet af identiteter, fx ved at flere tjenester tilbyder, at man kan bruge sin Facebook-identitet eller Google-identitet.

Et andet tiltag er NemID, som er etableret med henblik på anvendelse i stort set alle offentlige tjenester og hos bankerne. NemID kan også bruges hos mange private tjenester, fx pensionskasser, forsikringsselskaber, fagforeninger mv.

## Om relationen entitet – elektronisk identitet i fællesoffentlig brugerstyring

I fællesoffentlig brugerstyring har der indtil nu været arbejdet med, at en entitet kan have flere elektroniske identiteter:

- En privat NemID
- En eller flere NemID Erhverv tilknyttet forskellige virksomheder.

Særligt for små erhvervsdrivende har det været utilfredsstillende at skulle håndtere to eller flere akkreditiver som følge af den nuværende models stærke binding mellem identiteter og akkreditiver, som er implementeret i NemID. Derfor har der i næste generation NemID været arbejdet med at finde løsninger på dette. Der har været to grundlæggende modeller til overvejelse for fællesoffentlige løsninger og dermed for NDIS:

- En løsning med kun en identitet pr. entitet
- En løsning med flere identiteter pr. entitet.

### En løsning med kun en identitet pr. entitet

I denne løsning er der kun en identitet pr. entitet. Identiteten karakteriseres ved attributter. Nogle er tæt knyttet til den fysiske person som fx navn, adresse og CPR. Andre attributter udtrykker de rettigheder, som identiteten tildeles til at tilgå funktioner eller informationer. Skal entiteten tilgå løsninger som borger og som ejer af virksomhed eller medarbejder, udtrykkes det ved forskellige sæt af attributter.

#### !Figur 25 En identitet pr. entitet

Fordelene ved denne model:

- Den enkelte person skal kun have en elektronisk identitet og dermed et NemID. • Forskellige attributsæt for personrettigheder karakteriserer de rettigheder, som en person har, når de optræder i forskellige kontekster; det man også kan kalde roller.

Ulemperne ved denne model:

- For en række personer vil det være en ulempe kun at have en elektronisk identitet, fx hvis personen arbejder for mange virksomheder, så det kan være vanskeligt at skelne mellem rollerne, hvis det er den samme funktion og dermed det samme attributsæt, personen har. • Alle tjenester skal fra implementeringstidspunktet kunne understøtte, at valg af identitet kun sker gennem at registrere en og kun en NemID og ikke kan ske på anden måde. • Der kan ikke vælges at danne identiteter med tilhørende akkreditiver, der kan afspejle virksomheders forskellige ønsker til fx sikringsniveau eller funktionalitet, fx som i sundhedssektoren, hvor der ønskes akkreditiver, der kan anvendes i klinisk kontekst.

### En løsning med flere identiteter pr. entitet

I denne løsning kan hver entitet have flere elektroniske identiteter til fællesoffentlig brugerstyring. Skal entiteten tilgå løsninger som borger og som ejer af virksomhed eller medarbejder, sker det med forskellige identiteter. Nu er det identitetsattributter, der adskiller, om det er en identitet for en borger eller en medarbejder.

Løsningen svarer til den model, der anvendes i det nuværende NemID (i 2016).

#### !Figur 26 Flere identiteter pr. entitet

For at løsningen med flere identiteter pr. entitet tilgodeser brugerbehov, kan modellen implementeres, så en entitet kan anvende sit akkreditiv (fx NemIDnøglekortet) til flere identiteter.

Det sker på to måder:

For borgere, der er ejere af enkeltmandsvirksomheder eller er tegningsberettigede, kan det offentlige tilbyde brug af borgerakkreditiver i forbindelse med erhvervsidentiteten.

Konceptuelt sker det ved, at en elektronisk identitet (erhvervsidentiteten) dannes på grundlag af en anden elektronisk identitet (borgeridentiteten). Fx en ny virksomhedsejer med automatisk CVR-opmærkning. Identiteten kan bevares over tid eller være dynamisk.

Denne løsning implementeres fra februar 2017 i fællesoffentlig brugerstyring.

Der dannes en separat erhvervsidentitet med egne attributter. Denne erhvervsidentitet bevares over tid, uafhængigt af akkreditiver. Det betyder, at der kan skiftes akkreditiv, uden at der skal administreres en ny identitet med tilhørende rettigheder.

For virksomheder betyder modellen, at de kan vælge mellem borgerens akkreditiver eller at foranledige brug af en erhvervsidentitet med akkreditiver med andre styrker. Virksomheder kan skifte mellem alternativerne løbende og stadig bevare samme erhvervsidentitet. Løsningen muliggør, at både borger og virksomhed kan vælge, om

borgeridentiteten kan anvendes til erhvervsformål. Løsningen kan implementeres med begge valgmuligheder eller således, at kun den ene part (fx virksomheden) kan vælge.

# Index

---

## Terms defined by this specification

[Adgangskontrol](#), in §1.5

[Applikation](#), in §1.5.1

[Entitet](#), in §1.5

[Forretningstjeneste](#), in §1.5

[Identifikationsmiddel](#), in §1.5

[Identitet](#), in §1.5

[Juridisk enhed](#), in §1.5.1

[Person](#), in §1.5.1

[Princip 10: Tværoffentlig brugerstyring etableres i overensstemmelse med internationale standarder og løsninger](#), in §3.6

[Princip 1: Brugere oplever en sammenhængende adgangsstyring](#), in §3.6

[Princip 2: Brugerstyringsløsninger udvikles med fokus på brugernes behov](#), in §3.6

[Princip 3: Brugerstyringsløsninger respekterer brugernes privatliv](#), in §3.6

[Princip 4: Aktører indgår i føderationer baseret på tillid og aftaler](#), in §3.6

[Princip 5: Aktører i føderationer vurderer i deres styring af informationssikkerhed samspillet med andre aktører](#), in §3.6

[Princip 6: Administration af brugere flyttes så vidt muligt ud af fagapplikationer](#), in §3.6

[Princip 7: Tjenesteudbyder \(den dataansvarlige\) har ansvaret for at håndhæve brugernes adgange](#), in §3.6

[Princip 8: Brugerstyring realiseres i løst koblede komponenter](#), in §3.6

[Princip 9: Tværoffentlige brugerstyringsløsninger baseres på en kerne af fælles komponenter i samspil med øvrige komponenter i infrastrukturen](#), in §3.6

[Ting](#), in §1.5.1