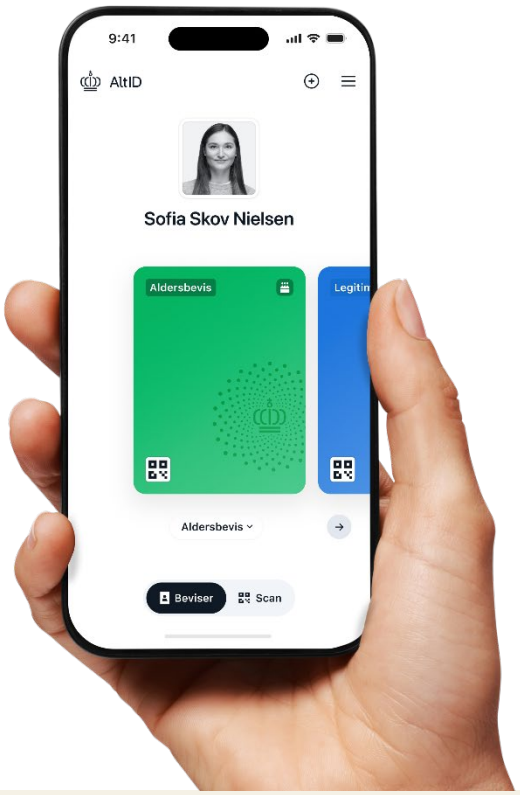
Om AltID


9:41
AltID
Sofia Skov Nielsen
Aldersbevis
Aldersbevis
Beviser
Scan

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
1.4	Gennemskrivning af indhold og struktur	Digitaliseringsstyrelsen	29-05-2026

Velkommen til AltID

Dette materiale er målrettet dem, som ønsker en dybere indsigt i AltID løsningen. Her kan du bl.a. læse om hovedaktører i AltID økosystemet, løsningens hovedkomponenter, hvilke beviser den første version vil indeholde og hvordan de kan benyttes.

God læselyst.

Generelt om AltID

AltID – din app til ID og digitale beviser

AltID giver en borger mulighed for at samle digitale beviser ét sted. De første beviser, man kan tilføje til AltID, vil være udstedt af Digitaliseringsstyrelsen. Digitale beviser kan være mange forskellige ting, det kan være alt lige fra et aldersbevis til et sundhedskort og kørekort.

AltID-appen er dermed et værktøj, som borgere kan benytte til at opbevare og dele digitale beviser på en sikker digital og privatlivsbeskyttende måde. Når borgeren har fået udstedt et bevis af en myndighed, ligger beviset lokalt på borgerens enhed. Dette betyder, at borgeren kan bruge beviserne og dele dem, med en virksomhed eller en anden myndighed, uden at udstederen af beviset kan følge med i, at beviset bliver brugt, og hvor det bliver brugt. Beviserne giver altså borgerne kontrol over deres egne data, og muligheden for at vælge, hvem de deler et bevis med.

Konkret vil AltID ved lancering kunne indeholde et legitimationskort, som kan bruges til identifikation, samt et aldersbevis som kan bruges til at bekræfte, hvorvidt borgeren er over eller under en given aldersgrænse, uden at der deles andre oplysninger. Hvis en bruger tilføjer et billede til AltID-appen, via deres pas, kan appen også bruges som et gyldigt billed-ID. Derudover kan beviserne fra AltID både bruges online og i fysiske situationer.

Digitale beviser indeholder information om brugeren, som kan deles og verificeres, uden at den myndighed, der har udstedt beviset, får kendskab om brugen.

I fremtiden er det hensigten, at andre offentlige myndigheder også kan udstede beviser til AltID, eksempelvis sundhedskortet og kørekortet. At appen kan bruges til at opbevare mange forskelligartede beviser betyder, at appen kan bruges i mange forskellige brugsscenarier.

AltID – baggrund for projektet

Udviklingen af appen indgår som første trin mod efterlevelsen af eIDAS2-forordningen. Forordningen forpligter alle EU-medlemslande til at stille en digital identitetstegnebog til rådighed for borgere.

AltID er dog først og fremmest en national digital identitetstegnebog, der bygger på standarder og specifikationer fra EU-kommissionen og eIDAS2-forordningen. Den nationale digitale identitetstegnebog har således ikke til formål fuldt ud at implementere kravene i eIDAS2-forordningen. Danmark har valgt en tilgang med en trinvis implementering af forordningen, hvilket skal være med til at sikre, at AltID hurtigt kan skabe værdi i Danmark og mindske de risici, der kan være forbundet med gennemførelse af meget store it-projekter. Opdelingen i flere trin følger anbefalinger fra Statens It-råd.

Den nationale AltID app er reguleret af lov 301 af 24. februar 2026 om den nationale digitale identitetstegnebog. Denne lovgivning regulerer AltID som et redskab, men hvor og til hvad redskabet kan benyttes, vil ligeledes afhænge af anden regulering.

Sådan fås AltID

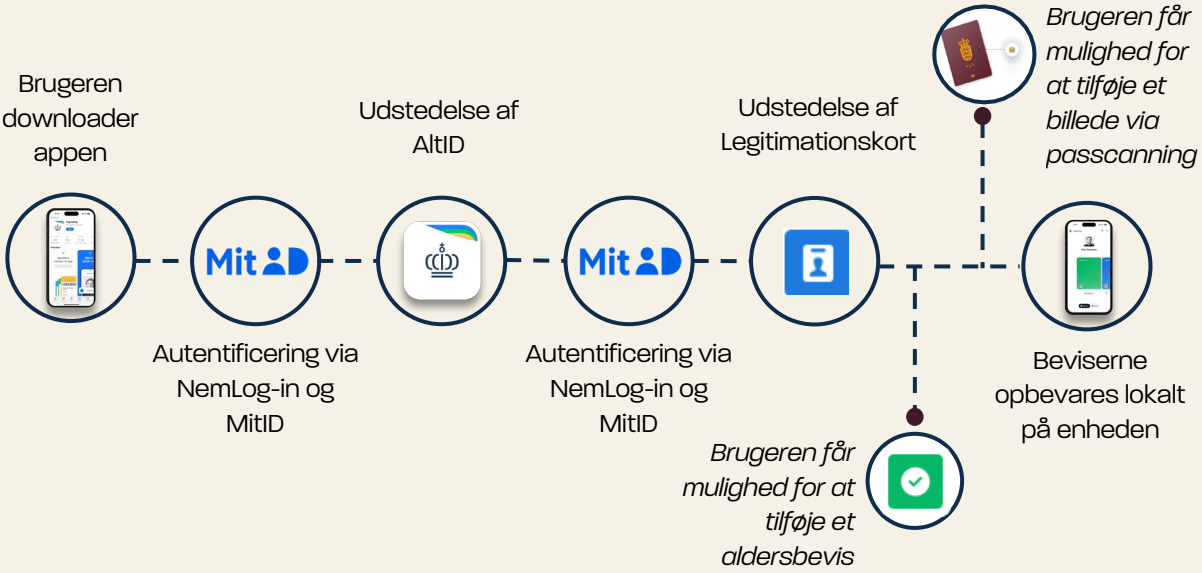
Aldersgrænsen for at få AltID er 13 år, da oprettelsen af appen kræver MitID eller et andet eID[1] knyttet til et CPR-nummer. For at kunne bruge AltID som billed-ID skal man desuden scanne sit pas for at tilføje et billede til appen.

Borgere kan erhverve AltID-appen på deres smartphone via Google Play og App store. Når appen er downloadet, er det første trin, at brugeren skal logge ind med MitID eller et andet understøttet eID. Det er kun muligt at have en aktiv AltID app ad gangen. Appen er frivillig og gratis at downloade.

Når brugeren har oprettet sin AltID-app, skal brugeren oprette et legitimationskort. Dette sker ved at brugeren igen logger ind, hvorefter beviset udstedes til brugerens AltID. For at kunne bruge AltID er det nødvendigt, 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 beviser udstedes til den korrekte person.

[1] eID anvendes i dette dokument i den betydning, der følger af eIDAS2-forordningen. Læs eIDAS2-forordningen her.

Figur 1: 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. Dette gøres 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.

Økosystem for AltID

I økosystemet for AltID er der tre primære aktører med veldefinerede roller og ansvarsområder. Formålet med denne opdeling er at etablere et økosystem hvor der kan være tillid imellem aktørerne, uden at én part får indblik i det fulde end-to-end flow fra udstedelse til deling af beviser. Samtidig tilgodeser denne model i højere grad privacy-by-design end tilfældet er for en typisk centraliseret tillidsløsning, hvor én part agerer mellemmand i alle transaktioner. Ved privacy-by-design forstås at 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 alle dele af løsningen og økosystemet.

De tre vigtigste roller er **bevisudstederen, bevismodtageren og brugeren (faciliteret af AltID-appen).** 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 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

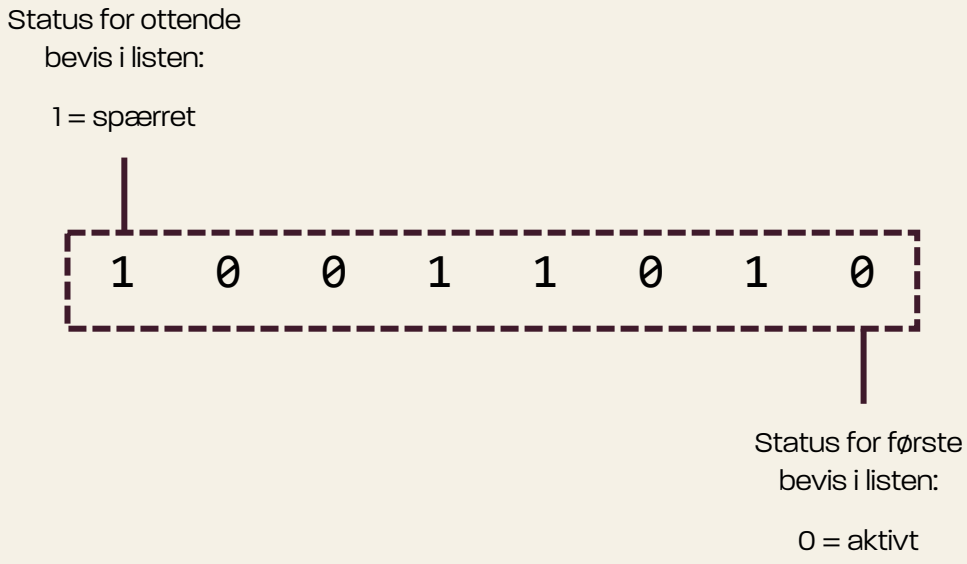
brug. Der er, med andre ord, ikke en forbindelse mellem udstedere og modtagere af beviser.

Aldersbeviset kan ikke anvendes til at kortlægge brugerens adfærd, hverken af myndigheder, der udsteder beviset, eller virksomheder, der modtager det.

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. Statuslisten er den mekanisme, som muliggør at aktørerne kan validere status for både beviser og hinanden, uden at være i kontakt med eller give indblik til andre aktører. Det betyder fx at bevismodtagere kan kontrollere gyldigheden af et modtaget bevis ved at slå op i en statusliste, uden at bevisudstederen får indblik i, at det er sket. Det er angivet direkte i det pågældende bevis, hvorvidt det findes på en statusliste, og i så fald hvorfra listen kan hentes.

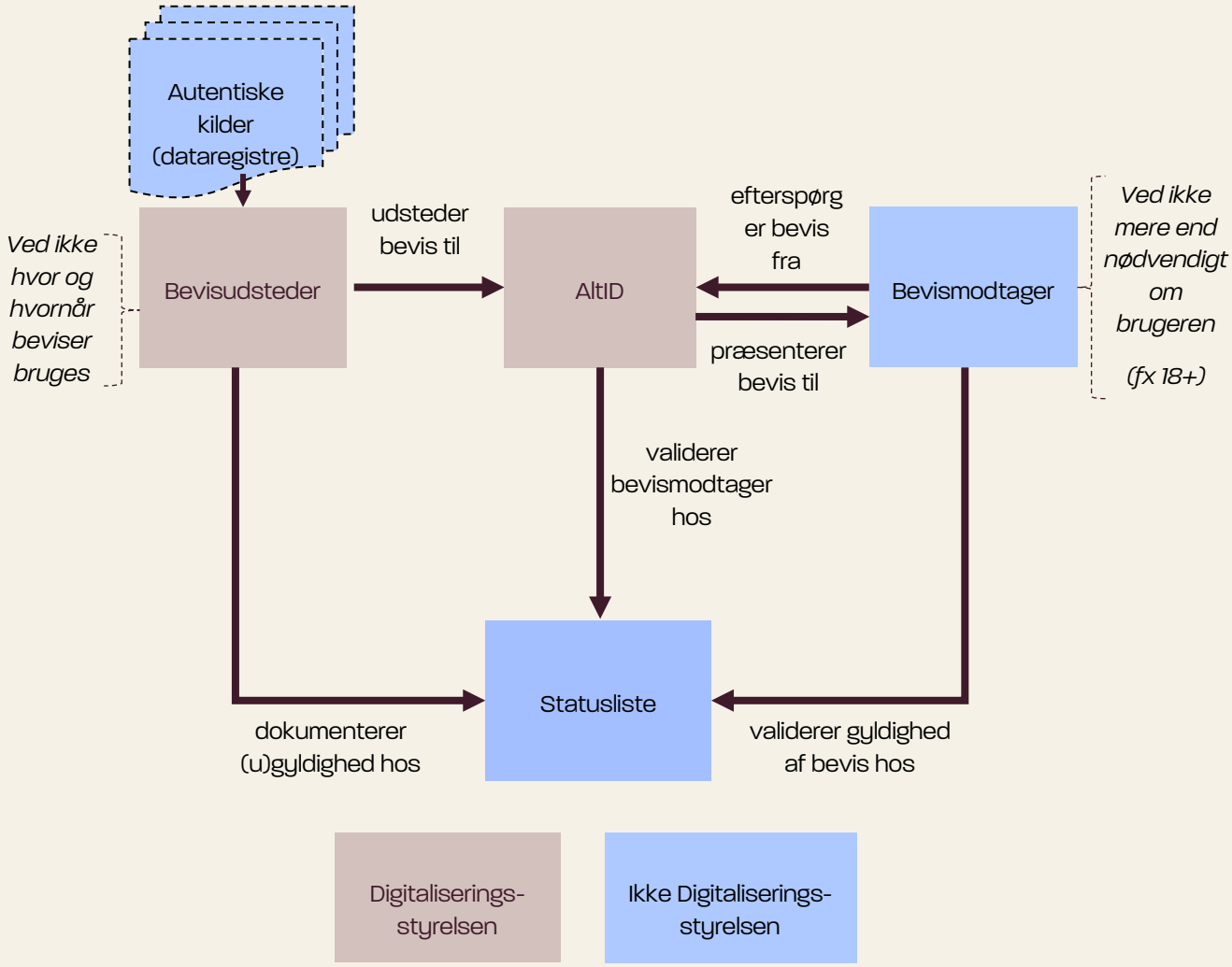
Figur 2: Eksempel på statusliste med otte beviser



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 aktivt og 1 betyder at beviset er blevet spærret. Når en bevismodtager skal kontrollere gyldigheden, har bevismodtageren, fra beviset, fået metadata om, hvilket nummer i talrækken, der repræsenterer det konkrete bevis. Bevismodtageren kan kun hente en samlet statusliste, som indeholder status for

titusindvis af beviser. Dermed får ingen andre end bevismodtageren indsigt i, hvilket bevis der kontrolleres.

Figur 3 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 **modtagerregister** hvor bevismodtagere skal være registreret, for at kunne anmode om andet end aldersbeviser, fx legitimationskortet, online.

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

- **Statuslisten** som er offentligt tilgængelig via internettet og dokumenterer bevisers gyldighed administreres af BUS. Der findes flere typer af statuslister, da der også findes statuslister for både indrullerede AltID-applikationer (som administreres af AltID back-enden) og for registrerede bevismodtagere (som administreres af modtagerregistret). En statusliste har desuden en maksimal kapacitet. Når denne overskrides, oprettes der en ny statusliste, som lever parallelt med de eksisterende. Der kan derfor i praksis eksistere flere statuslister af samme type. Statuslisterne udstilles af en CDN-udbyder, som sørger for at de er tilgængelige.

Legitimationskortet bliver først et gyldigt billed-id, når en bruger tilføjer et billede til. beviset. I mellemtiden er det et identitetsbevis, som fx 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 i den tekniske dokumentation for AltID.

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 præsenteres de to beviser.

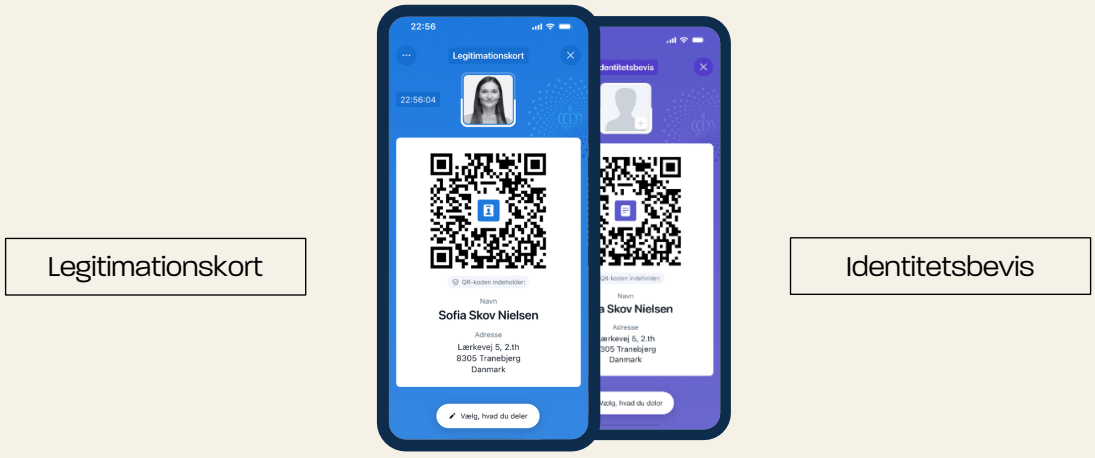
Hvad AltID kan benyttes til, afhænger af brugerens beviser. Der er stor forskel på, hvad legitimationskortet og aldersbeviset kan bruges til.

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. En fordel er, at beviset kan bruges mere dataminimerende, fx ved alene at bevise ens navn, uden nødvendigvis at dele data som CPR-nummer eller ens konkrete adresse.

Figur 4 viser Legitimationskortet og Identitetsbeviset. Hvis et billede tilføjes, bliver beviset et legitimationskort, hvis ikke vil beviset være et identitetsbevis, der kan bruges online, men ikke som et billed-ID.

Figur 4: Legitimationskort/Identitetsbevis



Legitimationskortet indeholder følgende data og metadata:

Data:

- Navn
- Fornavn
- Efternavn
- Fødselsdato
- Fødselsregistreringssted
- Nationalitet
- Adresse
- CPR-nummer

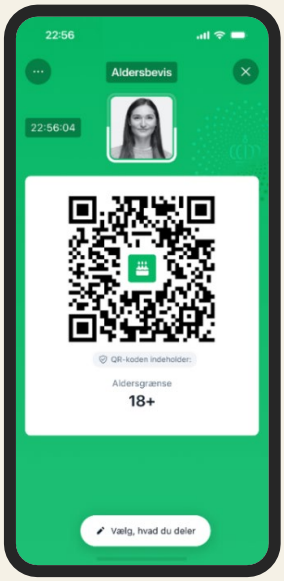
Metadata:

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

Aldersbeviset

Aldersbevisets **formål** er, at en bruger kan bevise, hvorvidt de er over en bestemt alder. Det kan fx være relevant hvis brugeren skal købe aldersbegrænsede varer som alkohol og tobak eller skal ind på aldersbegrænsede lokationer som natklubber og barer. Det kan også være relevant i online sammenhænge. Brugeren kan benytte beviset anonymt, da beviset ikke indeholder brugerens præcise alder, CPR-nummer eller andre personlige oplysninger.

Figur 5: Aldersbeviset



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+, 27+ 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 18-årig indeholde:

- age_over_13 = true
- age_over_15 = true
- age_over_16 = true
- age_over_18 = true
- age_over_21 = false
- age_over_23 = false
- age_over_25 = false
- age_over_27 = false
- age_over_67 = false

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 metadata.

Aldersbeviset indeholder dog også nødvendige metadata, der er unikke for det pågældende bevis. Selvom disse metadata ikke er personhenførbare, så giver de mulighed for at en bevismodtager kan genkende et bevis de tidligere har set. For at udelukke denne mulighed for sporing på tværs af sessioner er aldersbeviset designet som et engangsbevis. Det betyder, at når aldersbeviset bliver udstedt, så genereres der 30 unikke beviser 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, for at foretage en anonym aldersverifikation.

Sådan deles beviser fra AltID

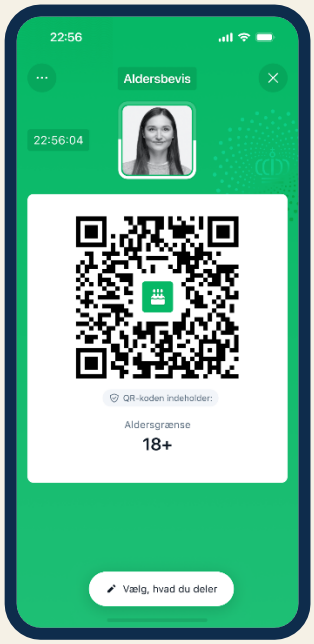
Beviserne fra AltID kan deles på tre måder. Den første måde er at bruge AltID og beviserne som var de et fysisk ID, der bliver fremvist til en bevismodtager. Beviserne indeholder visuelle kontrolelementer som en kontrollant vil kunne se efter, for at vurdere om det er en gyldig AltID app. De visuelle kontrolelementer som en bevismodtager skal holde øje med, er bl.a. en dynamisk QR-kode, et ur, et vandmærke og et billede med en gyroskopeffekt i rammen. Hvis AltID skal bruges som et billed-ID forudsætter det, at brugeren har tilføjet billedet fra deres pas.

Beviser fra AltID kan også deles elektronisk. Elektronisk verifikation af beviser tilbyder bevismodtagere en større grad af sikkerhed, for at beviset og appen er gyldig. Ved elektronisk deling anvendes ISO mdoc formatet, som er specificeret i ISO 18013-5. Beviser i dette format indeholder en række kontrolelementer, som gør bevismodtageren i stand til at validere at beviset er gyldigt og at det ikke er blevet ændret eller flyttet til en anden telefon. Samtidig understøtter formatet *selektiv videregivelse*, som betyder at en bruger kan dele et bevis uden nødvendigvis at dele alle attributter. Dertil vil elektronisk deling og modtagelse af beviser potentielt kunne tilbyde nye forretningsmuligheder og måder at betjene kunder på.

De to elektroniske metoder til deling af beviser med bevismodtager er henholdsvis 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 kan anvendes til deling online og i fysiske scenarier.

Figur 6: Måder at dele og modtage beviser fra AltID elektronisk

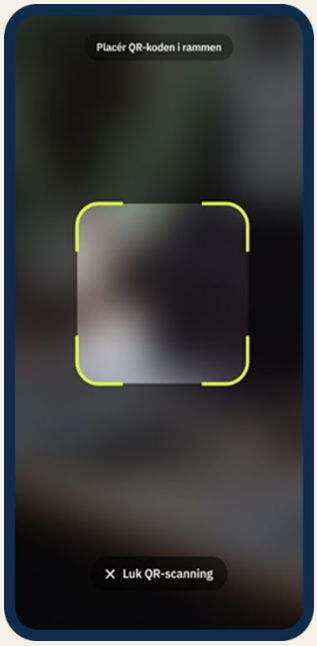
Mulighed 1: Signeret QR-kode



QR-kode indeholder data.

Data aflæses ved scanning.

Mulighed 2: OpenID4VP



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

Data overføres via internet.

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 tidsbegrænset signeret QR-kode, som en bevismodtager kan scanne for dermed at 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 offline, fx hvis man skal aldersverificeres et sted, hvor der ikke er internetdækning, eksempelvis på en festival, i metroen eller i en kiosk med dækningsmangel.

Signerede QR-koder er en protokol udviklet til AltID og denne metode er således et tillæg til Europa-Kommissionens arkitekturramme, som foreskriver at ISO 18013-5 skal anvendes 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 uprøvede eller svært anvendelige teknologier, fx **Near Field Communication (NFC), som stiller krav til særligt hardware hos modtageren.**

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 bevismodtagerens navn hvis denne er registreret i modtagerregistret. Herefter kan brugeren vælge at dele data ved at swipe, som man kender det fra MitID, hvis de vil godkende delingen. Dette kan eksempelvis være i forbindelse med køb af

aldersgrænsede varer online, eller ved oprettelse af en bruger på platforme, hvor legitimationskortet kan bruges til automatisk at udfylde ens oplysninger.

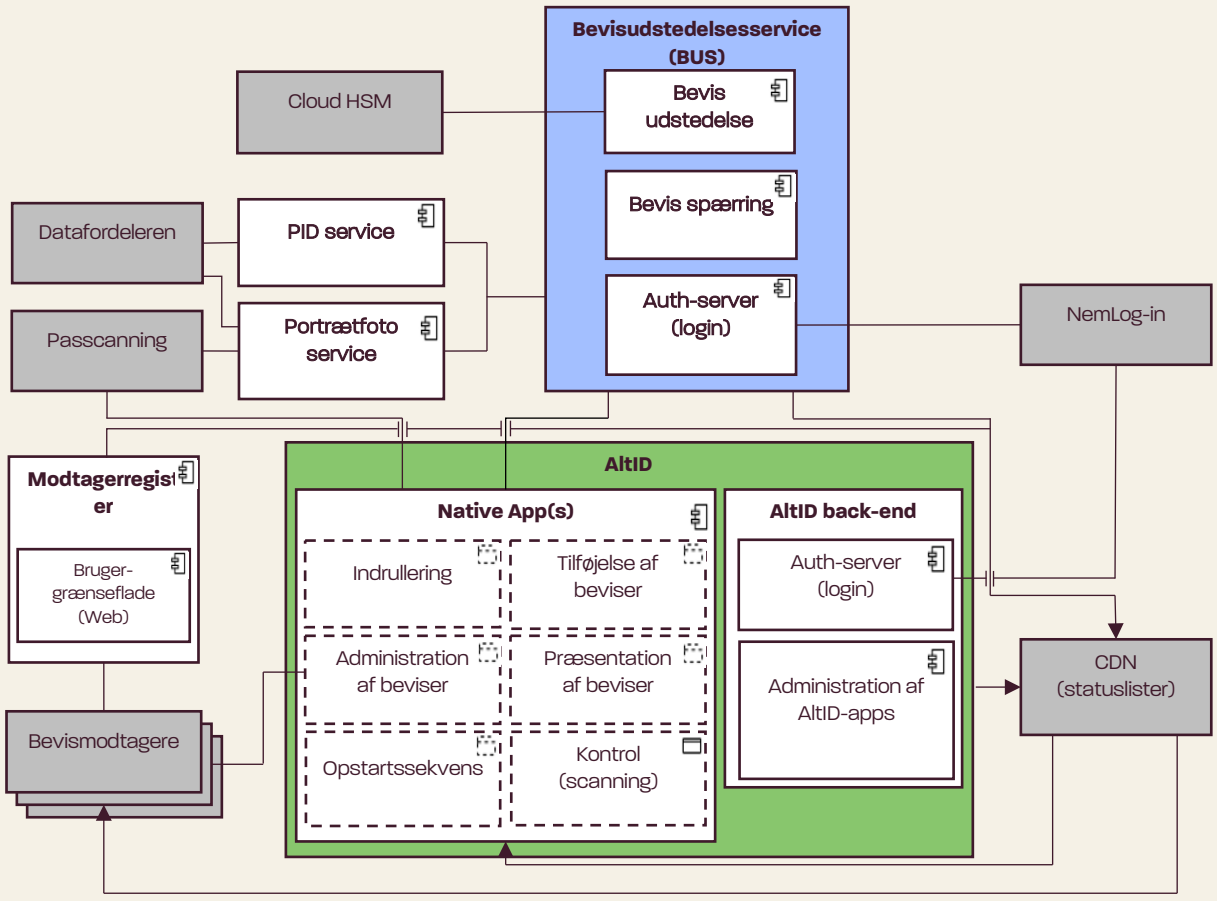
OID4VP er den protokol, der anbefales af Europa-Kommissionen til udveksling af beviser online. Det vil derfor også være den metode, der anvendes til aldersverificering på tværs af online platforme i EU. Protokollen forventes også brugt i fysiske brugsscenarier, da den for virksomheder muliggør, at de i fremtiden kan modtage EU-brugere, der benytter en eIDAS2-tegnebog.

Sådan er AltID opbygget

Arkitektur og byggeblokke

I dette afsnit præsenteres høj-niveauarkitekturen for AltID. AltID-projekt etablerer to separate it-systemer, som udgør hver deres aktør i økosystemet. 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

Den del af projektet, som vedrører det produkt som brugeren er i direkte berøring med, omtales samlet som "AltID" i Figur 7. 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 Figur 7, følgende funktionsområder:

1. **Indrullering**

Det er en forudsætning, at AltID-appen aktiveres, før den kan anvendes. I praksis betyder det, at brugeren skal logge ind via NemLog-in og at AltID-appen skal have udstedt en Wallet Unit Attestation (WUA) fra back-enden, som knytter brugeren til den specifikke AltID-app. Denne registrering ligger i AltIDs back-end så længe man har en aktiv AltID-app og deles aldrig med hverken bevisudstedere eller modtagere. På denne måde sikres det at brugerens AltID-app kan spærres, selvom brugeren ikke længere skulle have adgang til den. Samtidig sikrer det, at en bruger kun kan have én aktiv AltID-app ad gangen.

I forbindelse med udstedelsen af WUA kontrolleres det at enheden lever op til en række sikkerhedskrav, fx at den er beskyttet af PIN-kode eller biometri og at den ikke er jailbroken eller rooted. WUA udgør på den måde også AltID-appens bevis for, at den lever op til disse krav.

Status for WUA administreres via en statusliste, som løbende opdateres af AltID back-end, og som er tilgængelig via CDN. Status opdateres kun i tilfælde af at brugeren enten selv spærrer sin AltID-app, enten direkte ved at anvende "nulstil app"-funktionen, eller indirekte, ved at brugeren aktiverer en ny AltID-app, eller ved at brugeren kontakter supporten og beder dem om at få den spærret.

Log ind håndteres af AltID back-ends autorisationsserver ("auth-server"), som anvender OIDC autorisationskode flow udvidet med Pushed Authorizaion Requests (PAR), Proof Key for Code Exchange (PKCE) og Attestation-Based Client Authentication (ABCA). Efter succesfuldt flow udstedes et token afgrænset til et specifikt scope (her oprettelse af WUA) til AltID-appen. AltID-appen veksler løbende sine tokens til andre scopes alt efter hvilken funktion der skal udføres mod back-end. Det er kun i forbindelse med oprettelse af WUA at brugeren sendes til NemLog-in.

Som en del af indrulleringen skal brugeren oprette en PIN-kode, som skal anvendes når man åbner AltID-appen. Det er også muligt at vælge at anvende biometri i stedet. Selve PIN-koden opbevares i krypteret form i den hardware-beskyttede opbevaring på enheden, som kun AltID-appen har adgang til.

2. **Tilføjelse af beviser**

For at få udstedt beviser, agerer AltID-applikationen klient (Wallet) i overensstemmelse med OpenID4VC High Assurance Interoperability Profile (HAIP) afsnit 4 og 6 (ISO mdocs), som det er specificeret af Europa-Kommissionen i regi af eIDAS2. 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.

Forud for tilføjelsen af beviser veksler AltID-appen sin WUA til en Wallet Instance Attestation (WIA) hos back-enden. WIA er kun gyldig i fem minutter og dokumenterer dermed over for bevisudstederen at appen aktuelt lever op til sikkerhedskravene. Herudover indeholder den information om hvor AltID-

appens status kan kontrolleres, således at det er muligt for en bevisudsteder at kontrollere denne og eventuelt spærre udstedte beviser, hvis appen ikke længere er aktiv.

AltID-appen generer de kryptografiske nøgler som beviset skal bindes til, for at sikre at det ikke kan overflyttes til en anden enhed. Nøglerne genereres og opbevares kun på enheden hvor AltID-appen er installeret. Til det formål anvendes de hardware-baserede metoder som understøttes på henholdsvis Android (Strongbox eller Trusted Execution Environment) og iOS (Secure Enclave). Nøglerne deles med back-enden som kontrollerer dem og validerer at enheden kan bevise at den er i kontrol med dem. AltID-appen får herefter udstedt en Wallet Key Attestation (WKA), som ligeledes kun er gyldig i fem minutter, og som dokumenter overfor bevisudstederen, at nøglerne har bestået kontrollen.

De tre attester baseret sig på Europa-Kommissionens tekniske specifikation herfor.

I forbindelse med tilføjelse af portrætfoto fra pas (eller andet identitetsdokument) understøtter AltID-appen scanning og overlevering af pasdata til passcanningsleverandøren. Dette foregår ved at brugeren først scanner billedsiden i passet med enhedens kamera for at åbne op for passets RFID-chip. Derefter scannes chippen, som indeholder passets data, med enhedens NFC-læser. Disse data sendes fra AltID-appen til passcanningsleverandøren via BUS, som agerer proxy, men ikke kan tilgå pasdata, da disse er krypteret.

Efter udstedelse gemmes beviserne i krypteret form i den hardware-beskyttede opbevaring på enheden, som kun AltID-appen har adgang til. Dette er ikke muligt for portrætfotoet, grundet dets filstørrelse. Det opbevares i stedet i den normale app-opbevaring, men er krypteret med en nøgle som dannes og opbevares i den hardware-beskyttede opbevaring.

3. Præsentation af beviser

Der findes, som tidligere beskrevet, to metoder til præsentation af beviser: OID4VP og signerede QR-koder. Ved begge fremgangsmåder dannes og signeres præsentationen direkte på enheden i CBOR-format, som henholdsvis et ISO mdoc *DeviceResponse* eller et enkeltstående ISO mdoc *Document*. Forskellen skyldes at en signeret QR-kode altid kun vil indeholde et enkelt bevis ("document") per præsentation, mens en OID4VP præsentation kan indeholde flere beviser. For yderligere beskrivelse af dataformater i AltID henvises til afsnit 5 i den tekniske dokumentation for AltID.

Generering og præsentation af Zero-Knowledge Proofs (ZKP) understøttes ikke ved lancering. Teknologien forventes at blive implementeret i fremtidige versioner af AltID, når der er truffet beslutning om fremgangsmåden herfor i regi af Europa-Kommissionens arbejde med de tekniske specifikationer på området. Ved lancering benytter AltID som nævnt engangsbeviser for aldersbeviset, der sikrer anonymitet og et tilsvarende niveau af privatlivsbeskyttelse, da to modtagere aldrig ser det samme bevis.

a. 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 bevismodtagere på tværs af EU i forbindelse med aldersverifikation. Herudover understøttes HAIP afsnit 5, 5.1, 5.3.1 og 6 (ISO mdocs), som det er specificeret af Europa-Kommissionen i regi af eIDAS2, for at sikre en standardiseret og fremtidskompatibel implementering. I sidstnævnte flow understøtter AltID-appen at sende brugeren tilbage til den hjemmeside de kom fra

efter deling af beviset. Dette afhænger dog af at bevismodtageren medsender de nødvendige informationer. For yderligere beskrivelse af OID4VP i AltID henvises til afsnit 4 i den tekniske dokumentation for AltID.

b. Signerede QR-koder:

AltID-appen kan generere en signeret QR-kode direkte på enheden, som indeholder en tidsbegrænset præsentation af et bevis. Formatet for indholdet af QR-koden svarer til det der deles i OID4VP. Et bevis i ISO mdoc format er for stort til at kunne indeholdes i en enkelt QR-kode. Derfor er en signeret QR-kode i praksis en sekvens af QR-koder, som hver indeholder en del af beviset. For yderligere beskrivelse af signerede QR-koder henvises til afsnit 3 i den tekniske dokumentation for AltID.

4. Administration af beviser

Beviser, som er udstedt til AltID, er under brugerens fulde kontrol. Derfor er det også muligt at opdatere eller slette beviser via AltID-applikationen brugergrænseflade, 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, bliver opdateret eller slettet. 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. Konkret består opstartssekvensen af følgende kontroller:

- Enheden er (fortsat) beskyttet med PIN-kode eller biometri
- Enhedens sikkerhed og integritet er (fortsat) intakt
- Enheden har forbindelse til internettet*
- AltID-appen har en opdateret konfigurationsfil (hentes fra CDN)
- AltID-appen er på en understøttet version
- AltID-appen har bevisudstederen metadata (hentes fra BUS)
- AltID-appen har en gyldig WUA* (ved nærtstående udløb forsøges det at hente en ny)
- AltID-appen har et gyldigt legitimationskort* (ved nærtstående udløb forsøges det at hente en ny)

For de kontroller hvor der angivet * er det muligt at gennemføre opstartssekvensen selvom disse fejler, dog vil der være begrænsninger i hvilke funktioner der kan tilgås i appen i de tilfælde. Fejler de øvrige kontroller kan AltID-appen ikke anvendes. Hvis WUA fremgår som spærret af statuslisten, vil appen blive nulstillet.

Konfigurationsfilen, som AltID-appen henter, administreres af AltID back-end, som løbende uploader den som en signeret JWT til det anvendte CDN. Den indeholder 1) eventuelle driftsbeskeder, som skal præsenteres i brugergrænsefladen, herunder angivelse af om antallet af brugere, som kan tilgå appen, skal begrænses eller helt blokeres 2) minimums version som AltID-appen skal være på for henholdsvis Android og iOS, samt eventuelt specifikke versioner, som der blokeres for og 3) hostnavne og tillidsankre for eksterne integrationer.

Bevisudstedelsesservice (BUS)

Det system, der håndterer udstedelse af beviser til AltID, omtales samlet som Bevisudstedelsesservice (BUS). BUS fungerer som Issuer i henhold til OID4VCI og HAIP afsnit 4 og 6 (ISO mdocs), som det er specificeret af Europa-Kommissionen i regi af eIDAS2. Systemet er ansvarligt for at modtage anmodninger om udstedelse af beviser fra AltID-appen, autentifikation af brugeren og appen, indhentning af data fra de autentiske kilder og indkodning af beviser i ISO mdoc format. Herudover er systemet ansvarligt for at administrere beviser efter udstedelse ved at ajourføre statuslisterne, hvis fx et bevis spærres i den autentiske kilde.

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 beviser og 2) at enkelte myndigheder ikke skal forholde sig til omdannelsen fra rådata til bevisformat. Første version af AltID understøtter kun beviser i ISO mdoc format.

1. Initiering og autentifikation

Bevisudstedelsen starter, i forbindelse med en brugers oprettelse i AltID-appen, eller når de efterfølgende vælger at tilføje eller opdatere et bevis via appen. På brugerens foranledning sender AltID-appen en autorisationsforespørgsel til BUS. Denne forespørgsel håndteres af auth-server komponenten, der, ligesom AltID back-end, anvender et OIDC autorisationskode flow med PAR, PKCE og ABCA. AltID-appen autentificeres ved præsentation af WIA i forbindelse med ABCA-delen, mens brugeren autentificeres via NemLog-in såfremt der er behov for det. Hverken aldersbeviset eller portrætfoto kræver at brugeren autentificeres hos NemLog-in, da identiteten er kendt af AltID-appen fra legitimationskortet. Udstedelse eller opdatering af legitimationskortet kræver altid et nyt log ind via NemLog-in. Efter succesfuldt flow udstedes et token afgrænset til et specifikt scope knyttet til de enkelte bevistyper, fx er der et scope til "udstedelse af aldersbevis".

2. Forespørgsel og datavalidering hos autentiske kilder

Efter autorisationen viderestiller BUS forespørgslen til den relevante autentiske kilde. Entydig identifikation af brugeren sker med CPR UUID, som er et unikt ID alle borgere tildeles i CPR og som modtages fra NemLog-in. Den autentiske kilde validerer, at brugeren er berettiget til det pågældende bevis og returnerer i bekræftende fald de data, der skal indgå i beviset, til BUS. Ved lancering af AltID vil to autentiske kilder, som begge administreres af Digitaliseringsstyrelsen, være integreret med BUS:

a. PID service:

PID servicen håndterer levering af data til BUS i forbindelse med udstedelse af legitimations- og identifikationskort, samt udstedelsen af aldersbeviser. Data stammer fra CPR og hentes ved Datafordeleren. I forbindelse med indhentning af data har servicen ansvar for at validere at de nødvendige attributter er inkluderet i svaret fra Datafordeleren, samt at omforme data til det

strukturerede format, som skal inkluderes i beviset. Dette er fx relevant i forbindelse med aldersbeviset, hvor fødselsdato fra CPR skal omformes til en række "alder_over_X" attributter med sandt/falsk-værdier, inden data leveres til BUS.

Ved udstedelse af legitimationskortet foretager PID servicen en registrering af de informationer, som er nødvendige for at kunne spærre beviset igennem dets levetid. Det drejer sig om en unik identifikator for brugeren samt statusliste information for både beviset selv, samt den AltID-app det er knyttet til. Til en start spærres legitimationskortet kun når det detekteres at den tilhørende AltID-app ikke længere er aktiv. Dette sker i praksis ved at PID servicen dagligt henter og gennemgår statuslisten for AltID-apps (WUA). PID servicen kan ikke selv effektuere en spærring af beviset da statuslisterne håndteres af BUS.

På sigt er det hensigten at anvende Datafordelerens CPR hændelser til løbende ajourføring af legitimationskort efter udstedelse. For at kunne vurdere om en ændring i CPR er relevant for et eksisterende bevis, gemmes en samlet hashværdi af bevisets indhold. Dette er nødvendigt da CPR hændelser alene fortæller at der er sket en ændring i en persons data, ikke hvad den specifikke ændring går på. På denne måde kan en hashværdi af personens aktuelle CPR data sammenlignes med den gemte hashværdi, således at systemet ikke skal ligge inde med selve personoplysningerne for at foretage denne vurdering. Indtil denne funktionalitet er etableret, skal brugere selv opdatere deres beviser via AltID-appen, fx i tilfælde af flytning.

For aldersbeviser foretages ingen registrering. Rigtigheden af attributterne i aldersbeviset er i stedet bundet op på at det senest udløb på brugerens fødselsdag. For ikke at afsløre brugerens fødselsdato overfor en bevismodtager i det tilfælde, angives udstedelsesdatoen for aldersbeviser altid til 30 dage før udløbsdatoen.

b. Portrætfoto service:

Portrætfoto servicen håndterer tilføjelse af portrætfoto til AltID-appen. Data stammer fra brugerens pas (eller andet identitetsdokument) og hentes ved passcanningsleverandøren, som har fået det fra AltID-appen. I forbindelse med appens scanning af passet tildeles den et sessions ID, som den inkluderer i forespørgslen til BUS. **Portrætfoto s**ervicen henter de relevante data fra passcanningsleverandøren, som er knyttet til den pågældende session, og validerer at sikkerhedskontrollerne er bestået og at de nødvendige attributter er tilgængelige. Samtidig henter servicen borgerens CPR data fra Datafordeleren. Disse sammenlignes med data fra passet for at validere at passet tilhører rette bruger. Efter succesfuld validering returneres portrætfotoet til BUS og ingen data gemmes i servicen.

Selvom portrætfotoet teknisk set udstedes som et bevis, er det ikke muligt at dele det med bevismodtagere.

3. Konstruktion og udstedelse af beviser

Når data returneres fra den autentiske kilde, omdanner BUS det til bevisformatet ISO mdoc. For en nærmere beskrivelse af formatet henvises til afsnit 5 i den tekniske dokumentation for AltID. Omdannelsen til ISO mdoc indebærer også at beviset skal signeres af BUS. Dette sker konkret ved at

en hash af bevisets "MobileSecurityObject" sendes til signering ved en Cloud HSM, som indeholder den unikke kryptografiske signeringsnøgle for BUS, og at den returnerede, signerede data inkluderes i selve beviset. Signaturen tjener to formål: 1) den beviser overfor bevismodtagere at beviset er udstedt af BUS og derfor som udgangspunkt er validt og 2) de signerede data, gør bevismodtagere i stand til at validere at beviset hverken er blevet ændret eller flyttet efter udstedelsen. Signeringsnøglen beskyttes derfor af en HSM for at give størst mulig sikkerhed for at ingen andre end BUS kan få adgang til den.

Beviset leveres fra BUS til AltID-appen som specificeret i OID4VCI. Beviserne gemmes efter udstedelse udelukkende lokalt på brugerens enhed. BUS opbevarer ikke beviser, men behandler kun brugernes data i forbindelse med udstedelse.

4. **Spærring af beviser**

For visse typer af beviser er der behov for at kunne spærre et udstedt bevis, hvis dets indhold ikke længere er retvisende. Dette er en forudsætning for at beviser, hvis indhold kan ændre sig efter udstedelse, kan have en lang gyldighedsperiode. Det gælder ved lancering kun for legitimationskortet, men kan på sigt også blive relevant for andre beviser. For beviser hvor dette er tilfældet, vedligeholder den autentiske kilde en statusliste, der viser, om et bevis er aktivt eller inaktivt (spærret). Ved lancering er det kun PID servicen, der håndterer dette, og kun for legitimationsbeviser. BUS håndterer i praksis statuslisterne, i den forstand at den er ansvarlig for oprettelse, ændringer og upload af statuslisterne til CDN. Men BUS spærrer kun de indeholdte beviser på besked fra den autentiske kilde.

Modtagerregister

For at kunne modtage legitimationsbeviset via OID4VP skal bevismodtagere registreres, således at AltID-appen kan autentificere dem. Dette muliggør også at bevismodtagerens navn kan præsenteres for brugeren i AltID-appen. Selve registreringen foregår i modtagerregisteret, som er en selvbetjeningsportal, hvor en udpeget medarbejder hos en bevismodtager kan logge ind med MitID Erhverv og registrere organisationen. Modtagerregisteret indhenter automatisk stamdata om organisationen fra CVR, men bevismodtageren skal selv uploade den offentlige nøgle fra det OCES systemcertifikat, som bevismodtageren anvender til at signere sine præsentationsforespørgsler i AltID, for at blive registreret. Efter succesfuld registrering udstedes et token til bevismodtageren, som de skal inkludere i OID4VP forespørgsler til AltID-appen. På den måde kan AltID-appen validere bevismodtagerens identitet. Modtagerregisteret kontrollerer løbende status for uploadede OCES certifikater, og spærrer udstedte tokens hvis det tilknyttede certifikat ikke længere er aktivt. Til dette formål anvendes ligeledes en statusliste, som udstilles af CDN.

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

Nyttige links

Driftsstatus for AltID	digitaliser.dk - AltID
Teknisk dokumentation, der beskriver hvordan man integrerer med AltID	digitaliser.dk - Technical Integration: AltID (PDF)
Link til digst.dk med information til organisationer	Til organisationer – sådan modtager I beviser fra AltID