Klimadatastyrelsen

Identitetsnøgle og brugerrejse

Indhold

1. Fælles forudsætninger 3

2. Identitetsmodel A: Eksisterende identifikation 6

3. Identitetsmodel B: MitID UUID som identitetsnøgle 7

4 Identitetsmodel C: CPR for privatkunder og CVR for virksomheder .. 10

5. Adresse som udgangspunkt for identifikation ved komplekst samtykke 12

6 opsamling 14

Resume
Notatet beskriver, hvordan en digital samtykkeløsning for forsyningsdata kan identificere den samtykkekompetente, samt koble denne til det korrekte kundeforhold, adresse og målepunkt. Der gennemgås fire identitetsmodeller (kundenumre, MitID UUID, CPR/CVR og adresse) i tre infrastrukturscenarier (decentral, sektorfælles og statslig national).

I den decentrale løsning kan koblingen mellem samtykkegiver, kundeforhold og målepunkt håndteres lokalt hos forsyningen eller systemleverandøren. I den sektorfælles og den statslig nationale løsning er der derimod behov for en fælles identitetsmodel, der kan fungere på tværs af forsyninger, samtykkeløsningen og den fælles infrastruktur. Her vil eksisterende identifikation som kundenumre ikke være egnede som fælles identitetsnøgle, da de er forsyningsspecifikke og ikke nødvendigvis entydige på tværs af systemer.

Samlet peger notatet på, at UUID-modellen vurderes til at være den mest hensigtsmæssige model i både den sektorfælles og den statslig nationale løsning. UUID er en teknisk entydig identifikator, som kan anvendes på tværs af systemer uden behov for behandling af CPR-oplysninger, som vil kræve særskilt hjemmel til forsyningernes behandling og registrering af oplysningerne. CVR for erhvervskunder kan dog være den mest hensigtsmæssige identitetsnøgle til kundeforholdet, da CVR identificerer virksomheden frem for den enkelte bruger.

Klimadatastyrelsen

Sankt Kjelds Plads 11
2100 København Ø

T: 72 54 55 00
E: kds@kds.dk

www.kds.dk

Indledning
Et digitalt samtykkeflow forudsætter, at løsningen med tilstrækkelig sikkerhed kan dokumentere, hvem der afgiver samtykket. Et kundenummer eller lignende kan bidrage til at koble en bruger til et kundeforhold, men dokumenterer ikke i sig selv brugerens identitet. Der er derfor behov for en digital identifikations- og autentifikationsløsning.

Den tekniske problemstilling består således af to separate elementer:
- Identifikation og autentifikation af den person, der afgiver samtykke.
- Kobling af den autentificerede identitet til det relevante kundeforhold, den relevante adresse og det relevante målepunkt.

MitID og MitID Erhverv kan anvendes til autentifikation, fordi løsningerne giver en sporbar og dokumenterbar autentifikation af henholdsvis privatpersoner og personer, der handler på vegne af virksomheder. MitID løser dermed autentifikationen, men etablerer ikke nødvendigvis koblingen mellem identiteten og det konkrete kundeforhold eller målepunkt.

Forsyningerne anvender i dag typisk lokale identifikatorer, såsom kundenummer, til at koble en kunde til et kundeforhold i egne kundesystemer. Kundenummeret kan fortsat anvendes som intern identifikator, men er ikke egnet som en fælles identitetsnøgle på tværs af en samtykkeløsning, en fælles sektor- eller national løsning og flere forsyninger. Det skyldes blandt andet, at kundenumre er lokalt definerede, ikke nødvendigvis er entydige på tværs af forsyninger og ikke har en fælles eller standardiseret struktur.

Hvis en fælles løsning skal kunne skaleres, kræver det derfor en fælles identitetsnøgle, som kan anvendes til at koble den autentificerede identitet fra MitID med forsyningernes stamdata. Identitetsnøglen skal fungere som forbindelsespunkt mellem samtykkeløsningen, den fælles løsning og forsyningernes kundesystemer, mens forsyningerne fortsat kan anvende egne interne identifikatorer i deres interne processer.

Forsyningerne har i dag stamdata om kunder, adresser og målepunkter, som primært anvendes til fakturering. Kundesystemerne indeholder derfor typisk oplysninger om kundeforholdet, herunder koblingen mellem kunde, adresse og målepunkt. Forsyningerne har derimod ikke en fælles kobling mellem digital identitet, adresse og målepunkt, som kan anvendes på tværs af aktører ved dataudlevering.
Det centrale spørgsmål er derfor, hvilken identitetsnøgle der skal anvendes til at skabe sammenhæng mellem den samtykkekompetente og forsyningens stamdata.
I de tre infrastrukturscenarier håndteres denne kobling overordnet på to måder:

- **Scenarie 1 – decentral model**: Den enkelte forsyning eller systemleverandør håndterer identifikation og dataudlevering direkte.

- **Scenarie 2 og 3 – centrale modeller**: En fælles sektor- eller national løsning identificerer den relevante forsyning og formidler samtykke og dataudlevering.

I dette afsnit anvendes betegnelsen den fælles løsning om de funktioner i sektor- eller den nationale løsning, der identificerer den relevante forsyning, sammenholder identitetsoplysninger med stamdata og formidler den autoriserede anmodning. Der er således ikke tale om et selvstændigt infrastrukturscenarie, men om funktioner inden for scenarie 2 og 3.

Inden for de centrale infrastrukturscenarier behandles følgende identitetsmodeller:

- Eksisterende identifikation: Forsyningerne integrerer til den fælles løsning, men anvender fortsat deres eksisterende identifikationsmekanismer, eksempelvis kundenummer.
- MitID UUID som identitetsnøgle: UUID fra MitID anvendes som den fælles identitetsnøgle mellem MitID, den fælles løsning og forsyningernes kundesystemer.
- CPR/CVR som identitetsnøgle: MitID anvendes fortsat til autentifikation, mens CPR eller CVR udgør den fælles identitetsnøgle mellem den fælles løsning og forsyningernes stamdata.

Ved komplekst samtykke behandles desuden en adressebaseret model, hvor den fælles løsning tager udgangspunkt i en adresse og relevante registeropslag for at identificere den samtykkekompetente personkreds.

Decentral håndtering i scenarie 1
I den decentrale model findes der ikke et centralt opslagsværk, som kan identificere den relevante forsyning. Den enkelte forsyning kan derfor fortsat anvende eksisterende og lokale identifikationsmekanismer, eksempelvis kundenummer, da identifikation og autentifikation sker lokalt hos den enkelte forsyning eller systemleverandør. Der er således ikke samme behov for en fælles identitetsnøgle, fordi identitetsoplysningerne ikke skal kunne anvendes på tværs af flere forsyninger og en fælles løsning. Den decentrale håndtering er beskrevet som en del af infrastrukturscenarie 1 og behandles derfor ikke yderligere i dette afsnit.

1. Fælles forudsætninger
Uanset infrastrukturscenarie og valg af identitetsmodel er der en række tekniske forudsætninger, som skal være opfyldt, for at et digitalt samtykkeflow kan fungere. Alle de behandlede identitetsmodeller forudsætter, at den samtykkekompetente autentificeres med MitID eller MitID Erhverv. MitID anvendes dermed til at sikre, at den person, der afgiver samtykke, er korrekt autentificeret. Forskellen mellem identitetsmodellerne består i, hvilke identitetsoplysninger der anvendes efter autentifikationen til at identificere den samtykkekompetente og knytte vedkommende til det relevante kundeforhold og målepunkt.

Ved behov kan løsningen anmode om yderligere identitetsoplysninger fra MitID. For privatpersoner kan CPR-nummer indhentes som en del af den eksisterende MitID-session, hvis løsningen har behov for denne oplysning. CPR og CVR returneres ikke automatisk ved et MitID-login, men kræver en særskilt anmodning.
Der er forskel på, hvilke identitetsattributter der kan modtages, afhængigt af om løsningen anvendes i en offentlig eller privat kontekst.

De offentlige løsninger kan som udgangspunkt i højere grad automatisk modtage flere identitetsoplysninger automatisk gennem NemLog-in, end private løsninger. Oplysninger såsom CPR kræver derfor i flere tilfælde en særskilt anmodning eller et specifikt opslag.

De følgende tabeller giver et overblik over de relevante identitetsattributter for henholdsvis privatpersoner og erhvervsbrugere, samt hvilke oplysninger der returneres automatisk, og hvilke der kan efterspørges.

Skema for identitetsattributter for Privat MitID

Oplysning	Beskrivelse	Returneres automatisk
UUID	Et unikt teknisk ID, der identificerer brugeren til genkendelse ved senere login.	**Ja**
Authentication Assurance Level (AAL)	Angiver sikkerhedsniveauet for den gennemførte autentifikation.	**Ja**
Identity Assurance Level (IAL)	Angiver sikkerhedsniveauet for identitetskontrollen bag MitID.	**Ja**
Level of Assurance (LOA/ACR)	Samlet sikkerhedsniveau for identiteten og login'et.	**Ja**
MitID autentifikationsmetode (AMR)	Viser hvilken autentifikationsmetode der blev anvendt (fx MitID-app, kodeviser).	**Ja**
MitID Transaktions-ID	Unikt ID for den konkrete logintransaktion.	**Ja**
Reference tekst	Den reference/state, som løsningen eventuelt har sendt med login-anmodningen.	**Ja**
CPR-nummer	CPR-nummer.	**Offentlig: Nej**, *forudsætter at tjenesten er oprettet med CPR-rettighed i NemLog-in Administrationen* **Privat: Nej,** her skal systemet aktivt efterspørge/scope CPR-ved hvert login.
Adresse	Virksomhedsens adresse.	**Nej**, modtages ikke.

Skema for identitetsattributter for MitID Erhverv og MitID Privat til Erhverv.

Oplysning	Beskrivelse	Returneres automatisk
UUID	Unikt ID for virksomheden/medarbejderen.	**Ja**
Authentication Assurance Level (AAL)	Angiver sikkerhedsniveauet for den gennemførte autentifikation.	**Ja**
Identity Assurance Level (IAL)	Angiver sikkerhedsniveauet for identitetskontrollen bag MitID.	**Ja**
Level of Assurance (LOA/ACR)	Samlet sikkerhedsniveau for identiteten og login'et.	**Ja**
CVR	Virksomhedens CVR-nummer.	**Offentlig:** Ja. **Privat: Nej**, skal efterspørges ved Privat til Erhverv) / Ja, ved MitID Erhverv.
Virksomhedsnavn	Virksomhedsnavn.	**Offentlig:** Ja. **Privat: Nej**, Navnet på den organisation, som brugeren er autoriseret til at repræsentere. Feltet vises kun, når man bruger Privat MitID til at logge ind som repræsentant for en virksomhed.
Rettigheder	Medarbejderens delegerede rettigheder, fx i Virk/Digital Post.	**Offentlig:** Ja, hvis rettigheder findes **Privat:** Nej, skal efterspørges.
MitID Transaktions-ID	Unikt ID for den konkrete login-transaktion.	**Ja** (returneres som udgangspunkt ikke ved rene erhvervsidentiteter).
Virksomhedens adresse	Medarbejderens private bopælsadresse.	**Nej,** modtages ikke.

Fælles procesforløb i scenarie 2 og 3 ved simpelt samtykke

Valget mellem UUID og CPR/CVR ændrer ikke den overordnede brugerrejse, når der er tale om simpelt samtykke. I begge identitetsmodeller logger brugeren ind med MitID, og samtykket afgives på samme måde. Forskellen består i, hvilke identitetsoplysninger der udveksles mellem MitID, samtykkeløsningen og den fælles løsning, samt hvilken identitetsnøgle der fremgår af forsyningernes stamdata.

Brugerrejsen er beskrevet nedenfor:

1. Kunden indgår en aftale med en tredjepart om deling af forbrugsdata.

2. Tredjeparten anmoder den fælles løsning om adgang til kundens forbrugsdata, eksempelvis med udgangspunkt i en adresse.
3. Den fælles løsning identificerer på baggrund af de stamdata, som forsyningerne har stillet til rådighed, hvilken forsyning der betjener kunden, og hvilket kundeforhold, hvilken adresse og hvilket målepunkt anmodningen vedrører.
4. På baggrund af stamdataene initierer den fælles løsning et samtykkeforløb ved at fremsende de nødvendige oplysninger til samtykkeløsningen med henblik på at oprette samtykket.
5. Den samtykkekompetente person logger ind med MitID eller MitID Erhverv og afgiver samtykke.
6. Samtykkeløsningen returnerer oplysninger om den autentificerede identitet til den fælles løsning, herunder enten CPR/CVR eller UUID.
7. Den fælles løsning validerer brugerens identitet og sammenholder identitetsoplysningen fra MitID eller MitID Erhverv med den identitetsnøgle, som fremgår af stamdataene.
8. Hvis identitetsvalideringen er gennemført, registreres samtykket som gyldigt, og den fælles løsning autoriserer anmodningen om dataudlevering. Hvis identiteten ikke kan kobles til stamdataene, afvises anmodningen, og data udleveres ikke.
9. Forsyningen modtager den autoriserede anmodning og udleverer de relevante forbrugsdata til den fælles løsning.
10. Den fælles løsning viderestiller forbrugsdataene til tredjeparten i overensstemmelse med det afgivne samtykke.

2. Identitetsmodel A: Eksisterende identifikation

I denne identitetsmodel integrerer forsyningerne til den fælles løsning, men fortsætter med at anvende deres eksisterende identifikationsmekanismer til at koble brugeren til et kundeforhold, eksempelvis kundenummer eller andre lokale identifikatorer.

Modellen har den fordel, at den i høj grad bygger videre på eksisterende løsninger og kræver begrænsede ændringer i forsyningernes kundesystemer. Forsyningerne kan fortsat anvende de identifikatorer, som allerede indgår i deres interne processer, og der etableres ikke behov for at indføre en ny fælles identitetsmodel.

Modellen er dog ikke egnet som grundlag for en fælles og skalerbar samtykkeløsning på tværs af forsyninger. De eksisterende identifikatorer er udviklet til lokale formål og varierer mellem forsyningerne. Et kundenummer er eksempelvis kun meningsfuldt inden for den enkelte forsynings kundesystem og kan derfor ikke anvendes som en fælles identitetsnøgle. Derudover identificerer kundenummeret typisk et kundeforhold, men dokumenterer ikke i sig selv, hvilken fysisk eller juridisk person der er berettiget til at afgive samtykke. Det vil i princippet være muligt at lade brugeren angive et kundenummer og vælge den relevante forsyning ved login. En sådan model vil dog betyde, at brugeren selv skal identificere hvert enkelt kundeforhold. Hvis identifikationen i stedet baseres på eksempelvis UUID eller CPR/CVR, vil løsningen kunne identificere brugerens samlede kundeforhold og målere på tværs af forsyninger.

Der er også en praktisk udfordring ved at anvende kundenummer som identifikator. Kundenumre er ikke nødvendigvis unikke på tværs af forsyninger, og et kundenummer kan derfor ikke alene identificere et kundeforhold entydigt.

Modellen vurderes derfor ikke at være egnet som fælles identitetsmodel i scenarie 2 og 3 og behandles ikke yderligere.

3. Identitetsmodel B: MitID UUID som identitetsnøgle

I denne identitetsmodel for simpelt samtykke anvendes UUID fra MitID som den fælles identitetsnøgle mellem MitID, den fælles løsning og forsyningernes stamdata. MitID anvendes således både til autentifikation og som kilde til den identitetsnøgle, der anvendes efter autentifikationen.

Når en bruger logger ind med MitID eller MitID Erhverv, returneres som minimum et unikt bruger-ID, UUID, samt oplysninger om den gennemførte autentifikation, herunder sikkerhedsniveau og den anvendte autentifikationsmetode.

For at UUID'et kan bruges til at give adgang til forbrugsdata, skal der være etableret en sammenhæng mellem:

kunden → kundens UUID → kundeforholdet → den relevante måler.

Denne kobling kan overordnet etableres på to måder:

Mulighed 1 - koblingen etableres i den fælles løsning

Første gang kunden logger ind i den fælles løsning med MitID, vælger kunden den relevante forsyning og angiver eksempelvis et kundenummer eller en kode fra regningen. På baggrund af de stamdata, som forsyningen stiller til rådighed, kan den fælles løsning kontrollere, hvilket kundeforhold og hvilke målere oplysningerne vedrører.

Når oplysningerne er valideret, gemmer den fælles løsning koblingen mellem kundens UUID, kundeforholdet og de tilknyttede målere. Kunden behøver herefter ikke at gennemføre samme kobling igen for det pågældende kundeforhold.

Fordelen ved denne mulighed er, at forsyningerne ikke på forhånd behøver at have registreret UUID på alle deres kunder. De kan i højere grad bygge videre på de kundenumre, koder og stamdata, som allerede findes i deres systemer. Det reducerer behovet for at ændre forsyningernes kundesystemer og for at gennemføre en særskilt MitID-onboarding af hele den eksisterende kundebase.

Ulempen er en mere manuel brugerrejse for kunden**.** Den fælles løsning kender ved første login kundens UUID, men UUID'et findes ikke nødvendigvis i forsyningernes stamdata. Løsningen har derfor ikke en fælles nøgle, som den kan bruge til automatisk at søge på tværs af forsyningerne og finde alle kundens kundeforhold.

Kunden skal i stedet selv anvise det relevante kundeforhold, fx ved at vælge forsyning og indtaste kundenummer eller kode.

Hvis kunden eksempelvis har vand hos én forsyning, fjernvarme hos en anden og et sommerhus hos en tredje, skal de forskellige kundeforhold som udgangspunkt kobles særskilt. Hvis ét kundenummer eller omfatter flere målere hos samme forsyning, kan disse dog godt kobles samlet, hvis forsyningens stamdata understøtter det.

Derudover skal den centralt gemte kobling holdes ajour, når en kunde fx flytter, et kundeforhold ophører, eller målere ændres.

Mulighed 2 - koblingen etableres på forhånd hos forsyningen
Forsyningen har på forhånd etableret og vedligeholder koblingen mellem kundens UUID, kundeforhold og måler. Koblingen stilles sammen med de øvrige relevante stamdata til rådighed for den fælles løsning.

Når kunden senere logger ind med MitID, kan den fælles løsning anvende UUID direkte til at fremsøge de kundeforhold og målepunkter, hvor samme UUID allerede er registreret. Kunden behøver derfor ikke selv at angive forsyning eller kundenummer for hvert kundeforhold.

Fordelen er en mere sammenhængende og automatiseret brugerrejse. Ulempen er, at forsyningerne skal kunne registrere og vedligeholde UUID i deres kundesystemer, herunder etablere koblingen for eksisterende kunder og holde den opdateret ved ændringer i kundeforhold. Det stiller større krav til systemtilpasninger, datakvalitet og ensartede processer hos forsyningerne.

For erhvervskunder skal modellen suppleres med en entydig kobling til den virksomhed, som brugeren repræsenterer, fx via CVR, da brugerens UUID ikke i sig selv identificerer virksomhedens kundeforhold.

MitID kan desuden udstille identitetsattributter, der angiver, om der er tale om en privatperson eller en virksomhedsrepræsentant. MitID Erhverv kan tilsvarende indeholde oplysninger om, hvilken virksomhed brugeren repræsenterer. Disse oplysninger kan anvendes som supplement til identitetsvalideringen, men ændrer ikke ved, at UUID udgør den primære identitetsnøgle i denne model.

Mulighed 3 – koblingen etableres ved første brug og registreres hos forsyningen
I denne variant etableres koblingen mellem kundens UUID, kundeforhold og målepunkt ved kundens første brug af samtykkeløsningen. Koblingen valideres af forsyningen via dens API, hvorefter UUID registreres hos forsyningen.
Fordelen ved denne mulighed er, at registreringen af UUID kan opbygges løbende, efterhånden som kunderne anvender løsningen. Dermed er der hverken behov for

at etablere et centralt register over koblingerne eller for at registrere UUID for hele kundebasen på forhånd.

De tre muligheder adskiller sig primært ved, hvor koblingen mellem UUID og kundeforhold etableres og vedligeholdes, samt hvornår registreringen finder sted.

Mulighed 1 indebærer, at koblingen etableres ved første brug og registreres i den fælles løsning. Mulighed 2 indebærer, at koblingen på forhånd etableres og vedligeholdes hos forsyningen. Mulighed 3 indebærer, at koblingen etableres ved første brug, men registreres og vedligeholdes hos forsyningen.

Der er endnu ikke foretaget en samlet vurdering af de ved de tre muligheder. Valget har blandt andet betydning for behovet for systemtilpasninger hos forsyningerne, etablering af fælles funktionalitet og fordelingen af ansvaret for at registrere, validere og ajourføre koblingen mellem UUID og kundeforhold. Det udestår derfor at afklare, hvilken af de tre muligheder der er mest hensigtsmæssig.

Tekniske forudsætninger for UUID
Anvendelsen af UUID som fælles identitetsnøgle forudsætter, at forsyningernes kundesystemer kan registrere og vedligeholde UUID som en del af deres stamdata. Der skal etableres en entydig kobling mellem UUID, kundeforhold og målepunkt, så den fælles løsning kan validere den autentificerede bruger, inden der autoriseres adgang til forbrugsdata.

Styrker ved modellen
Den største styrke ved modellen er, at UUID returneres automatisk ved autentifikation med MitID og MitID Erhverv og derfor kan anvendes som identitetsnøgle mellem MitID, den fælles løsning og forsyningernes systemer.

UUID identificerer den autentificerede identitet. For privatkunder vil dette som udgangspunkt svare til én fysisk person. For brugere i MitID Erhverv tildeles der én UUID pr. erhvervsidentitet. Den samme erhvervsidentitet kan autentificeres med forskellige identifikationsmidler, eksempelvis privat MitID eller et særskilt MitID, uden at UUID ændres. Det giver en dokumenterbar og sporbar identitetsmodel, hvor identiteten kan genkendes på tværs af loginmetoder og integrationer.

Da UUID ikke er et personnummer, understøtter modellen samtidig et dataminimeringsprincip, hvor der ikke sker behandling eller opbevaring af CPR-oplysninger i de involverede systemer.

Begrænsninger ved modellen
Den væsentligste begrænsning ved modellen vedrører håndteringen af virksomheder med flere samtykkekompetente brugere. For erhvervskunder identificerer UUID én erhvervsidentitet i MitID Erhverv. Hvis flere brugere skal kunne afgive samtykke

på vegne af det samme kundeforhold, skal det derfor afklares, hvordan de relevante erhvervsidentiteter kobles til virksomheden og kundeforholdet.

En ændring af det identifikationsmiddel, som den samme erhvervsidentitet anvender til autentifikation, ændrer derimod ikke UUID. Koblingen mellem erhvervsidentiteten, samtykket og forsyningens kundesystem påvirkes derfor ikke af selve valget af identifikationsmiddel.

Modellen forudsætter endvidere, at UUID registreres og vedligeholdes som en del af forsyningernes stamdata. Det vil kræve ændringer i den nuværende identitetsmodel, herunder at det fællesoffentlige samtykkeløsning *Digitalt Samtykke* ændres fra at identificere samtykkegivere ved hjælp af CPR til i stedet at anvende UUID som identitetsnøgle.

Opsummering
For *Digitalt Samtykke* indebærer modellen, at identifikation af den samtykkekompetente skal baseres på UUID frem for CPR.

For forsyningerne indebærer modellen, at UUID skal kunne registreres, vedligeholdes og anvendes som identitetsnøgle i kundesystemerne. Eksisterende integrationer skal samtidig kunne udstille UUID som en del af de stamdata, der stilles til rådighed for den fælles løsning. Modellen har den fordel, at den bygger på MitIDs standardfunktionalitet og derfor er teknisk relativt enkel at implementere. Samtidig undgås behovet for at indhente CPR- eller CVR-oplysninger som led i processen.

4 Identitetsmodel C: CPR for privatkunder og CVR for virksomheder

I denne identitetsmodel for simpelt samtykke anvendes MitID fortsat som autentifikationsløsning, mens CPR eller CVR udgør den fælles identitetsnøgle mellem MitID eller MitID Erhverv, den fælles løsning og forsyningernes kundesystemer. MitID anvendes således til autentifikation, mens den efterfølgende identitetsvalidering baseres på CPR eller CVR.

Forsyningen skal have registreret relevante oplysninger om CPR eller CVR for sine kunder og stille oplysningerne til rådighed for den fælles løsning. Når den samtykkekompetente logger ind med MitID eller MitID Erhverv, gennemføres autentifikationen på samme måde som i UUID-modellen.

MitID returnerer som standard UUID, men løsningen kan anmode om yderligere identitetsoplysninger, eksempelvis CPR eller CVR. For privatkunder kan CPR indhentes gennem MitID. Ved erhvervssamtykker kan virksomhedens CVR-nummer anvendes som identitetsnøgle.

Den fælles løsning anvender herefter CPR eller CVR til at kontrollere, at den autentificerede bruger kan kobles til det relevante kundeforhold og målepunkt. Valideringen sker ved at sammenholde de identitetsoplysninger, der returneres fra MitID

eller MitID Erhverv, med den identitetsnøgle, der er registreret i forsyningens stamdata. Hvis der er overensstemmelse mellem oplysningerne, kan den fælles løsning autorisere anmodningen om dataudlevering.

Tekniske forudsætninger
Anvendelsen af CPR eller CVR som identitetsnøgle forudsætter, at forsyningernes kundesystemer kan registrere og vedligeholde CPR eller CVR som en del af stamdataene, så oplysningerne kan anvendes ved identitetsvalideringen.

For privatkunder indebærer modellen, at løsningen skal kunne anmode MitID om CPR-oplysninger som led i den eksisterende MitID-session. CPR returneres ikke som standard og skal derfor indhentes særskilt.

Den samtykkekompetente vil dermed kunne blive bedt om at afgive den nødvendige oplysning som en del af den login-session, der allerede er påbegyndt. Den overordnede brugerrejse har derfor de samme trin som UUID-modellen. Modellen forudsætter desuden, at der er hjemmel til behandling og registrering af CPR-oplysninger i forsyningernes systemer, når CPR anvendes som identitetsnøgle.

Styrker ved modellen
For privatkunder giver CPR en entydig kobling mellem den autentificerede bruger og det relevante kundeforhold.

For erhvervskunder giver CVR mulighed for at identificere virksomheden frem for den enkelte medarbejder. Det betyder, at flere autoriserede virksomhedsrepræsentanter kan handle på vegne af samme virksomhed gennem MitID Erhverv, uden at forsyningen skal registrere og vedligeholde flere individuelle UUID'er på det samme kundeforhold.

Modellen understøtter dermed erhvervssituationer med flere autoriserede repræsentanter bedre end en UUID-baseret model, hvor identitetsnøglen er knyttet til den enkelte erhvervsidentitet.

Begrænsninger ved modellen
Modellen indebærer behandling af CPR-oplysninger, hvilket stiller krav til hjemmelsgrundlaget for, at forsyningerne kan behandle og registrere kundernes CPR-numre. Det er den umiddelbare vurdering, at vand- og fjernvarmeselskaber kan gives adgang til at anvende Digitalt Samtykke ved ny regulering i sektorlovgivningen. For at være i overensstemmelse med EU-retten, er det formegentlig nødvendigt at gøre det frivillig for forsyningsselskaberne at anvende Digitalt Samtykke.

Der udestår endvidere en række afklaringer om den konkrete implementering, herunder om indhentning af CPR kan ske som en del af det samlede samtykkeforløb, samt hvordan erhvervssamtykker og eventuelle notifikationer via Virk håndteres i praksis.

CPR eller CVR kan anvendes til at validere en identificeret person eller virksomhed. Identitetsnøglerne løser imidlertid ikke i sig selv opgaven med at identificere hele den relevante samtykkekreds ved komplekst samtykke. Dette kræver desuden de adresse- og registerbaserede funktioner, der beskrives i afsnit 7.5.

Opsummering
Anvendelsen af CPR eller CVR som fælles identitetsnøgle vil påvirke både den fælles samtykkeløsning og forsyningernes eksisterende systemlandskab.

For erhvervskunder kan modellen bygge videre på de eksisterende rettighedsstrukturer i MitID Erhverv, idet identitetsvalideringen tager udgangspunkt i virksomhedens CVR frem for den enkelte medarbejders identitet. Det kan reducere behovet for at registrere og vedligeholde flere individuelle identiteter på samme kundeforhold. For privatkunder forudsætter modellen, at der etableres det nødvendige grundlag for at indhente, registrere og anvende CPR som identitetsnøgle.

5. Adresse som udgangspunkt for identifikation ved komplekst samtykke

Ved komplekst samtykke kan adressen anvendes som udgangspunkt for at koble et målepunkt med de personer eller virksomheder, der kan afgive samtykke til udlevering af forbrugsdata.

Modellen adskiller sig fra UUID- og CPR/CVR-modellerne ved, at den fælles løsning ikke tager udgangspunkt i et allerede identificeret kundeforhold eller en kendt identitet. Den fælles løsning tager i stedet udgangspunkt i en adresse og identificerer de personer eller virksomheder, der har en relevant relation til den adresse, bygning eller boligenhed, som anmodningen vedrører.

Forsyningen skal ikke kende eller vedligeholde oplysninger om alle personer bag et målepunkt. Forsyningen skal i stedet stille stamdata og relationer til rådighed, så den fælles løsning kan identificere sammenhængen mellem adresse, bygning, installationspunkt og målepunkt.

Den fælles løsning kan derefter anvende oplysningerne til opslag i relevante registre og identificere de personer eller virksomheder, der er knyttet til adressen eller boligenheden, eksempelvis gennem CPR-registeret. De identificerede personer autentificeres herefter med MitID eller MitID Erhverv, så de kan afgive samtykke.

Adressen fungerer dermed som udgangspunkt for at finde den relevante samtykkekreds, mens MitID fortsat anvendes til autentifikation af den konkrete person, der afgiver samtykket.

Tekniske forudsætninger
Modellen forudsætter, at forsyningen kan stille stamdata til rådighed, som gør det

muligt at etablere en entydig sammenhæng mellem adresse, installationspunkt og målepunkt. Den fælles løsning skal anvende eksterne registre til at identificere de personer eller virksomheder, der har en relevant relation til adressen.

Identifikationen kræver adgang til relevante registre, som den fælles løsning skal kunne anvende til at finde de samtykkekompetente personer. Ansvarsfordelingen ændres samtidig, fordi opgaven med at identificere den relevante personkreds placeres i den fælles løsning frem for hos den enkelte forsyning.

Korrekte og vedligeholdte relationer mellem adresser, boligenheder og målepunkter er en nødvendig forudsætning for, at identifikationen bliver præcis. Mangelfulde relationer kan føre til, at den fælles løsning identificerer forkerte personer, eller at datadeling ikke kan finde sted.

Procesforløb ved adressebaseret identifikation
Procesforløbet adskiller sig fra de øvrige identitetsmodeller, fordi den relevante samtykkekreds skal identificeres, før samtykket kan oprettes og afgives.

- Kunden indgår en aftale med en tredjepart om deling af forbrugsdata.
- Tredjeparten anmoder den fælles løsning om adgang til kundens forbrugsdata, eksempelvis med udgangspunkt i en adresse.
- Den fælles løsning identificerer på baggrund af forsyningernes stamdata, hvilken forsyning, adresse, bygning og hvilket målepunkt anmodningen vedrører.
- Den fælles løsning foretager opslag i relevante registre med udgangspunkt i adressen for at identificere de personer eller virksomheder, der kan være samtykkekompetente i relation til den pågældende adresse eller boligenhed.
- Den fælles løsning sender oplysningerne til samtykkeløsningen, som opretter samtykket for de identificerede personer eller virksomheder.
- De identificerede personer logger ind med MitID eller MitID Erhverv og afgiver samtykke.
- Samtykkeløsningen returnerer oplysninger om de autentificerede identiteter til den fælles løsning.
- Den fælles løsning validerer identiteterne i forhold til den identificerede samtykkekreds og de relevante stamdata.
- Hvis valideringen er gennemført, registreres samtykket som gyldigt, og den fælles løsning autoriserer anmodningen om dataudlevering. Hvis identiteterne eller samtykkekredsen ikke kan valideres, afvises anmodningen, og data udleveres ikke.
- Forsyningen modtager den autoriserede anmodning og udleverer de relevante forbrugsdata til den fælles løsning.
- Den fælles løsning viderestiller forbrugsdataene til tredjeparten i overensstemmelse med det afgivne samtykke.

Styrker ved modellen
En styrke ved modellen er, at den ikke kræver, at forsyningen på forhånd vedligeholder en direkte kobling mellem alle relevante personer og et målepunkt. Modellen placerer opgaven med at identificere den relevante samtykkekreds i den fælles løsning.

Begrænsninger ved modellen
Den væsentligste begrænsning er, at identifikationen af den samtykkekompetente bliver mere kompleks og afhængig af kvaliteten af eksterne registre og relationerne mellem adresse, bygning, boligenhed og målepunkt. Hvor UUID- og CPR/CVR-modellerne tager udgangspunkt i en kendt identitet, tager den adressebaserede model udgangspunkt i en lokalitet og skal efterfølgende udlede, hvilke personer eller virksomheder der kan afgive samtykke. Det stiller større krav til datagrundlaget og til den løbende vedligeholdelse af relationer mellem stamdata. Der kan desuden opstå komplekse situationer, hvor flere personer eller virksomheder har en relation til den samme adresse eller måle. Dette betyder, at samtlige personer eller virksomheder med relation til måleren eller adressen, vil modtage en samtykkeanmodning.

Opsummering
Den adressebaserede model adskiller sig fra de øvrige identitetsmodeller ved, at ansvaret for at identificere den samtykkekompetente personkreds placeres i den fælles løsning.

Hvor forsyningen i UUID- og CPR/CVR-modellerne stiller en identitetsnøgle til rådighed som en del af stamdataene, skal den fælles løsning i denne model selv identificere den relevante personkreds på baggrund af adresseoplysninger og opslag i eksterne registre.

For forsyningerne indebærer modellen, at de ikke nødvendigvis skal registrere eller vedligeholde identitetsoplysninger om alle samtykkekompetente personer. De skal derimod kunne stille de nødvendige stamdata til rådighed, herunder relationen mellem adresse, bygning og målepunkt, så den fælles løsning kan gennemføre identifikationen.

For den fælles løsning indebærer modellen, at der skal etableres funktionalitet til opslag i relevante registre samt logik til at identificere og validere den samtykkekompetente personkreds på baggrund af adresseoplysninger.

Den fælles løsning skal samtidig kunne håndtere ændringer i relationerne mellem adresser, boligenheder, virksomheder og personer over tid. Modellen placerer dermed en større del af identifikationsopgaven i den centrale infrastruktur og stiller større krav til dens datagrundlag, integrationer og løbende vedligeholdelse af relationerne mellem data.

6 Opsamling
Et digitalt samtykkeflow forudsætter, at det er muligt at dokumentere både, hvem der afgiver samtykket, og hvilket kundeforhold, hvilken adresse og hvilket målepunkt samtykket vedrører.

MitID og MitID Erhverv vurderes at være det mest hensigtsmæssige fælles grundlag for autentifikation, da løsningerne allerede er etablerede og sikrer sporbar

autentifikation af henholdsvis privatpersoner og personer, der handler på vegne af virksomheder.

MitID løser dog alene autentifikationen og etablerer ikke i sig selv koblingen mellem den autentificerede identitet og forsyningernes stamdata. Der er derfor behov for en identitetsnøgle, som gør det muligt at koble identiteten til det relevante kundeforhold og målepunkt.

Kundenummer eller andre lokale identifikatorer er ikke tilstrækkelige som fælles identitetsnøgle i scenarie 2 og 3, da de er forsyningsspecifikke og ikke kan anvendes som et skalerbart koblingspunkt på tværs af forsyninger, den fælles løsning og samtykkeløsningen. Forsyningerne kan fortsat anvende egne identifikatorer internt, men de centrale infrastrukturscenarier kræver et fælles og standardiseret koblingspunkt mellem systemerne.

Blandt de undersøgte identitetsmodeller vurderes UUID-modellen at være den mest hensigtsmæssige ved simpelt samtykke. UUID er en teknisk entydig identifikator, som kan anvendes på tværs af systemer uden behov for behandling af CPR-oplysninger. Modellen understøtter dermed dataminimering og giver et fælles koblingspunkt mellem den autentificerede identitet, samtykket og forsyningernes stamdata. CPR og CVR kan også bidrage med entydig identifikation, men har forskellige egenskaber: Anvendelse af CPR kræver særskilt hjemmel til forsyningernes behandling og registrering af oplysningerne, mens CVR for erhvervskunder kan være en mere hensigtsmæssig identitetsnøgle til kundeforholdet, fordi CVR identificerer virksomheden frem for den enkelte bruger.

Ved komplekst samtykke er en identitetsnøgle ikke tilstrækkelig i sig selv. Her skal den fælles løsning kunne tage udgangspunkt i adresse- og måleroplysninger, foretage relevante registeropslag og identificere den samlede samtykkekreds. Den adressebaserede model stiller derfor større krav til den fælles løsnings integrationer, registeradgang og løbende vedligeholdelse af relationerne mellem adresser, bygninger, målepunkter og personer.

Identitetsmodellerne ændrer ikke de tre overordnede infrastrukturscenarier. De beskriver, hvordan en nødvendig teknisk forudsætning for samtykke og dataudlevering kan realiseres inden for scenarierne. I scenarie 1 kan identifikationen håndteres lokalt, mens scenarie 2 og 3 kræver en identitetsmodel, der kan fungere på tværs af forsyninger, samtykkeløsningen og henholdsvis sektor- eller den nationale løsning.