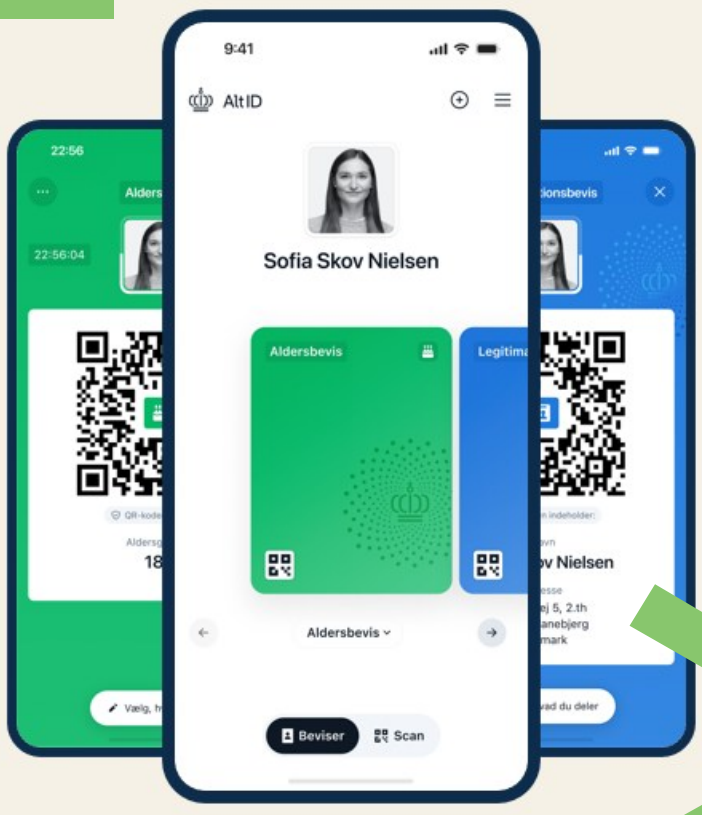
Digitaliserings-
styrelsen

Den nationale digitale identitetstegnebog

Notat om AltID

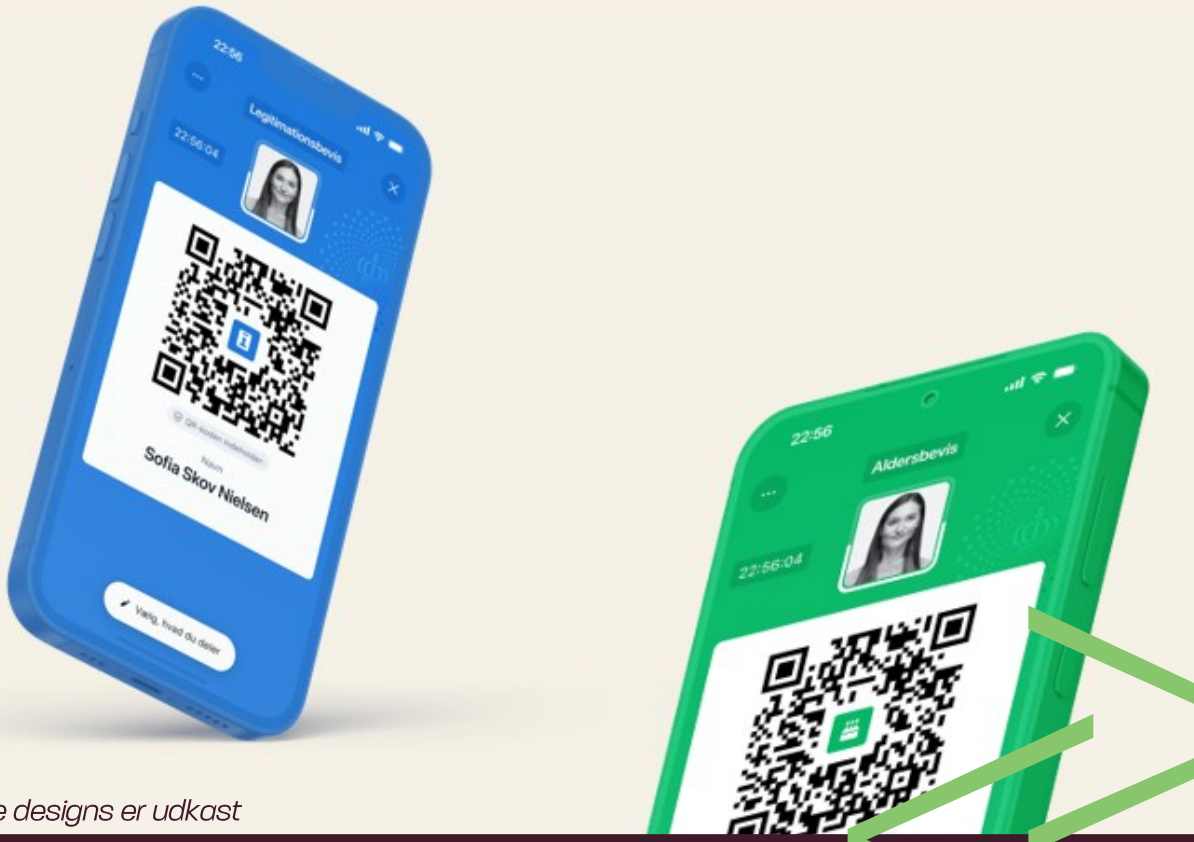


Alle designs er udkast

2025

Indhold

Version	Beskrivelse	Ansvarlig	Dato
1.0	Første udgave	Digitaliseringsstyrelsen	20-08-2025
1.1	Opdateret beskrivelse af signerede QR-koder	Digitaliseringsstyrelsen	12-11-2025
1.2	Opdateret navn til AltID og opdatering af layout	Digitaliseringsstyrelsen	19-12-2025
1.3	Mindre ajourføringer og opdatering af grafik	Digitaliseringsstyrelsen	29-01-2026



Alle designs er udkast

Notatets formål

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

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, kaldet AltID.**

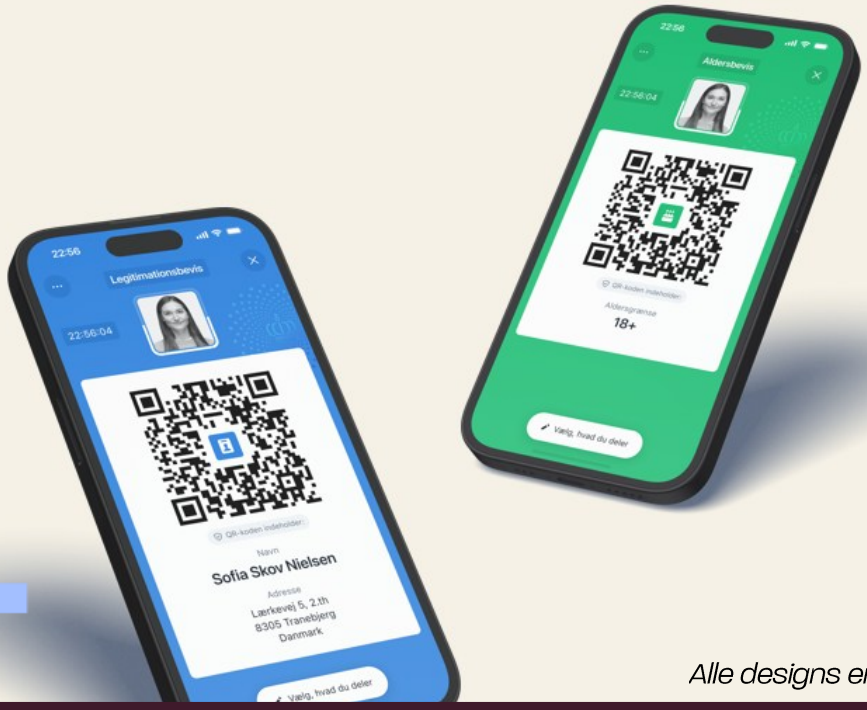
AltID er dermed en national forløber mod en eIDAS2-tegnebog. Af samme årsag udvikles AltID så vidt muligt på samme standarder og protokoller som eIDAS2 foreskriver, så opgaven med senere tilpasninger bliver minimeret. AltID er altså ikke lig med den fremtidige eIDAS2-tegnebog, der på sigt skal stilles til rådighed, men den bygger på samme grundlag.

AltID skal tænkes som et værktøj, som borgere kan benytte til at opbevare og dele digitale beviser på en sikker digital og privatlivsbeskyttende måde. Hvordan AltID som værktøj kan benyttes, afhænger af de beviser, der tilføjes til AltID. Ved lancering i foråret 2026 vil AltID kunne indeholde et legitimationskort som kan bruges til identifikation, samt et aldersbevis, som kan bruges til at bevise, hvorvidt brugeren er over eller under en given aldersgrænse, uden at der deles andre oplysninger.

Et digitalt bevis indeholder information om brugeren, som kan deles og verificeres uden, at en myndighed skal godkende brugen eller bekræfte

Brugen af AltID reguleres i *lov om den nationale digitale identitetstegnebog*. Lovforslaget blev fremsat for Folketinget 6. november, og er nu under behandling. AltID 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 AltID blive præsenteret for at forklare, hvordan AltID virker.



Alle designs er udkast

AltID bliver designet, så den beskytter dit privatliv og dine oplysninger mest muligt. Det særlige ved appen er, at dine beviser kun ligger lokalt på din telefon. Beviset er altså dit eksemplar af dine oplysninger.

Økosystem for AltID

I økosystemet for AltID er der forskellige aktører med veldefinerede roller og ansvarsområder. Formålet med denne rollefordeling og opsætning er at etablere et økosystem, der så vidt muligt understøtter privacy-by-design. Det vil sige, at privacy (privatlivsbeskyttelse) er tænkt ind fra starten i designet, udviklingen og driften af systemet, og at indvirkningen på brugernes privatliv er noget der aktivt tages stilling til i tilblivelsen af alle dele af løsningen og selve økosystemet – ikke som en eftertanke.

De fire vigtigste roller er **bevisudstederen, bevismodtageren, opslagstjenesten, og brugeren (bevisholderen)**. Med appen installeret kan en bruger vælge at hente relevante beviser til sin AltID-app, eksempelvis legitimationskortet 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.

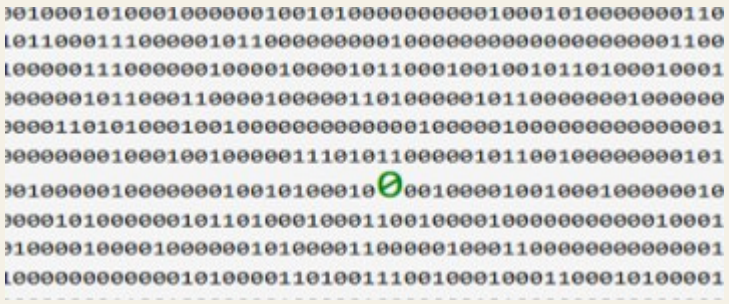
Når en bruger har fået et bevis fra en bevisudsteder, ligger beviset lokalt på telefonen. Dette er en afgørende del af systemet, for det betyder, at når en bruger vil vise beviset til en bevismodtager, for fx at købe cigaretter i et supermarked, får bevisudstederen ikke besked om, at det udstedte bevis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

Aldersbeviset kan ikke anvendes til at kortlægge brugerens adfærd, hverken af myndigheder eller virksomheder.

Det åbne spørgsmål, der opstår, når et bevis ligger lokalt på en brugers telefon, er, hvordan bevismodtagere kan vide sig sikre på gyldigheden af beviset? Svaret er, at beviserne i sig selv er "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.

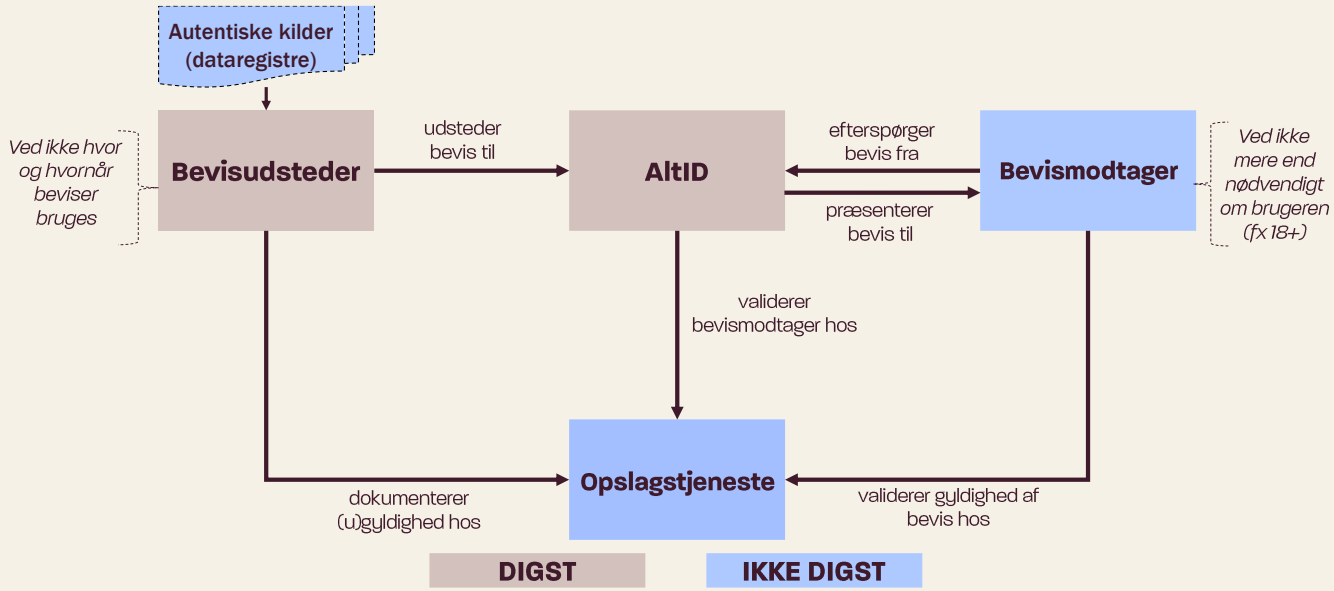
Der kan derudover, i visse tilfælde, være behov for at kontrollere om et bevis er blevet spærret af bevisudstederen efter det er udstedt. Det kan fx være aktuelt, hvis en bruger får et nyt efternavn. Bevismodtagere kan kontrollere gyldigheden ved at slå op i en statusliste, som hentes hos en opslagstjeneste. Det er angivet direkte i det pågældende bevis, hvorvidt det findes på en statusliste, og i så fald hvorfra listen kan hentes.

Figur 1: Eksempel på udsnit af statusliste



Statuslisten indeholder ingen information om brugerne, men angiver kun om beviser 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 det konkrete bevis. Bevismodtageren kontrollerer herefter eksempelvis tal nummer 1888 på listen. Bevismodtageren kun kan hente en samlet statusliste, som indeholder status for tusindvis af beviser. Dermed får opslagstjenesten ikke indsigt i, hvilket bevis der kontrolleres.

Figur 2: Hovedaktører i økosystemet



I økosystemet for AltID vil Digitaliseringsstyrelsen være ansvarlig for to separate it-systemer samt et supplerende register:

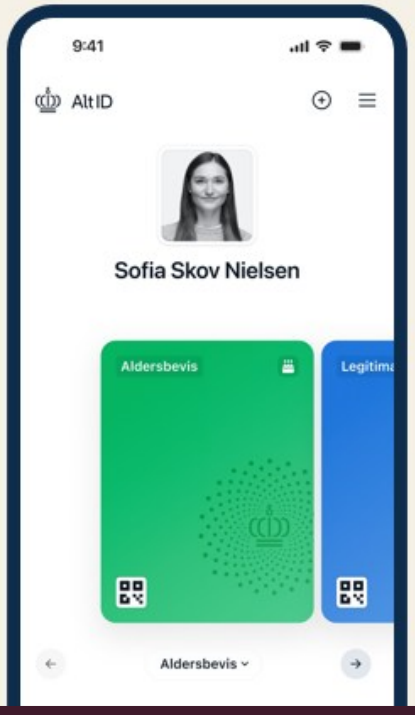
- **AltID-applikationen** der vil kunne downloades fra Google Play eller Apples App Store af brugere, samt en tilhørende back-end med understøttende funktioner, fx til at håndtere integration til NemLog-in.
- **Bevisudstedelsesservicen (BUS)** som står for at integrere til datakilder, omforme data til beviser og udstedelse af disse til AltID. Denne komponent vil også blive stillet til rådighed for andre offentlige myndigheder, som skulle ønske at udstede beviser til AltID.
- 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 online.

Derudover har Digitaliseringsstyrelsen, i regi af sine øvrige roller, ansvar for ajourføring af data hos:

- **Opslagstjenesten** som er offentligt tilgængelig via internettet og udstiller blandt andet de føromtalte statuslister for bevisers gyldighed. Derudover udstiller den også statuslister for både indrullerede AltID-applikationer og for registrerede modtagerparter. I praksis varetages rollen af en CDN-udbyder, som sørger for at statuslisterne er tilgængelige for hentning.

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

Bevismodtagere har selv ansvar for deres tekniske integrationer til AltID-applikationen, 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.



Alle designs er udkast

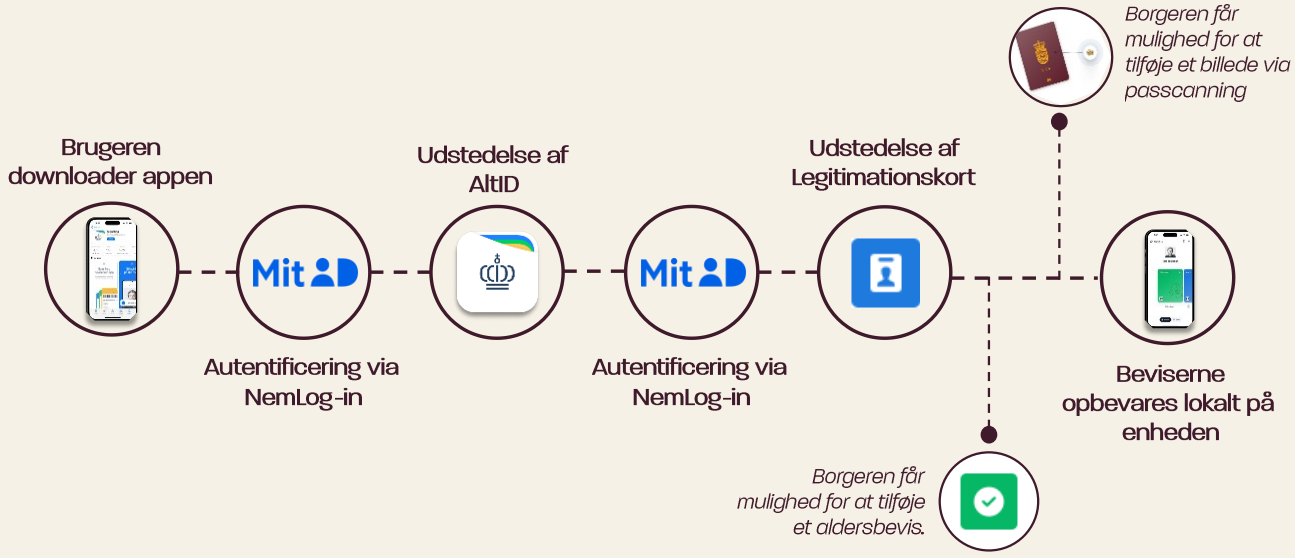
Det vil være frivilligt, om man ønsker at downloade og bruge AltID, og det vil fortsat være muligt at bruge pas, kørekort eller et andet analogt eller digitalt alternativ til at vise sin alder eller identitet. En af fordelene ved AltID er, at appen giver brugeren bedre kontrol over, hvilke oplysninger der deles, og med hvem de deles.

Erhvervelse af AltID

Brugere kan erhverve AltID-appen på deres smartphone 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 AltID-applikationer samtidig, samt at en AltID-app kan spærres af brugeren, hvis man mister sin mobile enhed.

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

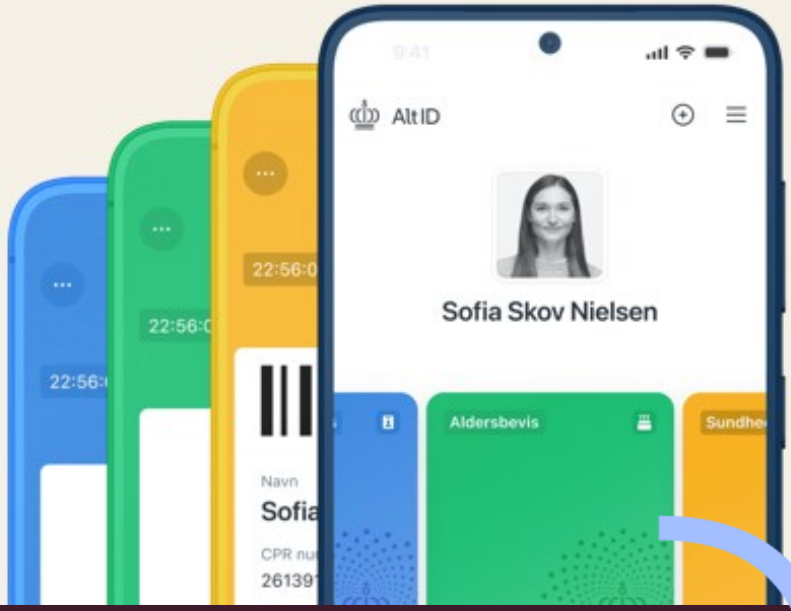
Figur 3: Oprettelsesflow for AltID



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

Som en del af oprettelsen får brugeren mulighed for at tilføje et billede til sin AltID-app. 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 legitimationskortet som et gyldigt billed-id. En lignende tilgang har tidligere været anvendt i forbindelse med kørekort-appen.

Alle designs er udkast



De første beviser i AltID vil være et legitimationskort og et aldersbevis. I fremtiden vil du kunne tilføje mange flere beviser og bruge appen i hele EU.

De første beviser i AltID

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

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

Legitimationskortet

Legitimationskortets **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.

Figur 4: Legitimationskortet

Alle designs er udkast

Legitimationskortet indeholder følgende data og metadata:

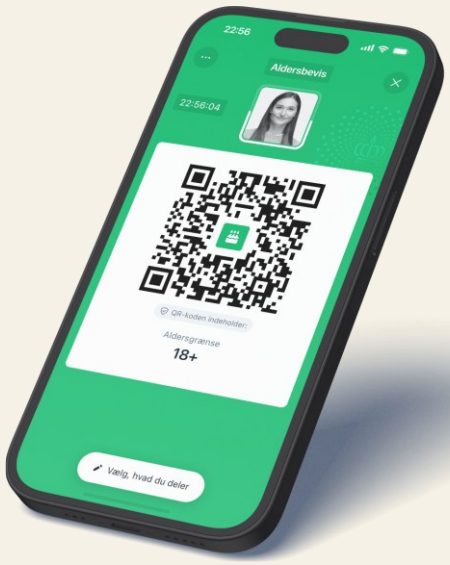
Data:
- Navn
- Fornavn
- Efternavn
- Fødselsdato
- Fødselssted
- Nationalitet
- Adresse
- CPR-nummer

Metadata:
- Udstedelsesdato
- Udløbsdato
- Udstedende myndighed
- Udstedende land
- Link til statusliste
- Position på statusliste

Aldersbeviset

Aldersbevisets **primære formål** er, at en bruger kan bevise, hvorvidt de er over en bestemt alder, fx hvis brugeren skal købe aldersbegrænsede varer som alkohol eller tobak eller skal ind på aldersbegrænsede lokationer som eksempelvis natklubber og barer. Brugeren er helt anonym, når de bruger aldersbeviset, da det ikke indeholder information om præcis alder, CPR-nummer eller andre personlige oplysninger.

Figur 5: Aldersbeviset



Alle designs er udkast

Aldersbeviset indeholder en række attributter, der angiver om brugeren er over (eller under) en given aldersgrænse. Initialt indeholder beviset følgende aldersgrænser: 13, 15, 16, 18, 21, 23, 25, 26 og 67. Attributterne har enten værdien sandt eller falsk alt efter om brugeren er over eller under den specifikke alder, for eksempel vil aldersbeviset for en 17-årig indeholde:

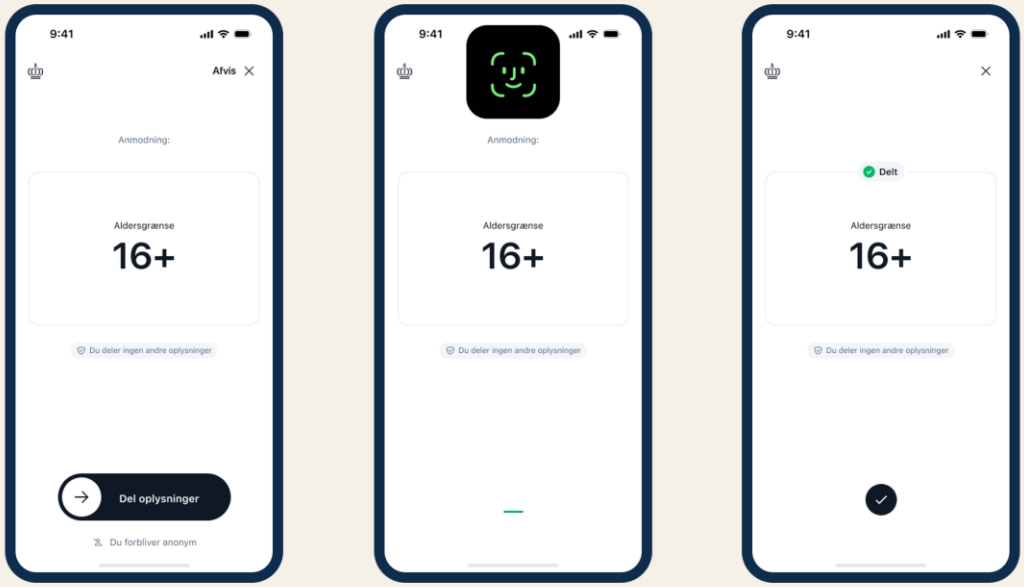
- age_over_13 = true
- age_over_15 = true
- age_over_16 = true
- age_over_18 = false
- age_over_nn = false

Aldersbeviset indeholder dog også nødvendige metadata, der er unikke for det pågældende bevis. Selvom disse metadata ikke er personhenførbare, introducerer de 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 unikt, hver gang det benyttes. Dette udelukker muligheden for at brugeren kan genkendes af bevismodtagere ud fra bevisets indhold.

Det er hensigten, at det også skal være muligt at præsentere beviser ved anvendelse af et **Zero-Knowledge Proof (ZKP)**, hvor selve beviset ikke deles med bevismodtageren. I stedet deles blot et matematisk bevis, som AltID-applikationen selv kan genere, der beviser at AltID-appen 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. 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.



Alle designs er udkast

Der er forskellige måder man kan bruge og dele de beviser man har i AltID. Hvilken måde man skal bruge afhænger af, hvor man bruger det henne.

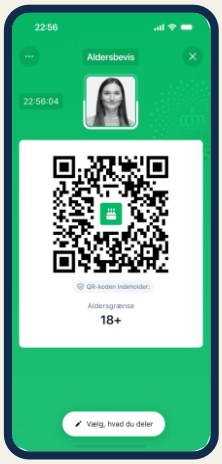
Brug af AltID

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 6: Måder at dele og modtage beviser fra AltID

Mulighed 1: Signeret QR-kode

1. Borger **vælger aldersbevis**
2. **Viser QR kode** til scanner

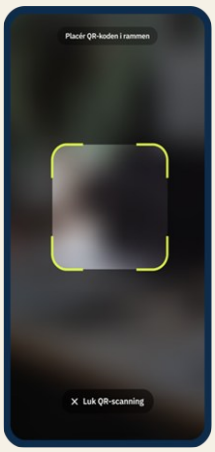


QR-kode indeholder data

Data aflæses ved scanning

Mulighed 2: OpenID4VP

1. Borger **scanner QR-kode**
2. **Godkender deling af data**



QR-kode henviser brugeren til modtagerens systemer der anmoder om data

Data overføres via internet

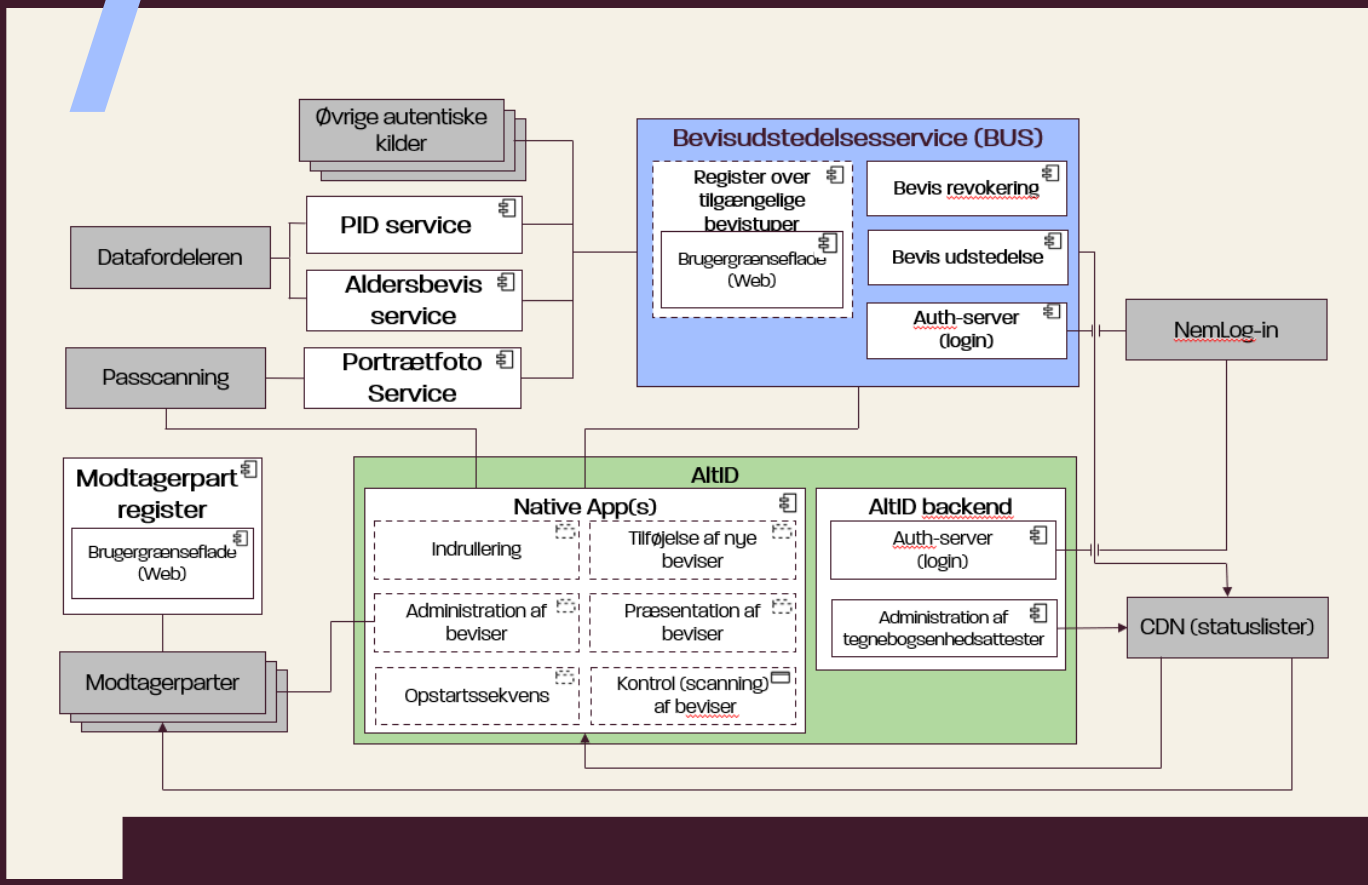
Alle designs er udkast

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 AltID, hvilket bevis, og hvilke attributter fra dette, som bevismodtageren ønsker at få. Hvis brugeren tilgår bevismodtagerens hjemmeside fra samme enhed som AltID er installeret på, kan linket også vises direkte, fx som en knap. 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 et bevis fra AltID til en bevismodtager og søge godkendelse den vej igennem. Det er dog kun med en elektronisk godkendelse, at en bevismodtager kan vide sig helt sikker på bevisets ægthed

I fremtiden vil der potentielt være andre måder, hvorpå beviser fra AltID 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.

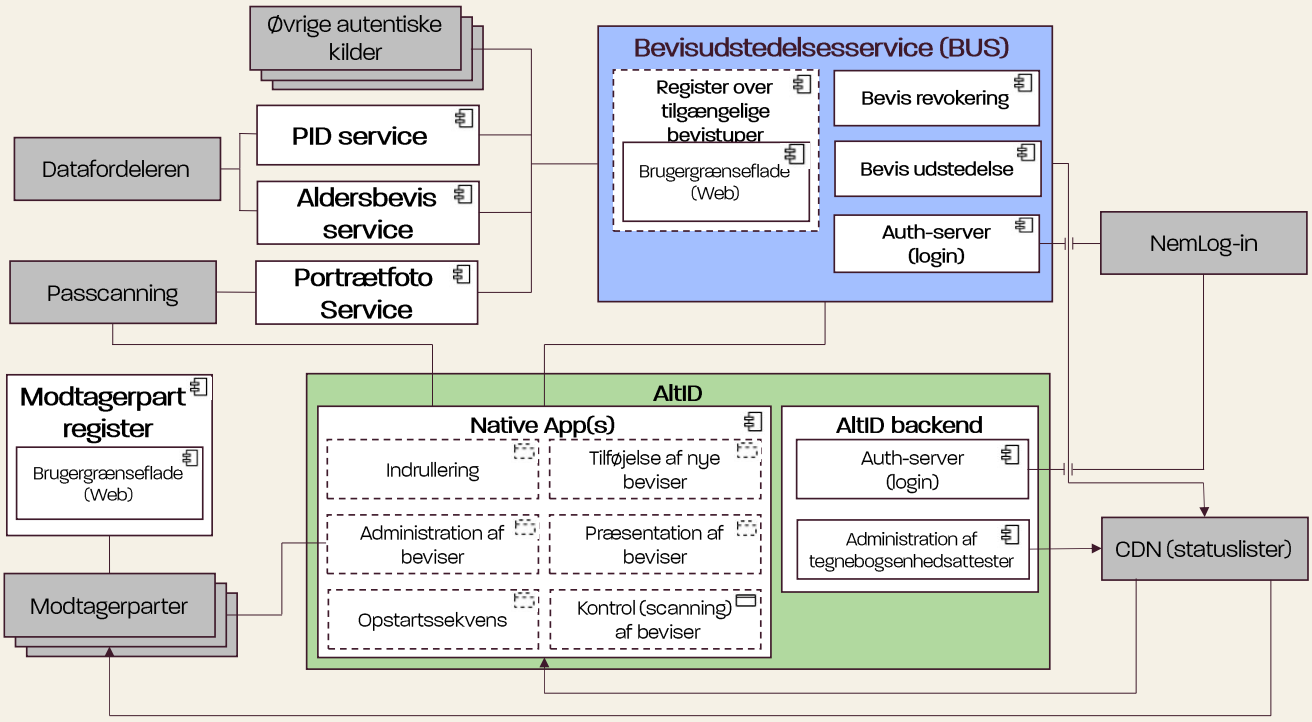


Digitaliseringsstyrelsen udvikler ikke kun AltID appen, men også infrastruktur, der gør det let for myndigheder at udstede beviser.

Arkitektur og byggeblokke

I dette afsnit præsenteres høj-niveauarkitekturen for AltID. Det er en vigtig forudsætning, at det samlede AltID-projekt etablerer to fuldstændigt separate og adskilte it-systemer. Dette udmønter sig i en overordnet arkitektur, hvor der er en skarp opdeling mellem **AltID** (både applikationer og supplerende back-end) 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 7: Højniveauarkitektur



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

Selve AltID-applikationerne udvikles og vedligeholdes af Digitaliseringsstyrelsen og vil som udgangspunkt være tilgængelige for installation via hhv. Google Play og App store. AltID-applikationen 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 AltID, som vist i figuren, følgende funktionsområder:

1. Indrullering

Det er en forudsætning, at AltID-appen aktiveres, før den kan anvendes som beskrevet i Europa-Kommissionens Architecture and reference framework (ARF). I praksis betyder det, at AltID-appen 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 AltID-enhedsattest) knyttes brugeren til denne, således at det bliver muligt at spærre AltID-applikationen, såfremt man mister sin telefon. Denne registrering ligger i AltIDs back-end og deles aldrig med hverken bevisudstedere eller modtagere.

2. Tilføjelse af nye beviser

For at få udstedt beviser, skal AltID-applikationen agere OpenID for Verifiable Credential Issuance (OID4VCI) klient (Wallet) i overensstemmelse med OpenID4VC High Assurance Interoperability Profile (HAIP). Formålet med at følge standarden og profilen er dels at anvende gennemarbejdede specifikationer, og dels for at muliggøre udstedelse af beviser til AltID fra andre bevisudstedere på sigt.

3. Præsentation af beviser

Der findes, som tidligere beskrevet, to metoder til præsentation af beviser OID4VP og signerede QR-koden.

OID4VP:

AltID-applikationen 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 suppleres med overholdelse af ISO 18013-7:2025 Annex B, samt HAIP for at sikre en standardiseret implementering, som muliggør udveksling af flere typer af beviser og med en større gruppe af modtagerparter på tværs af EU.

Generering og præsentation af Zero-Knowledge Proofs understøttes ikke fra lancering. Teknologien forventes dog at blive implementeret i fremtidige versioner af AltID, hvilket i så fald ske ved anvendelse af Anonymous credentials from ECDSA i overensstemmelse med Europa-Kommissionens nuværende anbefaling. 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.

Signerede QR-koder:

Signerede QR-koder er en protokol udviklet til AltID. Protokollen muliggør præsentationen og delingen af beviser via en signeret QR-kode, mellem en AltID-app og en bevismodtager. Protokollen kan kun benyttes i fysiske brugsscenarier, hvor en bevismodtager scanner en brugers bevis.

Signerede QR-koder tilbyder en løsning på en række andre behov end OID4VP, fx at protokollen kan benyttes offline. Deling af beviser via signerede QR-koder tilbyder en god brugeroplevelsen, og forøger potentielt udbredelsen af løsningen.

En signeret QR-kode vil være en multipart QR-kode som en bevismodtager skal scanne og samle, for at modtage beviset. Den signerede QR-kode vil have en begrænset levetid, ca. 30 sekunder, for at modvirke snyd, hvor brugere filmer hinandens QR-koder. Dertil er der introduceret en blokering af skærmoptagelser/-billeder inde fra app'en, samt mekanismer som portrætfoto og liveness-elementer, der ligeledes modvirker snyd.

"Man-in-the-middle" angreb vurderes derfor også usandsynlige, da det vil kræve at man:

i. Filmer en borgers skærm i tilstrækkelig høj opløsning til at QR-koden kan genaflæses og uden at det er tydeligt at der er tale om en optagelse, samtidig med, at der filmes tilstrækkeligt længe til at alle delelementer (parts) af QR-koden optages – alt dette uden at borgeren opdager det.
ii. Angriberen skal derefter, indenfor den meget begrænsede levetid for QR-koden, præsentere videoen til en kontrollant, som ikke opdager, at der er tale om en video, eller at hverken tidsstemplet eller billedet på AltID-appens ejer ikke matcher personen foran dem.

4. Administration af beviser

Beviser, som er udstedt til AltID, er under brugerens fulde kontrol. Derfor vil det også være muligt via AltID-applikationen 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 AltID-applikationen, 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 AltID-appen er installeret på, fortsat lever op til kravene for dette. Notatet vil blive opdateret med det endelige design af kontrollerne.

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

Bevisudstedelseskomponenten er designet til at understøtte, at strukturerede data kan hentes fra enhver godkendt autentisk kilde, omformes til og udstedes som et bevis til en AltID-app. 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 i rette format.

BUS er udvikles desuden i overensstemmelse med HAIP. Der vil dog i første version af AltID alene blive udstedt beviser i det format, der er defineret i ISO 18013-5, kaldet "mdoc". Dette format understøtter blandt andet 1) at beviser kan bindes kryptografisk til brugerens 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, når en bruger opretter sit AltID eller når de efterfølgende vælger at tilføje aldersbeviset via beviskataloget.

Efter brugeren har valgt et bevis, sender AltID-applikationen en forespørgsel til BUS. I forbindelse med udstedelse af legitimationskortet, vil brugeren blive bedt om at logge ind via NemLog-in med henblik på at identificere, hvem beviset skal udstedes til. Parallelt med brugerens login autentificeres selve AltID-applikationen via en WUA, der først bliver udstedt under indrulleringen og løbende fornys igennem AltID-applikationens levetid. Det sikrer, at kun godkendte AltID-apps kan få udstedt beviser fra BUS. For aldersbeviset vil det ikke være nødvendigt for brugeren at logge ind.

2. Forespørgsel og datavalidering hos autentiske kilder

Efter autentifikationen viderestiller bevisudstedelseskomponenten 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 AltID vil tre autentiske kilder være integreret med bevisudstedelseskomponenten:

- **PID-Servicen** håndterer udstedelsen af legitimations- og identifikationskort. Data stammer fra CPR via Datafordeleren.
- **PoA-servicen** (Proof Of Age) håndterer udstedelsen af aldersbeviser baseret på fødselsdato ligeledes fra Datafordeleren.
- **Portrætservicen** håndterer tilføjelse af pasfoto til AltID. Konkret scanner brugeren sit pas i AltID-applikationen, herefter leveres pasfotoet, via passcanningsleverandøren, til Portrætservicen, som blandt andet validerer at passet, og det dertilhørende pasfoto, tilhører rette bruger inden det endeligt tilføjes til AltID.

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 AltID 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.

Har du feedback?

Vi vil gerne høre fra dig! Der er flere måder, hvor du kan engagere dig og bidrage til projektet:

Send os din feedback – Har du forslag eller kommentarer til projektet? Skriv til altid@digst.dk

Digitaliserings-
styrelsen