

Notat om den nationale digitale identitetstegnebog

Indholdsfortegnelse

- Introduktion til projektet
- Økosystem for den nationale digitale identitetstegnebog
- Erhvervelse af den nationale digitale identitetstegnebog
- De første beviser i den nationale digitale identitetstegnebog
- Brug af den nationale digitale identitetstegnebog
- Arkitekturtegning og komponenter

Notatets formål

Formålet med nærværende notat er at give en dybere indføring til den nationale digitale identitetstegnebog med fokus på økosystemet for løsningen, hvordan den kan erhverves, hvilke beviser den første version vil indeholde, samt hvordan beviser kan benyttes. Slutteligt vil en arkitekturtegning og de forskellige hovedkomponenter for løsningen præsenteres.

Introduktion til projektet

Som følge af eIDAS2-forordningen er alle EU-medlemslande forpligtet til at udvikle og stille en digital identitetstegnebog til rådighed til borgere og virksomheder.

Som et trin frem mod efterlevelsen af forordningen, og for at løse eksisterende problemstillinger for virksomheder, borgere og myndigheder, er Digitaliseringsstyrelsen i gang med at udvikle en **national digital identitetstegnebog (herefter DKTB)**.

DKTB er derfor en forløber og fase 1 hen mod en eIDAS2-tegnebog. DKTB udvikles af samme årsag så vidt muligt på EU-standarder og EU-protokoller, så senere tilpasninger til en dansk eIDAS2-tegnebog bliver minimeret. DKTB er altså ikke lig med den fremtidige eIDAS2-tegnebog, der på sigt skal stilles til rådighed, men den bygger på samme grundlag.



Et digitalt bevis indeholder information om brugeren, og kan verificeres uden, at en myndighed skal godkende brugen af beviset.

DKTB skal tænkes som et værktøj borgere kan benytte til at opbevare og dele digitale beviser på en sikker digital og privatlivsbeskyttende måde. Hvordan DKTB som værktøj kan benyttes, afhænger af de beviser, der tilføjes til DKTB. Ved lancering, ca. april 2026, vil DKTB kunne indeholde et legitimationsbevis, som

kan bruges til identifikation, samt et aldersbevis, som kan bruges til at bevise, at brugeren overholder en given aldersgrænse.

Brugen af DKTB reguleres i *lov om den nationale digitale identitetstegnebog*. Lovforslaget fremsættes i Folketinget til oktober. Identitetstegnebogen er et værktøj som andre myndigheder mv. kan vælge at benytte. Den konkrete benyttelse vil skulle fastsættes af den ressortansvarlige myndighed.

I det næste afsnit vil de forskellige aktører i økosystemet for DKTB blive præsenteret for at forklare, hvordan DKTB virker.

Økosystem for den nationale digitale identitetstegnebog

I økosystemet for brugen af DKTB er der forskellige aktører med veldefinerede roller og ansvarsområder. Logikken med denne rollefordeling og opsætning er at bygge et økosystem, der er privacy-by-design baseret. Dvs. at privacy (privatlivsbeskyttelse) er tænkt ind fra starten som en af hovedårsagerne til at udvikle systemet, og som noget der skal sikres i alle dele af økosystemet.

De fire vigtigste roller er bevisudstederen, bevismodtageren, opslagstjenesten, og brugeren (bevisholderen). Med appen installeret kan en bruger vælge at hente relevante beviser til sin identitetstegnebog fx legitimationsbeviset og aldersbeviset. Disse beviser får brugeren fra en bevisudsteder, der i første omgang kun kan være en myndighed, men på sigt også virksomheder, når eIDAS2-forordningen er implementeret.

Når en bruger har fået et bevis fra en bevisudsteder, ligger beviset lokalt på telefonen. Dette er en afgørende del af systemet, for det betyder, at når en bruger vil vise beviset til en bevismodtager for fx at købe cigaretter i et supermarked, får bevisudstederen ikke besked om, at det udstedte bevis nu er i brug. Der er, med andre ord, ikke en forbindelse mellem udstedere og modtagere af beviser.



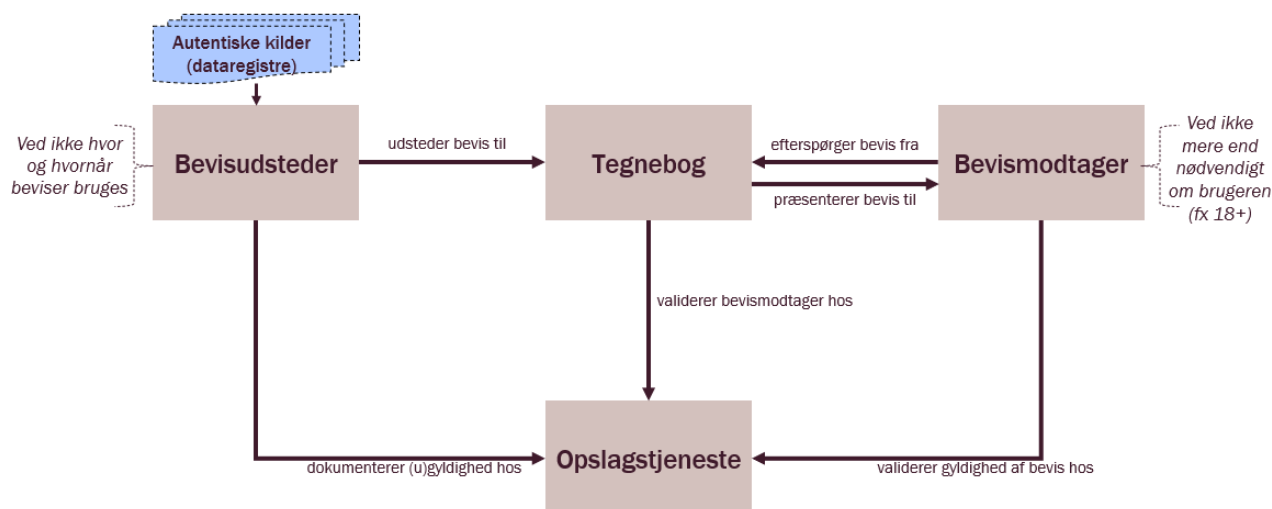
Den digitale identitetstegnebog kan ikke anvendes til at kortlægge brugerens adfærd, hverken af myndigheder eller virksomheder.

Det åbne spørgsmål, der opstår af dette, er, hvordan bevismodtagere kan vide sig sikre på gyldigheden af et bevis? Beviserne er i sig selv "verificerbare" - det vil sige, at når et bevis er udstedt, så indeholder det al den information en bevismodtager har brug for, for at kunne se at det er ægte og gyldigt.

Der kan derudover, i visse tilfælde, være behov for at kontrollere om et bevis er blevet spærret af bevisudstederen efter det er udstedt. Bevismodtageren kan kontrollere gyldigheden ved at hente en statusliste hos opslagstjenesten. Opslagstjenesten har ikke informationer om de enkelte brugere, men alene information om, hvilke beviser der er gyldige eller ej. Konkret indeholder statuslisten en lang række 0 og 1-taller, for udstedte beviser, hvor 0 betyder gyldigt og 1 betyder ugyldigt. Når en bevismodtager skal kontrollere gyldigheden, har bevismodtageren, fra beviset, fået metadata om, hvilket nummer i talrækken, der repræsenterer status for det konkrete bevis. Bevismodtageren kontrollerer herefter fx tal nummer 1888 på listen. Da bevismodtageren altid vil hente den fulde statusliste, indeholdende status

for tusindvis af beviser, får opslagstjenesten ikke indsigt i, hvem der spørger, og hvilket bevis der kontrolleres.

Figur 1: Hovedaktører i økosystemet



I økosystemet for DKTB vil Digitaliseringsstyrelsen udvikle to separate it-systemer, samt opslagstjenester:

- **Tegnebogsapplikationen**, der vil kunne downloades fra Google Play eller Apples App Store af brugere, samt en tilhørende back-end med understøttende funktioner, fx til at håndtere integration til NemLog-in.
- **Bevisudstedelsesservicen (BUS)**, som står for at integrere til datakilder, omforme data til beviser og udstedelse af disse til DKTB. Denne komponent vil også blive stillet til rådighed for andre offentlige myndigheder, som skulle ønske at udstede beviser til DKTB.
- **To opslagstjenester**, som vil være offentligt tilgængelige. Dels et modtagerpart-register hvor bevismodtagere, som ønsker at anmode om andet end aldersbeviser, skal være registreret, før det tillades, at de kan modtage data fra et bevis. Dels en tjeneste som udstiller de førnævnte statuslister for bevisers gyldighed.

Bevismodtagere har selv ansvar for deres tekniske integrationer til tegnebogsapplikationen, men vil være pålagt at følge de retningslinjer og specifikationer som Digitaliseringsstyrelsen fastsætter. Disse vil så vidt muligt følge Europa-Kommissionens anbefalinger for at tilgodese interoperabilitet på tværs af EU.

Erhvervelse af den nationale digitale identitetstegnebog

Brugere kan erhverve en DKTB på deres smartphone eller tablet via Google Play og App store. Når appen er downloadet, er det første trin, at brugeren skal autentificere sig via NemLog-in ved at logge på med et MitID eller et andet eID. Dette har til formål at sikre, at en bruger ikke har flere aktive tegnebogsapplikationer, samt at en identitetstegnebog kan spærres, hvis brugeren skulle have mistet sin mobile enhed.

Når brugeren har oprettet sin identitetstegnebog, skal brugeren oprette et legitimationsbevis. Dette sker ved at brugeren igen validerer sig via NemLog-in, hvorefter beviset udstedes til brugerens identitetstegnebog. Det er en forudsætning for anvendelsen af DKTB, at en bruger har oprettet et legitimationsbevis i forbindelse med aktivering. Det skyldes at legitimationsbeviset forbinder en bruger til én identitetstegnebog, i den forstand at alle fremtidige beviser, som udstedes til den givne tegnebog, skal være beviser, der tilhører samme person som legitimationsbeviset. På den måde sikres det, at de pågældende beviser udstedes til den korrekte person.



Legitimationsbeviset bliver først et gyldigt billed-id, når en bruger tilføjer et billede til beviset. I mellemtiden er det et identitetsbevis, som kan benyttes online.

Som en del af oprettelsen får brugeren mulighed for at tilføje et billede til sin identitetstegnebog. Konkret gøres dette ved at brugeren scanner chippen i sit pas, der indeholder et billede. Dette er et nødvendigt trin, hvis en bruger vil benytte legitimationsbevis som et gyldigt billed-id. En lignende tilgang har tidligere været anvendt i forbindelse med kørekort-appen.

Når man som bruger har aktiveret sin tegnebogsapplikation, vil det også være muligt at tilføje et aldersbevis. Det vil på sigt også være muligt at tilføje andre beviser til DKTB, og der vil i appen være et katalog over tilgængelige beviser, der løbende vil blive udbygget, med de beviser en bruger kan få udstedt.

De første beviser i den nationale digitale identitetstegnebog

DKTB vil som nævnt ved lancering indeholde et legitimationsbevis og kan, hvis brugeren vælger det, indeholde et aldersbevis. I dette afsnit vil de to beviser præsenteres.



Legitimationsbeviset primære formål er, at en bruger kan bevise, hvem de er, overfor en bevismodtager, fx hvis brugeren skal hente en pakke i en pakkeshop. Beviset kan dog også bruges mere dataminimerende til alene at bevise, at man fx er bosiddende i København, uden nødvendigvis at dele data som navn og fødselsdato.

Legitimationsbeviset vil forventeligt indeholde følgende data og metadata:

Data:

- Fornavn
- Efternavn
- Fødselsdato
- Fødselssted
- Nationalitet
- Adresse

- (potentielt også andre)

Metadata:

- Udstedelsesdato
- Udløbsdato
- Udstedende myndighed
- Link til statusliste
- Position på statusliste



Hvad tegnebogen kan benyttes til, afhænger af dens beviser. Der er stor forskel på hvad legitimationsbeviset og aldersbeviset tænkes brugt til.

Aldersbeviset kan indeholde en række attributter, der angiver om brugeren er over (eller under) en given aldersgrænse, fx:

- Age_over_13: True / False
- Age_over_15: True / False
- Age_over_16: True / False
- Age_over_18: True/ False
- Age_over_67: True / False

Når en bruger benytter aldersbeviset, deles der altså kun data om, hvorvidt brugeren er over (eller under) en given aldersgrænse samt metadata.

Aldersbeviset indeholder dog også metadata, der er unikke for det pågældende bevis. Selvom disse metadata ikke er personhenførbare, findes der en teoretisk mulighed for, at bevismodtagere vil kunne genkende et givent bevis, og sammenholde det med beviser modtaget tidligere, eller modtaget af en anden bevismodtager, for på den måde at spore en brugers færden. For at udelukke denne mulighed for sporing på tværs af sessioner vil aldersbeviset være et engangsbevis. Det betyder, at når aldersbeviset bliver udstedt, så genereres der (teknisk set) 30 unikke aldersbeviser med samme attributter, men forskellige metadata. Når de 30 unikke aldersbeviser er brugt, genereres automatisk en ny række aldersbeviser, så brugeren ikke aktivt skal anmode om nye aldersbeviser.

Aldersbeviset tænkes fx brugt til sociale medier og ved køb af aldersbegrænsede varer både online og i fysiske brugsscenarier. Der er dog en lang række af andre mulige brugsscenarier, hvor aldersbeviset også kan vise sig relevant at benytte.



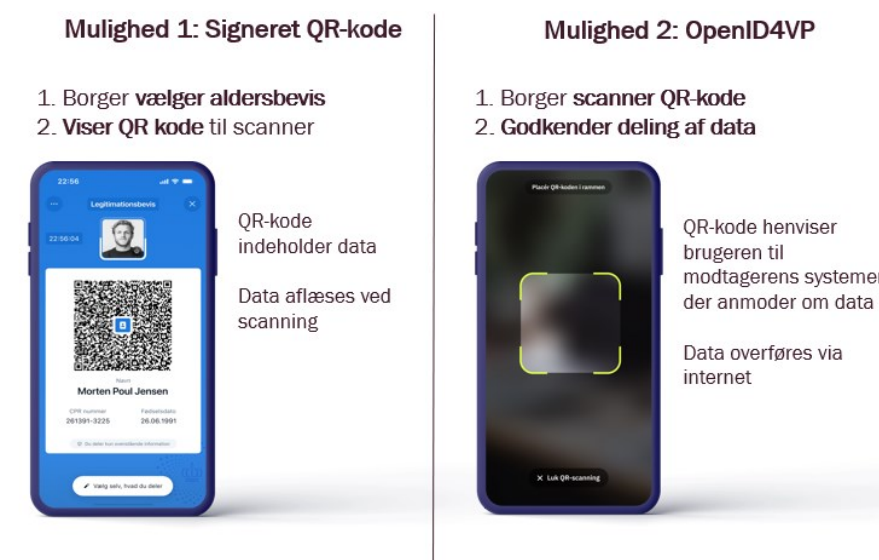
Aldersbeviset består af unikke engangsbeviser. Aldersbeviset er derfor teknisk set forskelligt, hver gang det benyttes. Dette udelukker muligheden for at brugeren kan identificeres af bevismodtagere.

Det er hensigten, at det også skal være muligt at præsentere sit aldersbevis ved anvendelse af et **Zero-Knowledge Proof (ZKP)**, hvor selve beviset ikke deles med bevismodtageren. I stedet deles blot et matematisk bevis, som tegnebogsapplikationen selv kan genere, der beviser at identitetstegnebogen er i besiddelse af et gyldigt bevis, som lever op til bevismodtagerens forespørgsel, fx at brugeren er over 18 år. Af hensyn til at sikre kompatibilitet med platforme på tværs af EU afventer projektet for nuværende endelig stillingtagen til udformningen af dette område fra Europa-Kommissionen. Projektet forventer at følge de anbefalinger der kommer, og i det omfang det er realiserbart allerede inden lanceringen. Indtil der er videre afklaring om brugen af ZKP i den europæiske kontekst, benytter projektet som nævnt engangsbeviser for aldersbeviset, der sikrer fuld anonymitet og et tilsvarende niveau af privatlivsbeskyttelse.

Brug af den nationale digitale identitetstegnebog

Der er to metoder til deling af beviser med bevismodtagere. Disse to er en signeret QR-kode, som man kender fra fx Coronapasset, til deling af beviser i fysiske scenarier og [OpenID for Verifiable Presentations \(OID4VP\)](#) protokollen, som skal anvendes til deling online.

Figur 2: Måder at dele og modtage beviser fra DKTB



Mulighed 1: Signeret QR-kode fungerer på den måde, at en bruger vælger, hvilket bevis, og eventuelt hvilke specifikke attributter fra dette bevis, de ønsker at dele med bevismodtageren. På baggrund af dette valg dannes en signeret QR-kode, som en bevismodtageren kan scanne og dermed aflæse beviset.

Denne måde at dele et bevis vil kun kunne bruges i fysiske brugsscenarier og ikke online. Fordelen er, at den også kan benyttes i offline sammenhænge, fx hvis man skal aldersverificeres et sted, hvor der ikke er internetdækning. Denne metode er et tillæg til Europa-Kommissionens arkitekturramme, som lægger op til at anvende ISO 18013-5 til udveksling af beviser i fysiske scenarier. Baggrunden for dette tillæg er, at ISO 18013-5 vurderes at være umoden som standard og afhænger delvist af uafprøvede eller svært anvendelige teknologier, fx **Near Field Communication (NFC)** og **Bluetooth Low Energy (BLE)**, og dels at det vil kræve en væsentligt større implementeringsindsats hos bevismodtagerne at modtage beviser på denne måde.

Mulighed 2: OID4VP fungerer på den måde, at en bruger scanner en QR-kode som udstilles af bevismodtageren. QR-koden indeholder et link, som fortæller DKTB, hvilket bevis, og hvilke attributter fra dette, som bevismodtageren ønsker at få. Brugeren præsenteres for forespørgslens indhold og kan herefter vælge at dele data ved at swipe, som man kender det fra MitID, hvis de vil godkende delingen. OID4VP er den protokol, der anbefales af Europa-Kommissionen til udveksling af beviser online. Det vil derfor også være den metode, der anvendes til aldersverificering på tværs af online platforme i EU. Protokollen forventes også i høj grad brugt i fysiske brugsscenarier, da den for virksomheder muliggør, at de i fremtiden kan modtage EU-brugere, der benytter en eIDAS2-tegnebog.



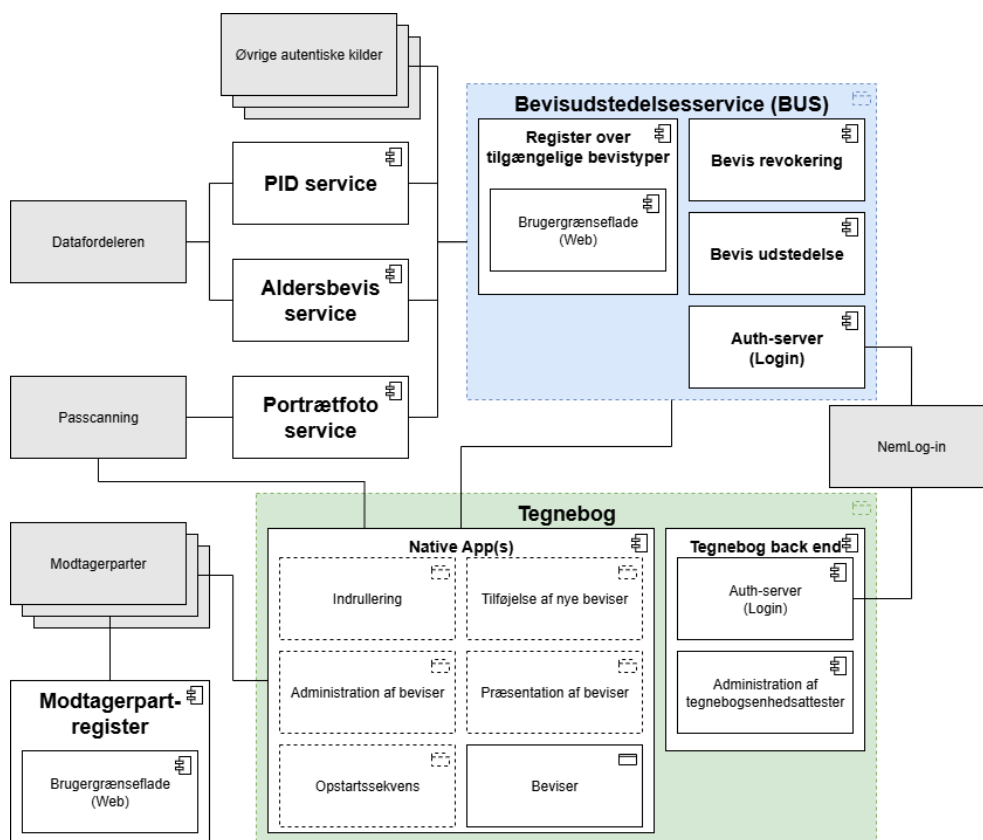
En bruger kan også visuelt fremvise sin identitetstegnebog til en bevismodtager og søge godkendelse den vej igennem. Det er dog først med den elektronisk godkendelse, at en bevismodtager kan vide sig helt sikker på bevisets gyldighed.

I fremtiden vil der potentielt være andre måder, hvorpå beviser fra tegnebogen kan deles. Dette kan fx være som foreskrevet i ISO 18013-5, hvor det er muligt at dele beviser via NFC. Det er den teknologi, som i dag benyttes ved betaling via en smartphone eller smartwatch. Det er under afklaring, om dette bliver en mulighed i en af de senere faser.

Arkitektur og byggeblokke

I dette afsnit præsenteres høj-niveau arkitekturen for DKTB. Det er en vigtig forudsætning, at det samlede DKTB-projekt etablerer to fuldstændigt separate og adskilte it-systemer. Dette udmønter sig i en overordnet arkitektur, hvor der er en skarp opdeling mellem identitetstegnebogen og **bevisudstedelsesservicen (BUS)**. Al kommunikation de to it-systemer imellem foregår via de standarder og specifikationer, der foreskrives af Europa-Kommissionen, for at sikre fremtidig kompatibilitet med øvrige potentielle bevisudstedere og/eller tegnebøger.

Figur 3: Høj-niveau arkitektur



Tegnebogen (grønt område i figuren)

Den del af projektet, som vedrører det produkt som brugeren er i direkte berøring med, omtales samlet som "Tegnebog" i figuren. Delen består primært af tegnebogsapplikationerne, som er *native apps* udviklet til hhv. Android og iOS, samt en back-end, der udstiller supplerende service til applikationerne.

Selve tegnebogsapplikationerne udvikles og vedligeholdes af Digitaliseringsstyrelsen og vil som udgangspunkt blive udstillet via hhv. Google Play og App store. Tegnebogsapplikationen er brugerens redskab til at hente, administrere og præsentere beviser. Beviserne findes efter udstedelse alene på brugerens enhed og er under dennes fulde kontrol. For at understøtte dette indeholder tegnebogen, som vist i figuren, følgende funktionsområder:

1. Indrullering

Det er en forudsætning, at tegnebogen aktiveres, før den kan anvendes som beskrevet i Europa-Kommissionens [Architecture and reference framework \(ARF\)](#). I praksis betyder det, at tegnebogen skal have udstedt en **Wallet Unit Attestation (WUA)** fra back-enden, baseret på Europa-Kommissionens specifikation for WUA. I forbindelse med udstedelsen af WUA (eller tegnebogensenhedsattest) knyttes brugeren til denne, således at det bliver muligt at spærre tegnebogsapplikationen, såfremt man mister sin telefon. Denne registrering ligger i tegnebogens back-end og deles aldrig med hverken bevisudstedere eller modtagere.

2. Tilføjelse af nye beviser

For at få udstedt beviser, skal tegnebogsapplikationen agere [OpenID for Verifiable Credential Issuance \(OID4VCI\)](#) klient (Wallet) i overensstemmelse med [OpenID4VC High Assurance Interoperability Profile \(HAIP\)](#) og Europa-Kommissionens krav og anbefalinger, i det omfang det giver mening i regi af DKTB. Formålet med at følge standarden og profilen er dels at anvende gennemarbejdede specifikationer, og dels for at muliggøre udstedelse af beviser til tegnebogen fra andre bevisudstedere på sigt.

3. Præsentation af beviser

Der findes, som tidligere beskrevet, to metoder til præsentation af beviser. Tegnebogsapplikationen skal dels agere [OpenID for Verifiable Presentations \(OID4VP\)](#) server (Wallet) i overensstemmelse med Europa-Kommissionens [Age Verification Profile](#) for at sikre interoperabilitet med online modtagerparter på tværs af EU. Dette skal på sigt overbygges med overholdelse af ISO 18013-7:2025 Annex B, samt [HAIP](#) for at sikre en standardiseret implementering, som muliggør udveksling af beviser med en større gruppe af modtagerparter. Hvorvidt dette sker før eller efter lancering afhænger af, om der frigives endelige specifikationer tidnok til, at de kan implementeres og testes.

På samme vis er det endnu ikke afklaret, om der fra lanceringen understøttes generering og præsentation af Zero-Knowledge Proofs. Dette vil i så fald ske ved anvendelse af [Anonymous credentials from ECDSA](#) i overensstemmelse med Europa-Kommissionens nuværende anbefaling. Dette afhænger dog fuldt ud af Kommissionens arbejde med at analysere og afprøve teknologien yderligere frem mod deres forventede ibrugtagning ultimo Q4 2025. Så snart teknologien vurderes produktionsmoden, forventes den at blive implementeret i tegnebogen. Det samme gælder i øvrigt for [W3C Digital Credentials API](#), som forventes at blive implementeret i overensstemmelse med ISO 18013-7:2025 Annex C, når der er tilstrækkelig modenhed og udbredelse til, at det giver værdi for både brugere og bevismodtagere. Indtil der er videre afklaring om brugen af ZKP i den europæiske kontekst, benytter projektet som nævnt engangsbeviser for aldersbeviset, der sikrer fuld anonymitet og et tilsvarende niveau af privatlivsbeskyttelse.

De signerede QR-koder er baseret på erfaringerne fra hhv. kørekort-app og coronapasset. Specifikationer er fortsat under udarbejdelse, men det er en forudsætning, at QR-koden genereres og signeres direkte på enheden, og at det betragtes som en udvidelse af OID4VP, i den forstand at der så vidt muligt anvendes samme formater og sikkerhedselementer som beskrevet i specifikationen.

4. Administration af beviser

Beviser, som er udstedt til tegnebogen, er under brugerens fulde kontrol. Derfor vil det også være muligt via tegnebogsapplikationen brugergrænseflade at opdatere eller slette beviser, såfremt brugeren ønsker dette.

5. Opstartssekvens

I supplement til brugerens egen mulighed for at administrere beviser vil der, ved opstart af tegnebogsapplikationen, blive foretaget en række kontroller. Dette bl.a. for at sikre, at beviser, der er ved at udløbe, bliver fornyet, og at beviser, som er blevet spærret, slettes. Der er derudover en række sikkerhedsmæssige kontroller, som har til formål at sikre at enheden, som tegnebogen er installeret på, fortsat lever op til kravene for dette. Det endelige design af kontrollerne udestår, og afsnittet vil blive opdateret, når det ligger fast.

Bevisudstedelsesservicen (blåt område i figuren)

Det system, der håndterer udstedelse af digitale beviser til tegnebogen, omtales samlet som Bevisudstedelsesservicen (BUS). BUS fungerer som *Issuer* i henhold til [OID4VCI](#) og er ansvarlig for at modtage anmodninger fra tegnebogen, identificere brugeren, indhente data fra autentiske kilder og udstede beviser i et standardiseret format.

Bevisudstedelseskompenten er designet til at understøtte, at strukturerede data kan hentes fra enhver godkendt autentisk kilde, omformes til og udstedes som et bevis til en tegnebog. På den måde sikres det, at 1) brugeren får en ensartet oplevelse ved udstedelse af digitale beviser, og 2) at den enkelte myndighed ikke skal forholde sig til omdannelsen fra data til bevis.

BUS er udvikles desuden i overensstemmelse med [HAIP](#). Samtidig vil der i første version af DKTB alene blive udstedt beviser i det format, der er defineret i ISO 18013-5 (mdoc). Dette format tillader 1) at beviset er bundet til én enhed (*device binding*), og 2) at brugeren kan vælge kun at dele visse attributter fra beviset med en bevismodtager (*selective disclosure*).

1. Initiering og autentifikation

Bevisudstedelsen starter typisk, når en bruger vælger et bevis i tegnebogens *beviskatalog*. Beviskataloget beskriver de tilgængelige beviser og bl.a. deres attributter og anvendelsesmuligheder. Kataloget dannes dynamisk på baggrund af metadata, der udstilles af bevisudstedelseskompenten. I nogen tilfælde kan udstedelsen også initieres via en QR-kode eller et link fra en autentisk kilde.

Efter brugeren har valgt et bevis, sender tegnebogen en **Pushed Authorization Request (PAR)** til BUS. Første gang brugeren får udstedt et bevis, vil de bedt om at logge ind via NemLog-in, med henblik på at identificere hvem beviset skal udstedes til. Efter det første aktive login vil det, så vidt muligt, ikke være nødvendigt for brugeren at logge ind igen for at få udstedt flere beviser eller forny eksisterende. I stedet anvendes et refresh token, som er en mekanisme, der muliggør, at en bruger, som tidligere er logget ind, uden behov for handling kan tilgå servicen igen.

Parallelt med brugerens login autentificeres selve tegnebogen via en WUA, der først bliver udstedt under indrulleringen og løbende fornyes igennem tegnebogsapplikationens levetid. Det sikrer, at kun godkendte tegnebøger kan få udstedt beviser fra BUS.

2. Forespørgsel og datavalidering hos autentiske kilder

Efter autentifikationen viderestiller bevisudstedelseskompenten forespørgslen til den relevante autentiske kilde. Den autentiske kilde validerer, om brugeren er berettiget til det pågældende bevis. Hvis valideringen resulterer i, at brugeren er berettiget, returneres de data, der skal indgå i beviset. Ved lancering af DKTB vil tre autentiske kilder være integreret med bevisudstedelseskompenten:

- **PID-Servicen** håndterer udstedelsen af legitimations- og identifikationsbeviser. Data stammer fra CPR via Datafordelerens CPR-service, og CPR UUID anvendes som nøgle. Såfremt en bruger ikke har et CPR-nummer, benyttes en anden fremgangsmåde.
- **PoA-servicen** (Proof Of Age) håndterer udstedelsen af aldersbeviser baseret på fødselsdato ligeledes fra via Datafordeleren.
- **Portrætservicen** håndterer processen, hvormed brugeren scanner sit pas i tegnebogsapplikationen, hvorefter fotoet sendes, via passcanningsleverandøren, til Portrætservicen, hvormed pasfotoet tilføjes til tegnebogen.

3. Konstruktion og udstedelse af beviser

Når data er modtaget fra den autentiske kilde, omdanner bevisudstedelseskomponenten det til et bevis i mdoc-format. Beviset repræsenteres som Concise Binary Object Representation (CBOR).

Beviset leveres fra BUS til tegnebogen som specificeret i OID4VCI. Beviset lagres udelukkende lokalt på brugerens enhed -BUS opbevarer ikke beviser. BUS foretager dog en logning af transmissionskald til og fra en offentlig myndigheds eller offentligretligt organs autentiske kilde. Logningen af transmissionskald er anonymiseret og anvendes til fejlsøgning.

4. Revokation og statusstyring

For visse typer af beviser er der behov for at kunne spærre eller tilbagekalde et udstedt bevis, hvis det ikke længere er gyldigt. For beviser, hvor dette er tilfældet, vedligeholder den autentiske kilde en *statusliste*, der viser om et bevis er gyldigt eller tilbagekaldt. BUS håndterer i praksis statuslisterne, men ajourfører dem udelukkende efter besked fra den autentiske kilde. Bevismodtagere kan hente den komplette statusliste, og slå et givent bevis op i denne, for at verificere om et bevis er gyldigt eller ej.

For PID-beviser sker opdatering af statuslisten via hændelsesdata fra Datafordeleren, der kan indikere navneændring, adresseændring, dødsfald eller andre ændringer, som påvirker bevisets gyldighed. Når en statusændring registreres, markeres beviset som ugyldigt i statuslisten.