



Tofaktorautentisering (2FA) ved bruk av Tidsbasert engangspassord (TOTP) i MinID

Two-factor authentication (2FA) using time-based onetime
password (TOTP) in MinID.

Kravdokumentasjon

Versjon 1.0

Dokumentet er basert på Kravdokumentasjon utarbeidet ved NTNU. Revisjon og tilpasninger til bruk ved IDER, DATA-INF utført av Carsten Gunnar Helgesen, Svein-Ivar Lillehaug og Per Christian Engdal. Dokumentet finnes også i engelsk utgave.



REVISJONSHISTORIE

Dat o	Versjon	Beskrivelse	Forfatter
13. Februar	0.1	interaktivt Wireframe	E.F, J.V.E
14. Februar	0.2	Brukstilfelle/-diagram	U.F
21. Februar	0.3	Brukstilfellebeskrivelser, Wireframes	E.F, J.V.E
22. Februar	0.4	Domenemodell	U.F.
25. Februar	1.0	Skrivekontroll	J.V.E
04. Mai	1.1	QR-kode flow endring	U.F



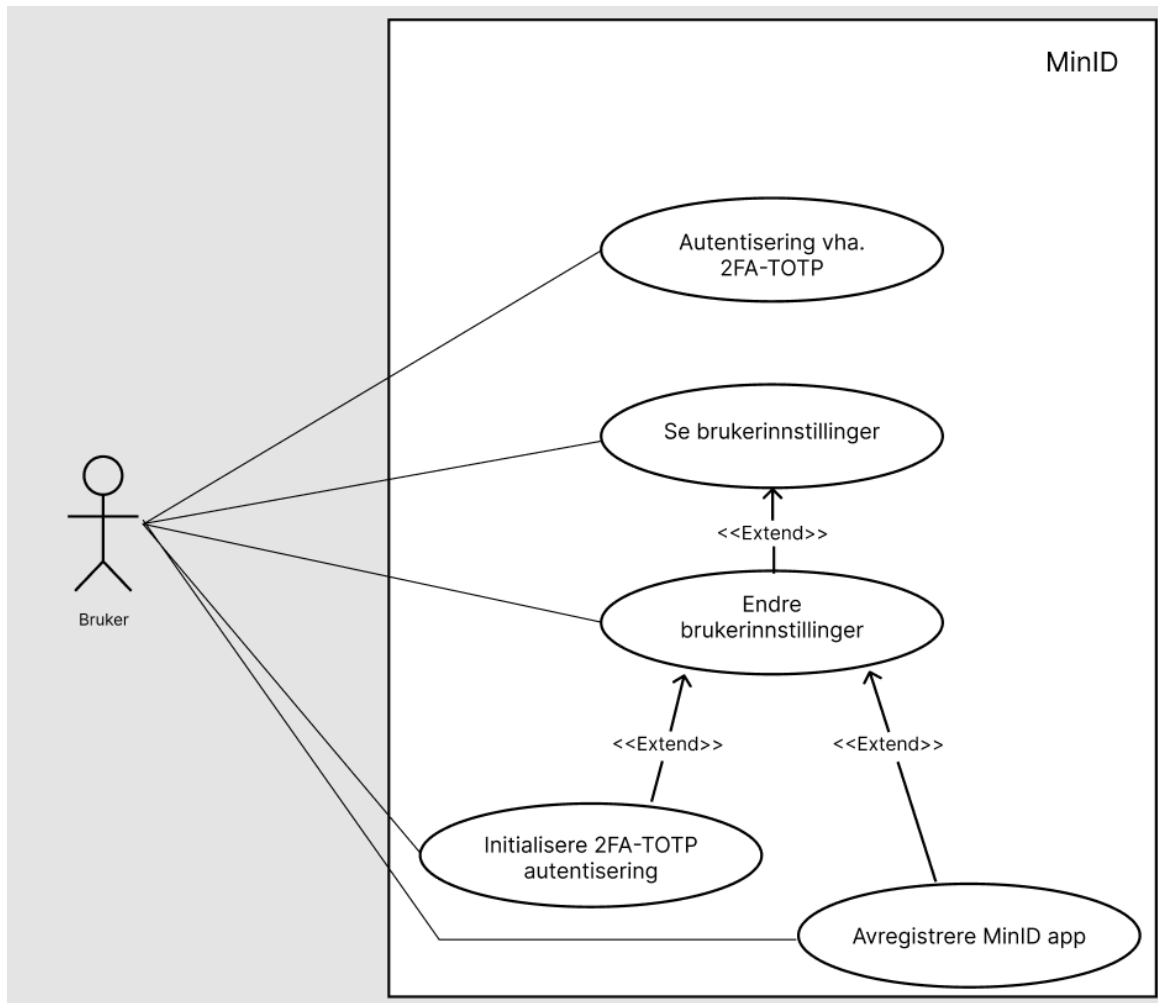
INNHALDSFORTEGNELSE

1	INNLEDNING	1
2	FUNKSJONALITET	2
3	DOMENEMODELL	6
4	PROTOTYPER	7
4.1	WIREFRAMES	7
4.2	HTML-PROTOTYPER	9
5	REFERANSER	10

1 INNLEDNING

Dette dokumentet er laget for å gi en lett oversikt over den planlagte løsningen rundt tofaktorautentisering for MinID. Dokumentet går først inn hvilke brukstilfeller som er aktuelle for en bruker av MinID tjenesten, og går videre inn i en mer detaljert beskrivelse for hvert brukstilfelle. Det er inkludert en domenemodell for å gi innblikk i hvordan systemet rundt løsningen er forstått/realisert. Det er også illustrert wireframes ved hjelp av screenshots og konseptuelle UI elementer som er demonstrert interaktivt i Figma.

2 Funksjonalitet



Figur 1 Brukstilfellemodell for ny MinID-løsning

Tabell 1 Brukstilfellebeskrivelse: "Se Brukerinnstillinger"

Navn:	Se Brukerinnstillinger
Aktører:	MinID-bruker
Normalflyt:	<ol style="list-style-type: none"> 1. Bruker velger MinID fra ID-portens meny av alternativer 2. Trykk på rullegardinmeny i innloggingsvindu 3. Velger MinID-Innstillinger 4. Velg innloggingsmetode for MinID tilgang 5. Logg inn med fødselsnummer og passord 6. Gjennomfør 2FA
Alternativ flyt [#1]:	<ul style="list-style-type: none"> • Bruker er allerede autentisert, må dermed skrive inn MinID-Innstillinger URL for å nå fram.
Unntaksflyt [#1]:	<ul style="list-style-type: none"> • 3 mislykkede innloggingsforsøk låser brukerkonto

Tabell 2 Brukstilfellebeskrivelse: "Endre Brukerinnstillinger"

Navn:	Endre Brukerinnstillinger
Aktører:	MinID-bruker
Normalflyt:	<ol style="list-style-type: none"> 1. Bruker velger MinID fra ID-portens meny av alternativer 2. Trykk på rullegardinmeny i innloggingsvindu 3. Velg MinID innstillinger 4. Velg innloggingsmetode for MinID tilgang 5. Logg inn med fødselsnummer og passord 6. Gjennomfør 2FA 7. Bruker endrer passord eller innloggingsmetode ved å trykke ikon ved høyre for egenskap som ønskes forandret.
Alternativ flyt [#1]:	<ul style="list-style-type: none"> • Bruker skriver inn et for svakt passord ved endring av passord og blir bedt om å skrive inn ett som fyller kriteriene.
Unntaksflyt [#1]:	<ul style="list-style-type: none"> • 3 mislykkede innloggingsforsøk låser brukerkonto

Tabell 3 Brukstilfellebeskrivelse: "Initialisere TOTP-autentisering"

Navn:	Initialisere 2FA-TOTP autentisering
Aktører:	MinID-bruker
Normalflyt:	<ol style="list-style-type: none"> 1. Bruker velger MinID fra ID-portens meny av alternativer 2. Trykk på rullegardinmeny i innloggingsvindu 3. Velg MinID innstillinger 4. Velg innloggingsmetode for MinID tilgang 5. Logg inn med fødselsnummer og passord 6. Gjennomfør 2FA 7. Bruker trykker på ikon for endring av autentiseringsmetode 8. Trykker så Hamburgermeny for å se alternativer til MinID app 9. Velger relevant autentiseringsapp 10. En QR-kode kommer frem, denne skannes av brukers mobilkamera via aktuelle app 11. Bruker må legge inn en bekreftelseskode frembrakt av app 12. Bruker har nå en ny autentiseringsmetode
Alternativ flyt [#1]:	<ul style="list-style-type: none"> • Bruker har ikke mulighet til å skanne QR-koden med kamera, må dermed skrive inn koden i appen sin manuelt.
Unntaksflyt [#1]:	<ul style="list-style-type: none"> • 3 mislykkede innloggingsforsøk låser brukerkonto

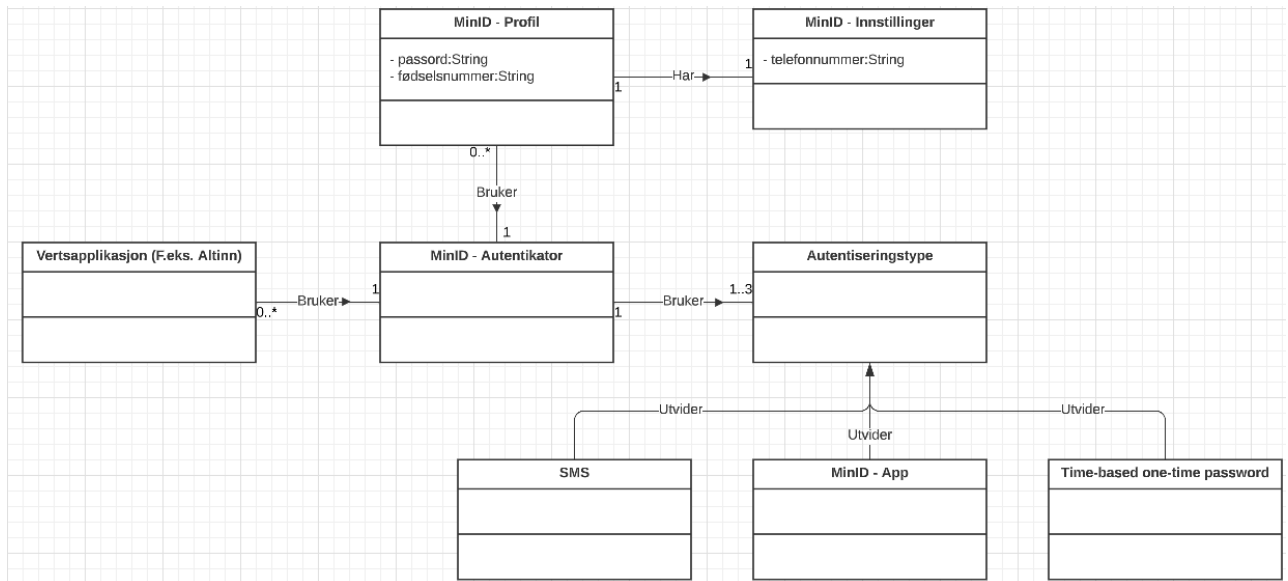
Tabell 4 Brukstilfellebeskrivelse: "Avregistrere MinID app"

Navn:	Avregistrere MinID app
Aktører:	MinID-bruker
Normalflyt:	<ol style="list-style-type: none"> 1. Bruker velger MinID fra ID-portens meny av alternativer 2. Trykk på rullegardinmeny i innloggingsvindu 3. Velg MinID innstillinger 4. Velg innloggingsmetode for MinID tilgang 5. Logg inn med fødselsnummer og passord 6. Gjennomfør autentiseringen 7. Bruker trykker på ikon for endring av autentiseringsmetode 8. Trykk på rødt kryss ved autentiseringsmetode som skal avregistreres 9. I meldingsboks for fjerning, trykker bruker 'ja' for å bekrefte 10. Autentiseringsmetode vil falle tilbake på SMS-kode
Unntaksflyt [#1]:	<ul style="list-style-type: none"> • 3 mislykkede innloggingsforsøk låser brukerkonto

Tabell 5 Brukstilfellebeskrivelse: "Autentisering vha. TOTP"

Navn:	Autentisering vha. 2FA-TOTP
Aktører:	MinID-bruker
Hensikt/Målsetting:	Sikker autentisering/innlogging ved nettsted som benytter seg av ID-porten sine tjenester
Normalflyt:	<ol style="list-style-type: none"> 1. Bruker velger MinID fra ID-porten sine alternativer. 2. Fyller inn fødselsnummer og passord i inputfeltene og trykker på "neste". 3. Blir bedt om å fylle inn Microsoft Authenticator kode i gitt inputfelt. 4. Bruker åpner Microsoft Authenticator appen sin og fyller inn koden sin. 5. Trykker "verifiser" for å fullføre autentisering/innlogging <p>Microsoft Authenticator brukes i dette eksempelet, men Google Authenticator, Authy og liknende ville hatt lik flyt om valgt.</p>
Alternativ flyt [#1]:	<ul style="list-style-type: none"> • Feil fødselsnummer eller passord blir skrevet inn fører til at bruker blitt bedt om å prøve igjen.
Alternativ flyt [#2]:	<ul style="list-style-type: none"> • Trykker på "nei, avbryt" istedenfor å godkjenne i 2FA-TOTP steget, må dermed starte fra steg 2 i normalflyt igjen.
Alternativ flyt [#3]:	<ul style="list-style-type: none"> • Bruker er allerede autentisert ved innlogging på annen side og blir automatisk sendt videre uten ny manuell autentisering.
Unntaksflyt [#1]:	<ul style="list-style-type: none"> • 3 mislykkede innloggingsforsøk låser brukerkonto

3 DOMENEMODELL



Figur 2 Domenemodell for ny MinID-løsning

4 PROTOTYPER

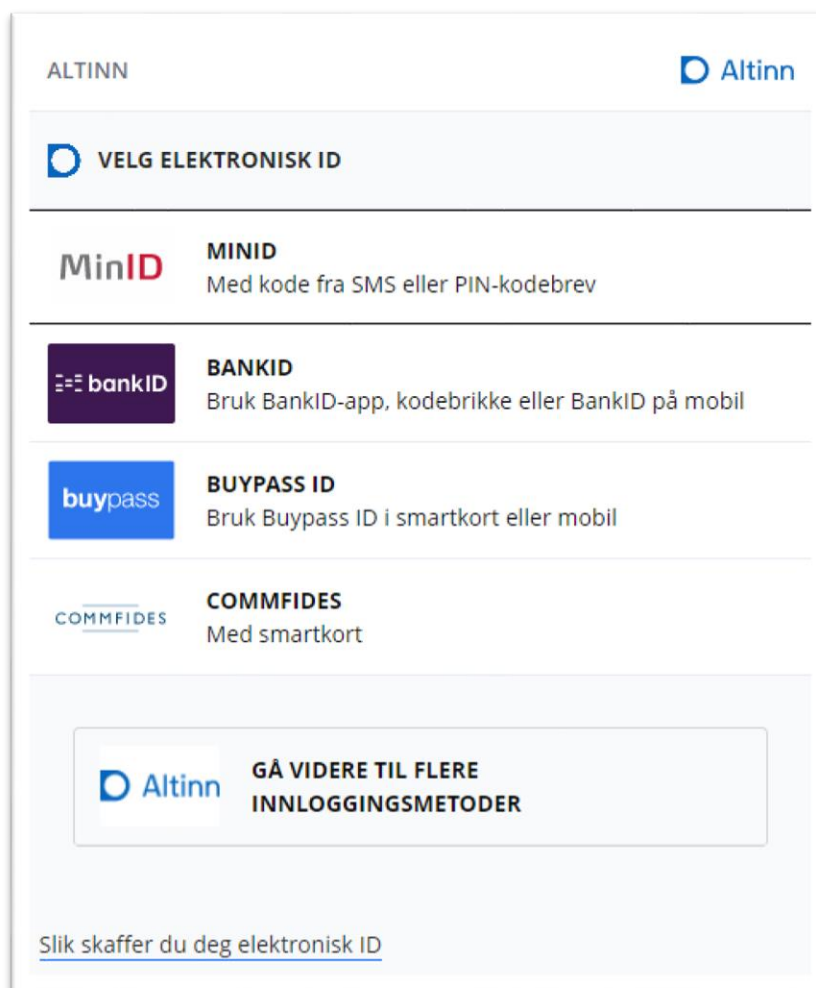
4.1 Wireframes

Link til interaktiv wireframe.

<https://www.figma.com/proto/WweRMqZ8NBnE0NIpIj69DB/Interactive-Demo?node-id=10%3A2&scaling=min-zoom&page-id=0%3A1&starting-point-node-id=10%3A2>

Se MinID-innstillinger:

Dette er skjermbildet en bruker vil møte når den skal logge inn på for eksempel Altinn eller nav. For denne oppgaven tas det utgangspunkt i at man bruker MinID som innloggingsmetode. Bruker velger MinID som innloggingsmetode.



Figur 3 Velg elektronisk ID

Da vil bruker møte dette skjermbildet, i dette tilfellet skal bruker se MinID-innstillinger og trykker derfor på MinID logo oppe til høyre på skjermbildet.

ALTINN

LOGG INN MED MINID

MinID

FØDSELSNUMMER

PASSORD

[Glemt passord](#)

AVBRYT

NESTE

[Bestill ny MinID](#)

Figur 4 Innlogging


Bruker får da opp en rullegardinmeny hvor en har muligheten til å se MinID-innstillinger, bestille ny MinID dersom man ikke har MinID, eller glemt passord dersom bruker har glemt sitt. I dette tilfellet vil bruker trykke på MinID-innstillinger.


The image shows a web interface for logging in with MinID. At the top left, it says "ALTINN" and "LOGG INN MED MINID". Below this are input fields for "FØDSELSNUMMER" (blacked out) and "PASSORD" (masked with dots). There are buttons for "AVBRYT" and "NESTE". A dropdown menu is open on the right, showing options: "MinID", "MinID-innstillinger", "Bestill ny MinID", and "Glemt passord". At the bottom left, there is a link "Bestill ny MinID".


Figur 5 Rullegardinmeny for MinID-innstillinger


Brukeren vil da bli sendt til et nytt valg av innloggingsmetode, dette er fordi en bruker skal ha muligheten til å logge seg inn på MinID-innstillinger uavhengig av innloggingsmetode. I dette tilfellet vil bruker benytte MinID som innloggingsmetode og trykker på det.


DIGITALISERINGS DIREKTORATET

 **VELG ELEKTRONISK ID FOR MINID-INSTILLINGER**

 **MINID**
Med kode fra SMS eller PIN-kodebrev

 **BANKID**
Bruk BankID-app, kodebrikke eller BankID på mobil

 **BUYPASS ID**
Bruk Bypass ID i smartkort eller mobil

 **COMMFIDES**
Med smartkort

[Slik skaffer du deg elektronisk ID](#)

Figur 6 Velg elektronisk ID for MinID-innstillinger

Bruker vil da igjen møtes av et slikt innloggings bilde hvor bruker må skrive inn fødselsnummer og passord deretter trykke neste.

DIGITALISERINGS DIREKTORATET

LOGG INN MED MINID MinID

FØDSELSNUMMER

PASSORD

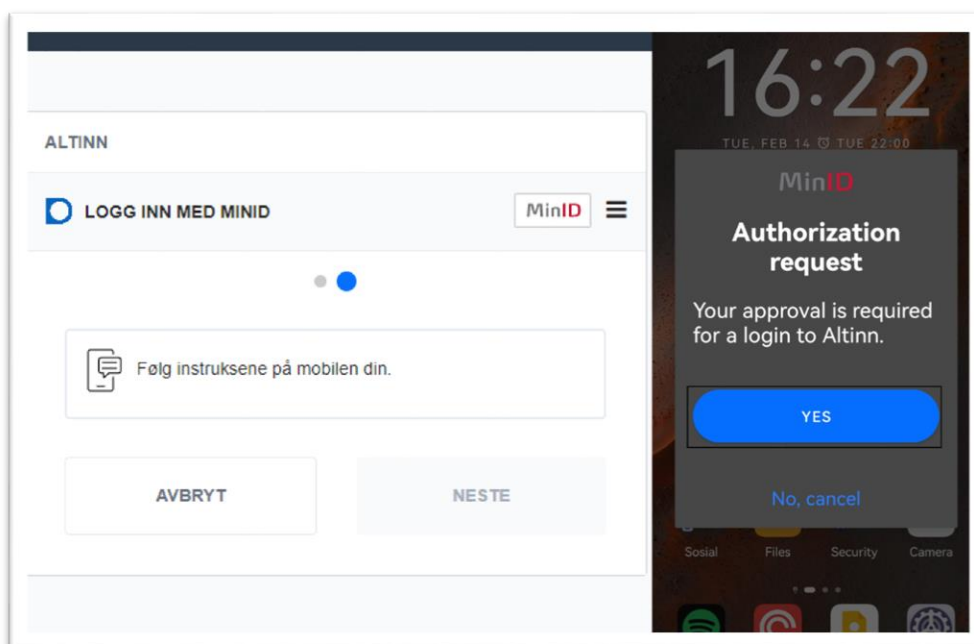
[Glemt passord](#)

AVBRYT NESTE

[Bestill ny MinID](#)

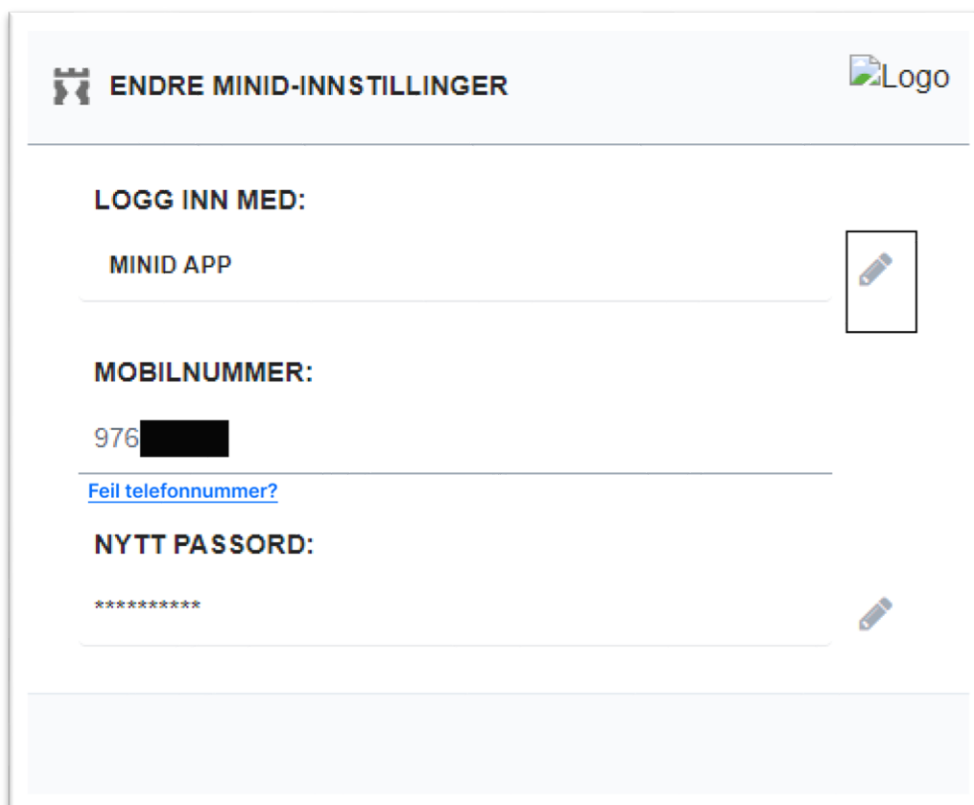
Figur 7 Innlogging for MinID-innstillinger

Dersom brukeren har valgt MinID-app som verifiseringsmetode er det dette skjermbildet som brukeren vil møte, hvor brukeren er nødt til å godkjenne innloggingen i sin MinID-app på brukeren sin smart-enhet. Dersom brukeren ikke har MinID-app som valgt innloggingsmetode vil det være ett litt annerledes skjermbilde for SMS-verifisering, med at brukeren vil få en SMS med en kode som må skrives inn for å verifiseres.



Figur 8 Avvent app godkjenning

Når brukeren er innlogget, vil dette skjermbilder vises. Brukeren vil da ha muligheten til å endre verifiseringsmetode eller passord. Hvis mobilnummer som er oppgitt på siden ikke stemmer overens med brukerens nummer kan bruker trykke på “Feil telefonnummer?” i blå tekst under mobilnummeret. Brukeren vil da få en popup med informasjon om hvordan brukeren kan få endret nummeret.



Figur 9 MinID-innstillinger

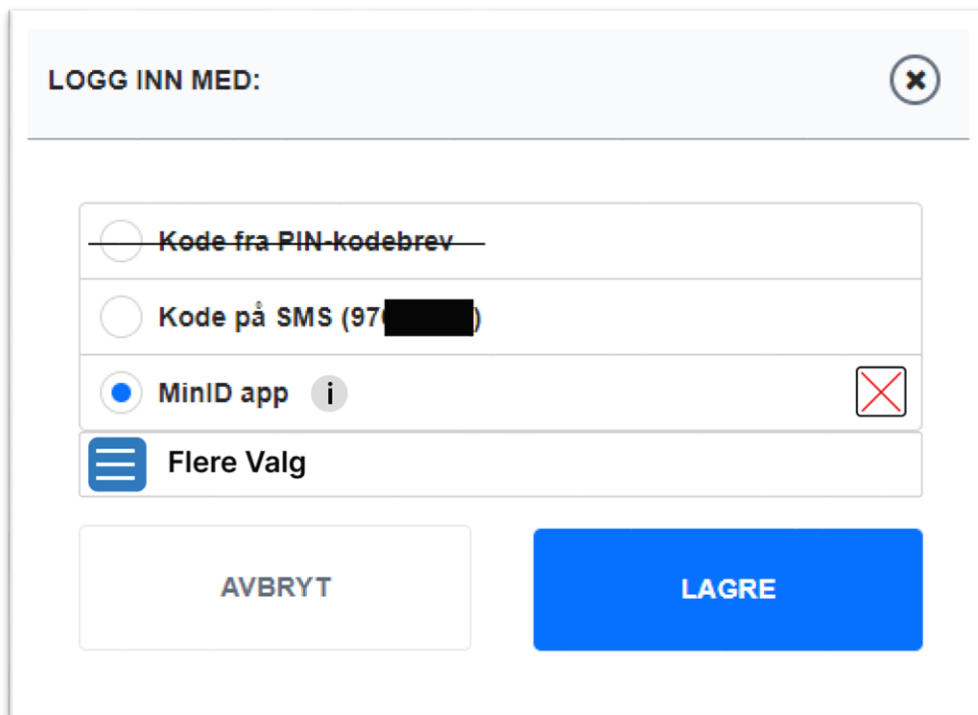
Endre MinID-innstillinger:

Dersom en bruker ønsker å endre innstillingene på MinID, vil bruker først følge de steg over i Se MinID-innstillinger og når en er kommet til Figur 9 trykke på blyant-tegnet oppe ved LOGG INN MED: for å endre innloggingsmetode, eller blyant-tegnet ved NYTT PASSORD: for endring av passord.

Initialere 2FA-TOTP:

Når en bruker skal for første gang initialere 2FA-TOTP må bruker følge stegene for å komme seg til å endre MinID-innstillinger og trykke på blyant-tegnet oppe ved LOGG INN MED: i Figur 9.

Brukeren vil da få opp et skjermbilde med MinID verifiseringsmetoder, der kan brukeren velge en annen metode til verifisering eller fjerne en app. Brukeren har også muligheten til å se hvilken modell og operativsystem det er på enheten som MinID-app er installert på ved å trykke/holde musepeker over infoboksen. Dersom brukeren ønsker å fjerne en applikasjon som verifiseringsmetode trykker brukeren på det røde krysset høyre i bildet. I dette scenarioet er brukeren ute etter å opprette en ny tredjeparts TOTP metode. Brukeren vil i dette tilfellet trykke på blå «Flere valg».



The screenshot shows a dialog box titled "LOGG INN MED:" with a close button (X) in the top right corner. Below the title bar, there are four rows of options, each with a radio button on the left and an information icon (i) on the right. The first row is "Kode fra PIN-kodebrev" with a radio button that has a horizontal line through it. The second row is "Kode på SMS (97 [redacted])" with an empty radio button. The third row is "MinID app" with a selected radio button (blue dot) and a red X icon in a box to its right. The fourth row is "Flere Valg" with a blue menu icon (three horizontal lines) to its left. At the bottom of the dialog, there are two buttons: "AVBRYT" (grey) on the left and "LAGRE" (blue) on the right.

Figur 10 Endre innloggingsmetode

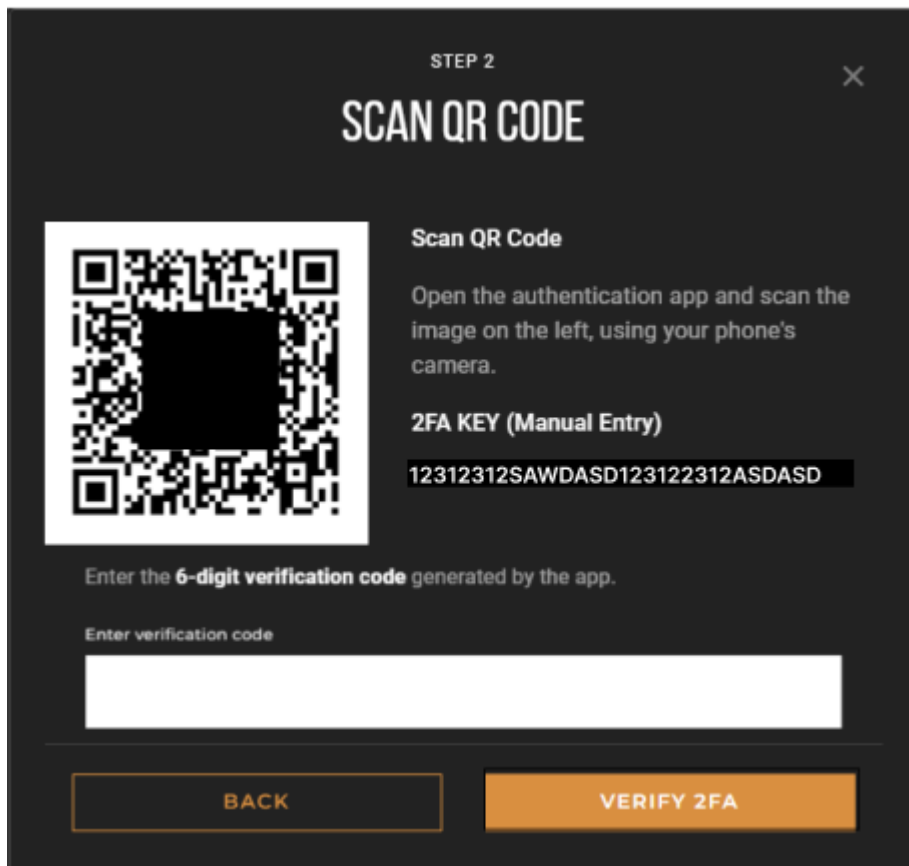
Brukeren vil da få opp denne rullegardinmenyen hvor bruker kan velge hvilke(n) den vil sette opp. I dette tilfellet vil brukeren sette opp tredjeparts autentikator og trykker derfor på dette.

Figur 11 Flere valg rullegardinmeny

Brukeren vil få se informasjon om hva bruker må gjøre før den kan ta i bruk tredjeparts 2FA-TOTP med lenker til de tre mest brukte applikasjonene. Når en bruker har installert en av disse vil bruker trykke neste.

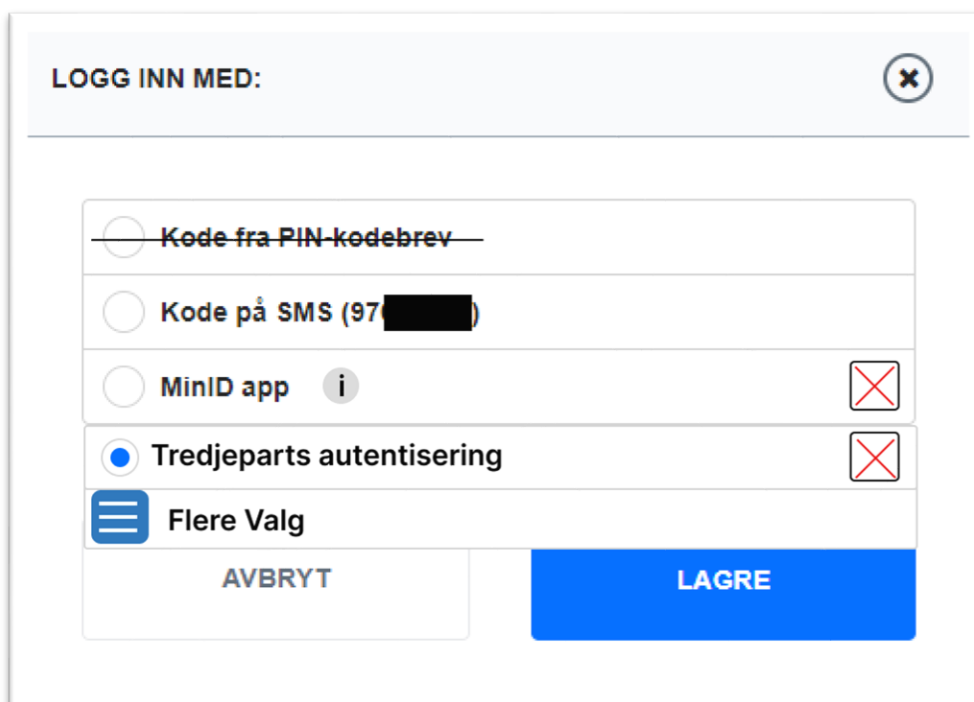
Figur 12 Installasjon og informasjon

Brukeren vil dermed få opp en QR kode og en 2FA nøkkel. Brukeren kan da gå inn i sin ønskede 2FA applikasjon og skanne QR kode eller manuelt skive inn 2FA nøkkel. På brukerens 2FA applikasjon vil det da vises en kode som endres hvert 30 sekund. Brukeren blir da bedt om å skrive inn verifikasjons kode som er generert i appen og hvis det stemmer overens med det som systemet krever vil det da når bruker trykker “VERIFY 2FA” bli verifisert at 2FA er satt opp riktig.



Figur 1313 Skann QR kode, fullfør steg på smart-enhet og innfylling av verifikasjons kode fra app

Bruker vil da bli sendt tilbake til valg av verifiseringsmetode hvor bruker vil se at valgt applikasjon er aktiv som valgt verifiseringsmetode, slik at neste gang en bruker logger inn med MinID vil dette bli brukt.

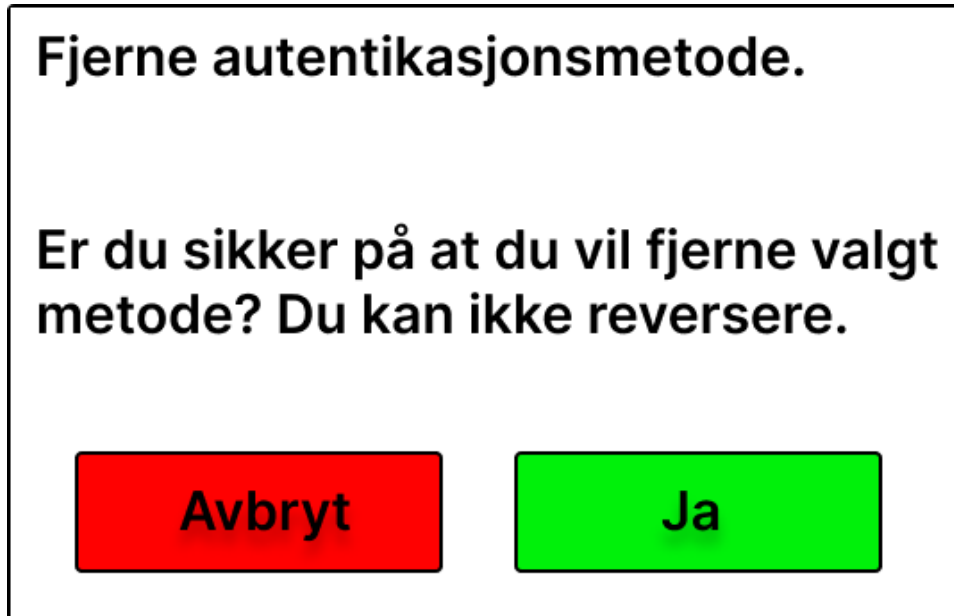


Figur 1414 Oppdatert valg av innloggingsmetode etter 2FA oppsett

Fjerne MinID-applikasjon

Dersom en bruker ønsker å fjerne MinID-app som mulig innloggingsmetode, må en bruker først logge inn og navigere til Se MinID-innstillinger, og trykke på blyant-tegnet oppe til høyre i Figur 9. Bruker vil dermed se skjermbildet vist i Figur 10, og kan trykke på kryss til høyre for MinID app.

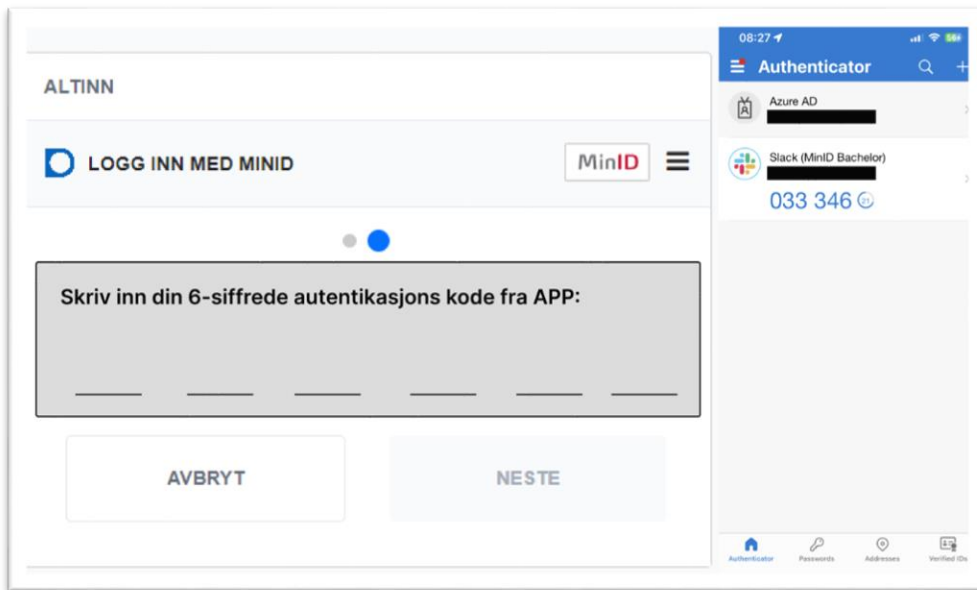
Brukeren vil da få en popup hvor brukeren må godkjenne fjerningen. Dersom brukeren trykker “Ja” vil metoden bli fjernet fra listen å dersom det er den aktive verifiseringsmetoden som fjernes vil det automatisk falle tilbake på SMS-verifikasjon.



Figur 1515 Fjerne innloggingsmetode popup godkjenning

Autentisering vha. 2FA-TOTP

Når en bruker har initialisert tredjeparts 2FA-TOTP og neste gang skal logge inn med MinID, vil brukeren bli møtt av skjermbildet i Figur 16, etter at den har trykket på MinID som innloggingsmetode i Figur 3. Brukeren må dermed skrive inn autentiseringskode generert av app, og hvis koden stemmer overens med kode generert av systemet vil bruker bli logget inn.



Figur 1616 Innlogging med 2FA