Høgskulen på Vestlandet

Fakultet for ingeniør- og naturvitskap

Institutt for datateknologi, elektroteknologi og realfag

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

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

Visjonsdokument

Versjon 2.1

Dokumentet er basert på Visjonsdokument 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

Dato	Versjon	Beskrivelse	Forfatter
29/Jan.	1.0	Første iterasjon av visjonsdokument	E.F, J.V.E, U.F
9/Feb.	1.1	Oppdatert problem og produktsammendrag. Oppdatert Alternativer til vårt produkt.	J.V.E, U.F
14/Feb.	1.2	Brukermiljø- og produkt i brukermiljøskisser og oppdateringer	U.F
21/Feb.	1.3	Ikke-funksjonelle egenskaper, brukermiljø oppdatert	U.F, E.F
22/Feb.	2.0	Oppdatert innledning, problemsammendrag, interessenter, brukernes behov, funksjonelle og ikke-funksjonelle egenskaper/krav, produktets rolle i brukermiljø, referanser og bilde/tabelltekst	E.F, J.V.E, U.F
7/Mar.	2.1	Oppdatert problemsammendrag, interessenter, brukermiljø, brukers behov, alternative produkter, ikke-/ funksjonelle egenskaper.	E.F

INNHOLDSFORTEGNELSE

1 INNLEDNING

Hensikten med dette visjonsdokumentet er å legge grunnarbeidet for prosjektet gjennom å reflektere over problemstillingen som er gitt og danne oversikt for behov rundt løsningen. Dette dokumentet skal bidra til å gi en felles forståelse for begge parter, oppdragsgiver og bachelorgruppen. Dokumentet skal skape en indikasjon over problemdefinisjon og produkt, samt mulige interessenter og brukere. Det vil også bli diskutert produktets rolle i brukermiljøet, hvilke forutsetninger og avhengigheter produktet trenger, samt hvilke funksjonelle og ikke funksjonelle egenskaper og andre krav som trengs for at produktet skal oppnå suksess.

2 SAMMENDRAG PROBLEM OG PRODUKT

2.1 Problemsammendrag

Tabell 1Problemsammendrag

Problem med	noe høy terskel for å ta i bruk MinID for sikker autentisering på sikkerhetsnivå 3
berører	Brukere av MinID
som resultatet av dette	Unnlater sluttbrukere å benytte seg av MinID til fordel for andre autentiseringsløsninger.
en vellykket løsning vil	Gjøre det enklere å ta i bruk MinID, med bruk av utbredt tredjeparts 2FA-TOTP autentikator.

2.2 Produktsammendrag

Tabell 2 Produktsammendrag

For	Brukere av MinID
som	Har behov for en enkel, effektiv og sikker måte å autentisere seg på
produktet navngitt	2FA ved bruk av TOTP i MinID
som	Tilbyr enkel, effektiv autentisering på sikkerhetsnivå 3
I motsetning til	Dagens løsninger basert på PIN (som fases ut), SMS og MinID App
Har vårt produkt	En enkel og effektiv autentisering, basert på 2FA og TOTP, ved bruk av tredjeparts autentikator, med stor utbredelse.

3 BESKRIVELSE AV INTERESSENTER OG BRUKERE

3.1 Oppsummering interessenter

Tabell 3 Interessenter

Navn	Utdypende beskrivelse	Rolle under utviklingen
Digitaliseringsdirektoratet (DigDir)	DigDir er prosjektets oppdragsgiver, som vil ta løsning og produkt videre med seg i bruk under egen utvikling.	DigDir har rolle som oppdragsgiver under utviklingen. Oppdragsgiver vil gi tilbakemeldinger under utviklingen, og bidra med ekspertise om nødvendig.
Offentlig etat i Norge (som tilbyr MinID autentisering til sine tjenester)	Som for eksempel NAV og Skatteetaten har nettsider med MinID innlogging og vil bli påvirket av eventuelle endringer i systemet.	Stiller krav til løsningen og produktet når det kommer til sikkerhet og universell utforming, slik som WCAG (W3C, 2005) og OWASP ASVS (OWASP, n.d.).
Prosjektgruppe	En gruppe bestående av 3 IT-studenter ved HVL.	Skal undersøke hvilke muligheter det finnes for tredjeparts autentifisering og utvikle et produkt som implementerer eksisterende og utbredt autentiseringsalternativ ved bruk av 2FA og TOTP i et sammenlignbart system.

3.2 Oppsummering brukere

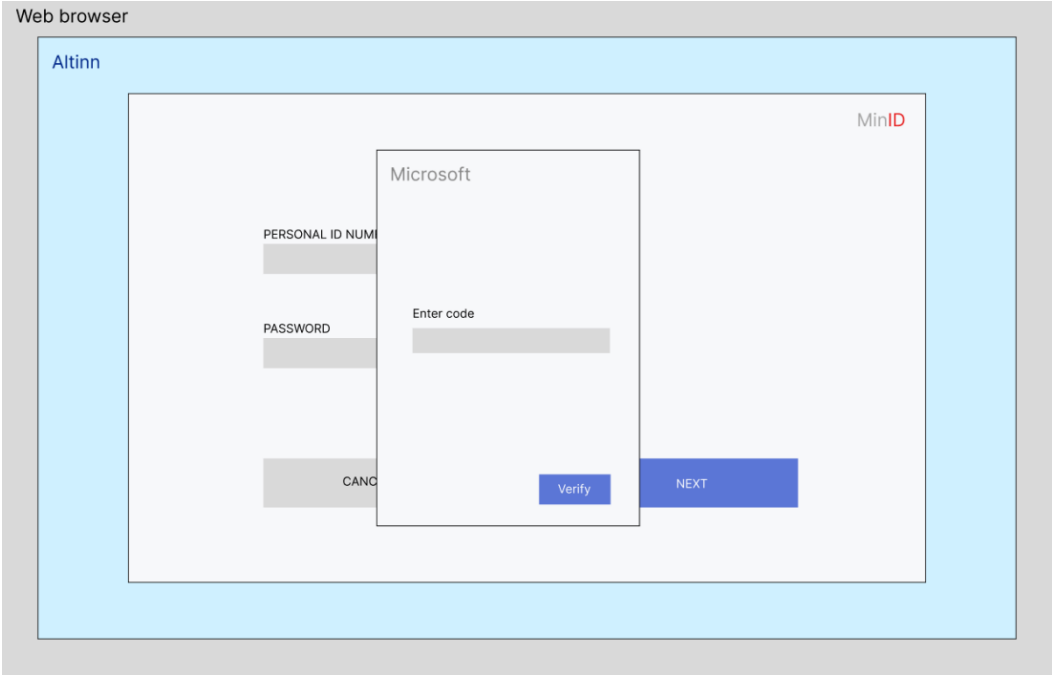
Tabell 4 Brukere

Navn	Utdypende beskrivelse	Rolle under utviklingen	Representert av
MinID brukere	Brukere som ønsker å ta i bruk MinID ved innlogging på For eksempel NAV/Skatteetaten/Altinn etc.	Brukere vil under testing kunne komme med tilbakemelding til produktets utviklere.	Utviklere og test-brukere

3.3 Brukermiljøet

Ved pålogging til en nettside under offentlig etat som f.eks. Altinn, vil ID-porten tilby MinID som en av flere alternative innloggingsløsninger. For innlogging via MinID vil det være nødvendig med en 2FA autentisering. Dette kan komme i form av kode på SMS, Digdirs egen MinID-app og tredjeparts-apper for TOTP (Time-Based One-Time Password)

Et eksempel på en tredjeparts app vil være Microsoft Authenticator som illustrert i Figur 1.



Figur 1 Skisse av brukermiljø

Tredjepartsautentiseringen består av å fylle inn den 6-siffrede koden som genereres på app innenfor det gitte tidsintervallet, brukeren vil ha et tidvindu på 30 sekunder på å fylle inn denne koden som vist i Figur 2.

Figur 2 TOTP på mobil

3.4 Sammendrag av brukernes behov

Tabell 5 Sammendrag av brukernes behov

Behov	Prioritet	Påvirker	Dagens løsning	Foreslått løsning
Behov for sikker og pålitelig innlogging med bruk av 2FA - TOTP authentisering	1	Bruker	Autentisering ved PIN-kode, kode sendt på SMS eller to-faktor autentisering med MinID appen.	Vil i tillegg til eksisterende løsning, tilby mulighet for å authentisere ved bruk av tredjepart TOTP authentikatorer.
Behov for å kunne registrere og avregistrere autentiseringsmetoder	1	Bruker	Både registrering og avregistrering av autentiseringsmetode er kun relevant for MinID-appen i dagens løsning, hvor begge må utføres gjennom appen.	Etter å ha logget inn for å se sine MinID-Innstillinger vil bruker kunne trykke på "Flere valg" og velge blant de tilgjengelige tredjeparts autentiseringsmetodene. Bruker vil deretter gjennomføre nødvendig førstegangsverifisering ved å skanne en QR-kode og fylle inn gitt kode i nettleseren sin. Bruker vil også kunne avregistrere seg fra autentiseringsmetodene ved å trykke på et rødt kryss til høyre for den uønskede metoden.
Behov for å kunne se og endre brukerinnstillinger	2	Bruker	Gir per nå mulighet for å endre innloggingsmetode, mobilnummer og passord.	Endringer må skje på valg av innloggingsmetoder hvor PIN-kodebrev ikke lenger vil være gjeldende. Det skal i tillegg ikke være mulig å endre mobilnummer fra disse innstillingene da denne informasjonen hentes fra KRR Digitaliseringsdirektoratet (n.d). Men gjeldene mobilnummer kan fremdeles vises på innstillingene. Bruker vil fremdeles kunne endre passord og valgt 2FA-metode herfra, men må følge en lenke for å endre registrert telefonnummer.

3.5 Alternativer til vårt produkt

Frem til januar 2023 er det tre alternativer for å autentisere brukere i MinID: SMS til mobil, en egen MinID autentiserings-app som er utviklet spesielt for å godkjenne MinID innlogging, og PIN-kode fra brev. PIN-koder fra brev ble fjernet som et gyldig valg da det var en svakere sikkerhetsmekanisme og ikke lengre oppfylte de krav til sikkerhet som MinID må oppfylle.

Tre andre alternativer til MinID tilbys også av ID-porten, disse er BankID, BuyPass ID og Commfides.

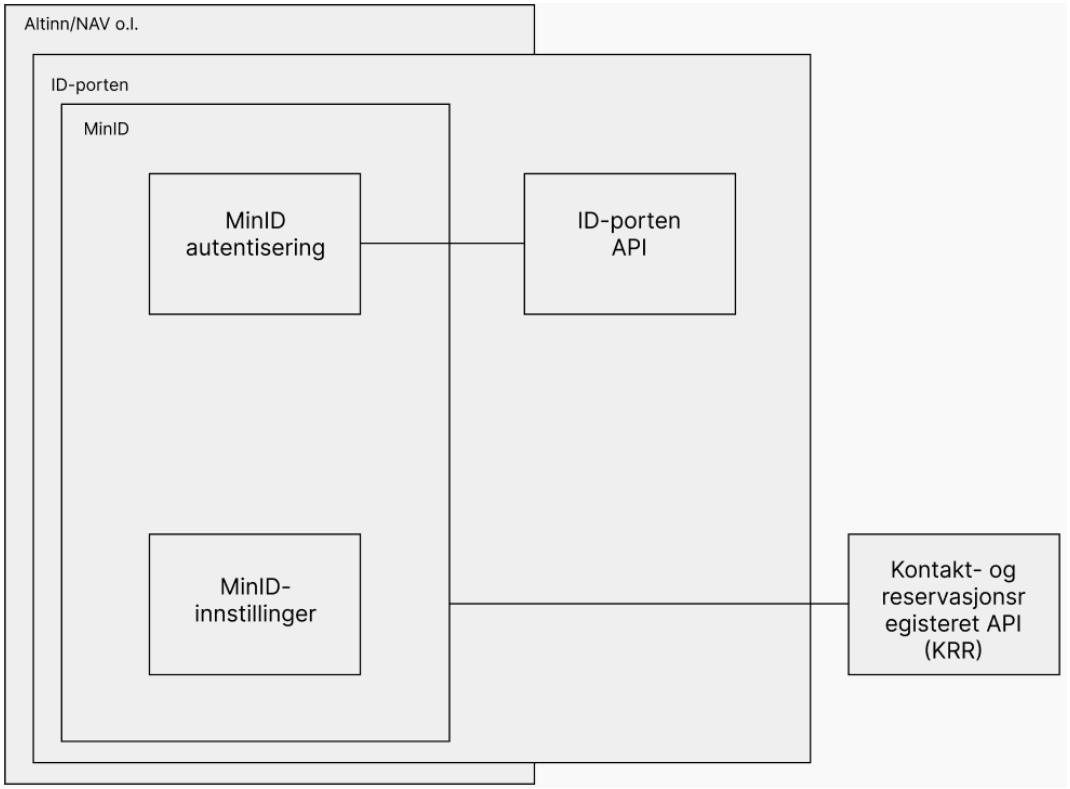
Alle tre tilbyr autentiseringsmetoder med det høyeste sikkerhetsnivået (nivå 4) som gjør de nødvendige der MinID per nå ikke strekker til. Nettsider som: Statens Vegvesen, Helsenorge eller forsikringsselskap som Gjensidige, vil da kreve autentisering vha. En av disse tre.

BankID er den mest brukte løsningen og omfatter over 95% av innlogginger på ID-porten, den tilbyr autentifisering via pushnotifikasjoner på app og engangskoder på kodebrikke. (personlig kommunikasjon 21 februar 2023)

BuyPass tilbyr smartcard som en tofaktor token, hvilket gjør det mulig å gjennomføre autentisering på en datamaskin vha. En tilkoblet kortleser. Commfides tilbyr også en lignende løsning med Commfides USB-pinne og PIN-kode.

4 PRODUKTOVERSIKT

4.1 Produktets rolle i brukermiljøet



Figur 3 Skisse av MinID sin rolle i brukermiljøet

Produktet representerer MinID sin innloggingsprosess ved bruk av 2FA-TOTP. Brukeren vil bli sendt til ID-porten sine sider ved å trykke "logg inn" fra for eksempel skatteetaten sine nettsider. Brukeren vil dermed kunne nå innloggingsiden produktet representerer ved å velge MinID. Etter gjennomført autentisering blir bruker sendt tilbake til den opprinnelige nettsiden. Ved bruk av SMS 2FA og ved visning av MinID-Innstillinger hentes telefonnummer fra KRR.

4.2 Forutsetninger og avhengigheter

Tabell 6 Forutsetninger og avhengigheter

Stikkord	Beskrivelse
Språk og rammeverk	Produktet skal utvikles ved bruk av DigDir sine programmeringsspråk, plattformer og rammeverk, som Java 17 og Spring.
Multiplattform	Systemet skal kunne benyttes gjennom en nettleser, på all type enhet som PC, mobil og nettbrett.
API	Produktet skal benytte seg av eksiterende tjenester og API fra ID-porten og KRR.
Design	For utforming og design av brukerdialog skal DigDir sitt eksisterende design og stiler benyttes.
TOTP	Produktet skal samsvare med eksisterende tredjeparts autentikatorer for generering av TOTP.

5 PRODUKTETS FUNKSJONELLE EGENSKAPER

Produktet skal gjør det mulig å bruke tredjeparts 2FA-TOTP applikasjon for autentisering.

Som del av innstillinger for MinID, skal bruker kunne legge til og velge 2FA-TOTP autentisering.

Produktet skal tilby mulighet for å endre passord.

Produktet skal tilby mulighet for å registrere ny TOTP basert 2FA app som autentiseringsvalg.

6 IKKE-FUNKSJONELLE EGENSKAPER OG ANDRE KRAV

Tabell 7 Ikke-funksjonelle krav

Ikke-funksjonelle egenskaper og krav	Beskrivelse
Brukervennlighet	Brukervennlig i form av antall trykk som trengs fra sluttbruker skal lik som ved bruk av SMS 2FA og sammenlignbar tid brukt ved innlogging som ved bruk av MinID-appen.
Utbredelse	Integrerte tredjepart autentiserings-app(er) må være blant de mest brukte alternativene.
Teknologi	Produktet skal utvikles med Java 17 og Spring Boot.
Design	Produktets design og utseende skal være tilnærmet den eksisterende løsningen så langt det lar seg gjøre for å redusere hvor mye tilvenning en bruker skal måtte gjøre.
Universell utforming	Produktet skal utvikles i henhold til krav stilt av WCAG 2.1 (W3C, 2005)
Sikkerhet	Produktet skal utvikles i henhold til OWASP ASVS (OWASP, n.d.)

7 REFERANSER

Digitaliseringsdirektoratet (n.d). *The common contact register | eid.difi.no*. Tilgjengelig fra: https://eid.difi.no/en/common-contact-register (Hentet: 14. februar 2023).

OWASP (n.d). *OWASP Application Security Verification Standard*. Tilgjengelig fra: https://owasp.org/www-project-application-security-verification-standard/ (Hentet 23. januar 2023).

W3C (2005). *WCAG 2 Overview | Web Accessibility Initiative (WAI) | W3C.* Tilgjengelig fra: https://www.w3.org/WAI/standards-guidelines/wcag/ (Hentet: 24. januar 2023).