Om MitID

Baggrund

Version 1.03

Om MitID

Indhold

Velkommen til MitID

Dette materiale har til formål at oplyse om MitID: Den nye nationale eID-løsning, som erstatter NemID – og som kommer til at kunne anvendes på tværs af offentlige og private tjenester.

Materialet her giver en lidt dybere indføring i f.eks. opbygningen af MitID, forskellene mellem NemID og MitID og de centrale sikkerhedselementer. Derudover er der en gennemgang af MitID appen.

Dette materiale 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 afløser NemID

I løbet af 2021-2022 vil MitID afløse NemID.

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.

Sådan kan du bruge MitID
MitID er primært en app, hvor man med et swipe kan godkende handlinger på nettet. Der vil dog være fysiske alternativer, hvis man ikke kan eller ønsker at bruge MitID app.

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, så ingen andre kan høre med.

MitID chip
MitID chip er primært tiltænkt anvendelse i erhvervsøjemed eller de brugere, der ønsker et alternativ til MitID kodeviser eller -kodeoplæser. Chippen kan tilkøbes efter endt migrering.

Der er forskellige måder at få MitID på
Men fælles er, at du skal bekræfte, hvem du er – så ingen andre kan udgive sig for at være dig. Du skal også vælge et bruger-ID - og beslutte, hvordan du vil bruge MitID, f.eks. med MitID app eller -kodeviser. En oprettelse af MitID kan ske ved brug af NemID, et gyldigt pas/internationalt ID-kort eller ved besøg i Borgerservice.

Derfor skal vi have MitID

Med MitID styrker vi sikkerheden – også i fremtiden. NemID er en sikker løsning i dag, men vi skal hele tiden være opmærksomme på vores digitale sikkerhed og på at leve op til forskellige internationale sikkerhedskrav. Derfor er det nødvendigt med en ny løsning, som kan ruste Danmark til fremtidens digitale udfordringer og muligheder. Med MitID sikrer vi, at det også fremover er trygt at færdes på nettet med sit digitale ID.

MitID giver Danmark en ny sikkerhedsinfrastruktur for digitale identiteter, hvor sikkerhedskravene lever op til de nyeste standarder for sikkerhed. Samtidig er MitID modulært og fleksibelt opbygget. Det betyder, at det er nemmere at tilpasse MitID til fremtidige trusselsbilleder og at reagere hurtigt på skiftende internettrusler.

Derudover betyder udbudsloven, at store aftaler mellem private parter og offentlige myndigheder løbende skal

konkurrenceudsættes. Den nuværende aftale med Nets om NemID står til at udløbe, og derfor har opgaven været i udbud.

Navnet

Navnet MitID er udviklet og udvalgt for at signalere, at MitID er ens eget, personlige digitale ID. Med navnet understreger vi dermed, at man skal huske og har ansvar for at passe godt på sin digitale identitet.

Logoet er udviklet i samme proces og understreger, at MitID er personligt. Derfor er den lille person integreret i logoet som et "i". Designet er enkelt og bruges gennemgående i al kommunikation om MitID.

For at beskytte MitID navnet har vi opkøbt flere domænenavne og får løbende lukket falske MitID-sider, som forsøger at svindle brugerne. I kommunikationsindsatsen har vi samtidig fokus på at informere brugerne om, at de officielle kanaler er Digital Post, bankernes net- og mobilbanker samt MitID.dk. Brugerne skal være opmærksomme på og forsigtige med kommunikation gennem andre kanaler. Erfaringsmæssigt ved vi, at ændring af systemer ofte af kriminelle bruges som anledning til f.eks. at gennemføre phishingangreb mod slutbrugerne

Forskellen på NemID og MitID

MitID afløser og udbygger sammen med det offentliges løsninger, NemLog-in og MitID Erhverv, den funktionalitet, der i dag ligger i NemID. I modsætning til den eksisterende NemID-løsning indeholder MitID ikke en signatur- og erhvervsløsning. Erhvervsdelen og signaturløsningen anskaffes alene 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.

MitID er elektronisk validering af en persons identitet
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.

EU-lovgivning regulerer området
Et af de områder, der har udviklet sig væsentligt siden introduktionen af NemID, 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.

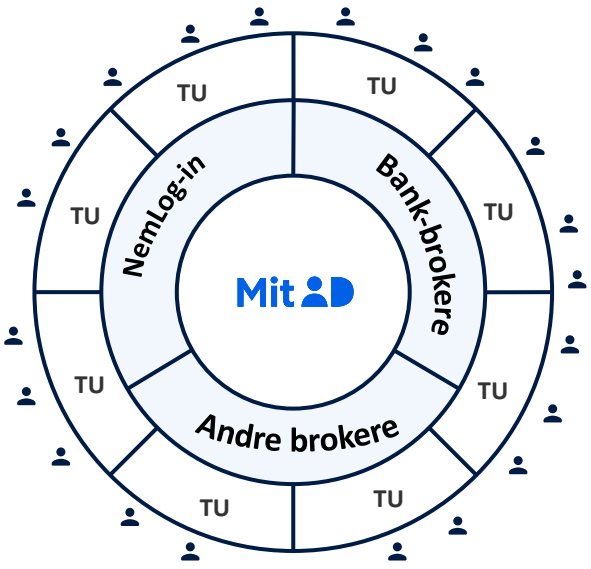
Danmark har anmeldt MitID som national eID-løsning, så identiteter herfra skal anerkendes på tværs af EU. Digitaliseringsstyrelsen har udarbejdet en National Standard for Identiteters Sikringsniveau (NSIS), der definerer de krav, der skal gælde for danske eID-løsninger for at leve op til eIDAS' tre sikringsniveauer for digitale identiteter. Fremover skal alle offentlige tjenesteudbydere, brokere og identitetsløsninger, der skal benytte den nationale infrastruktur, 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.

Ændringer i infrastruktur
Herudover vil overgangen fra NemID til MitID medføre en række infrastrukturelle ændringer:

- I MitID infrastrukturen er det ikke muligt for almindelige tjenesteudbydere at tilslutte sig MitID direkte, som det kendes fra NemID. I stedet skal tjenesteudbydere tilsluttes gennem en certificeret MitID broker, der formidler autentifikationsprocessen af slutbrugeren og den underliggende tekniske integration til MitID (se model nedenfor). Dette design giver en række fordele i forhold til NemID. Det er f.eks. kun brokere, der har behov for at forholde sig til ændringer i bl.a. MitID-snitflader og sikkerhedsprocedurer. Dette gør, at MitID bliver mere sikkert og robust. Derudover er det forventningen, at brokerne vil tilbyde egne løsninger med slutbruger-autentifikation via MitID.
- 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.

Endelig er der en række tekniske og sikkerhedsmæssige forbedringer i forhold til NemID, både brugerrettede og strukturelle sikkerhedselementer. Nogle af disse uddybes i næste afsnit og senere i afsnittene om MitID appen.



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.

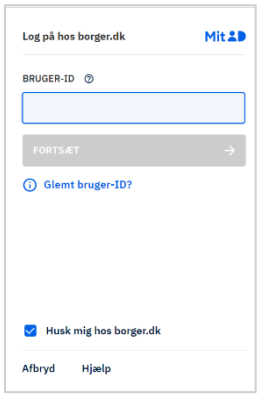
- Bank-brokerne giver bankerne adgang til MitID.
- NemLog-in giver offentlige myndigheder adgang til MitID.
- Andre brokere giver øvrige tjenesteudbydere adgang til MitID.

Generelt om sikkerheden

Med MitID styrker vi sikkerheden på især tre områder: 1) i den tekniske løsning 2) i forhold til den måde, som MitID bruges på og 3) i kravene til identitetssikring.

Sikkerheden styrkes i den tekniske løsning

- 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 personlige MitID bliver anvendt.
- 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.
- Man kan se en meddelelse, der karakteriserer den transaktion, man er i gang med (f.eks. 'Log på'). Man kan også se et tjenesteudbydernavn, som kommer fra MitID. Se billedet til højre.
- Man kan ikke 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.



En tekst fortæller, hvad man er i gang med. Skal tjekkes, inden man godkender med MitID.

Derudover er MitID's infrastruktur modulært og fleksibelt opbygget – og dermed kan der reageres hurtigt på skiftende internettrusler. Det betyder, at løsningen løbende kan tilpasses for at styrke sikkerheden.

Endelig introduceres med MitID den såkaldte broker-model. En broker er en virksomhed eller organisation, der formidler adgang for tjenesteudbyderen til MitID og dermed varetager den tekniske integration til MitID. Broker-modellen styrker sikkerheden, da MitID-løsningen kun kan tilgås af certificerede brokere og ikke af mange forskellige tjenesteudbydere. Brokeren skal være certificeret for at blive koblet direkte på MitID-løsningen.

En broker er en it-virksomhed, som skærmer identiteterne i MitID. I NemID har alle tjenesteudbydere (dba.dk, danskespil.dk osv.) direkte adgang til oplysningerne i NemID, men det stiller store krav til hver tjenesteudbyder, fordi de både skal vedligeholde systemerne teknisk og sikkerhedsmæssigt. Den funktion er nu lagt ud til brokerne.

Fordelen er, at i MitID er høj kontrol med, hvem der har adgang til identiteterne, og der er færre af dem. Det gør det sikrere – og så sparer tjenesteudbyderne for at vedligeholde systemer.

Sikkerheden styrkes med de nye måder at bruge MitID på (f.eks. MitID app og -kodeviser)
Med MitID siger vi på sigt farvel til NemID-nøglekortet, som kan kopieres og deles. MitID er i stedet primært en app, der 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 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.

Sikkerheden styrkes med 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. Det betyder blandt andet, at nogle skal opdatere deres ID-oplysninger for at blive klar til MitID.

Det 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. Det gør man ved f.eks. aldrig at dele koder eller bruger-ID med andre.

Lang indfasning

MitID er en meget stor omlægning af det digitale Danmark. Derfor sker overgangen fra NemID til MitID også over en længere periode og i forskellige faser. Det sker for at sikre, at der er god tid til at få brugerne over i den nye løsning – og fordi andre tekniske løsninger og systemer, som MitID skal spille sammen med, kræver tid til omstilling.

I de kommende måneder vil en lang række organisationer, virksomheder og funktionaliteter derfor løbende blive koblet på løsningen, så man fremover kan bruge MitID til endnu flere private og offentlige tjenester på nettet.

Behold NemID
Selvom man har fået MitID, skal man man beholde sit NemID, både nøgleapp – hvis man har det – og nøglekort. For der vil være steder og situationer, hvor man fortsat skal bruge NemID, indtil det er endeligt udfaset.

Flytningen af de cirka 5 mio. NemID-brugere skydes i gang den 6. oktober 2021 og fortsætter ind i 2022. Brugerne får besked, når de ikke længere skal bruge NemID. Er der NemID-brugere, som ikke har fået MitID i migreringsperioden – og har brug for det – kan de få MitID med gyldigt pas/internationalt ID-kort i MitID appen, ved at besøge Borgerservice med gyldig legitimation – eller med NemID på MitID.dk.

En tryg overgang

Vi har stort fokus på at sikre en tryg overgang for alle. Derfor står vi klar med support for at hjælpe alle godt i gang. Har man brug for hjælp til at få MitID i den kommende periode, kan man kontakte MitID supporten. Har man særlige udfordringer, kan man også få hjælp i sin lokale borgerservice.

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.

Om MitID app

Anskaffelsen og anvendelse af MitID app

MitID er gratis at få og anvende. MitID er nemt at bruge, og alle, der bruger NemID i dag, skal kunne bruge MitID. Derfor er der forskellige måder at bruge MitID på: MitID app, MitID kodeviser, MitID kodeoplæser og MitID chip.

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 få et MitID første gang eller få MitID app tilbage, hvis man f.eks. har mistet sin telefon eller har fået en ny.

MitID appen har derfor to forskellige måder at fungere på. I det følgende kalder vi de to virkemåder for ”MitID app” og ”MitID app med pasfunktionalitet”.

MitID appen fungerer ved at fortælle online-tjenester, hvem man er. MitID app med pasfunktionalitet skal man kun bruge til at få et MitID første gang eller få MitID app tilbage, hvis man f.eks. har mistet sin enhed eller har fået en ny. Læs mere om, hvordan MitID app med pasfunktionalitet fungerer længere fremme.

MitID app
MitID appen virker på de fleste smartphones – fra iPhone 5S / iOS12 og frem. 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.

I det følgende gennemgås anvendelsen af MitID app, designet bag løsningen samt de sikkerhedsmæssige forhold, der er tilknyttet løsningen.

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.

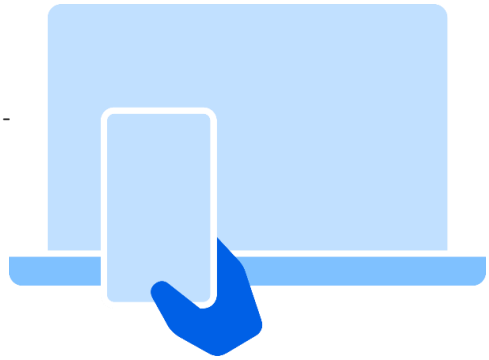
MitID app skal aktiveres før brug
Der kan kun være én MitID app på en mobilenhed. Appen hentet fra Google Play eller App Store kan ikke bruges til autentificering, før den er aktiveret – dvs. tilknyttet et specifikt MitID. En aktiv MitID app er personlig.

Brugeren kan enten aktivere appen under migreringen fra NemID til MitID eller ved ny-registrering hos et borgerservicecenter. 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 eller udleveret på papir af borgerservice – afhængig af, hvordan man får sit MitID. 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 til godkendelser mv. Brugeren kan 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.

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

Brugen af appen kan opsummeres således:

1. Gå ind på den hjemmeside, hvor du skal bruge MitID.
2. Indtast dit bruger-ID på hjemmesiden for at starte en anmodning til din MitID app.
3. Åbn MitID appen inden for fem minutter og besvar anmodningen, ellers udløber den.
4. Indtast din PIN-kode eller brug ansigtsgenkendelse/fingeraftryk, før du kan godkende anmodningen.
5. Swipe i MitID appen for at godkende den anmodning/handling, du startede på hjemmesiden.
6. Klik på 'Afvis' i MitID appen, hvis du ikke ønsker at gennemføre handlingen.

Hvis du benytter en app i stedet for en hjemmeside, f.eks. en mobilbank-app, hvor du skal bruge MitID app til at godkende en handling, kan du opleve, at denne app skifter direkte over til din MitID app og evt. tilbage igen, når du har swipet i MitID appen. Dette kaldes "app-switch". Det vil være op til den enkelte app, om dette sker, og hvordan det vil se ud. Ligeledes kan en app gemme dit bruger-ID, så du ikke selv skal indtaste det.

Pas godt på dit personlige MitID

MitID er et personligt ID, og derfor skal du passe godt på det. Det gør du blandt andet ved ikke at dele hverken bruger-ID eller koder med andre og aldrig at godkende en MitID-handling, som du ikke selv har igangsat.

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.

Den 7. juni 2022 er 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. Læs mere senere i dokumentet.

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 hørende 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.

Tjenesteudbyder
Sidstnævnte 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
Et ofte stillet spørgsmål om sikkerhedsdesignet af MitID app er, hvorfor brugerne ikke skal indtaste en adgangskode sammen med bruger-ID'et, som de gør i NemID i dag, men i stedet kan gå direkte i MitID app for at godkende en anmodning, efter de har indtastet deres MitID bruger-ID hos tjenesteudbyderen.

Dette er et naturligt spørgsmål, når man sammenligner de to løsninger i forhold til brugen af de forskellige autentifikationsfaktorer, og når man ser på det flow, brugerne er vant til fra NemID nøgleapp i dag.

Det korte svar på spørgsmålet 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 MitID appen, mens den i NemID

nøgleappen lå uden for appen (i form af den centralt validerede adgangskode, der blev indtastet sammen med bruger-ID'et).

Centralt valideret videnselement flyttet ind i MitID app
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 af 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 brugeren ikke altid kan gennemskue, om det er en falsk hjemmeside – eller om der eksempelvis er installeret en key-logger på den PC, der anvendes. Dertil kommer, at hvis man forsøger at angribe NemID nøgleappen kontra MitID appen, er det sværere i MitID, netop fordi videnselementet (PIN'en) er centralt valideret.

Brugerne modtager ikke notifikation til at åbne MitID app
Med MitID modtager brugerne ikke længere en notifikation på deres mobile enheder, hvorigennem de 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 brugeren benytter en app i stedet for en hjemmeside, f.eks. en mobilbank-app, hvor man skal bruge MitID app til at godkende en handling, kan man opleve, at denne app skifter direkte over til din MitID app og evt. tilbage igen, når man har swipet i MitID appen. Dette kaldes "app-switch". Det vil være op til den enkelte app, om dette sker, og hvordan det vil se ud. Ligeledes kan en app gemme ens bruger-ID, så man ikke selv skal indtaste det.

Almindelig sund fornuft og forholdsregler for den enkelte

MitID app lever op til gældende sikkerhedsstandarder og er udviklet med stort fokus på sikkerhed og brugervenlighed. Men som i alle sikkerhedsløsninger er det vigtigt, at brugeren udviser almindelig sund fornuft og lever op til følgende:

- Hent MitID app kun via de officielle app stores og kontroller, at det er Digitaliseringsstyrelsen, der er angivet som udvikler.
- Beskyt altid den mobile enhed med kode eller fingeraftryk/ansigtsgenkendelse – dvs. ud over PIN-kode til MitID app.
- Del aldrig din MitID app PIN-kode med andre.
- Del aldrig dit bruger-ID med andre – undtagen med supporten, hvis du selv kontakter den.
- Godkend aldrig en MitID-handling, som du ikke selv har igangsat.
- Root/jailbreak aldrig den mobile enhed (dvs. slå ikke sikkerhedssystemet i smartphone og tablet fra). Herved sikres, at enheden bliver holdt sikker og opdateret af producenten, ligesom risikoen for skadelig malware mindskes. MitID app er beskyttet med sikkerhedstiltag for at reducere risikoen for, at appen eksekveres på rootede og jailbroken enheder.

Derudover er der en række andre forholdsregler, der fortjener en uddybning:

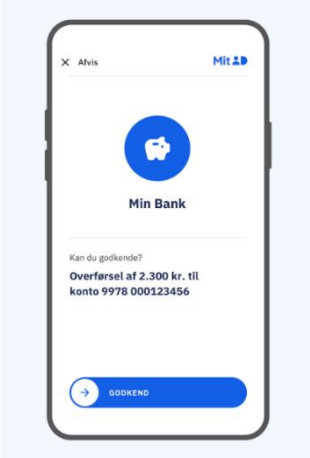
Tjek, hvem der sender anmodningen
Brugeren skal altid være sikker på to forhold:

- Man forventer en anmodning på baggrund af noget, man har foretaget sig i en selvbetjeningsløsning.
- Man genkender og forventer navnet på den service/tjenesteudbyder, der står i teksten i MitID app ud fra den handling, brugeren har startet.

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

Tjek, hvad der skal godkendes
Brugeren skal altid tjekke den handling, som han eller hun 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 anmodning, 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.

Brugen 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 eller din bank. Man vil aldrig blive kontaktet på den måde fra en legitim offentlig myndighed eller bank.

Det er meget vigtigt, at brugeren giver sig tid til at sikre, at anmodningen, 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 eller besvarer en anmodning i MobilePay eller betaler i et supermarked.

Hvis man er i tvivl, skal man altid afvise. Brugeren kan også altid gå ind på MitID.dk i sin aktivitetslog og se, hvad der faktisk er sket. Brugeren kan også ændre sin indstilling for notifikationsniveau på MitID.dk, så han eller hun får tilsendt flere informationer om, hvad der sker med hans eller hendes MitID, inkl. anvendelsen af det.

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 i det følgende. 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 låne 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 gerne i ro og mag derhjemmefra vil have MitID.
og dermed kan spare turen i Borgerservice. Det drejer sig bl.a. om:

1. Dem, der skal opdatere deres ID-oplysninger i NemID for at blive klar til MitID og ikke har NemID nøgleapp
2. Dem der ikke har en telefon, der kan scanne deres pas
3. Dem, der ikke har NemID i dag og skal have MitID, f.eks. unge borgere, som bliver gamle nok til at få MitID eller tilflyttere

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/inernationalt ID-kort med chip og en telefon, der kan scanne chippen i passet, dvs. mindst iPhone 7 og iOS 12 eller en nyere Android telefon.

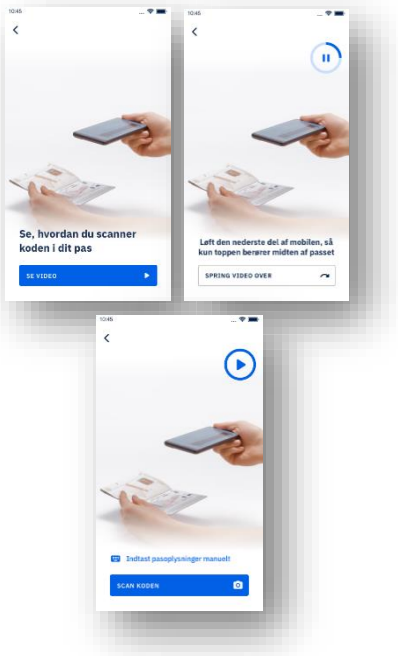
1. Find pas-funktionaliteten på forsiden af MitID app via indstillingerne (øverste ventre hjørne) under menupunktet “Få MitID med pas” (hvis man skal have MitID) eller ”Aktiver MitID” (hvis man f.eks. har mistet sin MitID app).
2. Scan koden og aflæs chippen i passet/ID-kortet.
3. Scan ansigtet – så 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 og aktiver MitID appen – eller bestil og aktiver f.eks. en MitID kodeviser eller kodeoplæser. Herefter er man klar til at bruge MitID.

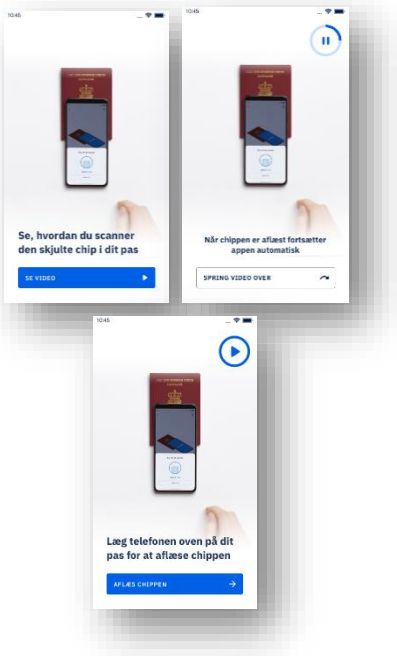
Hvis man har et udenlandsk pas/ID-kort – og man ikke har et dansk CPR-nummer til at indtaste i appen – skal man have en såkaldt P-kode. Den skal bruges som et led i at bekræfte ens identitet. P-koden får man f.eks. hos Borgerservice eller i MitID Supporten.

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

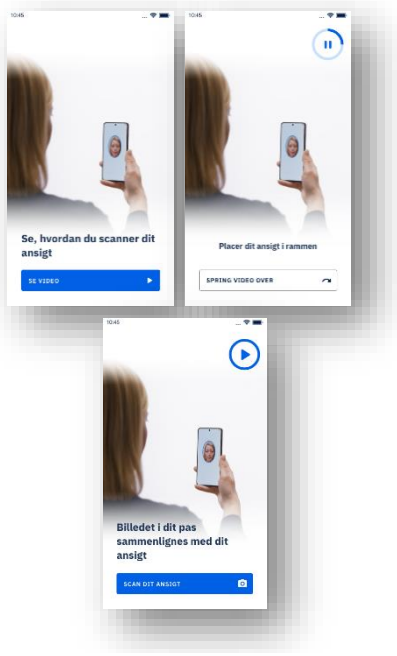
1) Scan koden i passet



2) Scan chippen i passet



3) Scan ansigt



Sådan bekræftes identiteten

Hvis man hjælper en anden med at få MitID
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. Man kan fortsat få MitID på MitID.dk med NemID eller hos Borgerservice med gyldig legitimation. Man kan også stadig

opdatere sine ID-oplysninger med NemID nøgleapp. Har man ikke et gyldigt pas og er blevet bedt om at opdatere sine ID-oplysninger, skal man fortsat i Borgerservice.

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/internationalt 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.

Appen gør 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” check.
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.

Sådan fungerer 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 og der genereres en aktiveringskode.

Aktivering af MitID app eller f.eks. MitID kodeviser
Brugeren kan herefter – hvis han eller hun ønsker det – nu indrullere og 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
Hvis brugeren ønsker at oprette et nyt MitID:

- CPR-nummer (hvis bruger har et sådant), 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.

Hvorfor er det sikkert at benytte MitID pas-funktionaliteten?
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. Teknologien 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.

Kan MitID pas-funktionaliteten misbruges til overvågning?
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.

Kan MitID pas-funktionaliteten tage fejl ved ansigtsvalideringen?
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. For MitID pas-funktionaliteten arbejdes med en FAR (False Acceptance Rate) på 1/10.000. Læs evt. mere på næste side.

Hvorfor kan MitID pas-funktionaliteten benyttes online til identitetssikring?
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.

Er MitID pas-funktionaliteten baseret på internationale standarder?
Som udgangspunkt understøtter pas-funktionaliteten internationale standarder. Her kan nævnes ICAO 9303, som benyttes i rejsepas – og at det software, som udfører "liveness"-tjek, er certificeret efter ISO/IEC 30107-3 "Biometric presentation attack detection".

Er MitID pas-funktionaliteten bedre eller dårligere til at lave svigagtige person-foto-sammenligninger end mennesker?
Der er lavet flere undersøgelser om dette emne. 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 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.

Er MitID pas-funktionaliteten sammenlignelig med f.eks. FaceID?
Nej, man kan ikke sammenligne de to metoder. 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.

Hvad er sammenhængen mellem NSIS og eIDAS og MitID pas-funktionaliteten?
NSIS er den danske udmøntning af eIDAS EU-forordningen. I begge stilles der de samme krav til identitetssikringen af en person, før der kan udstedes en elektronisk identitet til personen.

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 og uddybning af sikkerhed

Generelt om sikkerheden i MitID

Nedenfor er en opsummering af de generelle sikkerhedselementer 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 tilpasset for at styrke sikkerheden.

Broker-modellen
I MitID introduceres *broker*-modellen. En broker er en virksomhed eller organisation, der formidler adgang for tjenesteudbyderen til MitID og dermed varetager den tekniske integration til MitID. Broker-modellen styrker sikkerheden ved, at MitID-løsningen kun kan 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 nye, høje krav til identitetssikring. Det betyder blandt andet, at nogle skal opdatere deres ID-oplysninger for at blive klar til MitID.

Sikringsniveauer lav, betydelig og høj
I MitID indføres begrebet sikringsniveauer: lav, betydelig og høj. Disse sikringsniveauer og kravene til dem 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.

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 brugeren altid bliver orienteret om hændelser i MitID, der muligvis kræver aktion fra brugers side. Brugeren kan selv vælge, på hvilket niveau der skal sendes notifikationer, og hvilken kanal der skal benyttes. Disse indstillinger kan opdateres på MitID.dk af brugeren eller gennem supporten. Under registreringen af brugeren vælges en kanal, der efterfølgende kan ændres på MitID.dk.

Disse primære notifikationskanaler understøttes (kun de tre første kan vælges ved registreringen/migreringen): MitID app, SMS, e-mail, Digital Post (forventes understøttet ultimo 2022) og fysisk post (kan ikke tilvælges af brugerne, men vil blive brugt til vigtige hændelser, hvis brugeren ikke har valgt en anden notifikationskanal).

Det anbefales, at brugeren også vælger en sekundær notifikationskanal, hvis den primære notifikationskanal er sammenfaldende med et identifikationsmiddel, f.eks. hvis man vælger SMS som notifikationskanal og denne er tilknyttet samme fysiske enhed som MitID app. Så bør man vælge f.eks. e-mail som sekundær kanal. Hvis MitID oplever fejl ved forsøg på at sende en notifikation, vil MitID - afhængig af den valgte notifikationskanal - forsøge et antal gange. Herefter benyttes Digital Post ved vigtige hændelser, og endelig fysisk post, hvis brugeren ikke har Digital Post.

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 bruger-ID'et er brugerens eget unikke valg og ikke et brugernavn, man kan få kendskab til, hvis man f.eks. har fået adgang til cpr-numre.

Visning af tjenesteudbydernavn og handlingstekst
I MitID-visningen af tjenesteudbydernavn og handlingstekst for brugeren er udbygget i forhold til NemID. 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. Tjenesteudbyderen kan dermed ikke foranledige, at der vises brugeren et forkert tjenesteudbydernavn. Handlingsteksten og tjenesteudbydernavnet vises altid for brugeren, uanset hvilket identifikationsmiddel slutbrugeren anvender, og uanset om anvendelsen sker via en web- eller app-kanal.

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 tillige ved vedligeholdelsen af løsningen.

Der er implementeret sikkerhedsforanstaltninger i løsningen (f.eks. via risikodata), som brokeren kan bruge til at vurdere risikoen ved en specifik MitID autentifikation. Brokeren er den virksomhed eller organisation, som formidler adgang til MitID for tjenesteudbyderne.

Der bliver løbende holdt øje med trusler mod MitID, så der kan indføres tiltag, der kan imødegå nye risici og trusler.

MitID overvåges intensivt under hele driftsfasen, 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:

- Aktivering af MitID app kræver to uafhængige koder, der formidles til brugeren af to uafhængige kanaler.
- Anvendelse af en MitID app kræver indtastning af en 6-cifret PIN-kode eller anvendelse af biometri.
- Anvendelse af biometri er kun mulig på mobile platforme, som overholder relevante tekniske retningslinjer og anbefalinger.
- Det er muligt via regler, som kan iværksættes øjeblikkeligt, at suspendere aktive MitID apps, hvis konkrete mobile platforme vurderes sårbare. Suspenderingen kan fjernes igen, når disse sårbarheder er blevet adresseret.
- PIN-koden er underlagt regler ved generering, som gør, at ofte benyttede talsekvenser – og dermed lette at gætte – ikke kan benyttes.
- Validering af PIN-koden sker altid centralt i MitID, uanset om brugeren taster PIN-koden ind, eller den frigives via biometri. Valideringen sker aldrig lokalt på den mobile enhed.
- PIN-koden bliver automatisk suspenderet i en time efter tre forkerte forsøg og spærret efter seks forkerte forsøg.
- Indtastningen af PIN-koden i MitID app sker via et specielt udviklet tastatur kontrolleret af appen.
- PIN-koden i sig selv sendes aldrig 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.
- Der sendes aldrig “push”-notifikationer for anmodninger til brugerne for at skærpe opmærksomheden omkring anvendelsen af MitID appen – og dermed undgå, at brugerne godkender anmodninger, som de ikke selv har startet.
- Flere samtidige autentifikationsanmodninger fra den samme bruger kan ikke lade sig gøre, og brugeren gøres opmærksom på det, hvis dette sker.
- Når en anmodning er godkendt eller afvist på en mobil enhed, så er den pågældende anmodning ikke længere aktiv på brugerens evt. øvrige MitID apps på andre mobile enheder.
- En anmodning har en levetid på fem minutter, hvorefter den ikke længere kan anvendes til godkendelse. Dette tidsrum er konfigurerbart i MitID systemet med umiddelbar effekt, hvis der skulle være behov for ændringer.
- Det vil altid være muligt 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.
- Navnet på MitID tjenesteudbyderen vises altid i MitID appen, så brugeren 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.

- Brugeren har mulighed for at modtage notifikationer om sin aktivitet fra MitID, hvor brugeren selv kan fastsætte detaljegraden af disse notifikationer. Dette kunne f.eks. være, hvis der aktiveres nye MitID identifikationsmidler, eller der er foretaget ændringer i brugerens stamdata på MitID.dk. Brugeren kan altid se sin brug af MitID i aktivitetsloggen på MitID.dk
- Brugeren har altid selv mulighed for at spærre sine MitID apps enten på MitID.dk eller ved at henvende sig til MitID supporten.