Om MitID

Baggrund

Version 1.04

Om MitID

Indhold

Velkommen til MitID

Dette materiale har til formål at oplyse om MitID: Danmarks eID-løsning, som kan anvendes på tværs af offentlige og private tjenester.

Materialet giver en lidt dybere indføring i bl.a. opbygningen af MitID, de centrale sikkerhedselementer og af MitID appen. Det er målrettet dem, som har brug for lidt dybere teknisk indsigt og er derfor ikke udarbejdet med slutbrugeren for øje.

God læselyst.

Digitaliseringsstyrelsen og Finans Danmark
MitID-partnerskabet

MitID er resultatet af et veletableret og unikt samarbejde mellem det offentlige og landets pengeinstitutter. Samarbejdet har været drevet af et stærkt ønske om at skabe én attraktiv national eID-løsning, som bruges på tværs af offentlige og private tjenester – og dermed skaber sammenhæng for brugerne.

Generelt om MitID-løsningen

MitID – Danmarks eID-løsning

MitID er et digitalt ID, som kan bruges til blandt andet at overføre penge i netbanken eller logge på offentlige selvbetjeningsløsninger som skat.dk, borger.dk og sundhed.dk. MitID lever op til de nyeste internationale sikkerhedskrav og er desuden modulært og fleksibelt opbygget, så det kan tilpasses fremtidige trusselsbilleder, ligesom det kan imødekomme fremtidens digitale udfordringer og muligheder.

Aldersgrænsen for at få MitID er 13 år. Dog kan der være en højere aldersgrænse for at bruge de enkelte selvbetjeningsløsninger, hvilket besluttes af de enkelte udbydere af løsningerne.

Det er ikke et krav, at man skal have MitID.

Sådan bruges MitID

MitID er primært en app, hvor man med et swipe kan godkende handlinger på nettet. Der findes dog fysiske alternativer, hvis man ikke kan eller ønsker at bruge MitID app. MitID er gratis at få og anvende.

MitID app

MitID er først og fremmest en app til smartphone/tablet. Med MitID app kan man med et swipe overføre penge eller logge ind på en digital selvbetjeningsløsning.

MitID kodeviser

MitID kodeviser er et alternativ til dem, der ikke har mulighed for at bruge MitID app. MitID kodeviser er en lille elektronisk enhed, der viser en engangskode, som man indtaster, når man skal bruge MitID.

MitID kodeoplæser

MitID kodeoplæser er et alternativ til dem, der ser dårligt eller har et synshandicap. Kodelæseren har en stor skærm, hvor koden vises. Den kan også læse koden højt og kan tilsluttes høretelefoner.

MitID chip

MitID chip er primært til erhvervsbrugere eller til de brugere, der ønsker et alternativ til MitID kodeviser eller -kodeoplæser. Chippen kan tilkøbes.

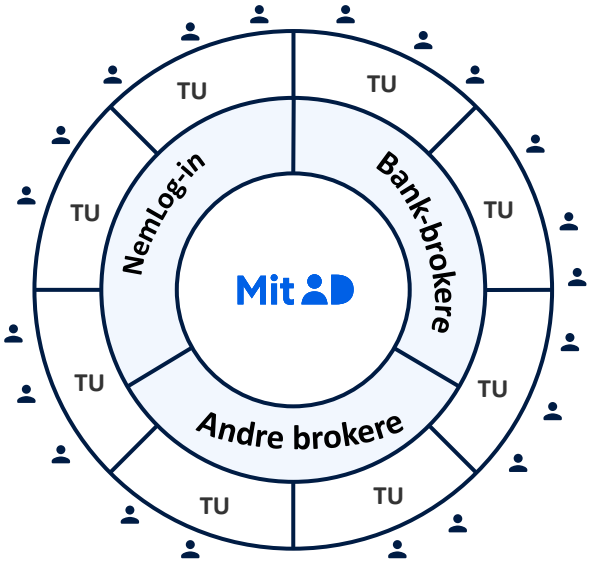
Sådan fås MitID

Der er to forskellige måder at få MitID på, men fælles er, at man skal kunne bekræfte, hvem man er – så ingen kan få MitID på en andens vegne. Man skal også vælge et bruger-ID - og beslutte, hvordan man vil bruge MitID, f.eks. med MitID app eller -kodeviser. Man kan få MitID ved at:

- scanne sit gyldige pas/internationale ID-kort i MitID appen
- besøge Borgerservice med gyldig legitimation.

Sådan er MitID opbygget

MitID's infrastruktur
MitID's infrastruktur er bygget op af forskellige lag, som tilsigter at beskytte MitID-kernen bedst muligt. Det er illustereret i denne model:



Forklaring

= brugeren, der skal anvende MitID

TU = tjenesteudbyder (det sted, hvor man som bruger skal bruge MitID, f.eks. netbank, borger.dk)

Broker = det lag, som giver tjenesteudbyderne adgang til MitID.

- Bank-brokerne giver bankerne adgang til MitID.
- NemLog-in giver offentlige myndigheder adgang til MitID.
- Andre brokere giver øvrige tjenesteudbydere adgang til MitID.

Alle tjenesteudbydere tilsluttes gennem en certificeret MitID broker. En broker er en it-virksomhed, som skærmer identiteterne i MitID, og som formidler adgang for tjenesteudbyderen til MitID samt varetager den underliggende tekniske integration til MitID.

Det er med til at styrke sikkerheden, da MitID-løsningen kun kan tilgås af certificerede brokere og ikke af mange forskellige tjenesteudbydere. Brokeren skal være certficeret for at blive koblet direkte på MitID-løsningen. Det betyder, at det f.eks. kun er brokerne, der skal forholde sig til ændringer i bl.a. MitID-snitflader og sikkerhedsprocedurer – og at der i MitID er høj kontrol med, hvem der har adgang til identiteterne.

MitID er elektronisk validering af en persons identitet
MitID er udviklet med modularitet og fleksibilitet som hovedkrav. Dette gør det nemt og hurtigt at omstille MitID til nye sikkerhedskrav – og at håndtere et trusselsbillede, der ændrer sig løbende. Der bliver løbende holdt øje med trusler mod MitID, så der kan indføres tiltag, der kan imødegå nye risici og trusler.

MitID er en løsning for elektronisk validering af en persons identitet – også kaldet autentifikation – som Digitaliseringsstyrelsen og pengeinstitutterne står bag. MitID er fokuseret på de dele af den digitale infrastruktur, hvor partnerskabet bag MitID har fælles behov. Øvrige naturlige elementer af den digitale infrastruktur, f.eks. inden for fuldmagt og digital signatur udvikles separat af de enkelte parter eller andre private aktører.

Erhvervsdelen og signaturløsningen er udviklet i regi af den offentlige sektor og tilbydes som en del af NemLog-in-projektet. NemLog-in varetager endvidere rollen som MitID broker for alle offentlige tjenesteudbydere, dvs. at det er herigennem, at f.eks. borger.dk og skat.dk får adgang til MitID.

Der er implementeret en række sikkerhedsforanstaltninger i løsningen, f.eks. kan brokeren benytte risikodata afleveret af MitID til at vurdere risikoen ved en specifik MitID-autentifikation.

EU-lovgivning regulerer området
Et af de områder, der udvikler sig løbende, er den EU-lovgivning, der regulerer området.

For den offentlige sektor er det især eIDAS-forordningen, der har betydning. Her defineres krav og standarder til de nationale, offentlige selvbetjeningsløsninger, der muliggør brug af digitale identiteter på tværs af EU's medlemslande. Fra 18. september 2018 er offentlige tjenesteudbydere i alle EU-lande forpligtet til at modtage og anerkende officielle, digitale identiteter fra andre EU-lande på linje med landets egne digitale identiteter.

Danmark har anmeldt MitID som national eID-løsning, så identiteter herfra skal anerkendes på tværs af EU. Digitaliseringsstyrelsen har udarbejdet en National Standard for Identiteters Sikringsniveau (NSIS), der definerer de krav, der skal gælde for danske eID-løsninger for at leve op til eIDAS' tre sikringsniveauer for digitale identiteter. Alle offentlige tjenesteudbydere, brokere og identitetsløsninger, der skal benytte den nationale infrastruktur, skal forholde sig til denne standard, når de vurderer deres tjenester og de data, som kan tilgås via disse tjenester. Det gør de for at sikre, at de er beskyttet med autentifikation på et tilstrækkeligt højt sikringsniveau.

For den finansielle sektor er der fra 2018 indført en række nye krav med det reviderede betalingstjenestedirektiv (også kaldet PSD2). Direktivet stiller blandt andet detaljerede krav til, hvordan autentifikation og transaktionsgodkendelse skal foretages i forbindelse med udbud af betalingstjenester, f.eks. betalinger via netbank. Alle, som udbyder betalingstjenester, skal leve op til disse regler, der er implementeret i dansk lovgivning med lov om betalinger, der trådte i kraft 1. januar 2018. MitID understøtter disse regulatoriske krav i det omfang, de relaterer sig til MitID-funktionalitet.

Sikringsniveauer lav, betydelig og høj
I MitID findes derfor sikringsniveauerne 'lav', 'betydelig' og 'høj' (følger af NSIS og eIDAS). Det stiller krav til styrken af en autentifikationsproces, den underliggende identitetssikring og det anvendte identifikationsmiddel (MitID app, MitID kodeviser/kodeoplæser og MitID chip) – udtrykt som et samlet sikringsniveau. Dette kan også udtrykkes som graden af tillid, som en tjenesteudbyder kan have til en autentificeret identitet. Hovedreglen for offentlige tjenesteudbydere er, at de kræver mindst niveau betydelig. Det er op til tjenesteudbyderen at definere, hvilket sikringsniveau man ønsker i forhold til de brugere, der anvender ens tjenester. Når tjenesteudbyderen har angivet det ønskede sikringsniveau, klarer MitID resten, så brugeren autentificerer sig på det ønskede sikringsniveau.

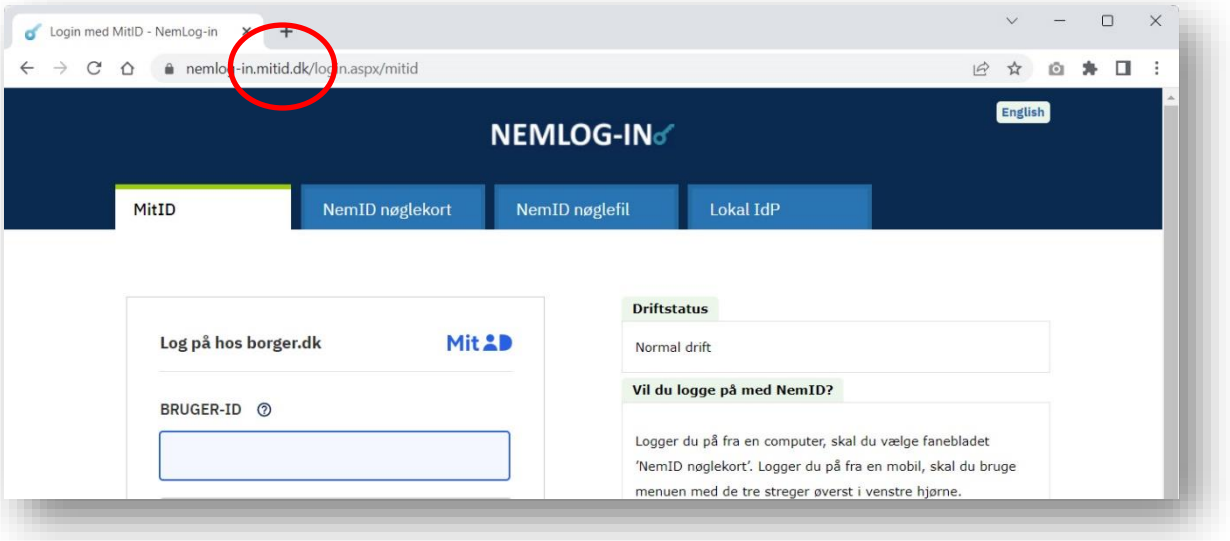
Generelt om sikkerheden

Ud over at MitID's infrastruktur beskyttes af en række brokere – og at MitID er modulært og fleksibelt opbygget, så der kan reageres hurtigt på skiftende internettrusler – så er der især fokus på sikkerheden på tre områder:
1) i den tekniske løsning 2) i forhold til den måde, som MitID bruges på og 3) i kravene til identitetssikring.

Sikkerhed i den tekniske løsning
Der er en række elementer, som gør, at man som bruger har mulighed for at sikre brugen af ens MitID. Eksempelvis at man ved oprettelsen af MitID ikke kan bruge sit CPR-nummer som bruger-ID. Det øger den samlede sikkerhed, at bruger-ID'et er ens eget unikke valg og ikke et brugernavn, andre kan få kendskab til, f.eks. ved adgang til CPR-numre.

Derudover er der en række sikkerhedselementer ved brugen af MitID:

Bedre beskyttelse mod falske hjemmesider
Man bliver bedre beskyttet mod falske hjemmesider. Logger man ind på MitID via en browser, vil der stå mitid.dk sidst i URL'en – så ved man, at man er på en rigtig side, og at det er sikkert at angive sine oplysninger.

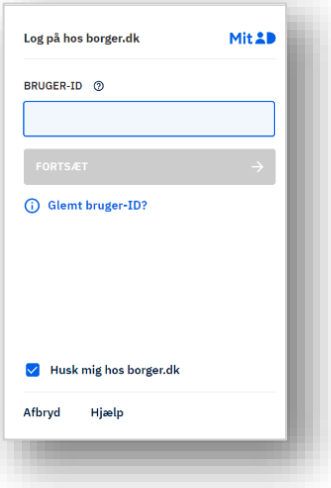


Besked ved vigtige hændelser

Man får besked via MitID appen, SMS eller e-mail, hvis der sker vigtige hændelser, f.eks. hvis MitID appen aktiveres på en ny enhed. Man kan også vælge at få besked, hver gang ens MitID bliver brugt. Det er en god ide at vælge to kanaler, man kan informeres igennem. Det kan man gøre på sin profilside på MitID.dk.

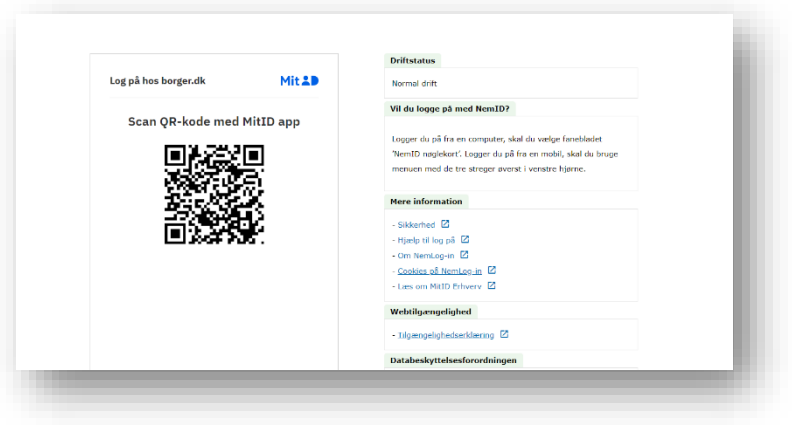
Beskrivelse af transaktion

Man kan se en meddelelse, der karakteriserer den transaktion, man er i gang med (f.eks. 'Log på'). Man kan også se et tjenesteudbydernavn (fx 'Borger.dk'), som kommer fra MitID.



Sammenkobling af kanaler

Man skal scanne en QR-kode med sin MitID app, når man f.eks. sidder ved sin computer og vil logge på. Det er med til at sikre, at det er slutbrugeren selv, der har igangsat handlingen. Tilsvarende skal man trykke på en knap, hvis man vil logge på via en mobilbrowser. Ved tryk på knappen åbnes MitID appen, og den ved nu, at det er slutbrugerens selv der har startet handlingen.



Sikkerhed i brugen af MitID (f.eks. MitID app og -kodeviser)
MitID er primært en app, da det vil være den nemmeste løsning for de fleste. Har man ikke mulighed for at bruge MitID app, findes der fysiske alternativer: En MitID kodeviser eller en MitID kodeoplæser. Man kan få en MitID kodeviser eller -kodeoplæser sendt med posten, men før de kan tages i brug, skal de aktiveres og tilknyttes den enkelte bruger.

I MitID er bruger-ID'et desuden afkoblet fra afgivelsen/anvendelsen af selve identifikationsmidlerne (MitID app, MitID kodeviser/kodeoplæser og MitID chip). Dette design giver langt større fleksibilitet og ikke mindst hastighed til at kunne introducere og/eller fjerne identifikationsmidler i løsningen uden at skulle lave om på det grundlæggende løsningsdesign.

Sikkerhed ved større krav til identitetssikring
Med MitID stilles der høje krav til, at man kan dokumentere sin identitet, når man skal have MitID. Dermed lever MitID op til EU's nye, høje krav til identitetssikring.

Pas godt på MitID

Selvom MitID lever op til de nyeste standarder for sikkerhed og er udviklet med stort fokus på sikkerhed og brugervenlighed, er dog vigtigt at understrege, at ingen løsninger er 100 procent sikre, blandt andet fordi de også afhænger af den enkeltes adfærd. MitID er et personligt ID, og derfor skal man passe godt på det.

- Man skal aldrig vise sine koder til andre.
- Man skal aldrig udlevere sin MitID app, -kodeviser, -kodeoplæser eller -chip til andre. Appen kan dog deles med andre i husstanden, så længe man har hvert sit bruger-ID og PIN-kode.
- Man skal aldrig dele sit bruger-ID med andre – undtagen med supporten, hvis man selv kontakter den.
- Man skal aldrig godkende noget med MitID på baggrund af f.eks. et opkald, e-mail eller besøg fra nogen, som udgiver sig for at være fra banken, Digitaliseringsstyrelsen, politiet, supporten eller lignende. Man vil aldrig blive kontaktet på den måde.
- Man skal altid læse, hvad man er ved at godkende med MitID. Hvis teksten ikke svarer til det, som man ønsker at gøre, skal man afvise handlingen.

Om MitID app

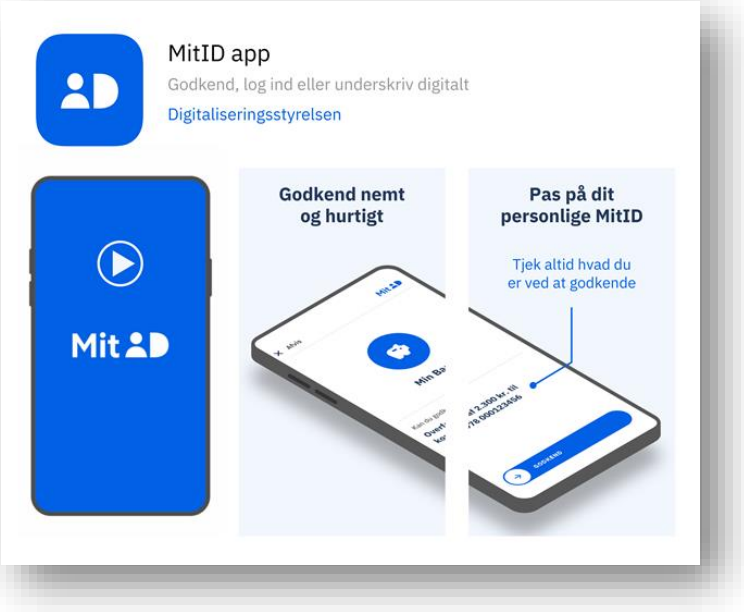
Anskaffelsen og anvendelse af MitID app

MitID appen virker på de fleste smartphones. Har man ikke lyst eller mulighed for at bruge MitID appen, kan man vælge f.eks. MitID kodeviser eller MitID kodeoplæser. Langt de fleste brugere har dog valgt at bruge MitID appen.

MitID appen kan anvendes til at fortælle online-tjenester, hvem man, hvis man allerede har en MitID app, men MitID appen kan også benyttes til at få et MitID første gang eller få MitID app tilbage, hvis man f.eks. har mistet sin telefon eller har fået en ny. Det kræver at man har et pas og en telefon, der kan scanne passet (en telefon med NFC-understøttelse).

Det er nemt og sikkert at få MitID app
MitID app er udviklet til alle brugere af MitID, og der er kun én version af MitID app - uanset om man bruger MitID app som borger/kunde eller erhvervsbruger til offentlige eller private tjenester.

Når man downloader MitID appen fra enten App Store eller Google Play, skal man tjekke, at Digitaliseringsstyrelsen står som udvikler.



MitID appen fungerer for mobile Apple- og Android-enheder (smartphone og tablet) og kan anvendes til alle tjenester – offentlige som private – på samme vis som MitID kodeviser, -kodeoplæser eller -chip.

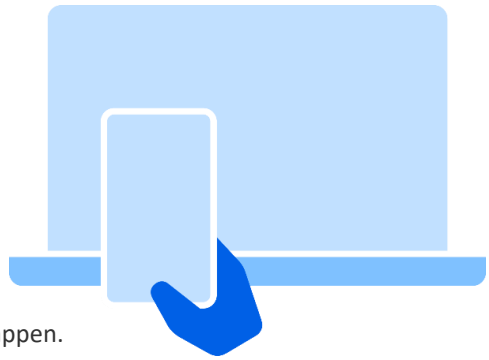
MitID app skal aktiveres før brug
Der kan kun være én MitID app på en mobilenhed. Appen hentet fra Google Play eller App Store kan ikke bruges til autentificering, før den er aktiveret – dvs. tilknyttet et specifikt MitID. En aktiv MitID app er personlig, om end at der kan være flere brugere, med hver sin PIN-kode, i appen.

Man har enten aktiveret appen under migreringen fra NemID til MitID eller ved ny-registrering hos et borgerservicecenter, eller ved brug af pas-funktionaliteten. Appen kan også tilføjes efter migrering eller ny-registrering ved hjælp af pas-funktionaliteten eller via selvbetjening på MitID.dk, forudsat at man allerede har f.eks. MitID kodeviser.

Sådan aktiveres MitID appen

Aktivering af MitID appen sker med en 6-tegns-aktiveringskode, som man enten får vist på skærmen ved brug af pas-funktionaliteten eller udleveret på papir af borgerservice. Derudover skal man have en 8-tegns midlertidig PIN-kode, som man får tilsendt på en SMS til ens mobilnummer. Dette mobilnummer skal enten allerede være valideret eller bliver valideret som en del af aktiveringen af appen. Det sker via en 6-tegns valideringskode, der sendes til mobilnummeret og indtastes under aktiveringen. På den måde sikres det, at telefonen tilhører personen, der er ved at aktivere appen – og dermed at SMS'en med den midlertidige PIN-kode til appen modtages af den rigtige person.

Ved aktiveringen af MitID appen erstattes den midlertidige PIN-kode med en personlig selvvalgt 6-cifret PIN-kode, som skal anvendes, når MitID appen benyttes. Ofte benyttede talsekvenser kan dog ikke bruges. Man kan desuden vælge at benytte enhedens biometri, f.eks. fingeraftryk/ansigtsgenkendelse, i stedet for indtastning af PIN-koden.



Man skal dog være sikker på, at man kan huske PIN-koden, selvom man bruger enhedens biometri til daglig brug, da man kan blive bedt om at bruge PIN-koden frem for biometri, f.eks. hvis man selv slår biometri fra, eller hvis ens enhed ikke kan 'genkende' en – eller hvis der oprettes endnu en bruger i appen.

Anbefaling

Man kan have op til tre aktive MitID apps tilknyttet sit personlige MitID, så man kan anvende appen på flere enheder, f.eks. både en smartphone eller en tablet. Dette anbefales, så man stadig har sit personlige MitID, selvom man mister sin smartphone.

Sådan bruges MitID app

Når man skal bruge MitID, skal man selv åbne appen på sin enhed, hvorefter man vil se anmodningen, man skal besvare – enten godkende eller afvise - i appen. Man kan besvare anmodningen på en hvilken som helst af de aktive MitID apps, man har.

I appen vises der en tekst, der er sat op af tjenesteudbyderen, eksempelvis den offentlige myndighed eller banken, som man prøver at få adgang til. Teksten fortæller, hvad der godkendes. Selve godkendelsen sker ved et "swipe". Hvis en anmodning afvises på én mobil enhed, vil den med det samme blive ugyldig på alle de andre mobile enheder, som appen evt. er aktiveret på.

Ud over teksten viser appen navnet på den tjenesteudbyder, hvor man har startet MitID, f.eks. "Log på hos Borger.dk".

Trin for trin

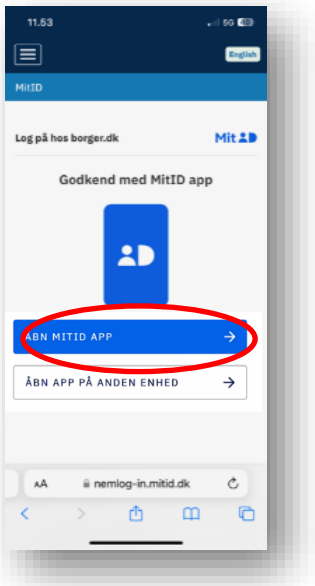
Man starter en anmodning ved at indtaste sit bruger-ID, fx på en hjemmeside eller i en app. Den måde, som man herefter skal bruge appen på for at godkende anmodningen, afhænger af om man sidder ved en computer eller tablet – eller måske den telefon, hvor man har MitID appen på.

Computer + telefon med MitID app

Bruger man sin computer og skal godkende med MitID appen, kommer der en QR-kode på computerskærmen. QR-koden skal man scanne med MitID appen, før man kan swipe og godkende den pågældende handling.

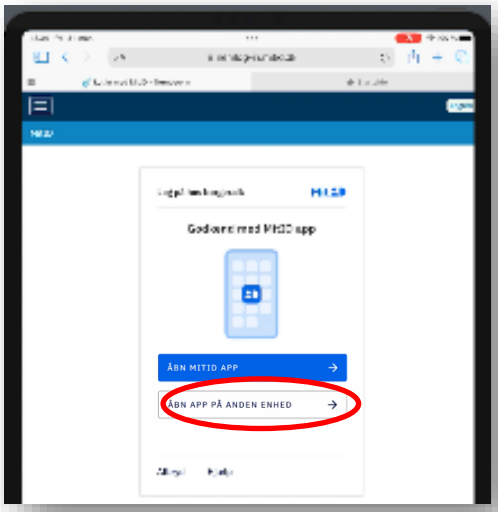
Kun telefon – med MitID app

Bruger man sin telefon og skal godkende med MitID appen, bliver man præsenteret for knappen 'Åbn MitID app', som fører én automatisk over i appen, når man trykker på den (app switch).



Tablet + telefon med MitID app

Bruger man fx en tablet og skal godkende med MitID appen, som man har på sin telefon, skal man trykke på knappen 'Åbn app på anden enhed', som kommer frem på tabletten. Herefter kan man åben MitID appen på telefonen og swipe og godkende.



Uanset om man sidder ved computer, tablet eller bare på sin telefon, skal man indtaste sin PIN-kode eller bruge ansigtsgenkendelse/fingeraftryk i MitID appen, før man kan besvare anmodningen. En anmodning udløber efter fem minutter. Når en anmodning er godkendt eller afvist, så vil den ikke længere være aktiv på evt. øvrige enheder.

Man skal kun godkende en anmodning, hvis man selv har startet den. Hvis man ikke ønsker at godkende, skal man trykke på 'Afvis' i MitID appen.

Hvis MitID app/smartphone mistes

Hvis man mister sin mobil, skal man straks spærre den MitID app, som er tilknyttet den mistede telefon. Det kan man gøre på MitID.dk eller ved at ringe til MitID supporten.

Man kan få en ekstra aktiv MitID app ved at installere appen på flere enheder, f.eks. en tablet. Så kan man også benytte den anden enhed til at genetablere MitID appen på en ny mobil. Hvis man f.eks. også har en MitID kodeviser, kan man logge ind på MitID.dk og få aktiveringskode og midlertidig PIN-kode til en ny MitID app.

Medio 2022 blev der lanceret en funktionalitet i MitID appen, der giver brugeren mulighed for at genetablere appen via scanning af brugerens pas/internationalt ID-kort, hvis han eller hun skulle miste sin MitID app.

Få MitID med pas-funktionalitet i MitID appen

Den 7. juni 2022 blev der tilføjet ny funktionalitet i MitID appen. Med opdateringen blev det muligt at få MitID i MitID appen ved brug af et gyldigt dansk, grønlandsk eller færøsk pas og en telefon, der kan scanne chippen i passet. Funktionaliteten og den bagvedliggende teknik er forklaret senere i dokumentet. I januar 2023 blev pasfunktionaliteten udvidet til også at omfatte udenlandske pas og internationale ID-kort med chip.

Først og fremmest kan man bruge pas-funktionaliteten til at få et MitID første gang eller få en aktiveret MitID app tilbage, hvis man f.eks. har mistet eller fået en ny telefon/tablet – og ikke har en reserve på en anden enhed. Endvidere kan den nye pas-funktionalitet også benyttes til at hjælpe andre, f.eks. pårørende, med at få MitID. Man kan også bruge en andens telefon og få MitID via den andens person MitID app, hvis ens egen telefon ikke kan scanne ens pas. Hvis man har fået hjælp af en anden, skal man aktivere sin MitID app på sin egen telefon efter selve oprettelsen af MitID. Man kan også bestille og aktivere f.eks. en MitID kodeviser via appen.

Pas-funktionaliteten er især et tilbud til de brugere, som vil have MitID hjemmefra og dermed kan spare turen i Borgerservice.

Derudover kan pas-funktionaliteten hjælpe dem, der har mistet deres MitID app, f.eks. hvis de har mistet eller fået en ny telefon/tablet – og ikke har den på en anden enhed.

Sådan får man MitID med pas og MitID appen

Inden man går i gang, skal man sikre, at MitID appen er opdateret til seneste version, at man har et gyldigt pas/internationalt ID-kort med chip og en telefon, der kan scanne chippen i passet. Man kan se på MitID.dk, hvilke krav der er til telefonen.

1. Find pas-funktionaliteten på forsiden af MitID app via indstillingerne (øverste venstre hjørne) under menupunktet "Få MitID med pas" (hvis man skal have MitID) eller "Aktiver MitID" (hvis man f.eks. har mistet sin MitID app).
2. Scan koden og aflæs chippen i passet/ID-kortet.
3. Scan ansigtet – så det kan sammenlignes med fotoet i passet/ID-kortet (MitID appen genererer nu et 3D FaceScan, og hvis resultatet af denne sammenligning er tilfredsstillende, bekræfter appen brugerens identitet)
4. Opret bruger-ID ved ny-oprettelse af MitID, eller få vist dit eksisterende bruger-ID – og aktiver herefter MitID appen – eller bestil og aktiver f.eks. en MitID kodeviser eller kodeoplæser. Herefter er man klar til at bruge MitID.

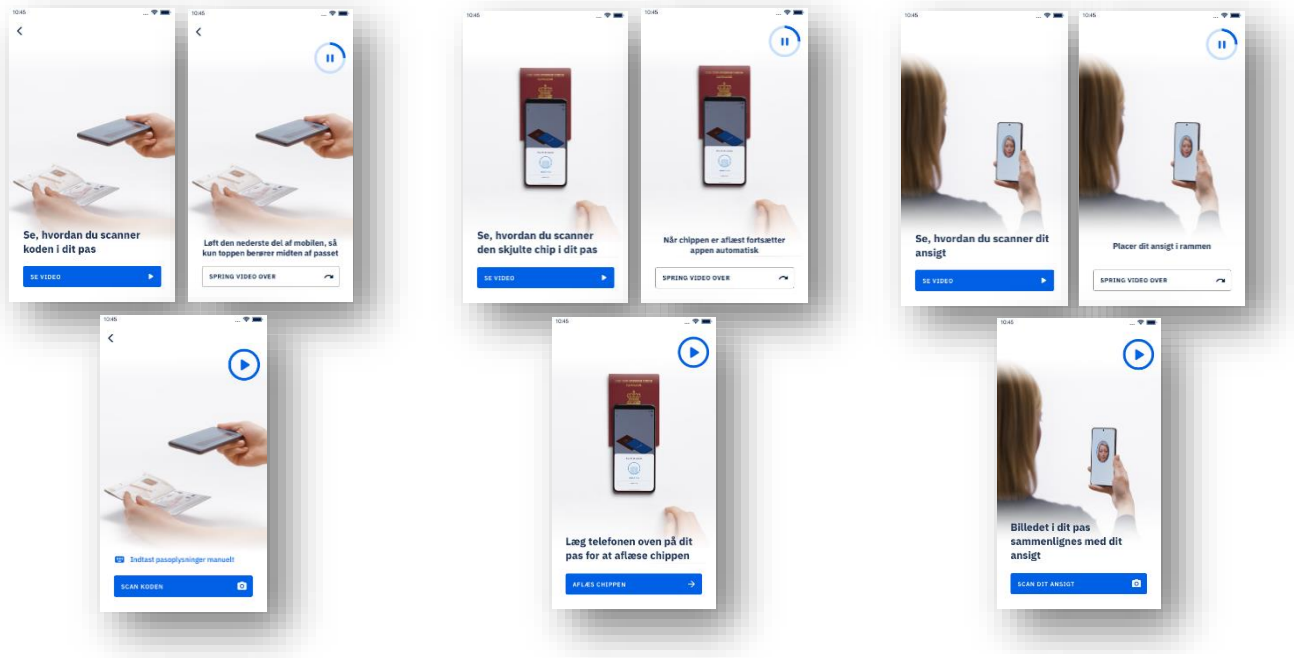
Hvis man har et udenlandsk pas/ID-kort – og man ikke har et dansk CPR-nummer til at indtaste i appen – skal man have en såkaldt P-kode. Den skal bruges som et led i at bekræfte ens identitet. P-koden får man f.eks. hos Borgerservice eller i MitID Supporten.

Alle oplysninger behandles krypteret, og MitID appen gemmer hverken data læst fra passet eller fra ansigtsscanningen.

1) Scan koden i passet

2) Scan chippen i passet

3) Scan ansigt



Sådan bekræftes identiteten

Hvis man hjælper en anden med at få MitID via pas-funktionaliteten
Hvis man hjælper en pårørende med at få MitID via sin MitID app, skal man sammen med den pårørende igennem samme trin – blot med den pårørendes pas og ved at scanne den pårørendes ansigt.

Her skal man som hjælper dog være opmærksom på, at man ikke må kende hverken bruger-ID eller personlig PIN-kode, som oprettes af den, som man hjælper. Man må heller ikke bruge dennes MitID efterfølgende, da MitID er strengt personligt. Dette fremgår også i de hjælpeguides, som er tilgængelige.

Pas-funktionaliteten kan benyttes, både når man lige har hentet sin MitID app fra app store, uden at MitID appen er aktiveret, og efterfølgende når MitID appen er aktiveret på telefonen.

Der er stadig hjælp at hente i Borgerservice
Mulighederne i MitID appen er et supplement til eksisterende muligheder for at få MitID eller support – og man kan fortsat få hjælp hos Borgerservice med gyldig legitimation.

Kan man være flere om MitID app?
Selvom der kun kan være én MitID app per mobil-enhed, kan der godt være flere forskellige brugere, der oprettes på samme MitID app.

Er der flere personer i samme husstand, som f.eks. benytter den samme tablet, kan de bruge den samme MitID app, men med hver deres bruger-ID tilknyttet appen og hver deres PIN-kode.

Ved flerbruger-anvendelse af MitID appen kan ansigtsgenkendelse eller fingeraftryk ikke bruges til at åbne MitID appen. Man skal i stedet altid bruge sin PIN-kode for at godkende anmodninger/handlinger i appen.

Hvad sker der ved forkert indtastet PIN-kode?
Hvis man indtaster forkert PIN-kode tre gange i træk, vil MitID appen automatisk blive suspenderet (låst) i 60 minutter, hvor brugeren ikke kan anvende den. Efter 60 minutter ophæves suspenderingen automatisk. Suspenderingen kan også ophæves via en aktiveringskode fra MitID supporten, inden de 60 minutter er gået.

Hvis suspenderingen ophæves automatisk efter 60 minutter, har man yderligere tre forsøg til at taste den rigtige PIN-kode. Efter seks forkerte indtastninger af PIN-kode låses MitID appen, og denne lås kan ophæves via supporten, eller ved at man bruger pas-funktionaliteten i sin MitID app til at skifte PIN-koden. Herefter kan man bruge sin app igen.

Sikkerhedsdesign i MitID app

MitID app er et såkaldt multifaktor-identifikationsmiddel. Det betyder, at MitID app - i modsætning til MitID kodeviser, -kodeoplæser, -chip og MitID adgangskode - i sig selv indeholder to uafhængige autentifikationsfaktorer:

1. Noget, du ved (PIN-kode)
2. Noget, du har (MitID appens sikkerhedselementer, der binder appen til den specifikke mobile enhed).

MitID appen behøver derfor ikke at blive kombineret med andre identifikationsmidler.

MitID kodeviser, -kodeoplæser, -chip og MitID adgangskode udgør derimod alle sammen såkaldte enkeltfaktor-identifikationsmidler og skal derfor kombineres for at opnå multifaktor-autentifikation med MitID, f.eks. ved at kombinere MitID adgangskoden (noget, du ved) med MitID kodeviseren (noget, du har).

Brugeren kan vælge at frigive MitID appens PIN-kode via de lokale biometriske løsninger, der er tilgængelige på de mobile enheder, som MitID app kan installeres på (f.eks. fingeraftryk og ansigtsgenkendelse). Dette kan lette anvendelsen yderligere.

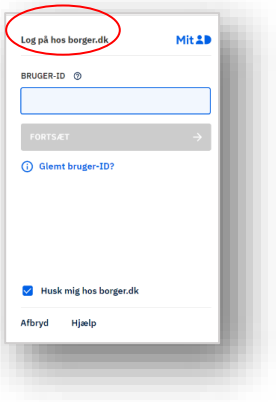
Aktivering før brug
MitID app kan downloades fra de officielle app stores fra Apple og Google. Når MitID app hentes, er den endnu ikke knyttet til et specifikt MitID og skal derfor først aktiveres, før den kan benyttes til MitID autentifikation. Aktiveringen sker ved at udnytte en række standardiserede sikkerhedsteknologier og mekanismer (bl.a. public-key cryptography).

Helt konkret indebærer det, at når MitID app tilknyttes en brugers MitID via aktiveringen, tilknyttes samtidig to kryptografiske nøglepar til brugerens MitID. Disse nøgler er delt mellem MitID app og MitID's servere. Nøglerne er unikke for hver enkelt bruger. Kryptografien, der anvendes, sikrer, at kun appen med de korrekte nøgler kan godkende en anmodning, og at en MitID app, der hører til en bruger, kun kan godkende på denne brugers vegne.

Der benyttes i denne sammenhæng to typer asymmetriske kryptografiske algoritmer, ECDSA (til elliptisk kurvebaseret signering) og RSA (til public-key kryptering) til henholdsvis kryptografisk signering og til dekryptering.

Krypteret transaktionstekst og navn på tjenesteudbyder
RSA spiller også en rolle i forhold til at beskytte brugerens privatliv, f.eks. bliver transaktionsteksten krypteret inden udsendelse, så kun brugerens MitID app kan dekryptere og læse teksten. Tjenesteudbyderen har, med en enkelt undtagelse, fuld kontrol over, hvad der skal stå i den tekst, der sendes ud.

Undtagelsen er, at det navn på tjenesteudbyderen, der står som den første del af teksten (f.eks. Log på <tjenesteudbyder navn>), kommer fra brokeren og er det tjenesteudbydernavn, som brokeren registrerede for tjenesteudbyderen i MitID-løsningen. Der kan derfor ikke vises et "falsk" tjenesteudbydernavn. I visse tilfælde kan navnet på tjenesteudbyderen været erstattet af navnet på brokeren, f.eks. NemLog-in, eller brokerens navn vil indgå i teksten.



MitID appen og samspillet mellem appen og serverdelen af MitID er beskyttet via en række sikkerhedsmekanismer, som f.eks. anvendelse af RASP (Runtime Application Self-Protection) teknologi og TLS.

Ingen adgangskode uden for MitID app
Når man bruger MitID appen skal man ikke indtaste en adgangskode sammen med bruger-ID'et, men i stedet gå direkte i appen for at godkende en anmodning efter indtastning af bruger-ID hos tjenesteudbyderen.

Grunden er, at man ikke skal bruge sit bruger-ID og en adgangskode, inden man godkender i MitID appen, da adgangskoden (i form af en centralt valideret PIN-kode) er indlejret i selve MitID appen – og ikke ligger uden for appen, hvilket den f.eks. gjorde i NemID nøgleapp.

Centralt valideret videnselement
Et centralt valideret videnselement er et videnselement, der bliver valideret i et backend-system og ikke lokalt på en enhed. Dette giver et mere robust design, da systemet kan lukke for forskellige typer af brute-force-angreb, der kan eksistere ved en lokal validering af et videnselement. I MitID anvendes ZKPP-teknologi kombineret med andre teknologier ved central validering af videnselementer.

Med andre ord har man i MitID flyttet det centralt validerede videnselement ind i selve appen, nemlig PIN-koden. Dette bevidste valg i MitID sikkerhedsdesignet har flere forskellige formål. Dels gør det brugen af MitID app betydeligt nemmere og mere intuitiv, og dels øger det sikkerheden i løsningen, at det centralt validerede videnselement indtastes (eller eventuelt kobles til biometri) i en app, i stedet for på en hjemmeside, hvor man ikke altid kan gennemskue, om det er en falsk hjemmeside – eller om der eksempelvis er installeret en key-logger på den PC, der anvendes.

Ingen notifikation til at åbne MitID app
Med MitID modtager man ikke notifikation på sin mobile enhed, hvorigennem man kan åbne MitID appen automatisk. Når en bruger har indtastet sit bruger-ID og skal godkende MitID autentifikationen, skal han eller hun selv gå ind i MitID appen og åbne denne. På den måde styrkes sikkerheden ved at mindske risikoen for, at brugere ikke uforvarende kommer til at godkende en handling med MitID, som de ikke selv har startet.

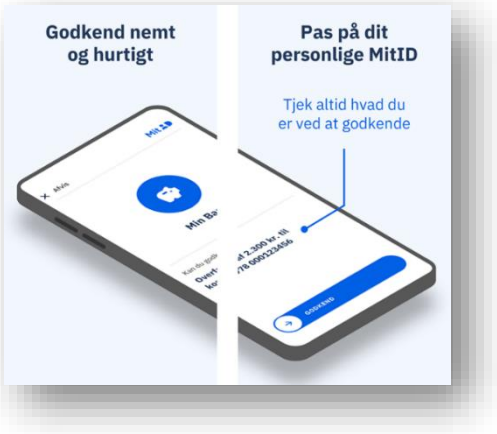
Hvis man bruger sin telefon – hvor man også har MitID appen på – vil man opleve, at når man har indtastet sit bruger-ID, skal trykke på en knap, som fører én automatisk over i MitID appen.

Brugerens mulighed for at tjekke inden godkendelse
Som bruger er der en række elementer, som man altid skal sørge for at tjekke, inden man godkender en handling med MitID.

Tjek, hvem der sender anmodningen
Når man skal godkende med MitID, skal man:

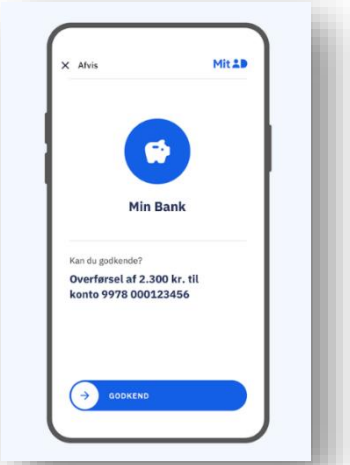
- kun godkende en anmodning, som kommer på baggrund af noget, som man selv har foretaget i en selvbetjeningsløsning.
- kunne genkende navnet på den service/tjenesteudbyder, der står i teksten i MitID app ud fra den handling, som man har startet.

F.eks. *Log på* **minbank.dk**. Hvis anmodningen ikke svarer til det, som man forventer, skal man straks afbryde handlingen ved at trykke på 'Afvis'.



Tjek, hvad der skal godkendes
Derudover skal man altid tjekke den handling, som man er ved at gennemføre - og læse teksten nøje, f.eks. *Overførsel af 2.300 kr. til modtagerkonto 9978 000123456*

Hvis teksten ikke svarer til det, som man ønsker at gøre – eller man ikke selv har igangsat den – skal man straks afbryde sin handling.



Vær opmærksom, inden der swipes
Når man swiper i MitID appen, betyder det, at man godkender den handling, som man er i gang med, f.eks. godkender overførsel af penge. Det er derfor vigtigt, at man er opmærksom på den tekst, der beskriver handlingen.

Man skal huske aldrig at swipe på baggrund af f.eks. et opkald, sms, e-mail eller besøg fra nogen, som f.eks. udgiver sig for at være fra en offentlig myndighed, banken eller supporten. Man vil aldrig blive kontaktet på den måde fra en legitim offentlig myndighed eller bank.

Det er meget vigtigt, at man giver sig tid til at sikre, at det, som skal godkendes, er det, som man ønsker at gøre. Man skal være lige så forsigtig med at godkende noget i appen, som hvis man laver en pengeoverførsel, besvarer en anmodning i MobilePay eller betaler i et supermarked.

Hvis man er i tvivl, skal man altid afvise. Man kan også altid gå ind på MitID.dk i sin aktivitetslog og se, hvad der faktisk er sket. Her er det også muligt at ændre sin indstilling for notifikationsniveau på MitID.dk, så man får tilsendt flere informationer om, hvad der sker med ens MitID – og hvor det f.eks. bliver brugt.

Sådan fungerer MitID pas-funktionaliteten

Med MitID stilles der høje krav til, at man kan bekræfte, hvem man er, når man skal have MitID. Med pas-funktionaliteten kan MitID appen bekræfte, at den person, som benytter funktionaliteten til f.eks. at få MitID, er den samme person, som er indehaver af det pas/internationale ID-kort, der bliver scannet af MitID appen.

Pas-funktionaliteten kan nemlig med stor sikkerhed afgøre, om ansigtet på den fysiske person, som holder en telefon med MitID appen installeret på i hånden, svarer til det billede, der er i det pas/ID-kort, som scannes af MitID appen. Derudover kan MitID appen afgøre, om det er en levende fysisk person, hvis ansigt scannes af MitID appen – og ikke bare et billede eller en maske eller tilsvarende.

Kort fortalt gør appen følgende, når man bruger pas-funktionaliteten:

1. Aflæser MRZ-koden fra billedsiden i passet/ID-kortet samt chippen i ens pas/ID-kort, herunder en digital udgave af det foto, der findes i passet/ID-kortet.
2. Scanner ens ansigt og sikrer, at der ikke benyttes et billede eller lignende i stedet for en levende person – dette kaldes også for et 'liveness'-tjek.
3. Sammenligner scanningen af ansigtet med pasfotoet – dette sker på MitID-backenden.

Når identiteten er blevet bekræftet, kan man benytte MitID appen.

Der gemmes ingen oplysninger på telefonen, som pas-funktionaliteten bruges på, hverken billede eller personlige oplysninger. Det gælder, både når man bruger sin egen telefon, eller hvis man hjælper f.eks. en pårørende med at få MitID. De biometriske oplysninger (billede og ansigtsscan) benyttes til at fastslå, om det er passets/ID-kortets ejer, der har anvendt pas-funktionaliteten. Disse oplysninger er krypterede og slettes automatisk på MitID-backenden efter maksimalt én dag.

Flere detaljer om teknikken bag pas-funktionaliteten i MitID appen

- MitID appen læser MRZ-koden fra billedsiden af personens pas/internationale ID-kort, eller personen indtaster selv pasnummer, udstedelsesdato og udløbsdato ind i appen. Herudfra dannes en nøgle, som gør, at MitID appen kan læse data fra NFC-chippen i personens pas/ID-kort.
- MitID appen læser data fra NFC-chippen i personens pas/ID-kort. Data krypteres med en nøgle, der er kontrolleret af MitID backend-systemet.
- Data (navn, CPR – hvis danskudstedt pas, fødselsdato og pasfoto) sendes krypteret til MitID-backenden, der dekrypterer og validerer data fra passet/ID-kortet. Data gemmes ikke i MitID appen, men holdes krypteret i backend-hukommelsen, så længe sessionen er aktiv.
- MitID-backenden tjekker, at indholdet på chippen er autentisk (dvs. et gyldigt pas/internationalt ID-kort), og at chip-indholdet ikke kan være blevet kopieret til en anden chip ('clone detection').
- MitID-backenden processerer data krypteret i hukommelsen på serveren.

- MitID appen gennemfører 'liveness'-tjek af personen (ved måling af 3D-dybde i kamerabilledet, hudstruktur, refleksioner i øjnene etc.) og genererer et såkaldt 3D-FaceScan (der indeholder en række attributter på brugerens ansigt inkl. liveness-data) af personen.
- 3D-FaceScan sendes krypteret til MitID-backenden, hvor det konverteres til et 3D-FaceMap og sammenlignes med fotoet i pas/ID-kort.
- Hvis resultatet af denne sammenligning opfylder de fastsatte krav, ved MitID, hvem personen er, og MitID validerer derefter oplysningerne mod CPR-registeret hvis relevant, ud fra CPR-nummeret, der enten kan være aflæst fra et danskudstedt pas eller indtastet af ansøger. I det sidst nævnte tilfælde gennemføres forskellige valideringer ud fra pasdata mod CPR-registeret. Sluttelig registreres en MitID-identitet for brugeren ved ny-oprettelse, og der genereres en aktiveringskode.
- Man kan herefter, hvis man ønsker det, nu aktivere en MitID app for sig selv ud fra den genererede aktiveringskode. Enten på den telefon, der blev brugt til at gennemføre ID-tjekket på – eller på en anden enhed. Det er også muligt at bestille og aktivere f.eks. en MitID kodeviser.

Oprettelse af nyt MitID vha. pas-funktionaliteten

Hvis man ønsker at oprette et nyt MitID, sker der dette:

- CPR-nummer (hvis brugeren har et), navn og fødselsdato gemmes i MitID, hvis identiteten oprettes. Foto fra pas/ID-kort gemmes ikke i MitID.
- Der logges en hash-værdi af pas-/ID-kortnummeret i MitID audit-loggen sammen med resultatet af sammenligningen mellem FaceMap og pas/ID-kortfoto. Resultatet af sammenligningen er et tal, der er udtryk for sandsynligheden for, at FaceMap og foto er af samme person.
- Personoplysninger og foto fra passet/ID-kortet opbevares krypteret i midlertidig hukommelse, mens sessionen er aktiv og i højst én time, hvorefter oplysningerne slettes automatisk.
- 3D-FaceScan (biometriske data og liveness-data) opbevares krypteret i en database, efter sessionen er afsluttet, og i højst én dag, hvorefter oplysningerne slettes automatisk.
- MitID gemmer kun de data, der er nødvendige for at kunne oprette brugeren i MitID. Ud over de data, der allerede gemmes i dag (uden anvendelse af pas-funktionaliteten), vil resultatet af foto-/3D-FaceMap sammenligningen blive audit-logget. Resultatet af sammenligningen er som nævnt et tal, der er udtryk for sandsynligheden for, at FaceMap og foto er af samme person.
- MitID appen gemmer hverken data læst fra passet/ID-kortet eller det genererede 3D-FaceScan.

Andre forhold ved pas-teknologien

I dette afsnit gennemgås en række forskellige tekniske forhold, der gælder for den anvendte pas-teknologi.

- Der benyttes en meget velafprøvet teknologi (ICAO 9303-standarden), som kendes fra rejsepas. Hvad angår valideringen af ansigtet på personen mod foto i passet/ID-kortet, sker det samme, som når man passerer en automatisk paskontrol i lufthavnen. Det software, som udfører 'liveness'-tjek, er certificeret efter ISO/IEC 30107-3 'Biometric presentation attack detection', og benyttes udelukkende til at bekræfte, at den person, som præsenterer sit pas/ID-kort for MitID appen, er den samme person, som bruger MitID appen til at scanne sit ansigt. På den måde ved MitID, hvem personen er, som f.eks. benytter MitID appen til at oprette et nyt MitID. Alle data er krypterede og slettes automatisk efter senest et døgn.
- Det er meget vigtigt at fastslå, at MitID pas-funktionaliteten ikke kan benyttes til at lave ansigtsgenkendelse ifm. overvågning. Teknologien benyttes udelukkende til at bekræfte, om en person, der benytter MitID pas-funktionaliteten matcher fotoet i det pas/ID-kort, som MitID appen præsenteres for. Endvidere slettes alle biometriske data efter maksimalt et døgn.
- Både automatiske ansigtsvalideringssystemer som MitID pas-funktionaliteten og manuel ansigtsvalidering (f.eks. ved at en Borgerservice-medarbejder sammenligner et pas-/ID-kortfoto med en person foran skranken) kan lave fejl. Undersøgelser har dog vist, at fejlraten for automatiske ansigtsvalideringens systemer

er langt mindre end manuel ansigtsvalidering. En anerkendt undersøgelse fra 2014 fandt, at meget erfarne pasbetjente fejlagtigt accepterede 14 % af svigagtige person-foto-sammenligninger. Dette er en væsentlig højere falsk accept rate (FAR) end ved brug af automatisk billedgenkendelse. Undersøgelsen 'Passport Officers' Errors in Face Matching' kan findes her (https://pubmed.ncbi.nlm.nih.gov/25133682/). MitID pas-funktionalitet har til sammenligning en FAR på 1/10.000 ved anvendelse på sikringsniveau Betydelig – svarende til 0,01%. Det betyder dog ikke, at 0,01% af alle MitID app-resultater er fejlbehæftede, da tallet kun er udtryk for en sandsynlighed.

- Pas-funktionaliteten kan ikke sammenlignes med FaceID, som der anvendes på en iPhone, eller tilsvarende. FaceID er baseret på en 3D-optagelse af et ansigt, som gemmes på telefonen og løbende opdateres. Pas-funktionaliteten er derimod baseret på en sammenligning af en 3D-optagelse af et ansigt, som ikke gemmes på telefonen, med et 2D-foto fra et pas/ID-kort, hvor dette foto kan være op til 10 år gammelt. Derfor vil FaceID kunne operere med en lavere FAR end MitID pas-funktionaliteten.

- Pas-funktionaliteten kan bekræfte, om personen, der benytter funktionaliteten, svarer til fotoet i det pas/ID-kort, der scannes i MitID appen, og at fotoet i passet er tidssvarende. I chippen i passet findes der nok oplysninger til at sikre en tilstrækkelig stærk binding mellem personen, der betjener MitID appen, og den person, som passet er udstedt til under forudsætning af, at person og pasfoto matcher tilstrækkeligt. Hvis dette er tilfældet, er identitetssikringen tilstrækkeligt til, at der kan udstedes et MitID, både i forhold til den danske NSIS-standard og EU eIDAS-forordningen. Det skal understreges, at MitID stadigvæk understøtter identitetssikring ved at en borger møder fysisk frem i borgerservice med legitimationsdokumenter og svarer på spørgsmål eller medbringer et vidne – præcis som før MitID pas-funktionaliteten blev tilføjet til MitID.

Opsummering af sikkerhed

Generelt om sikkerheden i MitID

Modulær infrastruktur
MitID's infrastruktur er modulært og fleksibelt opbygget og dermed bedre i stand til hurtigt at reagere på skiftende internettrusler. Det betyder, at løsningen løbende kan tilpasses for at styrke sikkerheden.

Flere lag beskytter MitID-kernen
I MitID introduceres de såkaldte brokere. En broker er en virksomhed eller organisation, der formidler adgang for tjenesteudbyderen til MitID og dermed varetager den tekniske integration til MitID. På den måde kan MitID-løsningen kun tilgås af certificerede brokere og ikke af mange forskellige tjenesteudbydere. Brokeren skal være certificeret for at blive koblet direkte på MitID-løsningen.

Høje krav til identitetssikring
Med MitID stilles der høje krav til, at man kan dokumentere sin identitet, når man skal have MitID. Dermed lever MitID op til EU's høje krav til identitetssikring.

Sikringsniveauer lav, betydelig og høj
I MitID opereres med sikringsniveauer 'lav', 'betydelig' og 'høj', som stiller krav til styrken af en autentifikationsproces, den underliggende identitetssikring og det anvendte identifikationsmiddel (MitID app, MitID kodeviser/kodeoplæser

og MitID chip) – udtrykt som et samlet sikringsniveau. Det er op til tjenesteudbyderen at definere, hvilket sikringsniveau man ønsker i forhold til de brugere, der anvender ens tjenester.

En-faktor- og to-faktor-autentifikation
MitID tilbyder både en-faktor- og to-faktor-autentifikation - afhængig af det sikringsniveau, som tjenesteudbyderen ønsker for sine tjenester. Autentifikationsfaktorer kan være:

- vidensbaserede ('noget, man ved', f.eks. en adgangskode eller PIN-kode)
- besiddelsesbaserede ('noget, man har', f.eks. en MitID app eller en MitID kodeviser)
- iboende egenskabsbaserede ('noget, man er', f.eks. et fingeraftryk eller anden form for biometri).

I MitID er autentifikationsfaktorerne uafhængige, dvs. at hvis én autentifikationsfaktor kompromitteres, påvirker det ikke den anden. MitID anvender ikke egenskabsbaserede autentifikationsfaktorer – anvendelse af biometri på f.eks. ens smartphone eller tablet (fingeraftryk eller ansigtsgenkendelse) sker kun lokalt på enheden og anvendes kun til at frigive anvendelse af et videnselement (f.eks. en PIN-kode).

Bruger-ID
I MitID er bruger-ID afkoblet fra afgivelsen/anvendelsen af selve identifikationsmidlerne (MitID app, MitID kodeviser/kodeoplæser og MitID chip). Dette design giver langt større fleksibilitet og ikke mindst hastighed til at kunne introducere og/eller fjerne identifikationsmidler i løsningen uden at skulle lave om på det grundlæggende løsningsdesign.

Aktivering før brug
Man kan få en MitID kodeviser eller kodeoplæser sendt med posten, eller man kan hente den hos borgerservice efter forudgående bestilling. Før de kan tages i brug, skal de aktiveres og tilknyttes den enkelte bruger. Det sker via en række trin, hvor man tilknytter serienummeret på f.eks. MitID kodeviseren til sit bruger-ID og adgangskode. Her skal man bruge en aktiveringskode, og den kan man kun få, når man har dokumenteret sin identitet. Det betyder at man ikke risikerer, at kriminelle kan stjæle en MitID kodeviser fra postkassen og benytte denne på ens vegne.

Besked ved vigtige hændelser
Man får besked via MitID appen, SMS eller e-mail, hvis der sker vigtige hændelser, f.eks. hvis MitID appen aktiveres på en ny enhed, eller hvis man aktiverer en MitID kodeviser. Man kan også vælge at få besked, hver gang ens personlige MitID bliver anvendt. Disse beskeder/notifikationer benyttes til at sikre, at man altid bliver orienteret om hændelser i MitID, der muligvis kræver aktion. Man kan selv vælge, på hvilket niveau der skal sendes notifikationer, og hvilken kanal der skal benyttes. Det er en god ide at vælge to kanaler, så man er sikker på at få besked.

Hændelseslog
Alle hændelser/aktiviteter for et MitID logges i hændelsesloggen – her kan man se, alt hvad man har foretaget sig med sit MitID.

Sammenkobling af kanaler
Man skal scanne en QR-kode med sin MitID app, når man f.eks. sidder ved sin computer og vil logge på. Det er med til at sikre, at det er slutbrugeren selv, der har igangsat handlingen. Tilsvarende skal man trykke på en knap på skærmen, hvis man starter en MitID handling via en mobilbrowser på ens telefon – herved startes MitID appen, og MitID ved derfor, at det er slutbrugeren der har startet anmodningen.

Beskyttelse mod falske hjemmesider
Man bliver bedre beskyttet mod falske hjemmesider. Logger man ind på MitID via en browser, vil der stå *mitid.dk* sidst i URL'en – så ved man, at man er på en rigtig side, og at det er sikkert f.eks. at angive sine oplysninger.

CPR-nummer må ikke benyttes som bruger-ID
I MitID kan CPR-nummer ikke benyttes som bruger-ID, da det øger den samlede sikkerhed, at man selv vælger sit bruger-ID'et – og det ikke er brugernavn, andre kan få kendskab til, f.eks. via adgang til cpr-numre.

Visning af tjenesteudbydernavn og handlingstekst
Der vises en meddelelse til brugeren, der karakteriserer transaktionen (f.eks. 'Log på'). Denne meddelelse kommer normalt direkte fra tjenesteudbyderen. Brugeren vises også et tjenesteudbydernavn, som kommer fra MitID. Tjenesteudbydernavnet kommer fra brokerens registrering af tjenesteudbyderen i MitID.

Sikkerhed – løbende tiltag
Sikkerhed er en indbygget del af udviklingsprocessen – fra evaluering af det første design til den sidste sikkerhedstest af den færdige løsning – dette gælder også ved vedligeholdelsen af løsningen. F.eks. er der implementeret sikkerhedsforanstaltninger i løsningen, som brokeren kan bruge til at vurdere risikoen ved en specifik MitID autentifikation.

Der bliver løbende holdt øje med trusler mod MitID, så der kan indføres tiltag, der kan imødegå nye risici og trusler. MitID overvåges intensivt, og der kan udtrækkes rapporter og statistikker, som dynamisk benyttes til at belyse og analysere ændrede aktivitetsmønstre.

Generelt om sikkerheden i MitID app

Den samlede sikkerhed i MitID app opnås ved en kombination af mange tiltag, som tilsammen giver en meget høj grad af sikkerhed. Tiltagene strækker sig fra specifikke MitID app relaterede funktioner og sikkerhedselementer til generelle sikkerhedsforanstaltninger i den samlede MitID-løsning:

- Man aktiverer sin MitID app med to uafhængige koder, som man får på to uafhængige kanaler.
- Man kan kun bruge sin MitID app ved at indtaste en 6-cifret PIN-kode eller ved at bruge biometri (brug af biometri er kun muligt på mobile platforme, som overholder relevante tekniske retningslinjer og anbefalinger).
- Man kan ikke lave sin PIN-kode med ofte benyttede talsekvenser, som er lette at gætte (skyldes særlige regler i forbindelse med generering af PIN-koden). Derudover gælder det, at PIN-koden:
    - automatisk suspenderes i en time efter tre forkerte forsøg og spærret efter seks forkerte.
    - indtastes i MitID app via et specielt udviklet tastatur kontrolleret af appen.
    - aldrig sendes fra MitID appen til MitID systemet for validering, det er et derivat af PIN-koden, der sendes via en såkaldt 'zero knowledge password proof'-protokol. Det centrale MitID-system vil afvise valideringsanmodningen, medmindre den kommer via den aktive MitID app, hvor den indtastes.
    - valideres centralt i MitiD – uanset om man taster PIN-koden ind eller om man bruger biometri. Valideringen sker aldrig på den mobile enhed.
- Man kan via en transaktionstekst at se, hvilken transaktion man som bruger godkender. Transaktionsteksten krypteres inden udsendelse og kan kun dekrypteres af den rigtige brugers MitID app.
- Man kan se navnet på MitID tjenesteudbyderen i MitID appen, så man kan koble godkendelsen sammen med brugssituationen hos den konkrete tjenesteudbyder. Navnet kommer fra brokeren, som er underlagt strenge sikkerheds- og certificeringskrav. En ondsindet tjenesteudbyder kan således ikke vise brugeren et forkert tjenesteudbydernavn.
- Man har altid selv mulighed for at spærre sine MitID apps enten på MitID.dk eller ved at henvende sig til MitID supporten. Det er også muligt øjeblikkeligt at suspendere aktive MitID apps fra centralt hold, hvis konkrete mobile platforme vurderes sårbare. Suspenderingen kan fjernes igen, når disse sårbarheder er blevet adresseret.

- Man får aldrig en 'push'-notifikation for anmodninger – netop for at skærpe opmærksomheden og dermed undgå, at man godkender anmodninger, som man ikke selv har startet. Derudover gælder det, at:
    - en anmodning har en levetid på fem minutter, hvorefter den ikke længere er aktiv; dette tidsrum kan ændres i MitID-systemet med umiddelbar effekt, hvis der skulle opstå behov.
    - man ikke kan få samtidige anmodninger – og man bliver opmærksom på det, hvis dette sker.
    - når man har godkendt eller afvist en anmodning på en mobil enhed, så er anmodningen ikke længere aktiv på evt. øvrige MitID apps på andre mobile enheder.

Baggrund

Fra NemID til MitID

MitID blev indfaset fra oktober 2021 til juni 2023. Indfasningen var en meget stor omlægning af det digitale Danmark, og derfor skete overgangen fra NemID til MitID også over en længere periode og i forskellige faser. Det skulle være med til at sikre, at var god tid til at få brugerne over i den nye løsning – og fordi andre tekniske løsninger og systemer, som MitID skulle spille sammen med, også krævede tid til omstilling.

Derfor blev både organisationer, virksomheder og funktionaliteter løbende koblet på løsningen, så man kunne bruge MitID til flere og flere private og offentlige tjenester på nettet. Undervejs i udviklingen af MitID har der været et godt samarbejde med en lang række organisationer for at understøtte og forberede overgangen til MitID for de brugere, der har brug det.

Forskelle på NemID og MitID
Med MitID sagde vi f.eks. farvel til NemID-nøglekortet, som kunne kopieres og deles. Derudover lever MitID op til den EU-lovgivning, der regulerer området – noget, som har udviklet sig væsentligt siden introduktionen af NemID. Det betyder, at der er helt andre standarder, som f.eks. offentlige tjenesteudbydere, brokere og identitetsløsninger skal leve op til end tidligere (læs mere på side 5).

Derudover er der række elementer i infrastrukturen, som er anderledes fra NemID til MitID. I MitID infrastrukturen er det nemlig ikke muligt for almindelige tjenesteudbydere at tilslutte sig MitID direkte, som de kunne i MitID NemID. I stedet skal tjenesteudbydere tilsluttes gennem en certificeret MitID broker, der formidler autentifikationsprocessen af slutbrugeren og den underliggende tekniske integration til MitID.

Til forskel for NemID er MitID desuden udviklet med modularitet og fleksibilitet som hovedkrav. Dette gør det nemt og hurtigt at omstille MitID til nye sikkerhedskrav – og at håndtere et trusselsbillede, der ændrer sig løbende. Derudover er der en række tekniske og sikkerhedsmæssige forbedringer i forhold til NemID, både brugerrettede og strukturelle sikkerhedselementer. F.eks. er det muligt for slutbrugeren at se tjenesteudbydernavn samt transaktionstekst, så der er større sikkerhed for, at man kun godkender det, som man ønsker at godkende.