|  |
| --- |
| **Referencearkitektur for brugerstyring 2020**  **Version 1.1** |
| Januar 2020 |

Indhold

Forord 3

Summary (in english) 4

Resume 4

1. Introduktion 4

1.1 Formål, anvendelse og målgrupper 4

1.2 Omfang og afgrænsning 5

1.3 Centrale begreber 6

1.3.1 Brugere og identiteter 7

1.3.2 Typer af brugere 7

1.3.3 Begrebsoverblik 8

1.3.4 Relationer imellem brugere 9

1.4 Tilblivelse, styring og andre referencearkitekturer 9

1.5 Anvendt metode, notation og signaturforklaring 10

2. Strategi 10

2.1 Forretningsmæssige behov 11

2.1.1 Lettilgængelige sammenhængende tjenester 11

2.1.2 Retten til privatliv 11

2.1.3 Sikkerhed og tillid 12

2.1.4 Delegering og fuldmagt 12

2.1.5 Effektivitet 12

2.2 Vision 13

2.3 Principper 13

2.3.1 Princip 1: Brugerne oplever en relevant og sammenhængende adgangsstyring 14

2.3.2 Princip 2: Brugerstyringsløsninger respekterer brugernes privatliv 15

2.3.3 Princip 3: Tjenesteudbyder har ansvaret for at håndhæve brugernes adgange 15

2.3.4 Princip 4: Brugerstyring er adskilt fra forretningstjenester 16

2.3.5 Princip 5: Brugerstyring realiseres via løst koblede og harmoniserede tillidstjenester 16

2.3.6 Princip 6: Tjenesteudbydere indgår i føderationer 17

2.4 Værdiskabelse 18

2.5 Juridiske rammer 19

2.6 Sikkerhed 20

2.6.1 Risici vedr. brugere 20

3. Forretningsarkitektur 21

3.1 Om tillidstjenester og eIDAS 22

3.2 Forretningsmæssig kontekst 23

3.3 Tillidstjenester 24

3.3.1 Udstedelse af identifikationsmidler 25

3.3.2 Autentifikation 26

3.3.3 Registrering af attributter 27

3.3.4 Attestering af attributter 27

3.4 Forretningsfunktioner hos tjenesteudbydere 28

3.4.1 Udformning af adgangspolitik 28

3.4.2 Udformning af tillidspolitik 29

3.4.3 Adgangskontrol 30

3.4.4 Forebyggelse og kontrol 30

3.5 Logiske arkitekturmønstre 32

3.5.1 Mønster 1: Forretningstjenester med egen autentifikationstjeneste 32

3.5.2 Mønster 2: Delt, intern autentifikationstjeneste 33

3.5.3 Mønster 3: Føderation med central autentifikationstjeneste 34

3.5.4 Mønster 4: Fælles domænebroker for decentrale autentifikationstjenester 36

3.5.5 Mønster 5: Interføderation mellem domæner 37

4. Teknisk arkitektur 39

4.1 Attestation via push/pull 39

4.2 Attributhåndtering 41

4.2.1 Attributkontrakter 42

4.2.2 Brugerkataloger 43

4.3 Discovery-tjenester 44

4.4 Billetudstedelse og -omveksling 45

4.4.1 Tillidskæder i økosystemer 46

4.5 Identitetsbaserede services 47

4.5.1 Identitetsbaseret kald via billetomveksling 49

4.6 Adgangskontrol 50

4.7 Softwarerobotter 52

4.7.1 Løsning for autonome robotter via føderation 53

4.7.2 Robotter uden føderation 55

4.8 Brugerstyring for (native) apps 56

4.9 Digitale fuldmagter 59

4.10 Områder for standardisering 60

4.10.1 Eksisterende standarder 60

4.10.2 Behov for nye fællesoffentlige standarder 61

4.10.3 Igangværende standardisering internationalt 62

Bilag 1. Kilder og baggrundsmateriale 64

Bilag 2. Begrebsmodel 70

## Forord

Denne referencearkitektur er udarbejdet for at understøtte implementeringen af Den fællesoffentlige digitaliseringsstrategi 2016-2020 [1] og gennemføre initiativ 5 i Fællesoffentlig strategi for brugerstyring [10]. Målet er, at referencearkitekturen skal fungere som et teknisk pejlemærke for udvikling af brugerstyringsløsninger i den offentlige sektor. Den er en del af den fællesoffentlige rammearkitektur, der er affødt af Digitaliseringsstrategiens initiativ 8.1 og bidrager til realiseringen af ”En digitalt sammenhængende offentlig sektor: Hvidbog om arkitektur for digitalisering” [2].

2017-udgaven af referencearkitekturen [3] omfattede brugerstyring af personer. Denne udgave af referencearkitekturen (version 1.1) er udvidet med de særlge aspekter vedrørende brugerstyring for apparater, organisationer og applikationer - samlet betegnet som Non-Person Entities (NPE) og IoT - Internet of Things. Brugen af føderationer og tillidstjenester er uddybet.

Siden første udgave af referencearkitekturen er De fællesoffentlige regler for begrebs- og datamodellering [4] blevet godkendt og udgivet. Derfor er begreberne i denne udgave opdateret og modelleret jfr. disse regler. Figurerne [nr. indsættes] viser centrale dele af begrebsmodellen og Bilag [nr. indsættes] viser hele begrebsmodellen i listeform. Øvrige figurer, der illustrerer referencearkitekturen, følger begrebsmodellen mht. anvendelse af begreber, men indgår ikke som en del af begrebsmodellen.

## Summary (in english)

## Resume

[Skrives inden offentlig kommentering]

# Introduktion

## Formål, anvendelse og målgrupper

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. Referencearkitekturens 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.

Referencearkitekturen skal kunne anvendes til at udpege standarder, der understøtter arkitekturen og dermed understøtte udarbejdelse af løsningsarkitektur i konkrete projekter. Arkitekturen anviser ikke i detaljer, hvordan myndigheder og virksomheder skal bygge løsninger, men fastlægger rammer og anviser standarder for løsninger, jfr. Hvidbog om arkitektur og digitalisering [2], hvor det fremgår, at fællesoffentlige referencearkitekturer “…definerer genbrugelige arkitekturbyggeblokke, som projekterne skal tage bestik af.” Referencearkitekturen kan anvendes i sammenhæng med andre fællesoffentlige referencearkitekturer, enten direkte eller ved domænearkitekturer, der bygger på de fællesoffentlige.

Dette dokument har tre målgrupper, som vil have forskelligt fokus i forhold til referencearkitekturens kapitler:

* Strategiske beslutningstagere inden for digitalisering og it, typisk digitaliseringschefer, it-chefer, afdelings- og kontorchefer og andre med rollen som systemejer. Kapitel 1 og 2, der indeholder introduktion til brugerstyring, strategi, centrale begreber og principper er særligt rettet mod denne målgruppe.
* Projektledere, arkitekter og udviklere hos myndigheder, virksomheder og leverandører, der har til opgave at kravspecificere, designe eller udvikle løsninger, hvor der indgår eller anvendes tværoffentlig brugerstyring. Ud over de to første kapitler er kapitel 3 og 4, der handler om forretningsarkitektur og teknisk arkitektur, særligt rettet mod denne målgruppe.
* Arkitekter der udarbejder domænearkitekturer på basis af denne referencearkitektur. De vil have særlig opmærksomhed på kapitel 3 og 4.

## Omfang og afgrænsning

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

Arkitekturen omfatter rollerne som leverandør af tillidstjenester - udstedere af identifikationsmidler, autentifikationstjenester, identitetsbrokere, attributtjenester mv. Arkitekturen omfatter desuden private virksomheders mulighed for at indgå som brugerorganisation herunder udstille bruger- og rolledata om egne medarbejdere.

Arkitekturen omhandler 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).

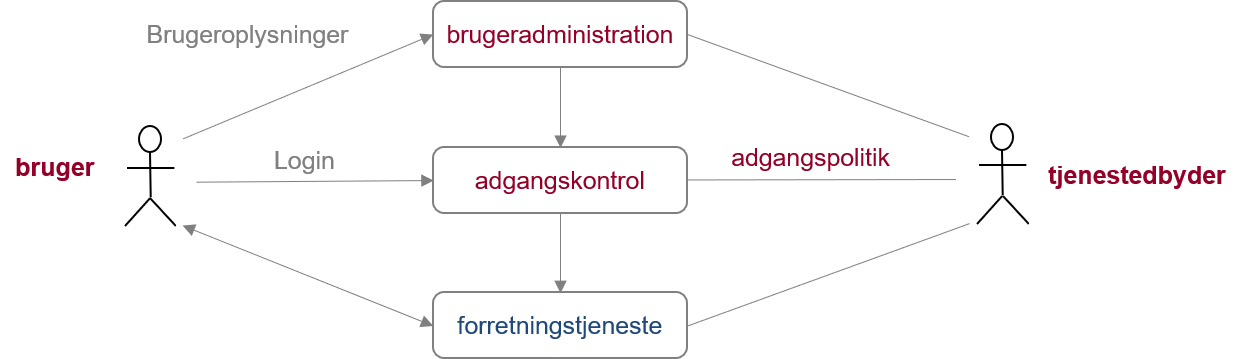
Referencearkitekturen definerer, hvad en føderation omhandler i rammerne af brugerstyring, og den beskriver de opgaver, en føderation løser i denne ramme.

Denne version 1.1 af Referencearkitektur for brugerstyring er udvidet med de særlige aspekter vedrørende brugerstyring for ting, organisationer og applikationer - samlet betegnet som Non-Person Entities (NPE).

Med udspring i Digitaliseringspagten [5] er der parallelt med opdateringen af denne referencearkitektur igangsat en analyse af håndtering af samtykke på tværs af den offentlige sektor 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.

## Centrale begreber

Referencearkitekturen beskriver administrationen og kontrollen med brugeres adgang til digitale tjenester. Tjenester udbydes af private og offentlige organisationer, og anvendes af borgere eller andre organisationer og deres ansatte.



Figur 1 Kapabiliteter omkring brugerstyring

De primære kapabiliteter i brugerstyring er

* Brugeradministration aspekt af brugerstyring hvor digitale identiteter og deres attributter administreres.
* Adgangskontrol proces, der afgør hvilke, om nogen, funktioner og data en bruger får adgang til på baggrund af brugerens identitet, attributter, roller/rettigheder og tjenestens adgangspolitik.
* Forretningstjeneste, tjeneste der understøtter forretningskapabiliteter gennem en eksplicit defineret snitflade og som er eksplicit styret af en organisation.

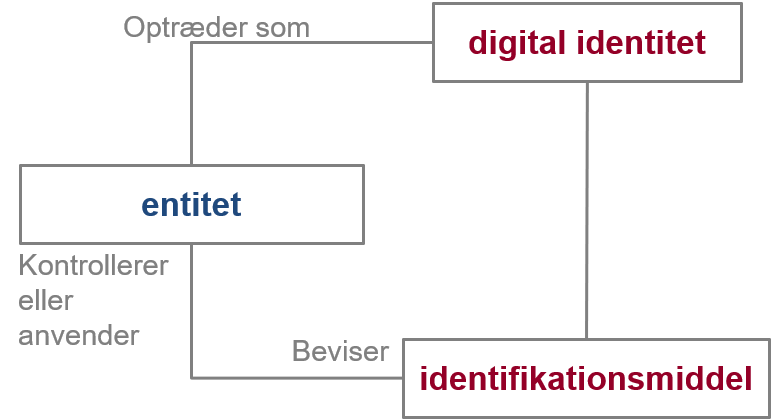
Ved siden af forretningstjenester findes tillidstjenester, der udfører betroede funktioner, der understøtter brugerstyring i forretningstjenester. I denne referencearkitektur beskrives hvordan forskellige tillidstjenester og forretningstjenester samarbejder, typisk i sammenslutninger i form af føderationer.

Tillidstjeneste tjeneste der udfører betroede funktioner der understøtter brugerstyring i forretningstjenester.

Føderationer sammenslutning af tillids- og forretningstjenester med gensidig tillid.

### Brugere og identiteter

I en digital sammenhæng defineres brugere som den rolle en entitet har i forhold til den tjeneste eller det system entiteten tilgår. Rollen som bruger binder entiteter til digitale identiteter.



Figur 2 Entitet, identitet og identifikationsmiddel

Entitet, noget der har en selvstændig eksistens. Entiteter er i denne kontekst en person, organisation, apparat 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 en eller flere erhvervsidentiteter.

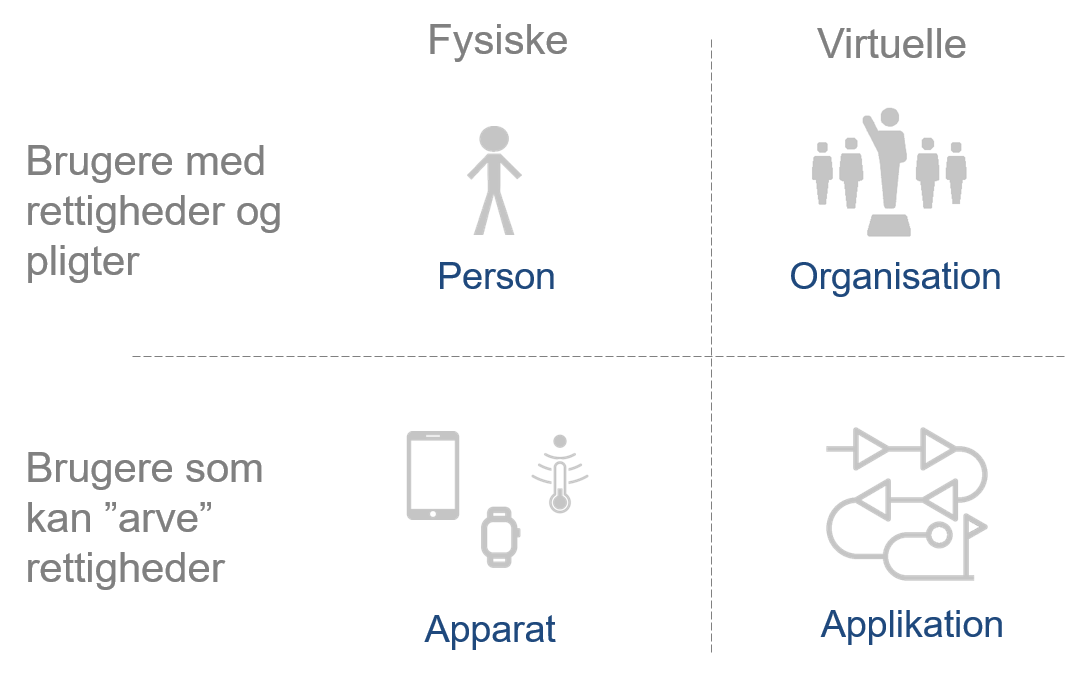
Digital identitet digital persona der repræsenterer en entitet i rollen som bruger v.hj.a. et sæt attributter. En digital identitet kan indeholde data der identificerer en bestemt person (personidentifikationsdata), men kan også være pseudonym.

Identifikationsmiddel middel som en entitet får udstedt til brug for autentifikation og som benytter en eller flere autentifikationsfaktorer. Midlet vil typisk basere sig på faktorer, som er svære at efterligne, fx viden som kun brugeren har - kodeord, noget kun brugeren er – biometri, eller noget kun brugeren er i besiddelse af - enhed.

Det er vigtigt at være opmærksom på dynamikken og fleksibiliteten i ovenstående model. Eksempelvis kan en fysisk person have mange forskellige identiteter og mange forskellige identifikationsmidler. Et bestemt identifikationsmiddel er ikke nødvendigvis koblet til en bestemt identitet og omvendt.

### Typer af brugere

I forbindelse med brugerstyring kan brugere være personer eller organisationer med rettigheder og pligter, og mulighed for at delegere rettigheder. Brugere kan også være apparater eller applikationer, der ikke i sig selv har juridiske rettigheder eller pligter, men som kan arve rettigheder via delegation og dermed agere på vegne af personer.



Figur 3 Brugertyper

Person fysisk person, der kan være levende eller død, men ikke imaginær. Fysiske personer kan have identiteter som borger, medarbejder eller deltage i fællesskaber, som for eksempel Facebook.

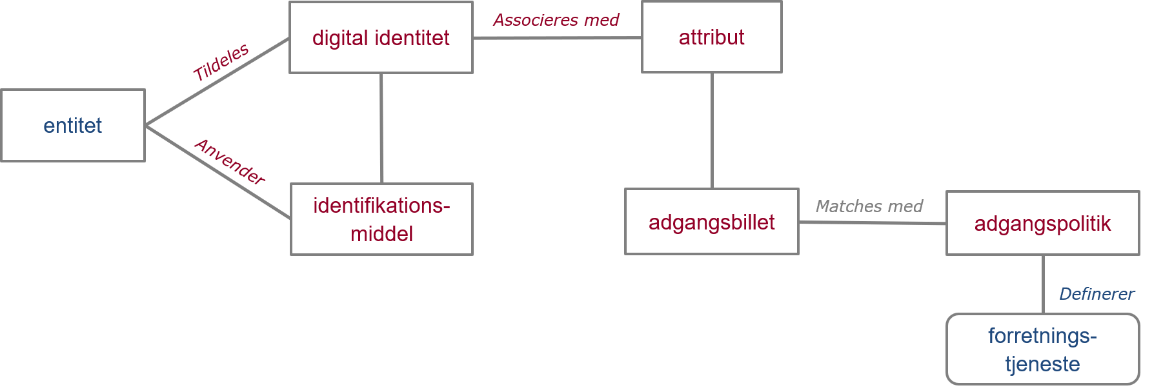
Organisation en organisation, der -især i juridisk forstand- er bredt anerkendt og har tilhørende rettigheder og ansvar. Adgange og rettigheder kan delegeres til medarbejder eller applikation.

Apparat fysisk redskab med indlejret software, der kan udføre specifikke funktioner. I apparater der kan optræde som brugere er den indlejret software uløseligt forbundet med apparatet. Der er typisk tale om apparater der har en enkelt funktion og ikke kan få installeret yderligere applikationer, hvorfor apparatet optræder som bruger.

Applikation software med specifik forretningsfunktion. Applikationer er uafhængige af den platform, de er installeret på. Applikationer der kan optræde som brugere vil være installeret på noget hardware, men kunne flyttes fra et stykke hardware til et andet uden at ændre identitet, hvorfor det er applikationen der optræder som bruger.

### Begrebsoverblik

I forbindelse med implementeringen af arkitekturen, benyttes adgangsbilletter til at samle de attributter der indgår i adgangskontrollen for en given tjeneste, herunder både identitet, rettigheder og andre attributter.



Figur 4 Begrebsoverblik

Ud over de her viste begreber er alle begreber forklaret i Bilag [1 Begreber.]

### Relationer imellem brugere

Brugere kan have indbyrdes relationer af betydning for brugerstyring i forbindelse med tildeling og delegering af adgangsrettigheder. Rettigheder og hvordan de tildeles er ikke indeholdt i denne referencearkitektur, hvorfor nedenstående blot er eksempler på relationer af betydning for brugerstyring.

* 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 til organisation. Tilhøret i sig selv giver implicit en række adgangsrettigheder fra organisationen til personen. Fx har en borger i Danmark implicit adgang til en række tjenester som fx Borger.dk og e-Boks.
* Eksplicit adgangsrettighed der gives fra en organisation til en person. Dette kan være adgang til systemer eller steder, eller prokura til at handle på organisationens vegne.
* Bruger af et apparat. Fx brugeren af en mobiltelefon eller en blodtryksmåler. I begge tilfælde er det en mulighed, at apparatet som bruger arver adgangsrettigheder fra personen der bruger det.
* Delegering af adgangsrettigheder fra en person eller organisation til en applikation. Fx en automatiseringsrobot, der får delegeret rettigheder til at håndtere en givet sagsforløb.
* En applikation kan have særlige rettigheder på grund af enheden den afvikles på.

## Tilblivelse, styring og andre referencearkitekturer

Denne version 1.1 af Referencearkitektur for brugerstyring er udarbejdet i Center for teknik og datastrategi (CTD) i Digitaliseringsstyrelsen med konsulentbistand fra IT Crew og Capgemini.

En følgegruppe af arkitekter fra den offentlige sektor har bidraget til opdateringen gennem en række af workshops og reviews. Følgende organisationer har været repræsenteret i gruppen: Kommunernes Landsforening, Danske Regioner, Styrelsen for Dataforsyning og Effektivisering, Styrelsen for It og Læring, Naturstyrelsen, Miljøstyrelsen, KOMBIT, Energistyrelsen, Energinet, Sønderborg Kommune og Københavns Kommune.

Inden godkendelse er referencearkitekturen blevet reviewet i regi af FDA ligesom der har været en offentlig høring af dokumentet med inddragelse af relevante offentlige og private interessenter.

[Referencearkitektur for brugerstyring godkendtes i version 1.1 af Udvalg for arkitektur og standarder under Den fællesoffentlige digitaliseringsstrategi 2016-2020 [1] i juni 2020. Udvalget er herefter ejer af dokumentet, med CTD som ansvarlig for vedligehold af referencearkitekturen, der indgår i FDA.]

Referencearkitekturen publiceres på arkitektur.digst.dk, hvor man kan finde beslægtede dokumenter vedrørende FDA.

En række offentlige domæner har udfærdiget egne arkitekturer på brugerstyringsområdet. [Her indsættes referencer]

## Anvendt metode, notation og signaturforklaring

Metodemæssigt er referencearkitekturen udarbejdet inden for rammerne af FDA og følger så vidt muligt den fælles skabelon for referencearkitekturer, som er udarbejdet i sekretariatet for Styregruppen for Data og Arkitektur under Den fællesoffentlige digitaliseringsstrategi 2016-2020 [1].

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 referencearkitekturer
* Grå tekst: At et element eller en relation er identificeret, men ikke nærmere defineret i denne referencearkitektur.

# Strategi

Referencearkitekturen udmønter og understøtter beslutninger i Den fællesoffentlige digitaliseringsstrategi 2016-2020 [1]. Strategien har tre, overordnede målsætninger:

Det digitale skal være let, hurtigt og sikre god kvalitet

Offentlig digitalisering skal give gode vilkår for vækst

Tryghed og tillid skal i centrum

De tre målsætninger er understøttet af en række, specifikke initiativer, hvoraf Initiativ 7.3 Digitale identiteter og rettighedsstyring er det konkrete ophæng for denne referencearkitektur.

## Forretningsmæssige behov

Forretningsbehovene tager udgangspunkt i de udfordringer, offentlige virksomheder skal være i stand til at håndtere i forbindelse med brugerstyring. Fokus for Referencearkitektur for brugerstyring er især understøttelse af behov vedrørende sammenhængende, effektive, sikre og brugervenlige løsninger på tværs af domæner, nationalt og transnationalt.

### Lettilgængelige sammenhængende tjenester

Borgere og medarbejdere forventer, at tjenester er let tilgængelige og sammenhængende. Let tilgængelige hvor tjenester kan nås med samme identifikation og med samme login. Ekstra login giver kun mening for brugeren, hvis sikkerhedsniveauet skal hæves i forhold til et tidligere login. Hvis en tjeneste gør brug af en anden tjeneste, er der behov for nem og sikker adgang til denne tjeneste. Da brug af tjenester fra andre tjenester er stigende, er der behov for ensartede metoder til at tilgå disse tjenester. eIDAS forordningen [6] 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.

### Retten til privatliv

Der skal være mulighed for en højere grad af kontrol over, hvilke data tjenester får adgang til og indsigt i, hvilke aktiviteter der udføres med en elektronisk identitet og mulighed for anonymitet, hvor det er muligt og relevant. En tjeneste har ikke altid behov for at kende den fysiske identitet for brugeren (fx CPR-nummer) for at kunne afgøre dennes adgang til en service. Kun relevante attributter sendes til tjenesten i henhold til dataminimeringsprincippet.

* Ved et køb af billet til bus eller tog er der, et behov for at levere et bevis for betaling, men ikke for kundens identitet.
* Nogle tjenester har blot brug for oplysninger om hvorvidt brugeren er myndig (alder>18) eller vedkommendes bopælskommune.

I den nye NemLog-in3 løsning kan private identifikationsmidler anvendes i erhvervsmæssig sammenhæng med henblik på at reducere mængden af identifikationsmidler der skal administreres og anvendes for den enkelte. For at sikre retten til privatliv og mulighed for at adskille privatsfæren fra arbejdssfæren for den enkelte medarbejder, er denne funktionalitet underlagt det såkaldte ‘dobbelte frivillighedsprincip’[9] som sikrer, at private identifikationsmidler kun kan bruges i erhvervsmæssig sammenhæng, hvis både medarbejder og virksomhed siger god for det.

### Sikkerhed og tillid

Tjenester skal til enhver tid bygge på tilstrækkelig sikkerhed, så borgernes data ikke kompromitteres eller tjenesterne misbruges. Mange offentlige tjenester rummer fortrolige data (herunder følsomme personoplysninger), som kræver høj sikkerhed, mens andre er mindre kritiske og derfor har lavere sikkerhedsbehov. Det er helt centralt for realiseringen af en effektiv digitalisering, at brugerne har tillid til de tjenester, der udbydes og den sikkerhed, de beskyttes med. Når tjenester bliver mere sammensatte, skal denne tillid kunne opfyldes af alle tjenester, der er omfattet.

### Delegering og fuldmagt

En del borgere og virksomheder har behov for at kunne give andre fuldmagt til at løse opgaver for sig. Myndigheder er omfattet af reglerne om partsrepræsentation, og deres digitale tjenester skal derfor understøtte anvendelse af fuldmagt. Ellers skal myndigheden etablere manuelle løsninger til partsrepræsentation. I forhold til automatiseringsrobotter er der et behov for, at en person eller en organisation kan delegere rettigheder til en automatiseringsrobots identitet, således at den kan agere på et veldefineret grundlag.

### Effektivitet

Offentlige tjenester skal leve op til kravene om forvaltningsrevision, hvor det vurderes om systemer og processer understøtter sparsommelighed, produktivitet og effektivitet. Private tjenester vil på den anden side være underlagt et ønske om profit. Alle tjenester har derfor et behov for at være effektive, hvilket kan udtrykkes i behov som:

* Enkel og samlet administration af brugere.
* Sammenhæng imellem brugerstyring i forskellige organisationer både private og offentlige.
* En sammenhængende brugerstyring, så tjenester kan implementeres effektivt.
* Kontrol af medarbejdernes anvendelse af elektronisk identitet på virksomhedens vegne, da det både juridisk og kommercielt kan være forpligtende for brugerorganisationen.

Når man bygger en forretningstjeneste, er det ofte dyrt og komplekst selv at bygge brugerstyring. Det er derfor en positiv business case at udvikle forretningstjenesten for sig og tilgå brugerstyring som en fælles tjeneste.

## Vision

Digitaliseringsstyrelsen udgav i april 2017 “Fællesoffentlig strategi for brugerstyring” [10], efter at den var blevet godkendt i Styregruppen for udbud af fællesoffentlige komponenter. Her blev fastlagt en vision, som også er gældende for denne version af referencearkitekturen:

Borgere, virksomheder og myndigheder har adgang til en let og effektiv brugerstyring på tværs af løsninger. Løsningerne bindes sammen på tværs af domæner. Brugerstyring sker på en måde, som fremmer sikkerhed, tillid, privatlivsbeskyttelse, valgmuligheder, innovation, og som øger anvendelsen af tjenester.

Visionen er at skabe fælles rammer for brugerstyring og dermed grundlag for, at de fællesoffentlige parter kan udvikle brugerstyring inden for fælles arkitekturmæssige rammer. På den måde vil organisationer og brugere opleve en lettilgængelig brugerstyring, der kan anvendes på tværs af løsninger, og fx minimere gentagende logins i samme brugerrejser. Det er centralt i visionen, at den omfatter både borgere, virksomheder, myndigheder og ansatte brugere i offentlige myndigheder samt anvendelsen af autonome robotter. Brugerstyringen skal understøtte enkel administration og rettighedsstyring på tværs af løsninger. Den danske brugerstyring skal ligge sig i forlængelse af internationale initiativer som fx eIDAS-forordningen og den internationale teknologiske udvikling, som Danmark har store fordele ved at udnytte og være en del af. Derudover skal brugerstyringsløsninger have tilstrækkelig høj sikkerhed i balance med effektivitet og brugervenlighed. Både sikkerhed, effektivitet og brugervenlighed fremmes ved, at brugerstyring er sammenhængende på tværs af den offentlige sektor.

## Principper

Dette afsnit beskriver et sæt principper for brugerstyring. Myndigheder og leverandører bør tage stilling til disse i forbindelse med overordnet it-styring og konkret løsningsudvikling. Principperne beskriver de væsentligste egenskaber i forhold til brugerstyring, som har betydning for at understøtte de overordnede fællesoffentlige visioner og mål for brugervenlig, sammenhængende og sikker digitalisering. Principperne har et snævert fokus på emnet brugerstyring og supplerer de overordnede arkitekturprincipper i Hvidbog om fællesoffentlig digital arkitektur (FDA) [2]. For hvert princip er angivet de væsentligste relationer til disse.

Principper for brugerstyring

1. Brugerne oplever en relevant og sammenhængende adgangsstyring
2. Brugerstyringsløsninger respekterer brugernes privatliv
3. Tjenesteudbyder har ansvaret for at håndhæve brugernes adgange
4. Brugerstyring er adskilt fra forretningstjenester
5. Brugerstyring realiseres via løst koblede og harmoniserede tillidstjenester
6. Tjenesteudbydere indgår i føderationer

### Princip 1: Brugerne oplever en relevant og sammenhængende adgangsstyring

Brugere vil i deres opgaveløsning og dialog med det offentlige skulle betjene sig af en række forretningstjenester og disse bør opleves sammenhængende, uanset hvor mange tjenester eller myndigheder, der er involveret i et (selvbetjening)forløb.

Princippet understøtter særligt FDA arkitekturprincip 4: Sikkerhed, privatliv og tillid sikres, samt princip 5: Processer optimeres på tværs.

Rationale

* Brugerne vil være mere tilfredse og effektive, hvis de oplever en bedre og mere gnidningsfri løsning af deres opgaver, der involverer tjenester og forretningsprocesser på tværs af organisationer og sektorer.
* Brugerne får nemmere ved at anvende delegation af opgaver via fuldmagt, hvis det sker på en ensartet måde på tværs af offentlige myndigheder og relevante private aktører.

Implikationer

* Brugerne skal i offentlige digitale løsninger have brugergrænseflader, hvor krav til sikkerhed og privatliv forenes med krav om brugervenlighed.
* Brugerne skal kunne tilbydes Single Sign-On i brugerforløb, der krydser flere tjenester også når de går på tværs af domæner.
* Brugere skal, hvor det er relevant, kunne afgive samtykke til brugen af deres oplysninger, samt at oplysningerne kan bruges inden for en føderation i forbindelse med brugerstyring.
* Brugerne skal kunne delegere fuldmagt til andre elektroniske identiteter.
* Brugerne skal have et samlet overblik over afgivne og modtagne fuldmagter på tværs af tjenester.
* Brugerne skal opleve en sammenhængende administration af oprettelse af identiteter, brugere, administration af fuldmagter og administration af rettigheder.
* Kravene til sikringsniveau i digitale forløb skal svare til det sikkerhedsniveau, der kræves af de enkelte tjenester, der indgår i forløbet.

### Princip 2: Brugerstyringsløsninger respekterer brugernes privatliv

Brugerstyringsløsninger skal beskytte information om brugerne og sikre fortrolighed, og bør indhente og udveksle så lidt information som muligt ud fra princippet om dataminimering.

Princippet understøtter særligt FDA arkitekturprincip 4: Sikkerhed, privatliv og tillid sikres.

Rationale

* Databeskyttelsesloven og EU-forordningen GDPR om beskyttelse af personoplysninger, stiller en række krav til beskyttelse af borgernes privatliv.
* Tjenester der respekterer brugernes privatliv er nemmere at have tillid til.
* Dataminimering kan understøtte risikominimering i forhold til informationssikkerhed.

Implikationer

* I forbindelse med brugerstyring skal der ikke registreres og videresendes overflødige informationer om brugerne. Det vil sige, at fx standardsamlinger af attributter fra brugerstyring ikke altid er hensigtsmæssig.
* Danske offentlige tjenester må fortsat bruge CPR-nummeret, men bør kun anvende det, hvor det er nødvendigt.
* Det skal være tydeligt for brugeren, hvad anvendelseskonteksten er, dvs. hvad oplysningerne anvendes til.
* 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.

### Princip 3: Tjenesteudbyder har ansvaret for at håndhæve brugernes adgange

Tjenesteudbyder har ansvaret for at specificere reglerne for adgang i en adgangspolitik og dernæst at håndhæve reglerne i adgangspolitikken i forbindelse med at bruger gives adgang til tjenesten.

Rationale

* Tjenesteudbyder har dataansvaret og dermed det juridiske ansvar.
* Tjenesteudbyder har viden om konsekvenserne af at give adgang.

Implikationer

* • Tjenesteudbyder skal sikre at adgangskontrollen sker i henhold til adgangspolitikken, uanset hvor og hvordan adgangskontrollen implementeres.
* Der kan inden for føderationer være en gevinst i at vedligeholde fælles adgangspolitikker og i sammenhæng hermed et sæt fælles attributter på tværs af aktører og tjenester i sikkerhedsdomænet.

### Princip 4: Brugerstyring er adskilt fra forretningstjenester

Historisk har forretningstjenester selv varetaget brugerstyring med det resultat, at den samme bruger kan have mange forskellige identiteter, og at en identitet ikke kan anvendes på tværs af tjenester. Forretningstjenester skal i stedet benytte tværgående brugerstyring baseret på tillidstjenester adskilt fra forretningstjenesten.

Rationale

* Det giver større brugervenlighed, når samme identitet kan benyttes til flere tjenester, med mulighed for adgangsstyring på tværs af løsninger og domæner.
* Brugeradministrationen effektiviseres, idet brugerne ikke skal vedligeholdes flere steder og det øger sandsynligheden for korrekt oprydning i brugere og rettigheder.
* Det giver mindre overlap og dublering, når brugerstyring kan anvendes til mange tjenester, hvilket sparer penge ved udvikling og drift af applikationerne og resulterer i mere effektive løsninger.
* Sikkerheden øges når brugerstyring foregår i dedikerede tjenester, hvor fokus er på brugerstyring.

Implikationer

* Forretningstjenesten skal kunne samarbejde med tillidstjenester, der leverer brugerstyring.
* Brugerstyring skal baseres på fælles standarder således at samarbejde imellem forretningstjenester og tillidstjenester kan etableres enkelt, sikkert og effektivt.
* Der skal etableres aftaler imellem udbyderne af forretningstjenesterne og udbyderne af tillidstjenesterne, således at den nødvendige tillid for samarbejdet er til stede.

### Princip 5: Brugerstyring realiseres via løst koblede og harmoniserede tillidstjenester

Brugerstyring er som fagligt domæne præget af stigende arbejdsdeling og opdeling i løst koblede komponenter, der kan kombineres efter behov. For at sikre et effektivt samarbejde imellem tillidstjenesterne og forretningstjenesterne såvel som mellem tillidstjenesterne indbyrdes og for at kunne kombinere tillidstjenester på nye måder er det en fordel, når tillidstjenesterne lever op til harmoniserede krav.

Princippet understøtter særligt FDA arkitekturprincip 2: Arkitektur fremmer sammenhæng, innovation og effektivitet og princip 7: It-løsninger samarbejder effektivt.

Rationale

* En opdeling i logisk adskilte komponenter reducerer den samlede kompleksitet af den fællesoffentlige brugerstyring.
* Harmoniserede krav til funktionalitet og snitflader giver større fleksibilitet og bedre udnyttelse af udvikling og innovation i markedet.
* En åben og modulær arkitektur giver større agilitet og ændringsparathed i forhold til at udskifte eller variere delløsninger, integrere nye teknologier og implementere ændrede regler og politikker.

Implikationer

* Tillidstjenester bør overholde fællesoffentlige aftaler og krav til egenskaber og anvendelse af standarder.
* Anvendelse af åbne, løst koblede komponenter håndteret af flere aktører forudsætter, at der er tillid mellem parterne.
* Standarderne for informationsoverførsler mellem de løst koblede komponenter bør tage udgangspunkt i internationalt anerkendte standarder inden for EU eller globalt (med dansk profiler, hvor det er nødvendigt).
* Når brugerstyringsopgaven løses af forskellige aktører bygget 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.
* Den fællesoffentlige arkitektur for brugerstyring indeholder et overordnet sæt arkitekturbyggeblokke og en række realiserede løsnngsbyggeblokke, herunder tjenester og standarder for, hvordan disse udveksler adgangsbilletter og attributter. Enhver løsning inden for brugerstyring bør tage udgangspunkt i disse arkitektur- og løsningsbyggeblokke.

### Princip 6: Tjenesteudbydere indgår i føderationer

For at effektivisere samarbejdet imellem udbydere af forretningstjenester og anvendte tillidstjenester kan disse indgå i føderationer. Inden for føderationen aftales fælles standarder, samt tillids- og adgangspolitikker. Deltagere i føderationen kan omfatte både myndigheder og virksomheder i rollerne som organisationer, tjenesteudbydere og udbydere af tillidstjenester.

Rationale

* Brugen af føderationer forenkler samarbejdet imellem udbydere og man kan samle mange ens bilaterale aftaler til samlede aftaler i føderationen.
* Der er klare regler for den enkelte aktørs ansvar for sikkerheden, og tilsynet hermed kan varetages af overliggende myndigheder (fx Datatilsynet) og revision (fx Rigsrevisionen).

Implikationer

* Der er behov for definition af samspillet mellem aktørerne i føderationer.
* 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.
* I en føderation skal der udøves kontrol og defineres sanktionsmuligheder.
* 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 [16].
* Aktører i føderationer skal i relevant omfang informere andre aktører i føderationen om risikovurderinger og sikkerhedshændelser.

## Værdiskabelse

Ved af efterleve principper og mønstre i denne referencearkitektur opnås værdiskabelse på en række områder:

* Det bliver hurtigere og billigere at etablere forretningstjenester med en høj grad af sikkerhed, fordi kompleks håndtering af brugerstyring tilvejebringes som en service af tillidstjenester, der er specialiserede i området, og som ofte finansieres i fællesskab.
* Risikoen for tab som følge af svindel og misbrug nedbringes, når sikkerheden øges gennem professionelle, dedikerede tillidstjenester.
* De administrative udgifter til administration af brugere reduceres, når brugere kan administreres samlet og effektivt frem for i en række adskilte siloer.
* Udgifterne til systemintegration reduceres, når de underliggende forretningstjenester er baseret på de samme arkitektoniske principper for brugerstyring. Ofte er uheldigt udformet brugerstyring et stort praktisk problem for integration af systemer og processer.
* Brugerne spilder mindre tid på at udføre deres opgaver i forretningstjenester, når skift mellem disse kan ske sømløst (fx via single sign on) og identifikationsmidler kan genbruges på tværs. Brugerne vil således opleve færre barrierer for udførelse af deres egentlige arbejde og kan dermed være mere effektive.

## Juridiske rammer

De mest relevante love og forordninger, der har særligt fokus på brugerstyring og adgangskontrol, er:

* eIDAS forordningen [8] (electronic IDentification, Authentication and trust Services) som regulerer tillidstjenester og elektroniske identifikationsordninger.
* Lov om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester [12], der er den supplerende lov for eIDAS forordningen i Danmark.
* EU-databeskyttelsesforordningen (GDPR)[13] som beskriver pligter og rettigheder ved behandling af persondata.
* Databeskyttelsesloven [14] som i dansk kontekst supplerer GDPR.
* Forvaltningsloven [15] som indeholder regler om borgernes retsstilling over for den offentlige forvaltning. I forbindelse med sagsbehandling i offentlige forvaltninger regulerer loven blandt andet retten til partsrepræsentation.
* Lov om udstedelse af NemID [11], der regulerer borgeres og virksomheders retsstilling gennem et klart lovgrundlag for forvaltningen NemID. Loven vil blive erstattet af den kommende lov om MitID.

Dertil kan der være særregulering inden for visse domæner som fx sundhedsområdet.

Som eksempler på hvordan ovennævnte regulering påvirker brugerstyring kan nævnes:

* eIDAS-forordningen [8] stiller i artikel 6 krav om, at en række tjenester udstillet af offentlige myndigheder skal kunne tilgås af borgere og virksomheder i andre EU-lande ved brug af de elektroniske identifikationsmidler, som det enkelte EU-land har udstedt. Uden brug af føderationer og eksterne tillidstjenester ville det være en helt uoverskuelig opgave for den enkelte forretningstjeneste, at skulle integrere med alle øvrige EU-landes nationale identifikationsordninger.
* Databeskyttelsesforordningen [13] stiller krav om, at dataansvarlige træffer relevante sikkerhedsforanstaltninger ved behandling af persondata på baggrund af en risikovurdering.
* Forvaltningsloven [15] stiller krav om at den, der er part i en sag med det offentlige, skal kunne lade sig partsrepræsentere. Dette kan betyde, at en myndighed, som udstiller fuldt digitale løsninger, er nødt til at kunne håndtere digitale fuldmagter.

## Sikkerhed

Fastlæggelse af niveau for og håndtering af informationssikkerhed skal foretages af alle offentlige organisationer og tage udgangspunkt i ISO/IEC 27001-standarden [16] for styring af informationssikkerhed. Med udgivelse af den danske oversættelse af ISO 27001 standarden i januar 2014 blev det obligatorisk for de statslige myndigheder at følge ISO 27001 standarden. Kommunerne er også forpligtet til at følge principperne.

Realiseringen skal ske gennem et ledelsessystem for informationssikkerhed (Information Security Management System, ISMS). Digitaliseringsstyrelsen har i samarbejde med Erhvervsstyrelsen udarbejdet vejledninger, værktøjer og skabeloner hertil [17].

Hovedindholdet i ISO/IEC 27001 [16] 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.

ISO/IEC 27001 standarden [16] er opdelt i 14 domæner. For brugerstyring er domænet ‘Access Control’ særligt relevant, og managementdelen indgår i domænet ‘Information Security Policies’.

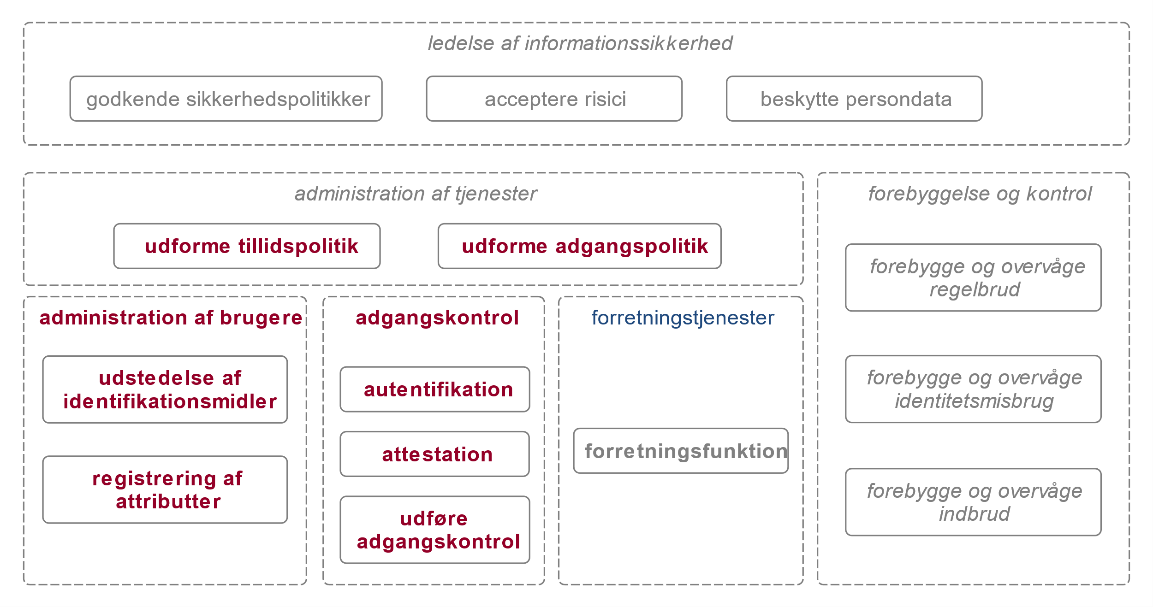
### Risici vedr. brugere

Indenfor domænet ‘brugerstyring’ er det særligt relevant at beskæftige sig med risici knyttet til håndtering af digitale identiteter, rettigheder og identifikationsmidler - herunder risikoen for, at ‘forkerte’ brugere tilgår en forretningstjeneste eller opnår forkerte adgange. National Standard for Identiteters Sikringsniveauer (NSIS) [18] 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-trins skala: Lav, Betydelig, Høj. Ved at benytte NSIS sikringsniveauer aktivt opnås en kvantificering af risici vedr. brugeridentiteter. NSIS kan benyttes både af brugerstyringstjenester, som leverer autentificerede identiteter, og af forretningstjenester som aftager identiteter. NSIS er en standard, som er udarbejdet og aftalt fællesoffentligt efter en bred offentlig høring, og den er en dansk pendant til eIDAS forordningens retsakt om sikringsniveauer.

# Forretningsarkitektur

Brugerstyring dækker opgaver og funktioner i forbindelse med håndtering af brugere af digitale løsninger. Det er således en fælles betegnelse for de foranstaltninger, som sikrer, at de rette brugere får adgang til de rette it-systemer (herunder data) - og at 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 adgangsstyring, 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.



Figur 5 Oversigt over brugerstyringsdomænet

Det øverste lag i figuren omhandler styringen 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).

For at realisere politikkerne opereres der med en række tillidstjenester, der udfører betroede funktioner i brugerstyringen. Disse omfatter udstedelse af elektroniske identifikationsmidler, som brugerne kan autentificere sig med, beskrivelse af attributter ved brugerne (fx navn, egenskaber, roller, relationer, bemyndigelser osv.) samt 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 beskrives en række supplerende funktioner (fx billetudstedelse og anvendelse af brokere), som ikke optræder på forretningsniveau.

En tjeneste og et it-system er i denne kontekst synonymer 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.

Bemærk at en tillidstjeneste også kan optræde som forretningstjeneste, og herunder udføre adgangskontrol, hvor forretningsområdet omhandler brugerstyring.

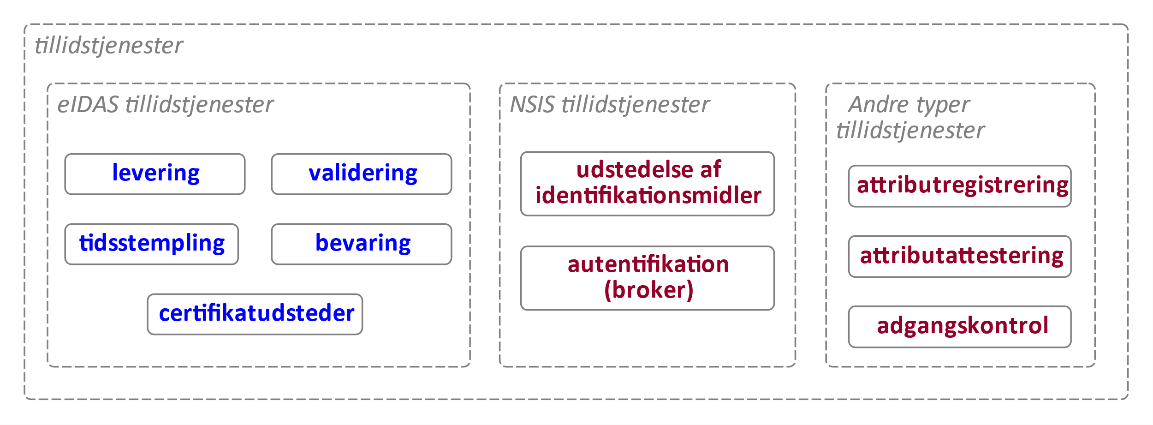
## Om tillidstjenester og eIDAS

I denne referencearkitektur anvendes betegnelsen ‘tillidstjeneste’ i bred forstand om en tjeneste, der udfører betroede funktioner til understøttelse af brugerstyring. Med denne terminologi opnås et tydeligt skel til forretningstjenester. 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)
* Tidsstemplingsservices
* 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 af (PKI)-tillidstjenester, som ikke skal forveksles med tillidstjenesterne i denne referencearkitektur. For eIDAS tillidstjenesterne findes et niveau af kvalificerede tillidstjenester, som er er underlagt særlige krav og tilsyn - men også har særlige privilegier. Eksempelvis vil en kvalificeret signatur udstedt på baggrund af et kvalificeret certifikat have samme retsvirkninger som en papirbaseret underskrift (eIDAS artikel 25).

De forskellige typer af tillidstjenester er illustreret på nedenstående figur:

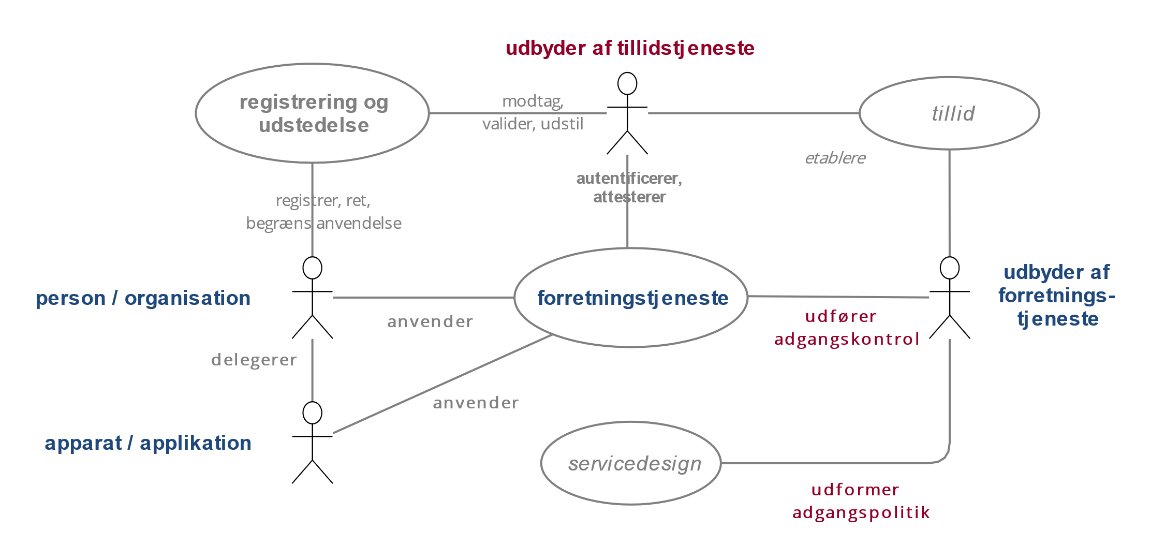


Figur 6 Oversigt over de forskellige typer af tillidstjenester

## 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 kan tillidstjenesterne opfattes som infrastruktur, der muliggør en sikker forretningsmæssig anvendelse af en forretningstjeneste. Grundlaget for samarbejdet er baseret på tillid, som gør det muligt for forretningstjenesten at uddelegere betroede funktioner til en tillidstjeneste udbudt af tredjepart. Tilliden kan være rodfæstet i lovgivning, i standarder og rammeværk med indbygget kontrol og styring eller i aftaler - herunder databehandleraftaler. Et vigtigt eksempel er National Standard for Identiteters Sikringsniveauer (NSIS) [18], 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 i form af en tillidstjeneste.

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



Figur 7 Samarbejde mellem tillidstjenester og forretningstjenester

Figuren viser de forskellige typer brugere, som anvender forretningstjenester. Tillidstjenester autentificerer og attesterer attributter om brugerne over for for-retningstjenesten, så brugerne passere adgangskontrollen og anvende forretnings-tjenesten. Grundlaget for tillidstjenester som autentificerer og attesterer (run time) er en forudgående registrering af attributter om brugerne og udstedelse af identifikationsmidler. Uddelegeringen af opgaver til tillidstjenester fordrer tillid fra forretningstjenesteudbydere.

Bemærk at figurerne 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, hvilke attributter forskellige tjenester har behov for, når de håndhæver deres adgangspolitik.

I det efterfølgende kapitel om den tekniske arkitektur beskrives det mere konkret, hvordan attributter kan håndteres i brugerstyring.

## Tillidstjenester

I dette afsnit beskrives funktionaliteten i tillidstjenesterne fra ovenstående figurer i lidt større detaljer. I beskrivelsen tages udgangspunkt i, at tillidstjenester udgøres af separate og specialiserede tjenester, som er er adskilt fra forretningstjenester. Tjenestebegrebet indikerer med andre ord, at funktionalitet udbydes til eksterne parter, og at der er rammer, som sikrer tillid til tjenesten. I praksis kan der naturligvis forekomme arkitekturer, hvor forretningstjenester selv udfører funktioner, der ideelt set burde leveres af en tillidstjeneste, hvilket kan lede til en række udfordringer. Disse beskrives nærmere i afsnittet om arkitekturmønstre nedenfor.

### 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 eventuelt tillidstjenester. National Standard for Identiteters Sikringsniveau (NSIS) [18] 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 i forhold til hvilke attributter, der valideres, og grænserne for den efterfølgende anvendelse.

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, der er udpeget af virksomhedens ledelse. En central del af registreringen består i at sikre relationen mellem virksomheden, som organisation, og medarbejderen, som fysisk person. For apparater kan en del af registreringen foretages 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 til denne.

I NSIS opereres der 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 tilknyttes til identiteten, fx kodeord, PIN, fingeraftryk. Identifikationsmidler anvendes til at autentificere identiteten i modsætning til attributter, som beskriver identiteten. En udsteder af identifikationsmidler skal dels sikre sammenhængen mellem identifikationsmidlet og identiteten, 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 kan bruges til at autentificere både en privatperson og en ejer (fuldt ansvarlig deltager) af 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.

### Autentifikation

Autentifikation er en proces, som genkender og verificerer en identitet gennem anvendelse af et identifikationsmiddel, der er koblet til identiteten som beskrevet ovenfor. Ved flerfaktor 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.

Autentikationsfunktionen varetages i nogle tilfælde af den part, der har udstedt identifikationsmidlet (fx fordi denne kender brugerens password eller en afledt værdi heraf), men den 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 [18] som AAL (Authenticator Assurance Level) og indplaceres på den sædvanlig tretrins 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 tjenesten, 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.

### Registrering af attributter

Termen attributter bruges i denne referencearkitektur som en generalisering over ‘data om brugere’ og kan dække over en lang række forskellige typer oplysninger. Funktionerne, som omhandler attributter, opdeles typisk i registrering og attestering.

Eksempler på opgaver inden for området kan være:

* Administration af brugere i et brugerkatalog, fx et AD, med navn, titel, email, afdeling osv. underlagt ledelse i en organisation.
* 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 som tidligere nævnt 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 samt sikre deres integritet mens de kommunikeres i en infrastruktur.

Traditionelt har ordet ‘autorisation’ også været anvendt i brugerstyring i forskellige betydninger 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.

### Attestering af attributter

Termen attestering dækker over, at attributter ikke blot udstilles som almindelige data, men at en tillidstjeneste står på mål for dem, således at forretningstjenester kan fæstne lid til dem og anvende dem til beslutninger i deres adgangskontrol. På engelsk benyttes ofte betegnelsen ‘verified claims’. Ved attestering forstås udstilling af troværdige data.

Tillidsbegrebet er således vigtigt for attributter, idet de indgår som væsentligt input til beslutninger i adgangskontrollen. I en adgangspolitik bør man derfor forholde sig til hvilke kilder til attributter, der er tillid til, og i hvilken grad. I visse tilfælde kan attributter endda være oplyst af brugeren selv (self-asserted claims), hvilket kan være helt på sin plads, forudsat at dette er beskrevet i adgangspolitikken, og dermed har været genstand for en risikovurdering.

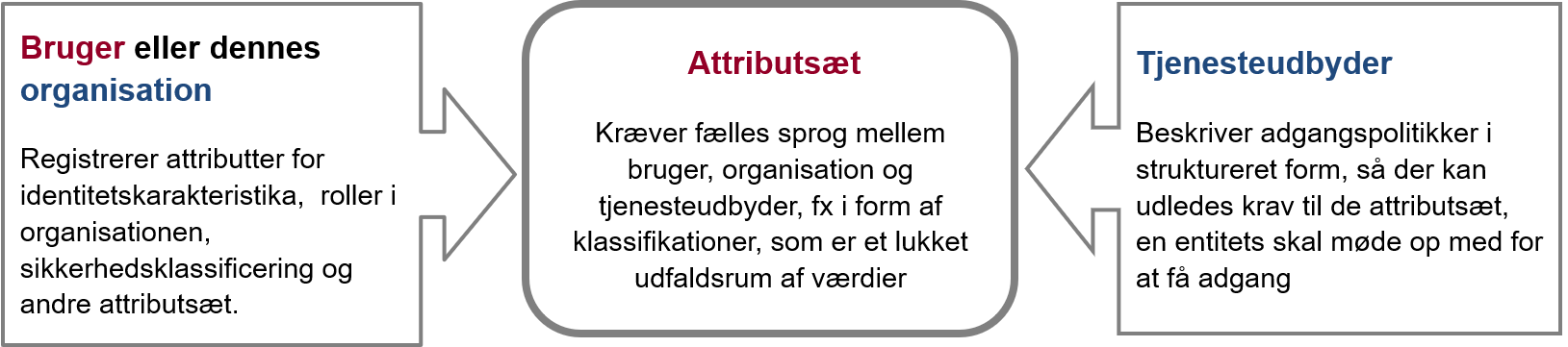
## Forretningsfunktioner hos tjenesteudbydere

I nedenstående afsnit beskrives funktioner og processer relateret til brugerstyring, der ofte udføres internt i en forretningstjeneste, og som derfor umiddelbart ikke falder ind under tillidstjenestebegrebet. Grænserne mellem de to kan dog i praksis være flydende - fx kan adgangskontrol i en forretningstjeneste i større eller mindre grad trække på eksterne tjenester.

### Udformning af adgangspolitik

Tjenesteudbydere skal 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 [19]), ligesom nogle domæner har standardiseret en række attributter (dette gælder fx på sundhedsområdet).



Figur 8 Adgangsrettigheder – Samspil mellem bruger og tjenesteudbyder

Adgangspolitikker kan benytte roller som basis (Role Based Access Control – RBAC), eller man kan arbejde 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.

### Udformning af tillidspolitik

Udformning af tillidspolitikker handler om at gøre det eksplicit, hvilke tillidstjenester der vurderes som troværdige til forskellige anvendelser ud fra en risikovurdering. En forretningstjeneste kan fx beslutte, at den kun vil anvende autentifikationstjenester, som er NSIS anmeldte på et givet sikringsniveau, mens en anden forretningstjeneste kan beslutte, at den stoler på autentifikationer fra en bestemt broker, der ikke er NSIS anmeldt - fx på baggrund af en aftale eller kontrakt med den pågældende broker. Et andet eksempel på en tillidspolitik kan være, hvorvidt en cloud-baseret tillidstjeneste anerkendes af en bestemt forretningstjeneste.

Det er vigtigt, at til og fravalg af tillidstjenester sker ud fra en informeret stillingtagen og forretningsmæssig vurdering af sikkerhed, tillid og andre former for garantier (SLA, lovkrav, revisionserklæringer).

#### Tillid gennem NSIS

I National Standard for Identiteters Sikringsniveauer (NSIS) [18] 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, men standarden 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.

### 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 [26]) opererer med begrebet ‘Policy Enforcement Point’. Adgangskontrollen kan endvidere benytte attributter om den aktuelle brugerkontekst (fx brugerens IP-adresse, geolokation, tidspunktet på dagen, data om brugerens enhed osv.) til yderligere kvalificering af risikoen ved at tillade adgang.

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

### Forebyggelse og kontrol

Forebyggelse af svindel og kontrol med brugeridentiteter er relevant i alle systemer, både i forretningstjenester og i tillidstjenester. Aftaler om og standarder for kontrol og audits kan være beskrevet i lovgivning, standarder (fx NSIS [18]), 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.

Regeringen har i april 2018 udgivet en ny version af National strategi for cyber- og informationssikkerhed [20], som har til formål at professionalisere statens arbejde med informationssikkerhed yderligere og øge samfundets robusthed mod cyberangreb. Strategien omfatter 25 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 25 initiativer.

Strategiens initiativer falder indenfor 3 pejlemærker:

1. Tryg hverdag
2. Bedre kompetencer
3. Fælles indsats

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 føderation.

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 ihændehaver 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.

Overvågningsfunktionen kaldes CERT, der står for Computer Emergency Response Team eller CSIRT, der står for Computer Security Incident Respinse Team (synonym til CERT).

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).

Der stilles desuden i højere grad krav om notifikation til relevante myndigheder i forbindelse med sikkerhedshændelser. Fx skal tillidstjenesteudbydere, jf. eIDAS [8], notificere Digitaliseringsstyrelsen, og i medfør af Databeskyttelsesforordningen (GDPR) [13], skal dataansvarlig notificere Datatilsynet ved sikkerhedshændelser. Som led i et beredskab skal man således sikre sig, at man kan informere de rette myndigheder 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 at 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 risikoscore, som forretningstjenesten herefter kan reagere på.

## Logiske arkitekturmønstre

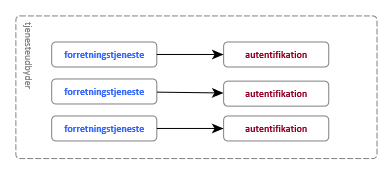
De ovenfor beskrevne funktioner kan udføres af forskellige parter i forskellige konstellationer med varierende kompleksitet. I simple scenarier kan alle funktionerne ligge inden for samme organisation, og tilliden følger af, at der er en fælles ledelse, mens der i komplekse scenarier kan være mange forskellige parter (tillidstjenester) i spil i et økosystem, hvor der er brug for at håndtere tillidskæder i flere led, discovery og orkestrering af services mv.

Dette giver anledning til en række arkitekturmønstre, som er temaet for dette afsnit. Der bliver beskrevet 5 mønstre i stigende kompleksitet men også med stigende skaleringsevne og sammenhæng. De første mønstre kan nærmest betegnes som ”anti-mønstre”, da der en række udfordringer relateret til sammenhæng, brugervenlighed, skalerbarhed og sikkerhed. Ikke desto mindre er de hyppigt forekommende, og det er derfor vigtigt at eksplicitere deres begrænsninger og vise, hvordan disse kan håndteres i de mere generelle mønstre.

### Mønster 1: Forretningstjenester med egen autentifikationstjeneste

Dette mønster er karakteriseret ved en forretningstjeneste med sin egen applikationsspecifikke brugerdatabase, hvor alle brugere vedligeholdes både i forhold til identifikationsmidler, typisk brugernavn og kodeord og i forhold til rettigheder.

I dette (anti)mønster håndterer forretningstjenesten de fleste funktioner i brugerstyring selv, herunder udstedelse af identifikationsmidler, autentifikation, vedligehold af brugerattributter og adgangskontrol. Tjenesteudbyder og brugerorganisation er med andre ord samme organisation, men det kan være forskellige organisatoriske enheder, som er ansvarlighed for hhv. at forvalte applikationen og administrere brugerne. Tilliden mellem disse følger som oftest af, at der er en fælles ledelse og derfor ikke behov for tillid til eksterne parter.



Figur 9 Mønster 1 - Forretningstjeneste med egne autentifikationstjenester

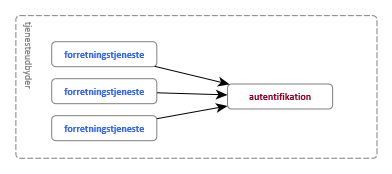
Der er en række udfordringer knyttet til dette mønster bl.a.:

* Brugerne får typisk tildelt et nyt brugernavn og kodeord, som ikke kan benyttes til andre applikationer - og med sin egen cyklus for fornyelse, nulstilling af kodeord osv. Dette leder til en usammenhængende brugeroplevelse.
* Brugeradministratorer får endnu et administrationsinterface, hvor roller og rettigheder manuelt skal vedligeholdes med heraf følgende risiko for, at de ikke holdes ajour når en medarbejder stopper, skifter afdeling osv. Administrationsbyrden stiger uforholdsmæssigt med antallet af applikationer.
* Alle brugere oprettes i samme brugerdatabase, hvilket er meget lidt skalérbart. Når en applikation skal udbredes fra én organisation til flere bryder arkitekturen ofte sammen. Det kan også ske, når applikationer fordrer samarbejde mellem flere organisationer.
* Forretningsapplikationer har typisk ikke fokus på sikkerhed og har heller ikke dette som kernekompetence. Fokus er rettet mod, at brugerne har adgang til funktionaliteten. Det er derfor ofte dyrt at opgradere sikkerheden fx med to-faktor autentifikation eller bedre overvågning, når det skal håndteres applikation for applikation.

På baggrund af ovenstående kan mønstret ikke anbefales, og det må betragtes som et antimønster.

### Mønster 2: Delt, intern autentifikationstjeneste

Dette mønster er karakteriseret ved, at en brugerorganisation har etableret et fælles directory (brugerkatalog og autentifikationstjeneste), som benyttes af flere interne applikationer – evt. med synkronisering mellem brugerkataloget og legacy applikationer (mønster 1), der ikke kan håndtere brugerstyring, via et IdM-system. Der er stadig tale om, at tjenesteudbyder og brugerorganisation er inden for samme organisation.



Figur 10 Mønster 2 - Intern delt autentifikationstjeneste

I forhold til mønster 1 opnås der en række fordele:

* Brugerne skal kun vedligeholdes ét sted – i det fælles brugerkatalog.
* Brugerne kan med ét identifikationsmiddel tilgå alle applikationer, der anvender den fælles autentifikationstjeneste.

Der er dog stadig nogle centrale begrænsninger i mønster 2:

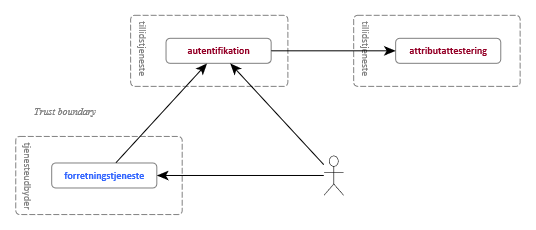
* Mønstret skalerer stadig ikke til scenarier, hvor tjenesteudbyder og brugerorganisation ikke tilhører én og samme organisation. Der er stadig kun én autentifikationstjeneste og ét administrationsinterface.
* Mønstret håndterer ikke scenarier med borgere som slutbrugere.
* Mønstret fordrer en homogenitet i de adgangspolitikker, der kan understøttes (typisk snævert baseret på attributter fx om medlemskab af grupper i brugerkataloget). Al viden om brugerne, der er relevant for adgangskontrol, skal således findes i brugerkataloget.
* Mulighederne for håndtering af forskellige identifikationsmidler og differentierede sikringsniveauer er typisk begrænset.

På baggrund af ovenstående kan mønstret kun anbefales i mindre og strengt interne applikationer, hvor der ikke forventes interaktion med eksterne organisationer.

### Mønster 3: Føderation med central autentifikationstjeneste

Dette mønster er det første, hvor bruger og tjenesteudbyder kan tilhøre forskellige organisationer, og der er derfor behov for mere eksplicit tillid, end når alle parter er under samme ledelse. Der er tale om en såkaldt ’3-corner model’, hvor brugeren har et identifikationsmiddel, der er udstedt til en autentifikationstjeneste, som tjenesteudbyderen kender og har tillid til – dvs. bruger og tjeneste har et fælles ’trust-anker’. Udstederen af identifikationsmidlet kan være sammenfaldende med udbyderen af autentifikationstjenesten (som det fx kendes fra NemID), men funktionerne kan også være adskilt. Det væsentlige er her, at forretningstjenesten stoler på autentifikationstjenesten.

Mønstret er kendt fra NemLog-in, der som fællesoffentlig log-in tjeneste kan autentificere danske borgere og virksomheder til (stort set) alle offentlige tjenester med behov for sikker autentifikation – herunder alle tjenester på Borger.dk og Virk.dk. Som følge heraf betegnes dette også som ’den fællesoffentlige føderation’, og grundlaget for tillid i denne er National Standard for Identiteters Sikringsniveauer (NSIS) [18] og i en vis udstrækning OCES certifikatpolitikkerne [21], der med krav til sikkerhed, revision og andet sætter et veldefineret kvalitetsniveau. F



Figur 11 Mønster 3 - Central autentifikationstjeneste

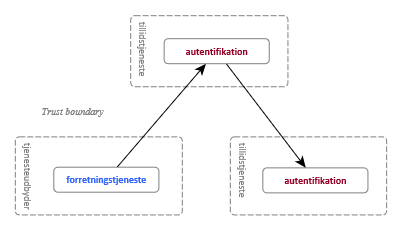
Fordele:

* Forretningstjenesterne afkobles teknisk fra at kende til detaljerne i validering af brugernes identifikationsmidler, idet dette sker i autentifikationstjenesten. Med et fælles tillidsrammeværk (som fx NSIS [18]) kan autentifikationstjenesten blot oplyse det opnåede sikringsniveau til forretningstjenesten, som herefter kan reagere på dette i henhold til sin adgangspolitik. Dette gør det let at indføre nye identifikationsmidler eller ændre på eksisterende uden at påvirke forretningstjenesterne, og generelt giver afkoblingen en fleksibilitet i arkitekturen, som i praksis er meget værdifuld.
* Mønstret kan skalere til nationalt plan og understøtte forretningstjenester, der skal tilgås af samtlige borgere eller samtlige virksomheder i landet. Dette skyldes bl.a., at de centrale autentikationstjenester i Danmark etableres og finansieres fællesoffentligt, og dermed får de national udbredelse. I mange andre lande er situationen langt mere broget med en række overlappende autentifikationstjenester og som følge deraf en mere kompleks arkitektur (se fx mønster 5).
* Autentifikationstjenesten er enkel at udvide med attributbeskrivelse (fx roller, rettigheder, fuldmagter) og kan dermed give ekstra funktionalitet til samtlige, tilsluttede tjenester.

### Mønster 4: Fælles domænebroker for decentrale autentifikationstjenester

Et andet velkendt mønster (særligt for medarbejderidentiteter) optræder, når alle forretningstjenester anvender en fælles autentifikationstjeneste, der agerer som broker for et antal bagvedliggende og decentrale autentifikationstjenester (IdP’er) inden for et bestemt domæne. Dette betegnes ofte som en ’hub-and-spoke’ føderation og er naturligt, når brugerorganisationer ønsker (og er i stand til) at agere som autentifikationstjeneste for egne medarbejdere.

Mønstret anvendes bl.a. i den fælleskommunale infrastruktur etableret af KOMBIT, hvor en såkaldt ContextHandler agerer som central broker/hub, og hvor hver kommune udstiller en autentifikationstjeneste (kaldet IdP) for egne medarbejdere. Mønstret er ligeledes kendt fra WAYF-føderationen på forsknings- og uddannelsesområdet, hvor den enkelte institution er IdP for egne medarbejdere/studerende.



Figur 12 Mønster 4 - Fælles broker for decentrale autentifikationstjenester

Fordele:

* Der er kun ét integrationspunkt for forretningstjenester og ét integrationspunkt for en brugerorganisation med egen IdP, hvilket gør det enkelt at tilslutte sig føderationen og samtidig opnå adgang til et stort økosystem.
* Brugere i en brugerorganisation kan genbruge et lokalt log-in til både in- og eksterne tjenester – og endda opnå single sign-on på tværs af disse.
* Brokeren kan indkapsle variationer i lokale IdP’er, så de er usynlige for tjenesterne – fx ved at foretage protokoltransformation, attributomveksling og berigelse af tokens.
* Den centrale hub giver ofte mulighed for stærk styring herunder fastlæggelse af attributter, protokoller mv., der kan give en stor homogenitet og et økosystem med rige tjenester. Som eksempel kan nævnes, at både det kommunale domæne og sundhedsområdet har defineret egne attributprofiler, som beskriver særlige karakteristika ved domænet: på sundhedsområdet er det fx attributter vedr. sundhedsfaglige autorisationer, og på det kommunale område er det anvendelse af den fælles kommunale emnesystematik (KLE), der er en taksonomi til at beskrive kommunale fagområder.

Ulemper:

* Mønstret er begrænset til situationer, hvor alle relevante tjenester for brugerne er koblet til samme ’hub’. Anvendelsen er derfor ofte begrænset til specifikke domæner – som fx det kommunale område. Hvis man skal på tværs af domæner / føderationer er det i stedet relevant at anvende mønster 5.
* Brugerne kan komme ud for at skulle angive deres lokale IdP i en liste blandt mange (såkaldt home realm discovery), første gang de logger på, således at brokeren kan finde ud af, hvilken lokal IdP der skal anvendes til autentifikation.

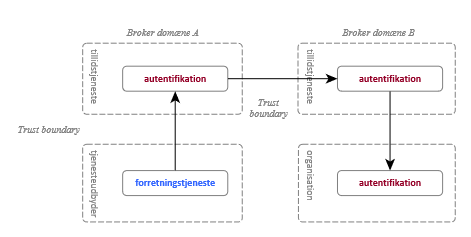
Variationer over mønstret kan optræde, ved at attributbeskrivelser kobles på forskellige steder i tillidskæden.

### Mønster 5: Interføderation mellem domæner

Det femte og sidste mønster er karakteriseret ved, at brugerorganisation og forretningstjeneste er koblet til hver deres broker/føderation (som beskrevet i mønster 4) hørende til hver deres domæne. Der er med andre ord tale om interføderation mellem to domæner. Brugerorganisation og forretningstjeneste forbindes således via de to brokere, der på ’bagsiden’ forbinder og oversætter mod deres eget domæne. Mønstret er uden for brugerstyringsverdenen kendt som ’four-corner’ modellen og anvendes grundet sin skalérbarhed i en lang række store infrastrukturer som fx OpenPEPPOL, ved indløsning af kreditkort mv.

Inden for brugerstyring er mønstret bl.a. kendt fra eIDAS-føderationen, der har til formål at gøre det muligt at foretage autentikation på tværs af landegrænser i EU. Her etablerer hvert land en såkaldt ’eID-gateway’, der dels er broker og opkoblingspunkt for nationale autentifikationstjenester og dels broker for nationale forretningstjenester. Herved kan en bruger med et identifikationsmiddel fra ét EU-land autentificere sig over for tilsluttede tjenester i alle andre EU-lande, forudsat at identifikationsmidlet er klassificeret på det nødvendige sikringsniveau.

Mønstret kendes også på nationalt niveau, når eksempelvis en kommunal bruger via den kommunale ContextHandler tilgår en national sundhedstjeneste, der er udstillet gennem sundhedsområdets broker (SEB). Her etableres forbindelsen således mellem brokere fra to forskellige domæner.



Figur 13 Mønster 5 - Interføderation mellem domæner

Fordele:

* Mønstret kan håndtere store føderationer uden centrale ankre. Der er m.a.o. stor skalérbarhed.
* Brokerne håndterer kompleksiteten i infrastrukturen for forretningstjenesten og brugerorganisationen.

Ulemper:

* Der kan være stor kompleksitet med flere lag af discovery.
* Governance er typisk noget svagere på tværs af føderationer og domæner.
* Det fælles forståede attributsæt er typisk mere begrænset, når tillidskæden er lang:
* Dette er fx en kendt udfordring i eIDAS føderationen, hvor det garanterede minimumsæt af attributter for en fysisk person på tværs af EU er meget fattigt og kun rummer navn, fødselsdato, og en unik ID (ikke meningsbærende). Det er således en udfordring for mange forretningstjenester at levere en meningsfuld tjeneste til brugerne baseret på dette attributsæt. Enten fordi der ikke kan laves et sikkert match til en lokal repræsentation af brugeren, eller fordi en tjeneste er konstrueret til at kræve flere oplysninger som fx et dansk CPR-nummer.
* Et mere simpelt eksempel på dette er, at tjenester på sundhedsområdet som regel kræver CPR nummer for brugeren, da sundhedsfaglige autorisationer er knyttet til dette, mens det i den kommunale verden ikke er sædvanligt at benytte CPR numre som grundlag for brugerstyring. Dette betyder konkret, at der er behov for ekstra opslag og omvekslinger, når en kommunal bruger skal tilgå en tjeneste under sundhedsdomænet.

# Teknisk arkitektur

I dette afsnit beskrives tekniske og praktiske forhold, der er relevante for realisering af forretningsfunktioner og mønstre for tillidstjenester. Dette omhandler eksempelvis støttefunktioner som discovery og billetomveksling, håndtering af apps på mobile enheder, softwarerobotter og identitetsbaserede services.

De strategiske temaer, principper og forretningsbehov, der er beskrevet i kapitel 2, peger entydigt frem mod en løst koblet arkitektur, hvor forretningstjenester understøttes af tillidstjenester og hvor forretnings- og tillidstjenester indgår i en føderation. Her vil de enkelte forretningstjenester håndhæve adgang, der er baseret på oplysninger attesteret af tillidstjenester. Forretningstjenesterne undgår selv at realisere en lang række funktioner vedr. registrering, udstedelse af identifikationsmidler, attributbeskrivelse, autentifikation osv.

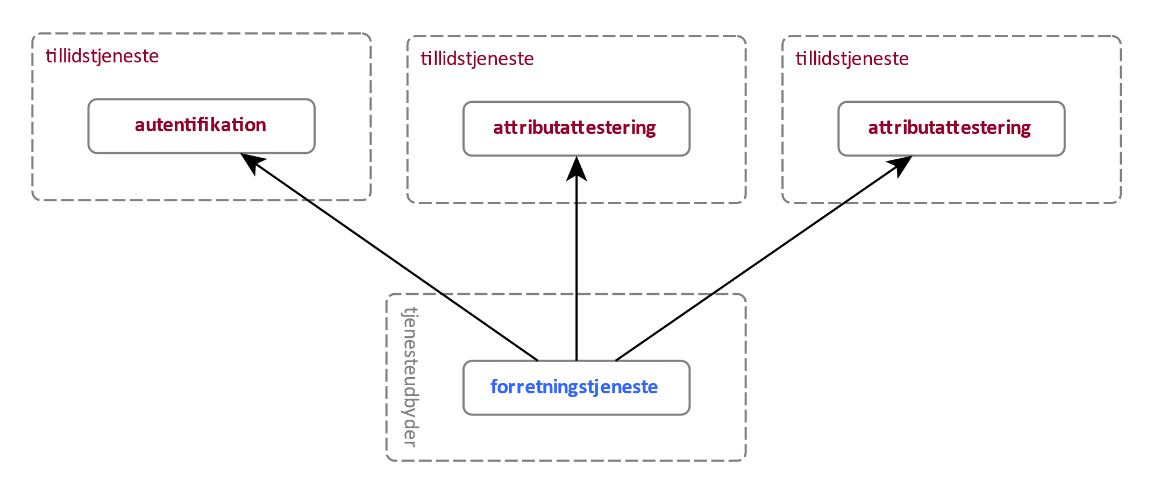
Der gives endvidere nogle eksempler fra det fællesoffentlige domæne i form af MitID og NemLog-in3 løsningerne. For andre domæner som fx det kommunale område og sundhedsområdet henvises til specifikke domænearkitekturer og målbilleder udarbejdet i de respektive domæner.

## Attestation via push/pull

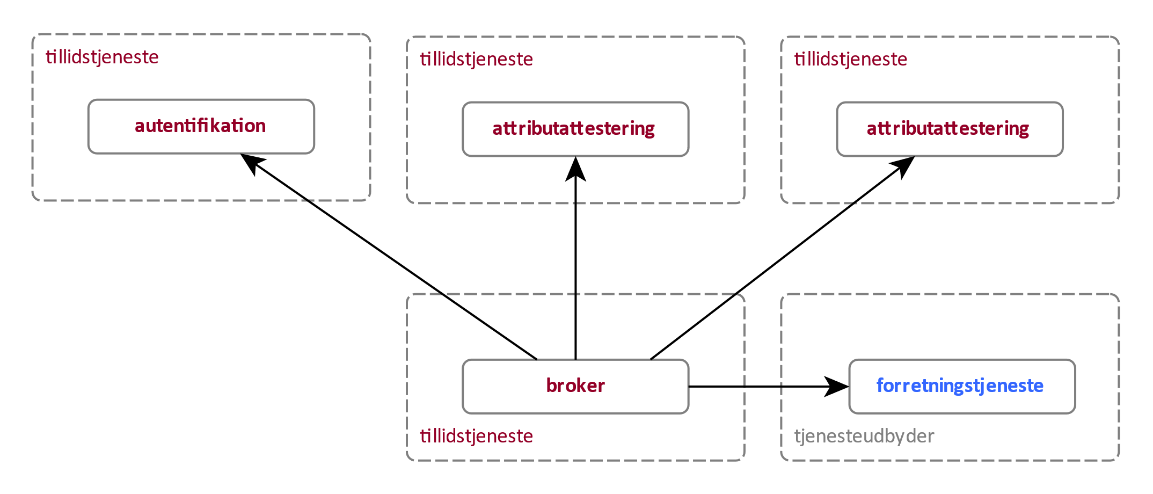
En forretningstjeneste kan få adgang til attesterede oplysninger om en bruger fra en tillidstjeneste på forskellige måder:

* Ved selv at foretage opslag hos tillidstjenesterne (pull) eller evt. i autoritative registre med grunddata af relevans for brugerstyring (fx CPR- og CVR-data).
* Ved at få leveret en adgangsbillet (security token) (push), hvor oplysninger om brugeren (inkl. dennes autentifikation) er samlet og signeret (typisk af en broker). Bemærk at tokens bør være specifikke og målrettede mod den aktuelle tjeneste. I OIOSAML standarden [19] er dette eksempelvis understøttet af Audience-elementet.

De to tilgange kan sagtens kombineres.



Figur 14 Attestation via pull



Figur 15 Attestation via push

Fordelen ved at få de attesterede oplysninger om brugeren leveret i et token via push-modellen er, at forretningstjenesten får en løsere kobling til tillidstjenesterne, idet forretningstjenesten typisk ikke skal bekymre sig om, hvilke tillidstjenester der er relevante for den aktuelle bruger, hvor de findes, hvordan der integreres med dem osv. Brokeren vil ofte påtage sig opgaven med at sikre afkobling for forretningstjenester og orkestrere tillidstjenesterne i et domæne (eller mod andre domæner) gennem opslag og omvekslinger af tokens. Omvendt kan det i nogen sammenhænge være vanskeligt at vide, hvilke attributter en forretningstjeneste på forhånd har behov for, idet det kan afhænge af brugerens ageren i fx en applikation. Derfor kan der opstå et naturligt behov for dynamiske opslag, mens brugeren anvender forretningstjenesten. Det kan hertil bemærkes, at det normalt ikke er god praksis at samle for mange oplysninger i et token, som en forretningstjeneste eventuelt kunne få brug for, da dette kan stride mod dataminimeringsprincippet i Databeskyttelsesforordningen (GDPR) [13], hvor kun absolut nødvendige oplysninger behandles.

## Attributhåndtering

Som tidligere nævnt spiller attributter en vigtig rolle i brugerstyring. Dels som grundlag for beskrivelse af brugerne, deres egenskaber og deres kontekst, dels som grundlag for håndhævelse af adgangskontrol. I dette afsnit fokuseres på attesterede attributter, hvor en tillidstjeneste udtaler sig om attributter, der er underlagt en eller anden form for kontrol.

Nedenfor gives eksempler på forskellige, vigtige kategorier af attributter:

* Identificerende attributter (eller identifikatorer), som beskriver identiteten entydigt i en bestemt kontekst (fx CPR, PID, RID, UUID osv.).
* Beskrivende attributter om identiteten (fødselsdag, øjenfarve, navn).
* Attributter, der beskriver relationer (fx ‘repræsentant for virksomhed xyz’, ‘forælder til’, ‘ejer af’).
* Rettighedsrelevante attributter (roller, rettigheder eller indhold af dataafgrænsninger, autorisation af læge/sygeplejerske/andre sundhedsprofessionelle).
* Fuldmagter eller samtykker udtrykt som attributter.

Derudover anvendes i nogle sammenhænge informationer om konteksten for en autentifikation som grundlag for adgangskontrol (fx IP-adresse, devicetype, tidspunkt for login, geolokation).

I forbindelse med anvendelse af attributter i adgangskontrol 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 i form af sikringsniveauerne LoA, IAL, AAL og FAL i National Standard for Identiteters Sikringsniveau (NSIS) [18], mens kvaliteten for øvrige attributter ofte er underforstået af den aktuelle sammenhæng. En simpel (men primitiv) mekanisme kan være at associere attributkvaliteten med den tillidstjeneste, der har attesteret den. Men her kan der opstå udfordringer, når attributter formidles gennem kæder med flere led og omveksles mellem tokens, idet det for slutmodtageren bliver mere uklart, hvem der oprindeligt udtalte sig om en bestemt attribut. I stedet er det bedre eksplicit at påstemple yderligere oplysninger om attributtens kvalitetsegenskaber fx ved henvisning til en klassifikation eller lignende mekanisme, så denne information bevares gennem tillidskæden.

Det er ligeledes vigtigt, at den fulde livscyklus for attributter kan håndteres, idet værdierne 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 det fremadrettede arbejde med fællesoffentlig brugerstyring vurderes der at være behov for at analysere fælles standarder for attributters kvalitet yderligere (ud over dem, som er beskrevet i NSIS [18]). Attributter defineres ofte inden for en bestemt sektor, men det kunne fællesoffentligt godt være relevant at specificere fælles mekanismer til at udtrykke og formidle kvalitetsinformation, så dette kan udveksles på en interoperabel måde. Det kræver ofte en vis modenhed og veldefineret governance at bygge klassifikationer og semantiske modeller. Som et eksempel på dette kan nævnes den kommunale emnesystematik (KLE) [33], der er en taksonomi til at beskrive kommunale fagområder. Ved at benytte KLE er det muligt at berige en rolletildeling til en bruger med en dataafgrænsning til et bestemt emneomåde, der angives ved en eller flere KLE-værdier på rolletildelingen. Tilsvarende kan nævnes for FORM [34], der er et opgavekatalog over det offentliges opgaver.

### Attributkontrakter

Forskellige forretningstjenester har behov for at modtage bestemte attributter for at kunne fungere, mens forskellige tillidstjenester kan levere forskellige sæt af attributter for bestemte identiteter. En konkret aftale eller specifikation af hvilke attributter der skal leveres til en bestemt tjeneste, kaldes i flere sammenhænge for en attributkontrakt. Beskrivelse af attributsæt indenfor bestemte domæner sker ofte i profiler af standarder som fx SAML:

* Den fællesoffentlige OIOSAML profil [19] definerer et attributsæt for private og professionelle med dels en række obligatoriske og dels en række frivillige attributter.
* KOMBIT har defineret en attributprofil som underprofil af OIOSAML, der definerer særlige attributter for kommunale medarbejdere.
* Sundhedsdatastyrelsen har ligeledes defineret en underprofil af OIOSAML med attributter, der er relevante for sundhedsområdet.

Ofte vil en forretningstjeneste ved tilslutning til en broker deklarere hvilke attributter, den pågældende forretningstjeneste har behov for (og ofte med henvisning til attributter defineret i en profil for domænet). Det er fx sædvanligt at definere attributsæt i SAML metadatafiler.

En anden mulighed, som dog sjældent ses implementeret i praksis, er at beskrive attributter som en del af snitfladen (fx som et forventet sæt af claims i WS-Security Policy [25]), så sikkerhedsinfrastrukturen kan foretage en automatisk orkestrering. Via en policy fil med deklaration af attributter kan en identitetsbroker evaluere forretningstjenestens attributbehov og herefter kontakte et antal tillidstjenester, som tilsammen kan levere de ønskede attributter (i rette kvalitet), hvorefter brokeren udsteder en samlet adgangsbillet mod tjenesten med foreningsmængden af attributter.

Endelig er der en velkendt fællesoffentlig udfordring i håndtering af CPR-nummeret. 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 [19] i stedet brug af CPR UUID’er, således at tjenester kan påbegynde migrering til disse.

### Brugerkataloger

Et brugerkatalog indeholder informationer om et sæt af brugeridentiteter typisk i form af attributter og i mange tilfælde også information til brug for validering af identifikationsmidler 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 administrationsmodel.

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 brugerdatabasen 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 (AD), 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 føderationsprotokoller som SAML, OpenID Connect [28] 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 4: Brugerstyring er adskilt fra forretningstjenester, 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 imødegåelse af problemstillingen med mange, adskilte brugerkataloger, 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, da de fastholder et lokalt brugerkatalog som deres eneste verdensbillede. 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 mulighed for at vælge at bruge deres eget lokale brugerkatalog, også i forbindelse med administration af adgang til offentlige løsninger.

## Discovery-tjenester

En støttefunktion, som ofte ses i større føderationer, er discovery-tjenester, som for en given bruger har til opgave at lokalisere de tilllidstjenester (fx autentifikation og attributtjenester), der kan tilvejebringe oplysninger om brugeren. Ofte er discovery-funktionen en integreret del af en broker, særligt i føderationer med en central broker.

Kendte eksempler på discovery-tjenester er fx:

* WAYF føderation (Where Are You From), hvor en bruger angiver hvilken institution, vedkommende kommer fra - og dermed hvilken autentifikationstjeneste, som kan autentificere brugeren og levere attributter.
* En tilsvarende funktion findes i KOMBIT’s ContextHandler, som kan afgøre hvilken kommune, en bruger kommer fra, for derved at lokalisere den relevante lokale (kommunale) autentifikationstjeneste (IdP).
* I eIDAS føderationen findes en obligatorisk “landevælger”, hvor brugeren vælger det EU-land, som kan autentificere ham.

Bemærk at en discovery funktion ikke nødvendigvis behøver at interagere med brugeren, idet discovery også kan baseres på cookies, URL parametre osv.

## Billetudstedelse og -omveksling

I praksis vil man ofte realisere attestering af information om autentifikation eller brugerattributter gennem ”billetudstedelse”.

En billet er typisk en signeret datastruktur baseret på XML (fx Assertions i SAML standarden [19]) eller JSON (JWT standarden [23]), hvilket sikrer mod manipulation eller forfalskning. I nogle sammenhænge kan billetter også være krypterede til sikring af fortrolighed under transport. Modtageren kan validere billetten ved at kontrollere signaturen, hvilket forudsætter kendskab til udstederens certifikat. Typisk vil modtagere af billetter derfor være konfigureret med et såkaldt ‘trust store’ for de billetudstedere og andre tillidstjenester, som skal kunne verificeres. Dette betegnes også som ‘trust ankre’.

Typisk udføres billedudstedelse af en broker på grundlag af en forudgående autentifikation, hvor brokeren kan tilføje attributter, der beskriver identiteten, samt anden relevant information som fx tidspunkt for autentifikation, NSIS sikringsniveau for autentifikationen mm. Attributterne udtrykker som tidligere beskrevet 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”).

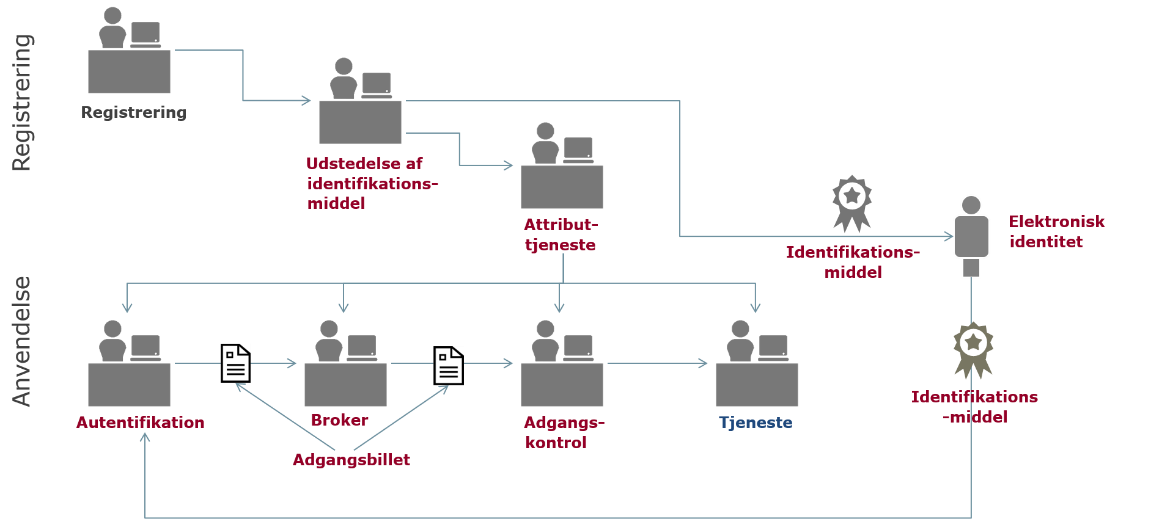
Et eksempel på dette mønster findes i NemLog-in, der efter autentifikation af en bruger (fx med NemID eller MitID) kan berige den udstedte SAML Assertion med CPR nummer baseret på opslag i CPR, med det aktuelle NSIS sikringsniveau for autentifikationen, samt rettigheder og fuldmagter baseret på opslag i NemLog-in’s egen rettigheds- og fuldmagtskomponent. Alle forretningstjenester, der er tilsluttet NemLog-in, har forinden udvekslet SAML metadata med NemLog-in, som indeholder certifikater, der bruges til signering og kryptering, og kan med udgangspunkt heri validere billetter fra NemLog-in.

I større føderationer eller i scenarier med interføderation, hvor to eller flere føderationer forbindes, kan der være flere tillidstjenester, der udsteder og signerer billetter - og det kan være urealistisk eller upraktisk at hver forretningstjeneste kender dem alle. Her er der ofte behov for, at brokere foretager en billetomveksling, ved at de udsteder og signerer en ny samlet billet, der er baseret på andre billetter udstedt af andre tillidstjenester, som der er en tillidsrelation til. Dvs. en broker, som forretningstjenesten kender og har tillid til, sørger for at håndtere tillidstjenester længere ude i tillidskæden, som forretningstjenesten ikke har direkte kendskab til. Den tekniske omveksling er udtryk for ‘transitiv trust’, der forstås på den måde, at tillidskæden kollapses over for tjenesten. Udover at foretage ‘trust brokering’ kan billetomveksling også anvendes til at oversætte attributter eller foretage protokolkonvertering mv.

### Tillidskæder i økosystemer

I et sammenhængende, skalérbart og sikkert økosystem af tillidstjenester og forretningstjenester, skal mange aktører som tidligere beskrevet kunne arbejde sammen i en orkestrering af de forskellige services. For at der kan ske en sådan specialisering og arbejdsdeling, er der behov for regler og aftaler, der gør, at aktørerne kan have tillid til hinanden. De aktører, som indgår i et tillidsforhold, udgør en føderation, som bl.a. bygger på et trust framework som fx NSIS, eIDAS eller aftaler i et domæne.

Nedenstående figur 18 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 16 Kæde af tillid i et tjenestekald

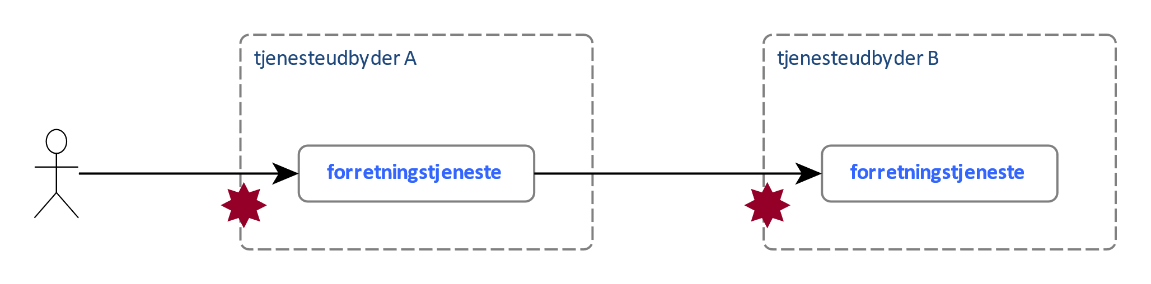
* Udbyderen af forretningstjenesten skal have tillid til, at adgangskontrollen (engelsk: Policy Enforcement Point, PEP) kun viderestiller identiteter, hvis adgangsbillet matcher adgangspolitikken for forretningstjenesten. Tjenesteudbyderen varetager som hovedregel selv adgangskontrollen, men denne funktion 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.
* Brokeren 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, brokeren 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 identiteterne, 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 styring sikre tillidskæden. Når en organisation vælger at basere sig på eksterne tillidstjenester, forudsætter det, at tillid er etableret gennem et trust framework, der bl.a. omfatter aftaler og standarder.

I en føderation mellem en række sektorer, der hver har deres sikkerhedsdomæne, 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.

## Identitetsbaserede services

En ofte forekommende problematik er, at en forretningstjeneste har brug for at kalde videre til andre forretningsservices for at servicere en bruger. Det kan fx være, at en portal som borger.dk, der tilgås af slutbrugere, har brug for opslag i en bagvedliggende service, der kan levere data om en bestemt borger, fx Digital Post. Nedenstående figur illustrerer et simpelt eksempel, hvor der kun er to forretningstjenester i spil:



Figur 17 Kald mellem forretningstjenester

Begge forretningstjenester udfører som tidligere nævnt brugerstyring (illustreret på figuren med røde stjerner). Det første kald er helt almindelig brugeradgang, men for kaldet til den næste forretningstjeneste er der grundlæggende to måder at håndtere det videre kald på mellem forretningstjenester:

* Enten kalder den første forretningstjeneste videre med sin egen identitet (også kaldet system-trust modellen).
* Alternativt kalder den første forretningstjeneste videre med kontekst af den specifikke bruger, som der ønskes data på vegne af (altså en delegeringsmodel).

Den sidstnævnte model kaldes for identitetsbaserede (web) services, idet den oprindelige brugeridentitet føres med videre i kaldet. Modellen forudsætter, at forretningstjenester er forberedt for en mere kompleks model, der understøtter delegering.

Fordelen ved den identitetsbaserede model er, at tilliden skabes gennem en konkret brugerforespørgsel, fremfor at den kaldende forretningstjeneste får fuld adgang på vegne af alle brugere. Endvidere bliver det enkelte kald sporbart til den konkrete bruger. Til gengæld fordrer det synkronisitet, idet brugeren som regel skal være logget ind i den kaldende forretningstjeneste, før et identitetsbaseret kald er muligt, hvilket er en udfordring i scenarier med batch-lignende kørsler. Omvendt kan system trust modellen fungere uafhængigt af, om brugeren er logget ind, men til gengæld vil et sikkerhedsbrud i den kaldende forretningstjeneste (fx kompromitteret privatnøgle) kunne skalere til samtlige brugere hos den anden forretningstjeneste. Som regel anses identitetsbaserede services for at være mere sikre, bedre at understøtte privatliv, samt indebære en højere grad af transparens.

Der er fællesoffentligt specificeret en række standarder for identitetsbaserede webservices, der går under betegnelsen OIO IDWS [24]. 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 OIO identitetsbaserede webservices [24] består af:

* OIO WS-Trust Profile (protokol til at anmode om Security Token).
* OIO WS-Trust Deployment Profile (konkretisering af ovenstående).
* 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).

Disse profiler er endvidere suppleret med open source referenceimplementeringer 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. Bemærk at alle disse profiler (pånær OIO IDWS Rest Profile) er baseret på XML/SOAP, og at der mangler tilsvarende profiler baseret på JSON/REST.

Sundhedsområdet benytter samme arkitekturprincipper og har defineret egne SAML-baserede standarder, suppleret med egne STS’er (Security Token Services) deployet i domænet. 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 ny, bagvedliggende tjeneste for at tilgå brugerens data.

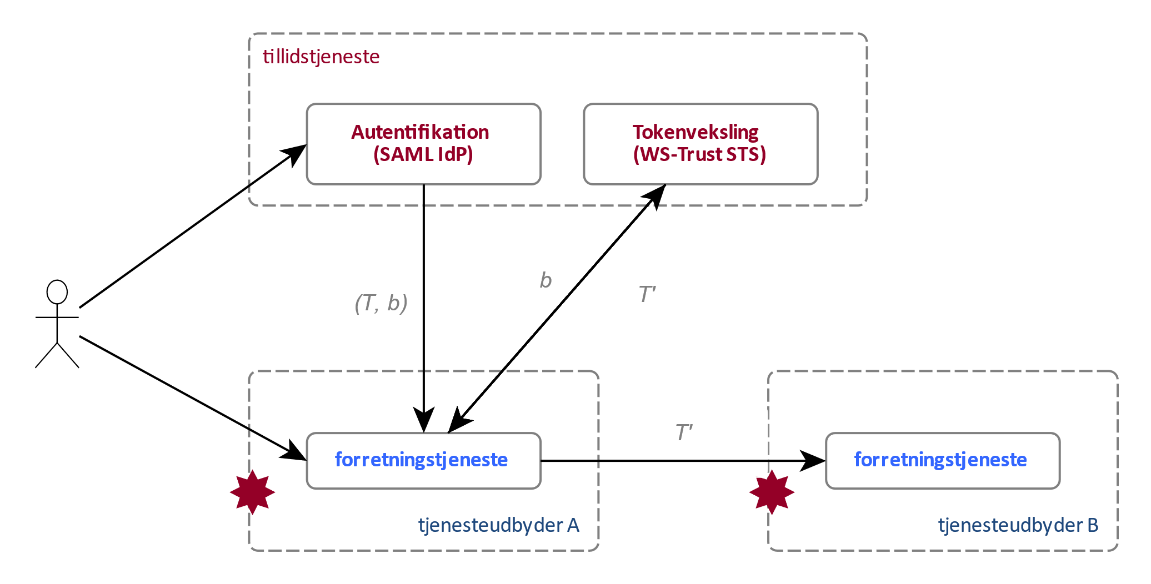
I grunddataprogrammet har man valgt en fælles, tværgående sikkerhedsmodel, baseret på udstedelse af Security Tokens for de services, der muliggør opdatering af registre. Dette giver en struktureret model på tværs af programmet frem for et virvar af punkt-til-punkt integrationer, der er baseret på certifikater.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

### Identitetsbaseret kald via billetomveksling

I dette afsnit præsenteres et simpelt eksempel på, hvordan et identitetsbaseret kald kan realiseres med OIO IDWS specifikationerne [24] og deres implementering i NemLog-in.

Eksemplet tager udgangspunkt i, at brugeren logger på en web-portal (tjeneste A) via SAML IdP, der agerer autentifikationstjeneste. Når brugeren autentificerer sig overfor IdP’en udstedes en adgangsbillet (T) til portalen, som har indlejret et såkaldt ‘bootstrap token’ (benævnt b på figuren nedenfor). Dette bootstrap token kan portalen omveksle hos en Security Token Service til et nyt token (T’), der kan anvendes i kaldet til den næste forretningstjeneste.

Scenariet er illustreret på nedenstående figur:



Figur 18 Identitetsbaseret kald via tokenveksling

Scenariet forudsætter, at begge forretningstjenester har tillid til samme IdP/STS - men ellers kan det udvides med yderligere omvekslinger af tokens udført af brokere. Desuden skal STS’en på forhånd kende den forretningstjeneste (B), som den udsteder et token til, herunder have defineret en politik for, hvilke omvekslinger, der tillades. I den forstand varetager STS’en en del af forretningstjeneste B’s adgangspolitik.

## Adgangskontrol

Tjenesteudbyderen er som tidligere nævnt den, der forvalter det juridiske ansvar for adgangen til de informationer og funktioner, som forretningstjenesten udstiller - som hovedregel i rollen som dataansvarlig i databeskyttelsesreguleringens forstand.

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, og kun kan ændres af autoriserede brugere.
* Tilgængelighed, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt, og kun kan slettes af autoriserede brugere.

Tjenesteudbyderen skal som led i 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 for 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-Security Policy [25] er der specificeret et sprog for at udtrykke en adgangspolitik. Dette giver en billetudstedende tillidstjeneste 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 OIOSAML standarden [19], 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 identifikationsmidler 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. Her kan en regelmotor 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 - foruden at selve billetten valideres (herunder signatur og tidsstempel på denne). 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 token [29], der er udvekslet til at holde sessionen åben i en bestemt tidsperiode.

Adgangskontrollen er tjenesteudbyders ansvar, men tekniske funktioner kan leveres af eksterne systemer. Dette er eksempelvis tilfældet i XACML standarden [26], der dog ikke er særlig udbredt i praksis. XACML står for ‘eXtensible Access Control Markup Language’ som definerer et finkornet sprog for adgangspolitikker baseret på attributter. Desuden beskriver standarden en arkitektur med forskellige komponenter bl.a. et ‘Policy Decision Point’ (PDP), som evaluerer et adgangsønske mod en adgangspolitik, et ‘Policy Enforcement Point’, som håndhæver PDP’ens adgangsbeslutning, et ‘Policy Administration Point’ (PAP), hvor adgangspolitikker administreres mv.

## Softwarerobotter

Behovet for softwarerobotter udspringer af et ønske om at automatisere processer, hvor de enkelte procestrin kræver interaktion med et eller flere it-systemer. Her indgår ofte systemer, der kun udstiller deres funktionalitet via en brugergrænseflade. Robotter kan derfor have behov for at kunne simulere en menneskebruger ved at interagere med brugergrænsefladen og dermed opnå den ønskede automatisering.

Det er ofte en grundlæggende præmis, at applikationerne ikke kan skrives om og gøres robot-venlige, men må bruges, som de er. Det kan her bemærkes, at den ideelle løsning formentlig vil være en ’API-first’ tilgang, hvor al funktionalitet i applikationer udstilles som services, således at procesautomatisering let kan opnås ved at orkestrere relevante services. Robot-tilgangen kan med andre ord opfattes som et teknisk work-around, som kompenserer for manglende service-enabling i eksisterende applikationer.

En anden grundlæggende præmis er, at sikkerheden ikke må kompromitteres ved anvendelse af robotter, herunder at menneskebrugere ikke må være nødsaget til at udlevere deres identifikationsmidler til robotter i strid med certifikatpolitikker, brugervilkår for NemID/MitID, krav i standarder som NSIS [18], lovgivning som eIDAS [8] mv.

I denne referencearkitektur forstås softwarerobotter som de såkaldte autonome robotter, der selvstændigt logger på applikationer og ikke agerer i kontekst af en medarbejder pc. De såkaldte ’Attended robots’, der fungerer på den enkelte medarbejders pc og afvikles i kontekst af den enkelte medarbejders brugerkonto og adgange, er således uden for afgrænsningen, og giver som regel heller ikke udfordringer i brugerstyringen.

For autonome robotter opstår derimod ofte udfordringer med brugerstyring, når applikationen er konstrueret til at forvente et log-in med et identifikationsmiddel, som alene må anvendes af menneskebrugere – eksempelvis et MOCES medarbejdercertifikat, der er særdeles udbredt. Her kan den autonome robot ikke få adgang – med mindre et menneske bryder reglerne og kompromitterer sikkerheden. I de næste underafsnit præsenteres et forslag til en løsning af denne udfordring baseret på føderationsprincippet.

### Løsning for autonome robotter via føderation

Til håndtering af autonome robotter kan man med fordel bygge på føderationsprincippet. Hvis applikationen således ikke selv står for autentifikation af brugere men anvender en ekstern broker eller autentifikationstjeneste, kan der foretages en afkobling, som tillader robotten at simulere et menneske. I det følgende tages udgangspunkt i et konkret scenarie, hvor applikationen kræver log-in med MOCES-certifikat, og anvender NemLog-in som autentikationstjeneste / broker. Dette vil være tilfældet for mange offentlige tjenester – og mønstret kan sagtens generaliseres til andre sammenhænge herunder andre brokere.

Når en applikation beder NemLog-in om at autentificere en medarbejderidentitet, sker autentifikationen i NemLog-in, og applikationen får blot en signeret billet tilbage (SAML Assertion) med en række attributter. Applikationens binding er således reelt til et forventet attributsæt (attributkontrakten), der beskriver en medarbejderidentitet (fx navn, e-mail, CVR, RID-nummer, rettigheder mv.) snarere end en binding til medarbejderens identifikationsmidler (fx MOCES certifikatet).

Denne afkobling gør det muligt for brokeren/autentifikationstjenesten at udstede en billet til en robot med samme attributsæt, som forventes til en medarbejder. Ideen er med andre ord at opfatte robotter som digitale medarbejdere, der blot har nogle andre typer identifikationsmidler, som er mere robotegnede (fx FOCES), men som i øvrigt ellers ligner medarbejdere til forveksling.

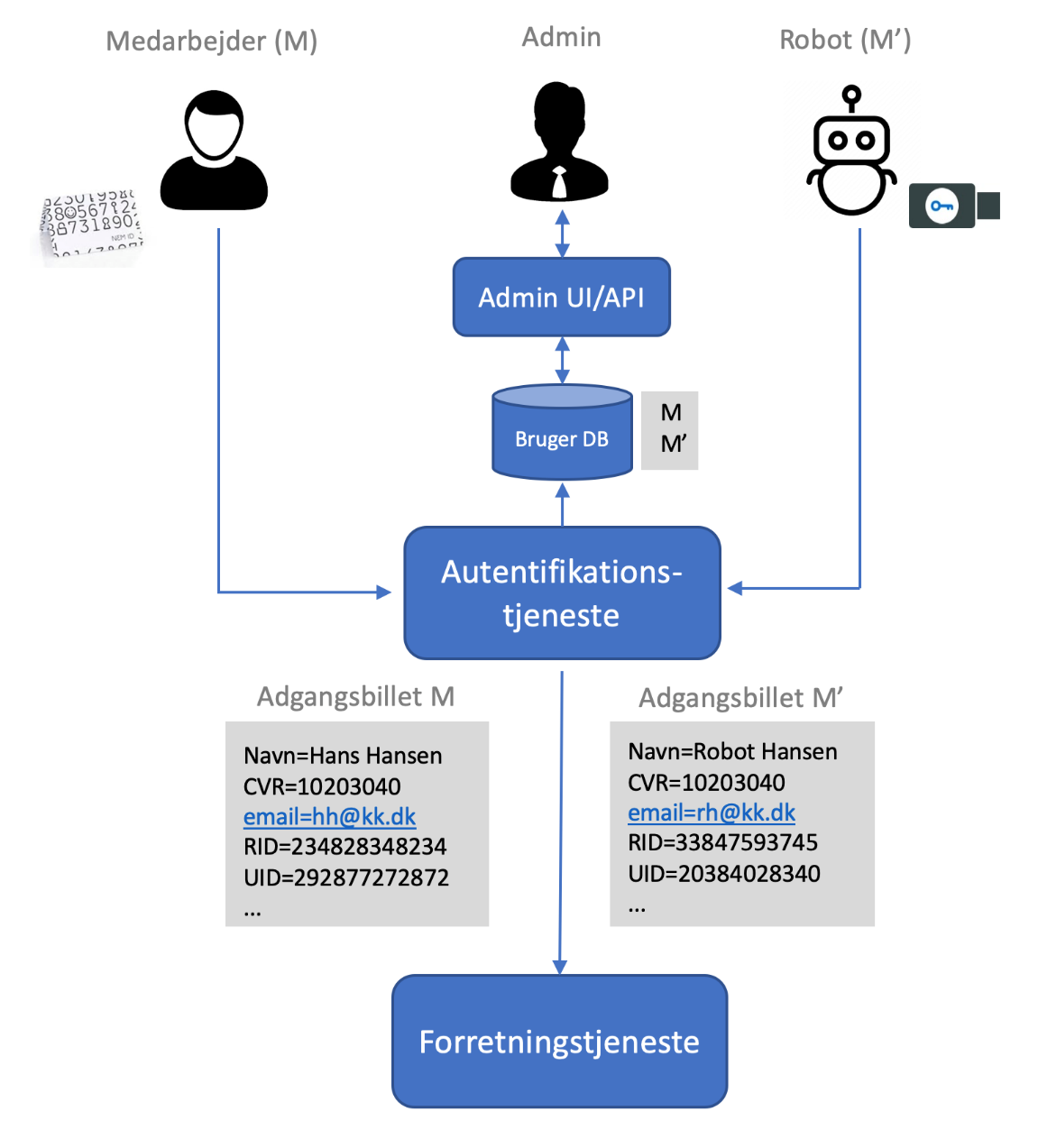
For at understøtte scenariet skal en brugeradministrator kunne oprette en robotidentitet (M’) med præcis de samme attributter som en almindelig medarbejderidentitet (M), og herefter udstede/tilknytte et robot-egnet identifikationsmiddel, fx FOCES-certifikat i en krypteret PKCS#12 nøglefil med privat nøgle og certifikat, der kan installeres i en robotinstans.

Adgangsprocessen til applikationen kan herefter udspilles på flg. måde:

* Robotten tilgår applikationen ved at simulere en browser.
* Applikationen laver redirect til NemLog-in’s autentifikationsservice og anmoder om autentifikation af en medarbejderidentitet via OIOSAML standarden [19].
* Robotten autentificerer sig overfor NemLog-in via sit tilknyttede identifikationsmiddel (her FOCES certifikat).
* Efter autentifikationen fremfinder NemLog-in den medarbejderidentitet (M’) i sin brugerdatabase, som er tilknyttet identifikationsmidlet, og danner et autentifikationssvar med de nødvendige attributter til applikationen.
* Applikationen validerer billettens signatur, og giver adgang til applikationen på baggrund af attributterne i billetten i henhold til applikationens adgangspolitik.

Ovenstående kan generaliseres til alle typer applikationer, der via føderation har en kontrakt med en broker om autentificering af medarbejderidentiteter.

Løsningen er illustreret på nedenstående figur:



Figur 19 Model til brug for brugerstyringstjenester i processer

Man kan evt. vælge at lade billetter for robotter indeholde en særlig attribut som indikerer, at der er tale om en robot. Herved kan ’robot-aware’ applikationer, hvis de vil, reagere på en særlig måde overfor robotter, mens ’ikke-robot-aware’ applikationer blot ignorerer attributten, og opfører sig på samme måde som hvis der var tale om medarbejderidentitet for en fysisk person.

### Robotter uden føderation

For forretningstjenester, som ikke understøtter føderationsmodellen men i stedet fx mønster 1 eller 2 som beskrevet ovenfor, må der anvendes en anden tilgang til understøttelse af softwarerobotter. Her kan en oplagt mulighed være at oprette en særlig ‘robotbruger’ med brugernavn+kodeord i applikationens lokale brugerkatalog (mønster 1) eller i det fælles directory (mønster 2). Herved optræder robotten som en selvstændig identitet, kan få egne rettigheder tildelt og autentificerer sig med et selvstændigt identifikationsmiddel, der er adskilt fra personbrugere.

Hvis forretningstjenesten har en hård teknisk binding, der kræver autentifikation med en bestemt type identifikationsmiddel, som kun må udstedes til mennesker (fx NemID medarbejdercertifikater), er der ikke umiddelbart nogen lette løsninger til at give softwarerobotter adgang til forretningstjenesten. Her må forretningstjenesten typisk omskrives på den ene eller anden måde.

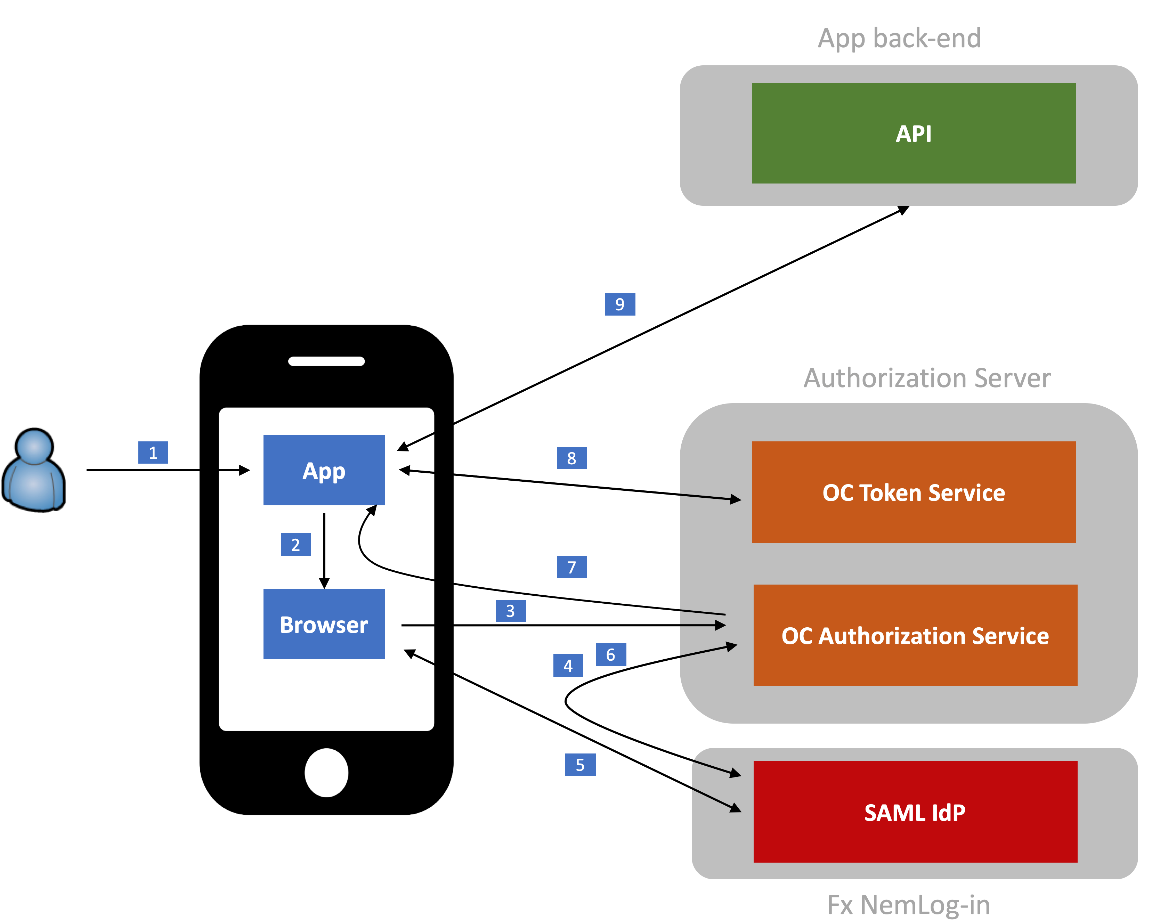
## Brugerstyring for (native) apps

Brugerstyring for apps på mobile enheder bringer sine egne udfordringer. I dette afsnit fokuseres udelukkende på native apps, idet mobile web applikationer som regel håndteres på samme måde som traditionelle web applikationer.

På mobile enheder er der ofte behov for at kunne autorisere en app til at kunne agere på brugerens vegne efter de tidligere nævnte principper om identitetsbaserede web service - eksempelvis give app’en muligheden til at kalde et REST API på vegne af brugeren. Der findes endnu ingen fællesoffentlige profiler eller standarder på dette område, men der tegner sig alligevel en række mønstre og best practices, baseret på anvendelse af OAuth 2.0 [27] samt OpenID Connect standarderne [28]. 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 et token (eller flere) til app’en, som kan anvendes til at autorisere kald til back-end services (typisk REST API’er). Herved er såvel app’ens identitet og identifikationsmiddel adskilt fra brugerens, og adgangen er eksplicit godkendt af brugeren.

Det skal bemærkes, at brugerautentifikationen (indlejret i OAuth eller OpenID Connect flows) sagtens kan være baseret på OIOSAML 2.0 [19], hvorfor eksisterende SAML-baserede autentifikationstjenester og brokere kan genanvendes. Eksempelvis er det fuldt ud muligt at benytte NemLog-in’s SAML IdP til at autorisere en app, og brugergrænsefladen er i NemLog-in’s implementering responsiv, og den vil dermed tilpasse sig den reducerede skærmstørrelse. Digitaliseringsstyrelsen har i 2011 udgivet en vejledning til OAuth 2.0 [27], der viser hvordan standarden kan anvendes.

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



Eksempel på autorisering af en mobil app via OpenID Connect med en indlejret SAML-baseret brugerautentikation

Sekvensen i figuren er som følger:

1. Brugeren installerer og åbner App’en.
2. App’en starter log-in flowet ved at åbne en browser på den mobile enhed og medsende et OpenID Connect Authentication Request. Dette specificerer via nogle parametre (i form af scopes), hvilke data, der ønskes adgang til.
3. Browseren sendes med HTTP redirect (302) til OpenID Connect Authorization Service endepunktet og overleverer herved Authentication Request fra App’en.
4. Authorization Servicen indhenter Brugerens accept til, at App’en kan tilgå de data (scopes), der er angivet i OpenID requestet. Herefter detekterer Authorization Servicen, at der tale om en ny bruger (ingen session cookie i browseren) og danner derfor et SAML Authentication Request mod en ekstern SAML IdP (sendes også via HTTP Redirect).
5. Brugeren autentificerer sig mod IdP’en.
6. IdP’en danner et SAML Response indeholdende brugerens attributter og sender browseren tilbage til Authorization Service endepunktet (HTTP POST).
7. Authorization Servicen verificerer den modtagne SAML Assertion fra IdP’en og persisterer brugerinformation. Herefter sendes med et browser redirect et OpenID Connect svar til klientens angivne modtageradresse (redirect\_uri), der bl.a. indeholder en autorisationskode.
8. App’en kalder Token Servicen og veksler her den modtagne autorisationskode til et OpenID Connect ID token samt access-token.
9. App’en validerer det modtagne ID token og kan herefter udtrække basale brugerattributter fra dette. Access tokenet kan nu benyttes til at kalde back-end API’er og få adgang til brugerens data i overensstemmelse med de scopes, som brugerne har autoriseret.

Ovenstående scenarie fungerer isoleret, men en væsentlig begrænsning er dog, at en konkret app autoriseres mod et konkret API, og at udstedelsen af tokenet typisk ikke sker af en fælles tillidstjeneste men af en ‘Authorization Server’, der er lokal for API’et. Forretningstjenesten er i mangel af fællesoffentlige komponenter tvunget til at etablere sin egen autorisationsserver (som tillidstjeneste), og de tekniske valg (fx tokenformat) for integrationen mellem app og API er typisk proprietære. Mønstret skalerer således ikke til føderationer, hvor apps skal tilgå forskellige back-ends, og standarderne på området understøtter heller ikke direkte, at app’ens backend kan kalde videre til andre API’er via princippet om identitetsbaserede services. Der foregår pt. internationalt standardiseringsarbejde på dette område i regi af IETF (se fx ‘OAuth 2.0 Token Exchange’ [29]), men standarden foreligger endnu kun som ‘draft’ og vil endvidere kræve væsentlig profilering (tilsvarende OIO IDWS [24]), før den er anvendelig og interoperabel i fællesoffentligt regi.

Der er således behov for videreudvikling af en arkitektur omhandlende brugerstyring for apps, der understøtter følgende forretningsbehov:

* Interoperabilitet gennem fælles standarder/profiler som sikrer at apps (serviceanvendere), API’er (serviceudstillere) og tillidstjenester (autorisationsservere og STS’er) udviklet af forskellige parter sømløst kan interagere med hinanden i et økosystem.
* Fælles trust model for hvordan apps autoriseres til at kalde API’er.
* Understøttelse af delegeringer og identitetsbaserede kald på tværs af API’er.
* Mulighed for konsolideret overblik for slutbrugere over deres apps og styring af afgivne samtykker til at apps kan tilgå deres data.

Ovenstående forretningsbehov vurderes at kunne blive opfyldt på et teknisk plan gennem udvikling af en række specifikationer og fællesoffentlige komponenter:

* Profilering af mobil-egnede tokens baseret på JWT, PASETO eller tilsvarende, herunder krav til attributter såvel som sikkerhedsmæssige egenskaber i form af signering, kryptering mv. Profilen skal modsvare de nuværende OIO profiler for SAML tokens i form af ‘OIO SAML Profile for Identity Tokens’ og ‘OIOSAML Web SSO Profile’.
* Etablering af model for at udtrykke ‘scopes’ i tokens på en interoperabel måde samt håndtering af Sikringsniveauer (NSIS) [18].
* Model for håndtering af SSO, sessioner samt fornyelse, revokering og omveksling af tokens.
* Etablering af fællesoffentlig Security Token Service (STS) som kan udstede tokens i henhold til ovenstående (HTTP/JSON) profiler på baggrund af en trust model underlagt veldefineret governance. Denne er en pendant til NemLog-in’s eksisterende STS, som i dag understøtter udstedelse af OIO IDWS tokens (SAML) gennem WS-Trust protokollen målrettet til SOAP-baserede web service klienter (WSC’er).
* Etablering af en administrationskomponent, hvor klienter og API’er til den nye STS kan administreres.
* Etablering af en brugergrænseflade (‘Mine apps’), hvor slutbrugere kan få et overblik over de apps, de har autoriseret til at tilgå deres (offentlige) data, samt let kan fjerne adgangen for alle apps på en given enhed til brug for situationer, hvor en enhed er mistet. Spærringsfunktionen bør endvidere være understøttet af fællesoffentlig support, idet en mistet mobil enhed samtidig kan bremse brugerens mulighed for at logge ind på en hjemmeside, hvis brugeren anvender sin enhed til NemID/MitID autentifikation.
* Etablering af fælles politikker for caching af data i apps, levetid for tokens, håndtering af brugersamtykker mv.

Uden ovenstående specifikationer og byggeblokke er der risiko for, at understøttelsen af apps sker gennem isolerede implementeringer, hvor hver applikation etablerer egne byggeblokke og tillidstjenester i mangel på en fælles model. Dette kan føre til manglende sammenhæng og interoperabilitet samt uens brugeroplevelser og sikkerhedsniveauer.

## Digitale fuldmagter

En komponent til digitale fuldmagter gør det muligt for borgere og virksomheder at lade en repræsentant agere på deres vegne i en forretningstjeneste. 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.

Som for øvrige områder af brugerstyring er det uhensigtsmæssigt, hvis den enkelte forretningstjeneste etablerer sin egen fuldmagtsløsning. Dette ville medføre, at brugerne taber overblikket over afgivne eller modtagne fuldmagter, og at muligheden for at danne tværgående fuldmagter reduceres. Der er derfor etableret en fællesoffentlig fuldmagtsløsning 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 det i 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 [19], 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 dataafgrænsninger i kombination med rollen, hvilket kunne udtrykke mere finkornede og præcise fuldmagter (fx ”se sagsnr. AZ-7291”). Fuldmagtløsningen skal med andre ord også respektere dataafgrænsninger, som beskrevet i afsnittet om adgangskontrol.

## Områder for standardisering

### Eksisterende standarder

En vigtig del af referencearkitekturen er at udpege hvilke områder, der skal være omfattet af standarder, for at referencearkitekturen fungerer. Der er gennem de seneste 12 års arbejde med fællesoffentlig brugerstyring etableret fællesoffentlige standarder og profiler inden for en række områder, som succesfuldt har bidraget til interoperabilitet, øget modenhed og fælles løsninger. De væsentligste eksisterende standarder er:

* National Standard for Identiteters Sikringsniveauer[18], som definerer et tillidsrammeværk for digitale identiteter som dækker fysiske personer, juridiske enhender og fysiske personer associeret med en juridisk enhed.
* OCES certifikatpolitikkerne[21] og deres afløsere[35], som definerer formater og sikkerhedskrav til certifikater dækkende privatpersoner (POCES), medarbejdere (MOCES), juridiske enheder (VOCES) og systemer (FOCES).
* OIOSAML Web SSO profilerne som definerer protokol og billetformat i forbindelse med browser-baseret adgang til web appliationer, herunder single sign-on.
* OIO Basic Privilege Profile som definerer hvordan rettigheder og roller kan udtrykkes i et token herunder ved brug af delegering (fx til brug i fuldmagter) og dataafgrænsninger.
* OIO IDWS familien af profiler[24], som definerer protokol og billetformat til brug ved udstilling og kald af identitetsbaserede web services.

### Behov for nye fællesoffentlige standarder

Som tidligere beskrevet er der en række områder, hvor der fællesoffentligt er behov for yderligere profiler og standarder med henblik på at sikre synergi og interoperabilitet. Der er behov for:

* yderligere standarder til beskrivelse af attributters kvalitet, så adgangsbeslutninger som tages på baggrund af attributter kan kvalificeres yderligere.
* fælles arkitektur, standarder og datamodeller for håndtering af samtykke, herunder så samtykker kan udveksles på tværs.
* profilering af mobil-egnede tokens baseret på JWT, PASETO eller tilsvarende samt protokoller til token-udstedelse baseret på fx OpenID Connect[28]. De nuværende OIO SAML profiler[19] er baseret på XML og SOAP og ikke velegnede til mobile anvendelser.
* en model til at udtrykke rettigheder (‘OAuth2.0 scopes’) i tokens på en interoperabel måde i JSON baserede tokens svarende til OIO BPP profilen.

Derudover kan der i takt med fremkomsten af nye autentifikationstjenester blive behov for yderligere arbejde omkring discovery og orkestrering af tillidstjenester. Dertil kommer naturligvis behov for en række domænespecifikke standarder og underprofiler. Et eksempel på sidstnævnte er IDWS XUA profilerne udviklet til sundhedsområdet, som bl.a. definerer en række attributter for sundhedsfaglige personers autorisationer, roller, patientrelationer mv.

Endelig vurderes det, at der kan blive behov for yderligere vejledning og standarder for kommunikation mellem føderationer, når erfaringerne med interføderation udbredes - et eksempel kunne være best-pratice for billetomveksling. Der er allerede arbejdet i EU-regi (STORK [36] og eIDAS [8]) med interføderation baseret på SAML, og i dansk regi er der planlagt piloter mellem kommunerne (KOMBIT’s adgangsstyring [37]) og Sundhedsvæsenets Elektroniske Brugerstyring (SEB) [38].



Figur 20 Kommunikation mellem føderationer

### Igangværende standardisering internationalt

En række internationale standardiseringsorganisationer er i gang med at udarbejde nye standarder, som kan påvirke denne referencearkitektur. I dette afsnit gives en introduktion til nogle få af disse, uden at oversigten på nogen måde kan siges at være udtømmende. Der er i gennemgangen prioriteret standarder, som ikke er domæne- eller industrispecifikke, og som vil have potentiale til at blive anvendt eller profileret fællesoffentligt, når behov og modenhed er tilstrækkelig udtalt.

#### Decentraliseret brugerstyring og -ID’er

Standardiseringsorganisationen W3C, som er kendt fra en række internetstandarder, har en arbejdsgruppe, som arbejder med såkaldte decentralized identifiers eller DIDs. Gruppen har udgivet et udkast til en standard, som specificerer datamodel og syntaks for DIDs [39], som har status som ‘W3C Working Draft’.

Standarden er en central brik i forhold til skabe standardisering og interoperabilitet inden for den bredere bevægelse som kan kaldes decentraliseret brugerstyring (‘decentralized identity management’), som ikke bygger på centrale autoriteter (fx tillidstjenester eller centrale registre) men i stedet benytter en mere decentral arkitektur ofte baseret på blockchains, distributed ledger technology (DLT) og lignende teknologier. Her bruges alternative mekanismer til at skabe tillid, herunder de egenskaber som en blockchain tilvejebringer. En anden karakteristisk egenskab er, at brugerne tager en mere aktiv rolle i håndtering af deres identiteter (‘brugercentrisk identity management’), herunder kan skabe så mange uafhængige identiteter som ønskes af fx privatlivshensyn.

En DID er basalt set en URL som relaterer et ‘DID subject’ til et ‘DID dokument’ på en måde der giver mulighed for troværdige interaktioner med subjektet (brugeren). Et DID dokument kan fx beskrive offentlige nøgler, som DID subjektet (og tilhørende services) kan bruge til at autentificere sig med, og beskrive serviceendepunkter, som kan benyttes til at interagere med DID subjektet. Hensigten med standardiseringen er at specificere syntaks (DID scheme) og et generisk sæt af operationer på DID dokumenter. Ved at publicere et DID dokument på en blockchain kan brugere på en generisk måde specificere, hvordan en bestemt identitet kan autentificeres.

Generelt har den fællesoffentlige brugerstyring tilhørt den traditionelle skole baseret på centrale autoriteter og -tillidstjenester, som sammenbindes gennem føderationer. Den decentrale brugerstyring er dog et interessant nyt paradigme, som vil blive observeret efterhånden som området modnes og standarderne færdiggøres. De to paradigmer kan godt forenes, eksempelvis kan klassiske identiteter og identifikationsmidler fra en centraliseret model udstilles som decentrale identifiers.

#### IoT initiativer

1. Kilder og baggrundsmateriale

Nedenstående liste viser kilder og baggrundsmateriale, der henvises til i Referencearkitektur for brugerstyring version 1.1. Links er verificeret i januar 2020.

| **Nr.** | **Kilde** | **Materiale** |
| --- | --- | --- |
| 1 | Regeringen, KL, Danske Regioner | Den Fælles Offentlige Digitaliseringsstrategi 2016-2020, https://digst.dk/strategier/digitaliseringsstrategien/ |
| 2 | Digitaliseringsstyrelsen | En digitalt sammenhængende offentlig sektor: Hvidbog om arkitektur for digitalisering, juni 2017, https://arkitektur.digst.dk/node/241 |
| 3 | Digitaliseringsstyrelsen | Referencearkitektur for brugerstyring version 1.0, april 2017, https://arkitektur.digst.dk/node/123 |
| 4 | Digitaliseringsstyrelsen | Fællesoffentlige regler for begrebs- og datamodellering Version 2.0., marts 2019, https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/modelregler-v-20 |
| 5 | Regeringen, KL, Danske Regioner | Digitaliseringspagten, marts 2019, https://digst.dk/strategier/digitaliseringspagten/ |
| 6 | Europakommissionen | European Interoperability Reference Architecture (EIRA), https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/about |
| 7 | Digitaliseringsstyrelsen | Den fællesoffentlige digitale arkitektur (FDA), https://arkitektur.digst.dk/ |
| 8 | Europaparlamentet og Rådet | eIDAS-forordningen, Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF, https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX%3A32014R0910 |
| 9 | Digitaliseringsstyrelsen | Beskrivelse af det dobbelte frivillighedsprincip på Digitaliseringsstyrelsens hjemmeside, https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/fra-det-eksisterende-til-det-kommende-nemlog-in/nye-erhvervsidentiteter-det-dobbelte-frivillighedsprincip/ |
| 10 | Digitaliseringsstyrelsen | Fællesoffentlig strategi for brugerstyring, april 2017, https://arkitektur.digst.dk/node/123 |
| 11 | Folketinget | Lov nr. 439, Lov om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder, https://www.retsinformation.dk/eli/lta/2018/439 |
| 12 | Folketinget | Lov nr. 617 Lov om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked, https://www.retsinformation.dk/Forms/R0710.aspx?id=180237 |
| 13 | Europaparlamentet og Rådet | Databeskyttelsesforordningen. Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32016R0679 |
| 14 | Folketinget | Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven), https://www.retsinformation.dk/Forms/r0710.aspx?id=201319 |
| 15 | Folketinget | LBK nr. 433 af 22/04/2014 Bekendtgørelse af forvaltningsloven, https://www.retsinformation.dk/forms/r0710.aspx?id=161411 |
| 16 | ISO/IEC | ISO/IEC 27001:2017 Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Krav, https://webshop.ds.dk/da-dk/standard/ds-en-iso-iec-270012017 0 |
| 17 | Digitaliseringsstyrelsen og Erhvervsstyrelsen | Vejledninger og skabeloner til ISMS, https://sikkerdigital.dk/myndighed/forstaa-arbejdet-med-informationssikkerhed/vejledninger-og-skabeloner/ |
| 18 | Digitaliseringsstyrelsen | National Standard for Identiteters Sikringsniveauer (NSIS), version 2.0.1, oktober 2019, https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/nsis-standarden/ |
| 19 | Digitaliseringsstyrelsen | OIOSAML Web SSO Profile 3.0, oktober 2019, https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/oiosaml-30/ |
| 20 | Regeringen | National strategi for cyber- og informationssikkerhed, april 2018, https://digst.dk/strategier/cyber-og-informationssikkerhed/ |
| 21 | Digistaliseringsstyrelsen | OCES-certifikatpolitikker, https://digst.dk/it-loesninger/nemid/om-loesningen/oces-standarden/oces-certifikatpolitikker/ |
| 22 | Digitaliseringsstyrelsen | OIOSAML, https://www.digitaliser.dk/group/42063/resources |
| 23 | The Internet Engineering Task Force (IETF) | JSON Web Token (JWT) rfc 7519, https://tools.ietf.org/ |
| 24 | Digitaliseringsstyrelsen | OIO IDWS, https://digitaliser.dk/resource/526486 |
| 25 | Oasis | WS-Security Policy, http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html |
| 26 | Oasis | XACML, https://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=xacml |
| 27 | The Internet Engineering Task Force (IETF) | OAuth 2.0 Authorization Framework rfc 6749, https://digitaliser.dk/resource/1246357 |
| 28 | OpenID Foundation | OpenID Connect Core 1.0, https://openid.net/specs/openid-connect-core-1\_0.html |
| 29 | The Internet Engineering Task Force (IETF) | OAuth 2.0 Token Exchange, https://tools.ietf.org/html/draft-ietf-oauth-token-exchange-19 |
| 30 | Kantara Inititative | Kantara Identity Insurance Framework, https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework |
| 31 | Kantara Inititative | User-Managed Access (UMA), https://kantarainitiative.org/confluence/display/uma/Home |
| 32 | ISO | ISO 29115, Information technology - Security techniques - Entity authentication assurance framework, https://www.iso.org/standard/45138.html |
| 33 | KL | KL Emnesystematik, kle-online.dk |
| 34 | Digitaliseringsstyrelsen | FORM-online, https://arkitektur.digst.dk/node/470 |
| 35 | Digitaliseringsstyrelsen | Certifikatpolitikker udarbejdet af Digitaliseringsstyrelsen, certifikat.gov.dk |
| 36 | Europa-Kommissionen | STORK, https://joinup.ec.europa.eu/solution/stork |
| 37 | KOMBIT | Det fælleskommunale Støttesystem Adgangsstyring, https://www.kombit.dk/indhold/adgangsstyring |
| 38 | Sundhedsdatastyrelsen | Sundhedsvæsenets Elektroniske Brugerstyring, https://services.nsi.dk/seb |
| 39 | W3C | Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/ |

1. Begrebsmodel

Begrebsmodellen findes i indeholdte Excel dokument.



|  |
| --- |
|  |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |
| digst.dk |