Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Raphael Storm Larsen
Sara Stentvedt Luggenes
Jørgen Teigen

Autentiseringsmetoder og brukergrensesnitt

- en kartlegging av brukervennlige alternativer for mennesker med lettere psykisk utviklingshemming

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Erik Hjelmås
Medveileder: Ernst Gunnar Gran
Mai 2024

NTNU
Kunnskap for en bedre verden

Raphael Storm Larsen
Sara Stentvedt Luggenes
Jørgen Teigen

Autentiseringsmetoder og brukergrensesnitt

- en kartlegging av brukervennlige alternativer for mennesker med lettere psykisk utviklingshemming

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Erik Hjelmås
Medveileder: Ernst Gunnar Gran
Mai 2024

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU

Kunnskap for en bedre verden

Abstract

Title:	Authentication Methods and User Interfaces - Mapping User-Friendly Alternatives for Individuals with Mild Intellectual Disabilities
Date:	21.05.2024
Authors:	Raphael Storm Larsen Sara Stentvedt Luggenes Jørgen Teigen
Supervisors:	Erik Hjelmås Ernst Gunnar Gran
Employer:	WeissTech AS
Keywords:	Usability, authentication, web design, cognitive impairments
Pages:	149
Attachments:	21
Availability:	Open
Abstract:	WeissTech AS is a company providing digital journal solutions to the healthcare sector. One of their web applications, Omhu, has been used by (user-driven) personal assistants working with individuals needing assistance and adaptation in daily life. A portion of this user group consists of individuals with mild intellectual disabilities. There is now a desire for a new version of Omhu to be designed, with secure and user-friendly login options, with the aim of enabling patients to also use the application. This report utilizes relevant literature within usability, authentication, and web design to map and outline user-friendly and secure methods for designing authentication methods and websites intended for individuals with mild intellectual disabilities. By user-testing different alternatives for both authentication and user interfaces, this report has identified effective solutions that can be implemented in a patient module tailored to the target audience.

Sammendrag

Tittel:	Autentiseringsmetoder og brukergrensesnitt - en kartlegging av brukervennlige alternativer for mennesker med lettere psykisk utviklingshemming
Dato:	21.05.2024
Deltakere:	Raphael Storm Larsen Sara Stentvedt Luggenes Jørgen Teigen
Veiledere:	Erik Hjelmås Ernst Gunnar Gran
Oppdragsgiver:	WeissTech AS
Nøkkelord:	Brukervennlighet, autentisering, web-design, kognitive nedsettelser
Antall sider:	149
Antall vedlegg:	21
Tilgjengelighet:	Åpen
Sammendrag:	WeissTech AS leverer digitale journal-løsninger til helsesektoren, med hovedproduktet Omhu, en webapplikasjon benyttet av brukerstyrte personlige assistenter som arbeider med personer som trenger hjelp og tilrettelegging i hverdagen. En betydelig del av brukergruppen inkluderer personer med lettere psykisk utviklingshemming. Det er nå ønskelig å designe en ny versjon av Omhu, med sikre og brukervennlige innloggingsmuligheter, med mål om at også pasientene selv kan bruke applikasjonen. Denne rapporten benytter relevant faglitteratur innen brukervennlighet, autentisering og webdesign for å kartlegge og skissere sikre og brukervennlige designmetoder for autentisering og nettsider, spesielt tilpasset personer med lettere psykisk utviklingshemming. Gjennom brukertesting av ulike alternativer for både autentisering og brukergrensesnitt, presenterer rapporten velutviklede løsninger som kan implementeres i en pasientmodul tilrettelagt for målgruppen.

Forord

Takk til oppdragsgiver Philip Weisser og WeissTech for utmerket kommunikasjon og uvurderlig støtte med kontakter og relevant informasjon gjennom hele prosjektet.

Vi vil også rette en stor takk til våre veiledere, Erik Hjelmås og Ernst Gunnar Gran, for verdifulle tilbakemeldinger og en innsats som langt overgikk forventningene.

Takk til alle fagfolk og eksperter som, til tross for en hektisk hverdag, tok seg tid til å dele sin kunnskap og erfaring med oss.

Takk til alle deltakere i brukertestene for deres tålmodighet og innsats gjennom lange økter med oppgaver, intervjuer og litt for mange tekniske problemer.

Denne oppgaven ville ikke vært mulig å gjennomføre uten deres bidrag.

Innhold

Ordliste

backend Den delen av et websystem som håndterer serverlogikk, databaseinteraksjoner, og bakgrunnsprosesser. 4

brukerstyrt personlig assistanse Brukerstyrt personlig assistanse (BPA) er en ordning hvor personer med funksjonsnedsettelser får muligheten til selv å organisere og styre sin egen assistanse. Dette innebærer at brukeren kan ansette assistenter for å hjelpe med daglige aktiviteter, noe som gir større frihet og selvstendighet. Assistentene kan bistå med alt fra personlig pleie til praktiske gjøremål i hjemmet, basert på brukerens behov og ønsker. 1, 137

cookie En cookie, også kjent som en informasjonskapsel, er en liten mengde data nettsider kan sende og lagre hos klienten for oppbevaring av informasjon. Cookies brukes ofte for å lagre informasjon gjennomførte autentiseringser hos brukeren, slik at brukeren ikke trenger å autentiseres på nytt for hver eneste forespørsel mot serveren . 43, 47–50

frontend Den delen av et websystem som håndterer brukergrensesnitt og interaksjon med brukeren. 4

grensesnitt Et grensesnitt er delen av et produkt-design som kommer i kontakt med brukeren. I en bil kan en si at rattet er en form for grensesnitt, og for nettsider er alt du ser en del av grensesnittet. Dette innebærer knapper, tekst, input-felt og andre visuelle elementer brukeren kan interagere med.. 19

legitimasjon En legitimasjon er *noe* som beviser brukerens identitet i en autentiseringsprosess. 46

mobile-first approach Mobil-først tilnærmingen, eller "mobile-first approach" på engelsk, er en tilnærming innen webdesign der design og utvikling starter med den mobile versjonen av et nettsted eller en applikasjon, før man utvider det til å inkludere større skjermstørrelser som nettbrett og datamaskiner.

Akronymer

2FA 2-faktor autentisering. 135, 139

BPA brukerstyrt personlig assistanse. 1, 142

CI/CD continuous integration and continuous delivery/deployment. 51

FAR false acceptance rate. 97, 102

FIDO fast identity online. 11

IKT informasjons- og kommunikasjonsteknologi. 17

JSON javascript object notation. 52, 69

MitM man in the middle. 119

MVA merverdiavgift. 122

MVP minimum viable product. 3

PAI presentation attack instrument. 102

SaaS software as a service. 116

SDLC software development life cycle. 55

SSB statistisk sentralbyrå. 120

TOTP time-based one-time password. 22

WCAG web content accessibility guidelines. 16, 55

Kapittel 1

Introduksjon

1.1 Bakgrunn

WeissTech AS er et norsk, innovativt teknologiselskap som fokuserer på å levere sikre og brukervennlige verktøy til helse- og omsorgssektoren. Selskapet tilbyr Omhu, et digitalt fag- og journalsystem, som både forenkler arbeidsdagen for ansatte i helsesektoren og gjør det lettere for brukerne å benytte seg av relevante helse- og omsorgstjenester. Omhu er en nettapplikasjon som anvendes i ulike tjenester, inkludert barnevern, miljøterapeutiske tjenester, psykiske helsetjenester og ordninger knyttet til brukerstyrt personlig assistanse (BPA).

Tidligere har Omhu kun vært tilgjengelig for ansatte innen BPA-tjenester. Systemet benyttes til å koordinere tjenestetilbudet, enten ved at brukeren selv, eller deres familie eller forsørger, administrerer det. De ansatte har tilgang til funksjoner som fremmer samarbeid på tvers av det profesjonelle nettverket rundt brukeren. Disse funksjonene inkluderer kalender, dagsplan, meldinger, mulighet for å sette opp individuelle planer, samt opplasting av bilder og videoer for opplæringsformål for fremtidige BPA'er.

WeissTech har nå som mål å utvide systemet slik at også brukere under BPA-tiltak får tilgang til Omhu, med de samme funksjonene som de ansatte allerede nyter godt av. Brukergruppen innen BPA-tjenester er svært variert, og denne utvidelsen retter seg spesielt mot personer med lettere psykisk utviklingshemming.

Mange av disse brukerne har ikke tilgang til BankID eller andre høynivå autentiseringsmetoder, og dermed heller ikke til offentlige digitale systemer. WeissTech ønsker å tilby et sikkert alternativ til BankID, slik at brukerne kan logge inn på Omhu's digitale systemer. Brukerne vil få tilgang til en pasientmodul hvor de blant

annet kan se en dagsplan over planlagte aktiviteter.

1.2 Oppgave

Oppgaven utdelt fra WeissTech er todelt. For hele oppgaveteksten, se vedlegg R. Oppgaven direkte sitert er:

Del 1 Kartlegge og skissere alternative innloggingsløsninger som i større grad tilgjengeliggjør Omhu for pasientene samtidig som vi ivaretar personvernet på en tilfredsstillende måte. Samt begrunne løsningsforslag på innlogging.

Del 2 Kartlegge og designe en MVP av en pasientmodul som er lett og venne seg til, intuitiv og enkel å benytte for pasienter med forskjellige forutsetninger for å nytte seg av teknologien vi tilbyr.

1.2.1 Problemområde

I Norge er det i dag registrert 25 000 personer med diagnosen psykisk utviklingshemming, og det er sannsynlig at mange flere burde hatt diagnosen uten å ha blitt diagnostisert [2]. Psykisk utviklingshemming innebærer kognitive utfordringer, som vansker med språk, sosial kompetanse og evnen til å håndtere daglige aktiviteter. Denne gruppen er ikke ensartet; det er betydelige individuelle forskjeller blant de diagnostiserte.

Mange av disse personene trenger hjelp i hverdagen og mottar støtte og tjenester fra det offentlige. Diagnosen psykisk utviklingshemming deles inn i fire grader: lett, moderat, alvorlig og dyp [2]. Funksjonsnivået og behovet for hjelp varierer derfor betydelig. Ifølge FN-konvensjonen for mennesker med nedsatt funksjonsevne, har personer med utviklingshemming både evne og rett til å bestemme over eget liv. Likevel finnes det flere årsaker til at de ikke får utøve selvbestemmelse i tråd med sin funksjonsevne. Blant annet:

> *"Personer med utviklingshemming får sjelden fortelle hva de trenger. Og kommunene som har ansvaret for tilbudene, mangler ofte et godt system for å holde styr på det de blir fortalt [3].*"

Dette sitatet fra en stortingsmelding fra Kultur- og likestillingsdepartementet påpeker at dagens grad av selvbestemmelse for utviklingshemmede ikke er tilfredsstillende.

Det er også betydelige variasjoner mellom kommunene i hvordan de implementerer tiltak og tjenester for mennesker med utviklingshemming. Mange av dagens journalløsninger i helse- og omsorgssektoren er rotete og vanskelige å bruke, noe som gjør det utfordrende å opprettholde en tilstrekkelig grad av autonomi blant utviklingshemmede. Se vedlegg L. Det er derfor mulig at de nåværende digitale løsningene ikke i tilstrekkelig grad støtter utviklingshemmede i å få den hjelpen og tjenestene de har rett på.

1.2.2 Oppgavedefinisjon

Del 1 av oppgaven er å skissere og kartlegge ulike autentiserings-alternativer for sluttbrukere av Omhu med psykisk utviklingshemming. Brukerene skal få tilgang til opplysninger tilsvarende nivå 3 i Altinn [4], og autentiserings-alternativene kartlagt må derfor tilsvare dette nivået eller bedre. Det er ønskelig at kartlagt autentiseringsmetode er så intuitiv og brukervennlig som mulig, spesielt mtp. målgruppens nedsatte kognitive evner.

Andre del av oppgaven er å designe en pasientmodul som er enkel og intuitiv å bruke, og som gir brukerene mulighet til å få oversikt over planlagte tjenester, og være deltakende i form av selvmonitorering og egenrapportering. Her skal det bli utviklet en MVP av et brukergrensesnitt, som minimum tilsvarer ønsket funksjonalitet av oppdragsgiver.

1.2.3 Avgrensing

Prosjektet vil primært levere en kartlegging og en skissering for både del 1 og del 2, og ikke et ferdig produkt. Ulike løsninger for autentisering vil bli kartlagt og undersøkt, og en prototype for et brukervennlig grensesnitt vil bli utviklet. I dette prosjektet har vi valgt å se bort i fra definisjonen av minimum viable product (MVP), da dette vil innebære å implementere funksjonell infrastruktur for at produktet skal kunne brukes. I stedet vil utrykket “prototype” brukes for å beskrive designet utviklet for pasientmodulen. En enkel demo av den mest lovende autentiseringsløsningen vil også bli utviklet. Gruppen vil derimot ikke utvikle ferdige løsninger, kun presentere forslag til oppdragsgiver, som kan videreutvikle ideene kartlagt og skissert i prosjektet.

Demoen for autentiseringsmetode vil ikke bli koblet til IDportalen eller Omhu. I

stedet vil det bli laget som en isolert løsning, med formål å demonstrere hvordan autentiseringen kommer til å fungere i praksis. Demoen vil bestå av en enkel innloggingsside der autentiseringsmetoden brukes for å logge inn på en bruker. Demoen trenger ikke å støtte avanserte funksjoner som endring av passord, registrering av bruker, integrasjon med Google-bruker eller IDportalen, og den trenger ikke å støtte registrering, lagring eller behandling av data.

Prototypen av pasientmodulen vil bli utviklet som en enkel nettside med fungerende frontend elementer, men uten infrastrukturen nødvendig for behandling av brukere, innlogging og annen generell bruk som krever kontakt med backend.

1.3 Rammer

- Gruppen skal kartlegge metoder for sikker autentisering som alternativ til IDportalen.
- Gruppen skal designe et nytt brukergrensesnitt for Omhus dashbord og arbeidsplan-fane.

Som det kan tolkes fra prosjekt-rammene, er oppdraget fra Weisstech et svært åpent prosjekt, der kravene for minste akseptable løsning er beskjedne. Det er derfor store muligheter for å utvide oppgaven i den retningen som gruppen selv ønsker. I kapittel 1.2.1 gjennomgås gruppens ønsker for hvordan prosjektet skal fullføres, og i kapittel 1.2.3 defineres interne avgrensninger satt av gruppen.

1.4 Prosjektmål

Resultatmål

1. Kartlegge og skissere flere alternative innloggingsløsninger.
2. Utvikle en demo som et konseptbevis for et potensielt autentiseringsalternativ til Omhu.
3. Utvikle en interaktiv demo for nytt brukergrensesnitt til Omhu.
4. Oppnå en målbar forbedring av brukervennligheten til Omhu's grafiske brukergrensesnitt for målgruppen.

Effektmål

1. Mer fornøyde sluttbrukere av Omhu.

2. Det blir enklere for sluttbrukerene å følge med på og gi tilbakemelding på deres behandling og aktiviteter.
3. En mer oversiktlig hverdag for sluttbrukere av Omhu.

Prosessmål

1. Holde en effektiv og god arbeidsflyt innad i gruppen gjennom hele prosjektet.
2. Ha en løpende og tett kommunikasjon med oppdragsgiver og veiledere.
3. Jobbe etter Scrum-metodikken.
4. Dokumentere og loggføre fremgangen av arbeid.

Læringsmål

1. Lære mer om brukervennlig design
2. Dokumentere og formidle resultatene av brukertester for å forbedre sluttproduktet
3. Gjøre oss kjent med prosessene rundt det å utvikle et produkt for en kunde
4. Bli kjent med alternative, sikre innloggingsmuligheter som ikke baserer seg på tilgang til BankID
5. Lære mer om standarder relatert til autentisering og brukersentrert design

Målene angitt ovenfor ble bestemt i forplanen. Prosessmålene og læringsmålene er ment som "interne" mål for gruppens egen arbeidsflyt og læring. Effektmålene ønskes oppnådd en stund etter prosjektets slutt, og resultatmålene er det som skal bli levert til oppdragsgiver.

1.5 Prosjektgruppa

Oppdragsgiveren er Philip Aspholt-Weisser, operativ leder hos WeissTech AS. Han er også gruppa's kontaktperson. Prosjektets to veiledere er Erik Hjelmås og Ernst Gunnar Gran, begge er førsteamanuensiser ved NTNU.

Studentgruppa består av tre personer; Sara Luggenes, Raphael Storm Larsen og Jørgen Teigen, alle går på studieprogrammet *Bachelor i digital infrastruktur og cybersikkerhet* på NTNU. Gjennom studieløpet har studentgruppa lært om og fått kompetanse på flere områder som er relevante til oppgaven. Blant annet programvareutvikling, cybersikkerhet og teamarbeid, skytjenester og webteknologier.

1.6 Arbeidsmetodikk

1.6.1 Rammeverk

Som nevnt i prosjektplanen, se vedlegg S, valgte vi å bruke Scrum som utgangspunkt for vårt rammeverk. Ettersom oppgaven ikke er en ren programmeringsoppgave, ble det bestemt at utviklingsmodeller som Extreme Programming og Open-source Software Development ikke var aktuelt. Vannfallsmetoden ble sett på som for lite smidig, ettersom en slik modell krever at alt i en del av prosjektet er ferdig, før man kan gå videre til neste del. Valget falt derfor på Scrum, ettersom dette er en smidig metodikk med fokus på jevnlige, korte møter, med sprintlengde på en uke. Scrum-master hadde ansvar for å skrive Scrum-rapport hver fredag, og denne rollen ble rullert på. En sprint startet hovedsakelig på mandager, og sluttet fredag kveld.

1.6.2 Kanban-tavle

Som Kanban-tavle ble issueboardet på GitHub benyttet. Under det ukentlige sprintmøtet på mandager ble oppgaver lagt inn i issueboardet og deretter fordelt til gruppemedlemmer. Issueboardet var delt opp i fire kategorier: *Todo*, *In Progress*, *Pending Review* og *Done*. Oppgavene ble først plassert i *Todo*, hvor gruppemedlemmene kontinuerlig gjennom sprinten kunne plukke oppgaver og flytte dem til *In Progress*. Når en oppgave var ferdig, ble den plassert i *Pending Review*. Dette fungerte som en kvalitetskontroll, hvor de to andre i gruppen gikk gjennom og dobbeltsjekket arbeidet før oppgaven til slutt ble flyttet til *Done*. Ved å bruke «labels» verifiserte vi at begge de to gruppemedlemmene hadde kvalitetssikret oppgaven før den ble flyttet til *Done*.

1.6.3 Dokumentasjon og kommunikasjon

Overleaf ble brukt for oppbevaring av alle slags tekstbaserte dokumenter. For logging av arbeidstimer ble det benyttet Excel, og møteinnkallelser ble publisert på Discord. For sikkerhetskopiering av dokumenter, ble hele Overleaf-repoet jevnlig lastet opp på GitHub.

1.7 Om rapporten

Rapporten er delt opp i 7 kapitler. I teori blir relevant fagstoff presentert. I metode blir teori angående metodikk brukt for å besvare oppgaven, presentert. I tillegg blir egne definisjoner til bruk for sammenligning av autentiseringsmetoder beskrevet i dette kapitlet. I utvikling blir utviklingsprosessen av de to demoene, beskrevet. I resultat blir resultatene fra både del 1 og del 2 av oppgaven gått gjennom. I diskusjon blir resultatene analysert og reflektert rundt, og til slutt konklusjon. Etter kildelisten, er alle vedlegg lagt inn.

Kapittel 2

Teori

I dette kapittelet blir relevant teori for oppgaven beskrevet. Dette innebærer relevant teori om autentisering, web-design, ulike standarder og lovverk, i tillegg til beskrivende tekst om brukervennlighet og universell utforming. Relevant teori om målgruppen blir også beskrevet.

2.1 Autentisering

For at brukerene skal kunne logge inn på pasientmodulen levert av Omhu, må de kunne bevise sin egen identitet på en sikker måte. I dette delkapittelet kommer teori om autentisering til å bli forklart.

2.1.1 Hva er autentisering?

«Autentisering er innen IT både prosessen med å bekrefte en påstått identitet, og prosessen med å bekrefte om informasjon er ekte og uendret.»[5]. I denne rapporten's kontekst brukes uttrykket primært for å bekrefte en påstått identitet. For å bekrefte en påstått identitet, bruker man i dag ofte et passord eller pin-kode. Autentiseringsmetoder blir vanligvis delt inn i tre kategorier:

- noe man *vet* - for eksempel et passord eller pin-kode
- noe man *har* - for eksempel en kodebrikke, autentiseringsapp på mobil, eller en sikkerhetsnøkkel
- noe man *er* - for eksempel fingeravtrykk, ansiktsgjenkjenning eller en hånd-

skrevet signatur

En *autentiseringsfaktor* er en konkret komponent brukt til autentisering, altså et passord, en kodebrikke eller et fingeravtrykk. En *autentiseringsmetode* refererer til metoden som blir brukt for å autentisere en person, og en autentiseringsmetode kan da altså bestå av en eller flere autentiseringsfaktorer.

Multi-faktor autentisering, ofte forkortet MFA, er å bruke flere ulike autentiseringsfaktorer til samme innlogging, for å redusere risikoen for uriktig autentisering. Det er da viktig å bruke autentiseringsfaktorer fra ulike kategorier som nevnt ovenfor.[5]. Den vanligeste formen for multi-faktor autentisering er to-faktor, der to faktorer fra to ulike kategorier blir brukt.

2.1.2 Eksempler på autentiseringsfaktorer

Den vanligeste formen for autentisering i dag er å logge inn med brukernavn og passord. Mange er i tillegg kjent med autentisering på mobil ved hjelp av biometri. Biometriske kjennetegn er kroppslige kjennetegn som er unike for hver enkelt person, og samtidig permanente over tid [6]. De vanligste formene for biometri er fingeravtrykk og ansiktsform, og det er disse biometriske faktorene som ofte blir brukt til mobilautentisering. De fleste moderne mobiler i dag har støtte for autentisering med fingeravtrykk eller ansiktsgjenkjenning. Biometri går under kategorien *noe man er*.

Blant autentiseringsfaktorer som er *noe man har*, er mange kjent med kodebrikke og autentiseringsapplikasjon. Det finnes mange flere faktorer i denne kategorien, blant annet *sikkerhetsnøkler*. Dette er en fysisk brikke som kan kobles til mobilen eller en pc, og brukes til autentisering på f. eks. en spesifikk konto eller et nettsted.

Om ansiktsgjenkjenning som autentisering

Et biometrisk system opererer enten i en verifiserings-modus (autentisering) eller i en gjenkjennelses-modus (identifisering)[7]. Et biometrisk system basert på gjenkjenning, tar et gitt ansiktsbilde som input, og sammenligner dette med alle bildene i en database, for så å finne ut om bildet er i databasen eller ikke. Denne teknologien blir gjerne brukt til fysisk tilgangsstyring, der kun verifiserte personer har tilgang til f. eks. et kontor-lokale. Dette skiller seg fra et biometrisk system i autentiserings-modus, der systemet tar et ansiktsbilde som input, og sammenligner dette med den gitte ansikts-malen, en *template*.

Direkte oversatt er altså ansiktsgjenkjenning ikke det samme som ansiktsautentisering, men i rapportens kontekst vil disse to begrepene bli brukt om hverandre, pga. at ansiktsgjenkjenning er et mer utbredt ord på norsk, i forhold til ansiktsautentisering. Uansett hvilket ord som er brukt i rapporten, betyr det altså ansiktsautentisering.

2.1.3 Krav til sikkerhetsnivå

I EU/EØS er det lovpålagt at bedrifter og offentlige instanser, gjennom en risikoanalyse, skal bestemme hvilket sikkerhetsnivå de digitale løsningene knyttet til autentisering skal ha. De norske tilpasningene av dette lovverket har tre sikkerhetsgrader; "lavt", "betydelig" og "høyt" [8, 9]. Blant løsningene som er på nivå "høyt", er Commfides, Buypass og BankID.

Den aktuelle brukergruppa av Omhu, skal ikke ha tilgang til helseopplysninger eller andre sensitive opplysninger i web-applikasjonen. Informasjon i applikasjonen skal likevel ha større grad av konfidensialitet enn det løsninger i kategori "lavt" kan tilfredstille, og skal være på sikkerhetsnivå rett under høyeste nivå. Derfor skal autentiserings-løsningen for målgruppa være på sikkerhetsnivå "betydelig". Dette er også blitt bekreftet av oppdragsgiver, se vedlegg P. IDporten's sikkerhetskategorisering er en annen vanlig metode for gradering av autentiserings-sikkerhet, og er mye brukt i Norge. Denne skalaen går fra kategori null til fire [4]:

0. Innlogging med selvlaget brukernavn og passord
1. Innlogging med brukernavn og passord med fødselsnummer
2. Innlogging med Altinns 2FA via SMS
3. Innlogging med MinID eller tilsvarende sikkerhet
4. Innlogging med BankID, Buypass eller Commfides

Kategorien "betydelig" tilsvarer "nivå 3" i IDportens nivå-kategorisering[10]. At et sikkerhetsnivå har kategorien "betydelig", betyr at det er krav til to autentiseringsfaktorer, og at utlevering av autentiseringsfaktorer, f. eks. passord, kan basere seg på kontaktinformasjon i Folkeregisteret [8]. Se tabell 2.1 for mer informasjon. Tabellen er hentet fra digitaliseringsdirektoratet [8].

Norske nivå	Antall autentiseringsfaktorer	Utleveringskrav
Lavt	En autentiseringsfaktor	Som for betydelig eller høyt
Betydelig	To autentiseringsfaktorer	Utlevering kan baseres på kontaktinformasjon i Folkeregisteret/ Kontaktregisteret
Høyt	To autentiseringsfaktorer	Førstegangs utlevering baseres på at fysiske egenskaper observeres og sammenlignes med f.eks. et autoritativt dokument (f.eks. ved personlig fremmøte eller maskinelt)

Tabell 2.1: Sikkerhetsnivå - autentisering

2.1.4 Standarder og lovverk

Ulike standarder og lover for autentisering, både nasjonalt og internasjonalt, gjør det nødvendig å sette seg inn i både lovpålagte krav og retningslinjer knyttet til autentisering. I dette underkapitlet blir lover og standarder som er relevant og nyttiggjort i prosjektet, beskrevet.

FIDO

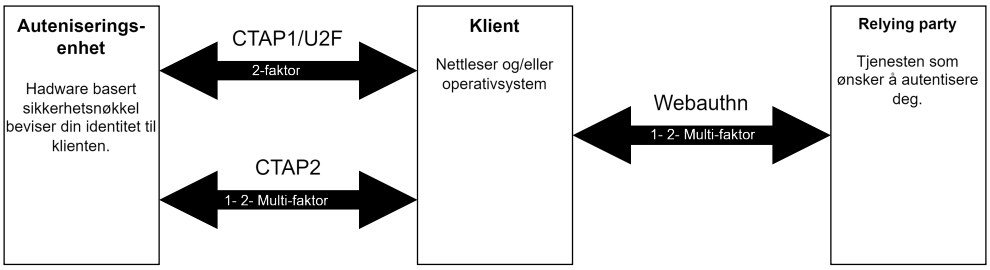
Fast identity online er en autentiseringstandard utviklet av FIDO Alliance [11], og har som hovedmål å styrke sikkerheten rundt pålogging og bekrefte identiteter på nett. FIDO er utviklet for å være et sikrere alternativ til passord som autentiseringfaktor. Standardene utviklet av FIDO Alliance, bruker standard kryptografiteknikker for å lage et godt autentiseringalternativ til passord. Den store fordelen ved å bruke FIDO som autentiseringstandard fremfor tradisjonelle passord, er at autentiseringsfaktoren man bruker aldri forlater enheten[12]. Autentiseringsfaktoren kan være biometri, en pin-kode eller en sikkerhetsnøkkel. Den tradisjonelle påloggingen består vanligvis av brukernavn og passord, der passordet er lagret i en ekstern database. Dette gjør passordet sårbart mot cyberkriminelle, ettersom en database kan bli hacket, og kriminelle kan få tilgang til passordene som er lagret der.

Webauthn API/FIDO2

Webauthn API er en standard utviklet av FIDO Alliance og W3C, støttet av flere store aktører innen IT verden, inkludert Google, Mozilla, Microsoft og Yubico [13]. Målet med webauthn er å etablere en standardisert metode for å gjennomføre offentlig-nøkkel-autentisering direkte i nettleseren. Dette eliminerer behovet for passordbasert autentisering. Webauthn er en del av FIDO2 arkitekturen, og er den spesifikke standarden som behandler kommunikasjon mellom servere og klienter i en autentiserings-kontekst.

Andre protokoller under FIDO2, som CTAP2, lar nettleseren kommunisere med fysiske sikkerhetsnøkler eller lokale autentiseringsmetoder innebygd i brukerens enhet. I sin helhet utgjør FIDO2 en mulighet for utviklere å designe web-applikasjoner som er i stand til å kommunisere med autentiserings-metoder som tidligere ikke var mulig å nå fra nettleseren. Dette kan være biometriske autentiseringsmetoder innebygd i brukerens mobil eller pc, som fingeravtrykk eller ansiktsgjenkjenning, eller det kan være en sikkerhetsnøkkel som er koblet til bruker-enheten [14].

Webauthn gjør det dermed mulig å flytte selve autentiseringen fra nettsiden over til eksterne enheter, eller selve plattformen. Da er det ikke nettsidens servere som lagrer brukerens påloggingsinformasjon, men informasjonen blir lagret i en brukerkontrollert enhet, som kan være brukerens mobil, pc eller sikkerhetsnøkkel. Webauthn og FIDO2 blir nærmere forklart i 4.2. Gjennom denne rapporten vil "platoform-autentisering" referere til autentiseringsmetoder innebygd i brukerens enhet. Dette er som regel fingeravtrykk eller ansiktsgjenkjenning, men kan også være pin-kode om enheten ikke har noen annen konfigurert autentisering.



Figur 2.1: Komponentene av FIDO2. Inspirert av figur fra Yubico[14]

.

Android klassifikasjon av biometrisk sikkerhet

Sikkerheten for fingeravtrykk kan variere utifra hvilken teknologi som brukes for å gjøre autentiseringen. Spesielt gjelder dette Android, som utnyttes i svært mange

modeller av smarttelefoner fra mange ulike leverandører. Kvaliteten her på autentisering vil variere[15]. Derfor bruker Android et felles klassifikasjons-system for å rangere styrken på biometrisk autentisering. Denne skalaen går fra klasse 1 til klasse 3, der klasse 1 tidligere var omtalt som "convenience", klasse 2 var "weak", og klasse 3 var "strong" autentisering[16]. Disse navngivningene har siden blitt avskaffet, men klassesystemet forblir[16]. Systemet fungerer som en standard for å måle sikkerheten med biometriske-sensorer, og må følges av leverandører av smarttelefoner, om de ønsker å la brukerene benytte seg av sensoren de setter i mobilen. Verdiene oppgitt i denne modellen kan dermed tolkes som en minimums verdi i henhold til å vurdere sikkerheten til biometriske autentiseringsmetoder for de fleste Android-enheter.

2.2 Eksisterende autentiseringsløsninger i Omhu

Omhu bruker IDporten som innloggingsløsning, og har implementert BankID, Buypass og Commfides som autentiseringsløsninger. Alle løsningene er på sikkerhetsnivå 4, og kan dermed gi tilgang til sensitive personopplysninger, som helseopplysninger. Ettersom Omhu ikke har planer om å gi tilgang til slike opplysninger i den aktuelle målgruppens brukerkontoer, behøver ikek autentiseringsløsningene diskutert i denne rapporten å oppfylle sikkerhetsnivå 4.

Årsaken til at disse løsningene ikke kan brukes med målgruppen omhandlet i denne studien, er at disse autentiserings-portalene vil gi brukerene tilgang til flere offentlige og private tjenester som Helsenorge og Lånekassen samt diverse nettbanker med BankID. Da det ikke er ønskelig at målgruppa skal ha full tilgang til enkelte tjenester som nettbank, samt andre tjenester der brukerene har fri tilgang til å styre sin egen økonomi, er BankID som autentiseringsløsning uaktuelt for denne gruppa.

BankID

Omhu har allerede BankID implemenert, og brukerene kan logge inn både ved hjelp av kodebrikke, BankID-applikasjon eller BankID på mobil. BankID blir utsendt av banken, men kan brukes til å logge inn på en rekke offentlige tjenester.

Buypass

Buypass kan brukes med smartkort, mobil eller nøkkel, alle alternativene er allerede implementert i Omhu. Buypass med smartkort krever at brukeren har en kortleser tilgjengelig, og er dermed et upraktisk alternativ for målgruppa.

Commfides

Commfides med smartkort er en allerede implementert løsning i Omhu. Commfides eID leveres som USB-pinne eller smartkort, men disse to alternativene har ulike bruksområder.

USB-pinne blir hovedsakelig levert til privatpersoner som skal bruke eID til å logge på offentlige tjenester som Helsenorge [17]. Smartkort blir hovedsakelig levert til ansatte i kundebedrifter hvor de ansatte bruker smartkortet i arbeidssammenheng, f. eks. digitale systemer kun ment for enkelte ansatte. Den ansatte kan også bruke sin ansatt eID til å logge på offentlige tjenester som privatperson.

2.3 Brukervennlighet

For å finne en autentiseringsmetode som er enklest mulig å bruke for målgruppa, og å finne et design på pasientmodulen som er intuitiv og enkel å benytte i størst mulig grad, er det nødvendig å måle både brukervennligheten til ulike produkt og grensesnitt. Gjennom brukertesting kan det bli hentet både kvantitativ og kvalitativ informasjon om autentiseringsmetoder og grensesnitt. Først må man definere hva brukervennlighet *er*. Ifølge ISO 9241-11 blir brukervennlighet definert slik:

> *Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.*

Flere lærebøker nevner også flere egenskaper ved brukervennlighet. Et system må være lett å lære, systemet bør være effektivt, det må være enkelt å huske over tid hvordan systemet brukes, systemet bør minimere muligheten for feil og være tolerant for feil, og systemet må være behagelig å bruke [18]. Det er mange norske og internasjonale lover og retningslinjer for brukervennlighet. Mer om det kan lesest i kapittel 2.3.2

Brukervennlighet må ikke forveksles med det engelske uttrykket "user experience", altså brukeropplevelsen.

Ifølge Tullis [19], har de fleste profesjonelle innenfor feltet sin egen beskrivelse av hva brukeropplevelse er. Tullis selv mener at brukeropplevelsen består av disse tre komponentene:

1. En bruker er involvert
2. Brukeren interagerer med et produkt, system, eller hva som helst med et grensesnitt
3. Brukerens opplevelse av interaksjonen er av interesse, og er både observerbart og målbart

Tullis påpeker at det er en forskjell mellom termene *brukervennlighet (eng. usability)* og *brukeropplevelsen (eng. user experience)*. Brukervennligheten refererer til hvor bra brukeren klarer å bruke et produkt for å fullføre en oppgave suksessfult, mens brukeropplevelsen handler mer om å se på individets totale interaksjonen med gjenstanden, ved å observere tankene, følelsene og opplevelsene knyttet til å bruke denne gjenstanden/grensesnittet.

2.3.1 Hvordan kvantifisere brukervennligheten?

For at det skal være mulig å sammenligne ulike produkter fra et brukervennlighetsperspektiv, er det nødvendig å finne en måte å kvantifisere brukervennligheten på. Å kvantifisere brukervennlighet, krever at man har noe å måle. Man kan bruke begrepene fullføringsrate, antall feil og tidsbruk som måleindikatorer i et brukervennlighetsperspektiv. Når ønskede måleindikatorer er identifisert, kan man telle opp og bruke disse til å sammenligne ulike produkt eller grensesnitt med hverandre. Dette er en metode som kan brukes når kvalitativ brukertesting ikke gir tilstrekkelige svar for å kunne svare på hvilke produkt som er mest brukervennlig, f. eks. ved å sammenligne to ulike autentiseringsmetoder.

2.3.2 Standarder og lovverk

For å best utvikle en prototype av en pasientmodul, er det nødvendig å sette seg inn i ulike lover og krav til web-design og tilgjengelighet på nett. Ulike retningslinjer og lover er beskrevet videre i dette kapitlet.

2.3.3 WCAG

Web Content Accessibility Guidelines er tekniske retningslinjer som skal hjelpe utviklere og designere, med å jobbe mot at internett skal være tilgjengelig for alle, uavhengig av funksjon og bakgrunn. Retningslinjene er utviklet av World Wide Web Consortium (W3C), sammen med mange forskjellige og internasjonale organisasjoner, bedrifter og myndigheter. WCAG er ikke lovpålagt internasjonalt, men fungerer som et sett med globale standarder som fokuserer på at nettsider, apper, elektroniske dokumenter og andre digitale verdier skal være tilgjengelige for mennesker med mange forskjellige funksjonshemninger, både fysisk og psykisk. WCAG har mange sukesskriterier, som hjelper web-designere og utviklere å fjerne og forhindre "barrierer", som mennesker med funksjonsnedsettelser opplever på internett og digitale tjenester [20].

WCAG har utviklet seg mye siden WCAG 1.0 ble introdusert i 1999, og bestod da av 14 retningslinjer/suksesskriterier. WCAG 2.0 ble ferdig utviklet i 2008 og introduserte prinsippene *oppfattelig, operativ, forståelig og robust* til retningslinjene. I 2018 ble WCAG 2.1 publisert, og la til oppdaterte standarder siden 2008, i tillegg til å fokusere på mobiler og nettbrett, samt 17 nye suksesskriterier. Den nyeste WCAG standarden, WCAG 2.2 kom høsten 2023, og la til 9 nye suksesskriterier [20, 21].

WCAG 2.1 er nå en del av det norske regelverket gjennom EUs webdirektiv (WAD). Standarden i WAD er EN 301 549, som igjen viser til WCAG 2.1. Suksesskriteriene er baklengs-kompatible, som betyr at dersom et nettsted tilfredsstiller alle kriteriene i WCAG 2.1, så tilfredsstiller nettstedet alle kravene i WCAG 2.0 også.

Ifølge norsk lov er det forskjell i hvor mange WCAG suksesskriterier som offentlig sektor må følge, i forhold til privat sektor. Virksomheter i offentlig sektor skal totalt følge 49 av de 78 suksesskriteriene i WCAG 2.1 standarden. Ettersom Omhu leverer sine løsninger til både offentlige og private bedrifter, er det nødvendig at deres løsninger følger de 49 lovpålagte kravene i WCAG 2.1 Eksempler på lovpålagte suksesskriterier er:

Prinsipp	Nummer	Suksesskriterie	Beskrivelse
1. Mulig å oppfatte - Oppfattelig	1.3.2	Meningsfylt rekkefølge	Presenter innhold i en meningsfull rekkefølge.
2. Mulig å betjene - Operativ	2.1.1	Tastatur	All funksjonalitet skal kunne brukes kun ved hjelp av tastatur.
3. Forståelig	3.2.4	Konsekvent identifikasjon	Elementer som har samme funksjonalitet på tvers av flere sider er utformet likt.
4. Robust	4.1.3	Statusbeskjeder	Brukeren skal få statusbeskjeder om viktige endringer på nettsiden uten at det gir kontekstendring.

Tabell 2.2: WCAG 2.1 - Eksempel på suksesskriterier

2.3.4 Universell utforming

Ifølge FN-konvensjon om rettighetene til mennesker med nedsatt funksjonsevne, blir universell utforming definert som følger:

> *Med "universell utforming" menes utforming av produkter, omgivelser, programmer og tjenester på en slik måte at de kan brukes av alle mennesker, i så stor utstrekning som mulig, uten behov for tilpassing og en spesiell utforming."Universell utforming" skal ikke utelukke hjelpemidler for bestemte grupper av mennesker med nedsatt funksjonsevne når det er behov for det.*

Universell utforming av IKT innebærer at brukerene, uavhengig av sine forutsetninger, skal kunne klare å ta i bruk både nettsider og automater på en god og enkel måte [22]. Universell utforming er et konsept, som handler om å utvikle løsninger på en måte som gjør at hovedløsningen kan brukes av flest mulig, uavhengig av funksjonnedsettelse [18]. For eksempel; i stedet for å lage to ulike innganger til en bygning, der rullestolbrukere må gå inn på baksiden, kan man heller lage en hovedinngang som tilfredsstiller behovet både til gående og rullestolbrukere. På denne måten er det heller ikke behov for å vedlikeholde flere spesialløsninger samtidig, noe som erfaringsmessig kan være ganske krevende. Dette konseptet kan videreføres til teknologi og webdesign, der man helst bør lage løsninger som dekker behovet til de aller fleste brukerene.

Universell utforming er altså ikke det samme som brukervennlighet og bruker-

opplevelse, men er et like viktig aspekt når det gjelder design av både web-apper, autentiseringsmetoder og alt annet.

2.4 Om målgruppen

Ved utforming av teknologiske løsninger, enten det gjelder autentisering eller en web-applikasjon, er det nødvendig å forstå brukernes behov. Hvem skal bruke løsningen? Er målgruppen slik at løsningen må tilfredsstille andre krav enn det som er vanlig for en gjennomsnittsbruker? Dette kapitlet presenterer definisjoner og teori om målgruppen for å legge til rette for et optimalt resultat.

2.4.1 Kort om psykisk funksjonshemming

Tidligere var det vanlig at forståelsen rundt begrepet funksjonshemming, fokuserte på individets medisinske funksjonsnedsettelser. I dag har synet på funksjonshemming endret seg, og fokuserer på at en funksjonshemming ikke er en hemning i seg selv, men oppstår når samfunnets krav overstiger individets evne til å fungere i samfunnet. Denne modellen blir kallet *Gap-modellen*, og retter fokus på at det er miljøets krav som er årsaken til de praktiske problemene som oppstår, og at det ikke er funksjonsnedsettelsen til individet i seg selv som er problemet. Det er når funksjonsnedsettelsen gjør at det oppstår praktiske problemer pga. krav fra samfunnet, at en *funksjonshemming* oppstår [23].

2.4.2 Personlig assistanse

Alle har rett til å kunne bestemme over sitt eget liv. Personer med utviklingshemming har ofte større utfordringer enn andre, til å både uttrykke seg og bli hørt. De trenger også ofte hjelp til å kunne leve selvstendig, og å få kunne delta på det de vil. Dette gjelder både jobb, skole, fritid og kultur. Derfor har personer med utviklingshemming krav på hjelp, uansett hvor de bor [24]. Minimumshjelpen de har krav på, er personlig assistanse. Personlig assistanse vil si at en assistent hjelper til med dagligdagse gjøremål, samt å legge til rette for et aktivt og mest mulig uavhengig liv til tross for utviklingshemmingen. Noen kan også ha rett på brukerstyrt personlig assistanse, der brukeren selv, eller en nær pårørende, kan bestemme når og hvordan hjelpen skal gis.

Kapittel 3

Metode

Prosjektet har, som nevnt i kapittel 1.2, to deloppgaver. Det første delen er å kartlegge ulike autentiseringsmetoder og undersøke potensielle løsninger grundig. Den andre delen er å utforme et brukergrensesnitt for den nye brukergruppen av Omhu. Dette kapitlet vil utforske den metodikken som ble benyttet for å løse disse utfordringene. Kapittelet fokuserer hovedsakelig på metoder for data-innsamling og -behandling, mens utviklingsmetoder vil bli behandlet i kapittel 5.

Gjennom prosjektet har det vært nødvendig å samle data ved flere anledninger for å kunne utføre grundige evalueringer og deretter gjøre velinformerte beslutninger. Gruppen har primært benyttet seg av brukertester og ekspertintervjuer for dette formålet. Forklaringen på hvorfor disse metodene ble valgt, vil bli gitt i de respektive underkapitlene.

3.1 Ekspertmøter og intervjuer

I løpet av prosjektet har vi benyttet møter og intervjuer som en metode for å skaffe subjektiv informasjon som ikke lett finnes i faglitteraturen eller gjennom annen tradisjonell informasjonsinnhenting.

Samtaler med erfarne fagpersoner innen spesifikke felt gir innsikt i bransjens arbeidshverdag, og kan gi verdifulle pekepinner og tips som ikke nødvendigvis er tilgjengelige gjennom litteratur eller nettlesing, i hvert fall ikke med samme effektivitet. Å kommunisere med slike eksperter muliggjør en helhetlig forståelse av problemstillingen og bidrar til bedre beslutningstaking i prosjektet.

I dette prosjektet har ekspertintervjuer primært blitt brukt for å innhente kunn-

skap og erfaringer om overordnede konsepter, og ikke som kilde for spesifikke tilbakemeldinger slik man ville gjort i et heuristisk intervju(ekspertintervju) [25, Kap 1 *Expert or Heuristic Evaluations*].

Gitt de åpenbare fordelene ved ansikt-til-ansikt-samtaler, var det naturlig å inkludere møter og intervjuer som en integrert del av arbeidsprosessen.

3.2 Brukertesting

Brukertesting er en metode der en ekstern deltaker tar rollen som sluttbruker for å evaluere funksjonaliteten og brukervennligheten til et produkt. Deltakeren utfører en serie oppgaver med produktet, og resultatene observeres og noteres som empirisk data, som deretter kan brukes for å identifisere hva som fungerer og ikke fungerer med designet.[25, Kap 1 *Usability Testing*] Denne metoden kan suppleres med intervjuer for å få ytterligere innsikt i produktets ytelse.

3.2.1 Valg av metode

I denne studien har brukertesting blitt anvendt i ulike sammenhenger for å samle data. Brukertesting er uvurderlig innen UX-design, da ingen mengde teori kan garantere at et produkt vil fungere som ønsket når det blir brukt av en faktisk sluttbruker.

Ekspertintervju kan være et alternativ til brukertesting, spesielt i tidlige utviklingsfaser, for å avdekke åpenbare feil og mangler[25, Kap 1 *Limitations of Testing*]. Men denne metoden kan ikke erstatte brukertesting og vil ikke gi samme type data. For prototypene som er utviklet i dette prosjektet, har det ikke vært gjennomført noen formell ekspertevaluering eller heuristiske intervjuer angående UX-elementene.

3.2.2 Bakgrunn

Brukertestene gjennomført som en del av dette prosjektet er designet i tråd med prinsippene presentert i boken "Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests"av Jeffrey Rubin-Dorsky. Boken inneholder informasjon og veiledning på konsepter, design og gjennomføring av brukertester.

Metodikken beskrevet i boken er ikke helt vitenskapelig, da dens formål er å gjø-

re brukertesting praktisk på en mindre skala enn en tradisjonell vitenskapelig tilnærming tillater. En fullstendig vitenskapelig test ville kreve hypoteseformulering, bruk av kontrollgrupper, tilfeldig utvalg av deltakere, gradvis endring av variabler og et stort antall tester for å unngå i utvalgsskjevhet [25, Kap 1 *Basics of the Methodology*]. Disse kravene, spesielt det siste, gjør denne tilnærmingen upraktisk for formålet med dette prosjektet.

Boken identifiserer fire grunnleggende typer brukertester:

1. Exploratory test, referert til som "Utforskende test"
2. Assestment test, referert til som "Vurderende test"
3. Validation test, referert til som "Validerende test"
4. Comparison test, referert til som "Sammnelignende test"

Hver type test har en unik tilnærming som passer best for ulike stadier av produktutviklingen.

En **utforskende test** utforsker hovedfunksjonene til produktet i de tidlige stadiene av utviklingen [25, Kap 1 *Exploratory or Formative Study*]. Disse testene involverer mye kommunikasjon mellom moderator og deltakere og ligner nesten på et intervju. Oppgavene er ofte abstrakte og fokuserer på å evaluere designets intuitivitet. Dataene som samles inn er hovedsakelig kvalitative og bidrar til å forstå brukernes oppfatning av produktet i de tidlige stadiene av dets utvikling

En **vurderende test** er den vanligste typen test, som har som mål å vurdere implementeringen av designkonseptene ved å identifisere problemer med produktet [25, Kap 1 *Assessment or Summative Test*]. Til forskjell fra utforskende tester fokuserer vurderende tester mer på detajler. Oppgavene gitt i en slik test er laget for å ligne på de en faktisk sluttbruker ville utføre på det reelle produktet. Kommunikasjonen mellom moderator og deltakere er mindre i slike tester. Dataene fra vurderende tester kan være både kvalitative og kvantitative, avhengig av testens utforming.

En **validerende test** bekrefter eller verifiserer at tidligere identifiserte feil er blitt korrigert [25, Kap 1 *Validation or Verification Test*]. Denne typen test utføres vanligvis på en nesten ferdig versjon av produktet sent i utviklingsprosessen. Dataene fra validerende tester måles opp mot etablerte standarder og produserer derfor kvalitative data.

En **sammenlignende test** sammenligner to versjoner av det samme produktet eller ulike produkter med samme formål [25, Kap 1 *Comparison Test*]. Denne tilnærmingen er ikke en separat metode i seg selv, og kan brukes i kombinasjon med de andre tre metodene. Sammenlignende tester er mest egnet for å følge

den tradisjonelle vitenskapelige metoden.

I dette prosjektet utføres hovedsakelig vurderende tester, da de er allsidige og egnet for alle tilfeller der testing er nødvendig. Valget av testtype vil bli ytterligere begrunnet i de følgende underkapitlene.

3.2.3 Undersøkelse av ulike autentiseringsmetoder

Test-planen for denne brukertesten kan bli funnet i vedlegg D.

Formål med testen

Målet med denne undersøkelsen var å identifisere den mest brukervennlige autentiseringsmetoden fra et utvalg av metoder. Vi ønsket å samle preferansedata fra brukere om hvilken type autentisering de fant mest brukervennlig. Autentiseringsmetodene som ble vurdert i testen inkluderte følgende:

1. Autentiseringsapp
2. Sikkerhetsnøkkel
3. Passord
4. Fingeravtrykk*
5. Ansiktsgjenkjenning*
6. Pinkode*
7. BankID App**

**Dersom brukeren hadde denne autentiseringsformen tilgjengelig på sin mobil*
***Dersom brukeren benyttet BankID appen*

Brukertesten besto av fire oppgaver, etterfulgt av et intervju etter testen. Den første oppgaven innebar at brukeren autentiserte seg ved hjelp av en sikkerhetsnøkkel på en DEMO-nettside utviklet av Google. I den andre oppgaven skulle deltakerne autentisere seg med passord, brukernavn og TOTP-autentiseringsapp. For den andre oppgaven ble det benyttet en liten TOTP-demo utviklet som en del av prosjektet. De to andre oppgavene var tilsvarende de første, men involverte registrering av autentiseringsfaktorene i stedet for selve autentiseringen. Resultatene fra brukertesten er presentert i kapittel 5.1.

Valg av metode

Mulige alternativer for å samle denne typen data inkluderte et kvantitativt online spørreskjema, en kvalitativ vurderingstest eller en kvantitativ validerende brukertest.

Et spørreskjema ville ha gitt fordelen av å samle inn større mengder data, men siden denne testen var ment å sammenligne autentiseringsmetoder, slik som sikkerhetsnøkkel, særlig blant personer med begrenset teknologisk kompetanse, ble det konkludert med at et slikt spørreskjema ville være upraktisk. Det er sannsynlig at det er en svært liten andel av personer som eier en sikkerhetsnøkkel og samtidig kan betraktes som å ha "lav teknologisk kompetanse".

Derfor var en brukertest det naturlige valget, da dette tillot observasjon av brukerne i kontakt med teknologiene som skulle testes, noe som ville gi enda mer data. Med tanke på at teknologiene som ble testet allerede var godt etablerte og tatt i bruk, kunne en validerende test mot en standard for autentisering, for eksempel brukernavn og passord, vært et alternativ. Men siden dette ville ha økt arbeidsbelastningen for testen uten å gi tilstrekkelig avkastning i form av data, ble det besluttet å gjennomføre testen som en ordinær vurderingstest.

3.2.4 Brukertest av autentiserings-demo

Den fulle test-planen for denne brukertesten ligger i vedlegg C.

Testens formål

Denne runden med testing var rettet mot demonstrasjonen for innloggingsløsning med sikkerhetsnøkkel og platform-autentisering. Testen ble utført etter at demonstrasjonen var ferdig utviklet, etter at alle beslutnigner angående valg av teknologier og design hadde blitt gjort. Teknologivalgene i demonstrasjonen ble valgt på bakgrunn av kartleggingen av autentiseringsmetoder gjort tidligere i studien. De valgte autentiseringsmetodene var vurdert til å være de mest lovende kandidatene, som det samtidig var realistisk å utvikle en demonstrasjon med innenfor tidsrammene til prosjektet. Testens formål var dermed å innhente informasjon om hvorvidt demoen fungerte som forventet, og om valgene av teknologi brukt i demoen fortsatt kunne anbefales i konklusjonen av studien.

Valg av metode

Formålet med denne brukertesten var å verifisere om teknologiene i autentiseringsdemoen oppfylte de tidligere fastsatte forventningene i studien, og å bidra med data til den samme evalueringen. Valget av metode for denne brukertesten var mellom en verifiserende test og en vurderingstest. Det kunne vært mulig å benytte vurderingen av brukervennlighet gjort tidligere i studien som en standard for å utføre en valideringstest, men siden denne vurderingen kun var en rangering fra én til fem angående brukervennlighet, ble det ikke ansett som presist nok til å gjennomføre en en slik test. Derfor ble det igjen valgt å gjennomføre en vurderingstest, da dette gir en god balanse mellom nøyaktige data, fleksibilitet og gjennomførbarhet. Denne metoden er også lik de andre testene som ble utført i samme test-økt, og da alle testene inkludert i den økten var vurderingstester, gjorde dette datainnsamlingen enklere for sekretærene og testmoderatoren og forholde seg til.

3.2.5 Brukertester av pasientmodul

Testplanen for versjon 1 av testen ligger i vedlegg A, og versjon 2 av testen ligger i vedlegg B.

Testens formål

Pasientmodulens utvikling gjennomgikk to faser med brukertesting mellom iterasjonene. Målet med testingen av pasientmodulen var å avdekke feil og mangler i nettsidedesignet for å kunne forbedre produktet i neste iterasjon.

Iterasjoner av brukertesting

Brukertesten for pasientmodulen ble gjennomført i to iterasjoner, som samsvarer med deres respektive versjoner av pasientmodulen. Det ble gjort mindre endringer mellom de to testene for å oppdatere dem og bedre fange data for den tilsvarende versjonen av pasientmodulen. Bortsett fra disse små endringene var testene nesten identiske. Derfor ble valget av metode det samme for begge brukertestene.

Metodevalg

Brukertestene for pasientmodulen ble primært utført tidlig i utviklingsfasen, der en utforskende test vanligvis ville vært passende. Siden den eksisterende Omhu-nettsiden allerede ga et solid grunnlag å arbeide ut ifra, var behovet for en slik test noe redusert. Selv om det fortsatt ville vært nyttig, ble det besluttet å gå direkte til vurderingstester for å optimalisere ressursbruken. Valideringstesting var ikke aktuelt på grunn av testens tidlige fase i utviklingen, samt at det manglet en tilgjengelig standard til å bruke som målestokk for testen. Det samme gjaldt sammenligningstester; selv om det kunne ha vært aktuelt å gjennomføre en sammenligning mellom iterasjonene av produktet, ble det vurdert som en ineffektiv bruk av ressurser å gjennomføre slike tester. Derfor var det naturlig å gjennomføre testene som vurderingstest, da slike tester passet godt inn i utviklingsfasen.

3.3 Vurderingskriterier for autentiseringsfaktorer

Denne studien omhandler en kartlegging av autentiseringsfaktorer for Omhu. For å effektivt kunne sammenligne og kartlegge forskjellige kvaliteter og egenskaper av de ulike autentiseringsmetodene, er det nødvendig med en standard å rangere disse egenskapene opp mot. Det finnes allerede enkelte standarder for spesifikke egenskaper, som sikkerhet (FAR, altinn sikkerherhetsnivå osv.). Det finnes derimot ikke en universal standard for måling av andre egenskaper, som brukervennlighet, kostnad, dekning og implementasjon. Dette er også relevante elementer å undersøke, for å kartlegge hvilken autentiseringsmetoden som er mest aktuell.

Denne seksjonen vil dermed omhandle en egen definisjon av verdier brukt til å rangere diverse egenskaper av autentiseringsmetoder. Rangeringene er bygd på eksisterende standarder der dette er mulig. For egenskapene der dette ikke lot seg gjøre, har det blitt gjort tiltak for å sikre at autentiseringsmetoder som senere rangeres med skalaen er skaffet på likt grunnlag, med empirisk data og støttende faglitteratur for et mest mulig nøyaktig resultat. Målet er at standarden beskrevet i denne seksjonen beholder faglig troverdighet til tross for den noe uortodokse visningen.

For å sammenligne de ulike autentiseringsfaktorene og løsningene skissert i denne rapporten, tar vi utgangspunkt i de kvantitative verdiene som vist under. Disse egenskapene er valgt for å representere de egenskapene som er mest relevante for WeissTech, i deres valg av autentiseringsmetode for den nye pasientmodulen.

	1	2	3	4	5
Sikkerhet	Svært Svak	Svak	Moderat	Sterk	Svært Sterk
Kostnad	Svært Kostbart	Kostbart	Rimelig	Svært Rimelig	Ubetydelig
Brukervennlighet	Svært Krevende	Krevende	Moderat	Enkelt	Svært Enkelt
Dekning	Svært Dårlig	Dårlig	Suboptimal	God	Optimal
Implementasjon	Svært Krevende	Krevende	Moderat	Enkelt	Svært Enkelt

Tabell 3.1: Kvantitative verdier

Sikkerhet

Sikkerhetsaspektet i autentiseringsfaktoren er vurdert mtp. at ingen andre faktorer er implementert, og den gitte autentiseringsfaktoren alene er den eneste sikkerhetsmekanismen som hindrer uvedkommede å få tilgang til en brukerkonto. Sikkerheten blir derfor vurdert i en tenkt situasjon der multi-faktor ikke er implementert.

Svært svak: Faktoren er sårbar for angrep fra ikke IT-kyndige trusselaktører, bruk av minimal tid/innsats for å spoofe eller forbipassere autentiseringsfaktoren. Sårbar for typisk ikke-målrettede angrep som gjennomføres automatisk i stor skala.

Svak: Avskremmende sikkerhet, resistant til opportunistiske angrep men oppnåelig for en mildt-kompenent og dedikert angriper og forbipassere eller spoofe gitt moderat tid.

Moderat: Motstandsdyktig for de fleste former for fysiske og digitale angrep. Oppnåelig for en dedikert angriper hvis gitt tilstrekkelig tid og ressurser.

Sterk: Vanskelig, men oppnåelig for en kompentent og dedikert angriper og forbipassere eller spoofe autentiseringsfaktoren. Liten angrepsflate og kontrollerte omgivelser.

Svært sterk: Motstandsdyktig til bortimot alle digitale angrep, men oppnåelig dersom en angriper tar i bruk svært avanserte teknikker, eller er villig til å gå særdeles langt innen sosial manipulasjon eller fysisk inngrep. Krever god planlegging eller særskilte omstendigheter for en vellykket gjennomføring.

Kostnad

Kostnadene er regnet med førstegangskostnader + eventuelle kostnader for det neste året med drift.

Svært kostbart: Mer enn 1 000 000kr i året.

Kostbart: 100 000kr - 999 999kr i året.

Rimelig: 10 000kr - 99 999kr i året.

Svært Rimelig: 1000kr - 9999kr i året.

Ubetydelig: Under 1000kr i året.

Brukervennlighet

Graderingen av brukervennlighet tar utgangspunkt i et svært lavt nivå av kompetanse og erfaring i bruk av digitale systemer. Det er derfor forventet at en del av brukerbasen vil oppleve at bruken av den gitte autentiseringsmetoden er langt enklere enn det som denne kategoriseringen tilsier.

Dette er for å unngå at konklusjonen, og dermed den anbefalte løsningen, ender opp med å ta utgangspunkt i at gjennomsnittsbrukeren i målgruppa har tidligere erfaring med bruk av digitale tjenester, slik som f.eks Facebook. Selv om en kan anta en slik erfaring i digitale systemer er grunnleggende, ville det blitt ekskluderende for brukere som ikke har interesse for sosiale medier og lignende, og dermed aldri har fått muligheten til å lære seg disse ferdighetene, som man ofte antar er "allmennkunnskap".

Svært krevende: Autentiseringen krever utvidet og dedikert opplæring over en lengre periode. Autentiseringen kan oppleves som innviklet og vanskelig å benytte seg av med mange trinn og høyt press på brukeren, noe som krever betraktelig konsentrasjon og innsats for å gjennomføre.

Krevende: Autentiseringen krever opplæring over en begrenset periode. F.eks. at vedkommende trenger hjelp til å logge inn de 5 første gangene. Autentiseringen innebærer flere steg og et moderat nivå av memorering og konsentrasjon for å gjennomføre.

Moderat: Autentiseringen krever introduserende opplæring med førstegangs bruk. Etter dette krever autentiseringen en mindre mengde memorering og konsentrasjon fra brukeren for å gjennomføre.

Enkelt: Autentiseringen krever ingen dedikert opplæring fra kompetent personale, men hjelp fra andre med enkel autentiseringskompetanse kan trenges ved førstegangsbruk. F.eks. en ekstern person som har erfaring fra sosiale medier. Autentiseringen krever minimal memorering, og kan i hovedsak fullføres ved hjelp av svært få trinn uten krav om konsentrasjon i form av tidsbegrensning eller lignende.

Svært enkelt: I utgangspunktet skal alle sluttbrukere intuitivt forstå hvordan autentiseringen gjennomføres uten hjelp fra noen ekstern person og uavhengig av erfaring med andre verktøy, som Facebook. Ingen memorering eller konsentrasjon er krevet av sluttbrukeren for å gjennomføre autentiseringen.

Dekning

Dekning beskriver hvor stor del av brukerbasen som vil ha mulighet til å dra nytte av løsningen. Dette kan f. eks. være hvor stor andel av brukerbasen har en enhet som tilfredsstiller kravene til den gitte autentiseringsfaktoren. Dersom faktoren krever at brukeren har en mobil som støtter NFC, vil andelen av brukerbasen som kan dra nytte av løsningen, være avhengig av hvor mange som har moderne smartmobiler tilgjengelig.

Svært Dårlig: 0% til 20% av brukerbasen vil ha mulighet til å dra nytte av løsningen.

Dårlig: 21% til 50% av brukerbasen vil ha mulighet til å dra nytte av løsningen.

Suboptimal: 51% til 80% av brukerbasen vil ha mulighet til å dra nytte av løsningen.

God: 81% til 95% av brukerbasen vil ha mulighet til å dra nytte av løsningen.

Optimal: 96% til 100% av brukerbasen vil ha mulighet til å dra nytte av løsningen.

Implementasjon

Implementasjon beskriver hvor ressurskrevende det er å implementere den gitte autentiseringsfaktoren inn i Omhu, gitt at Omhu allerede har en utvikler som har ansvar for den tekniske delen av Omhu. Implementasjonen omrammer både de tekniske vanskelighetene med å implementere autentiseringsformen, samt organisatoriske problemer som kan oppstå som følger av implementasjonen. Om disse

to måtene og rangere implementasjon på står i konflikt, velges den med lavest vurdering.

Svært krevende: Det finnes ingen eksisterende løsninger som kan implementeres i applikasjonen. Koden må utvikles fra bunnen av over flere operativsystemer med separate krav og avhengigheter. Dette krever kompetente utviklere med bred erfaring innenfor programvareutvikling. Implementasjon av autentiseringen krever store endringer innad i institusjonens som rammer en svært høy andel av institusjonens ansatte og/eller medlemmer.

Krevende: Utvidet programvareutvikling eller bruk av avanserte softwaresystem, behov for å leie en ekstern konsulent for rådgivning eller utvikling. Implementasjonen av autentiseringen har har en utbredt negativ innflytelse på institusjonens daglige drift, med moderate endringer som må innføres i arbeidshverdagen for en stor andel av institusjonens ansatte og/eller sluttbrukere.

Moderat: Behov for programmering, men ikke mer avansert enn at en gjennomsnittlig utvikler kan kode og implementere løsningen selv, gitt et realistisk tidsbudsjett. Implementasjonen av autentiseringen har en lettere negativ innflytelse på kunden/institusjonens daglige drift, med mindre endringer som må implementeres i arbeidshverdagen til en større gruppe ansatte for at teknologien skal kunne utnyttes som ment.

Enkelt: Løsningen eksisterer allerede, er veldig utbredt og godt dokumentert. En utvikler skal kunne implementere løsningen selv, uten store problemer og med et realistisk tidsbudsjett. Implementasjonen av autentiseringen har en minimal negativ innflytelse på kunden/institusjonens daglige drift, med mindre endringer som må implementeres i arbeidshverdagen til et lite utvalg personale for at teknologien skal kunne utnyttes som ment.

Svært enkelt: Løsningen eksisterer allerede som en “software as a service” med svært enkel implementasjon. Ansvar for den videre driften og utviklingen av løsningen ligger på den eksterne bedriften som leverer løsningen. Implementasjonen av autentiseringen har ingen merkverdig innflytelse på kundenes/institusjoners drift og organisering.

3.4 Datapresentasjon

3.4.1 Condorcet-metoden

I kapittel 5.1.3 vises en rangering av autentiseringsmetoder basert på brukertesting. Metodikken for denne brukertesen ble gjennomgått i kapittel 3.2.3. I bru-

kertesten ble testdeltagerne bedt om å rangere et utvalg autentiseringsmetoder, utifra hvor enkelt de syntes det var å autentisere ved bruk av hver enkelt autentiseringsmetode.

Rangeringen var ikke kategorisert. Testdeltagerne fikk dermed ikke valget med å plassere metodene inn i kategoriene "enkelt", "moderat" og "vanskelig" eller lignende. Dette gir en effekt av at rangeringen var helt fri, der metodene i seg selv var den eneste referansen for hvor enkel testdeltagerene syntes den var. Testen tillot også deltagerne å rangere flere metoder på samme nivå. Resultatet er et datasett som gir gode sammenligningsdata, men var noe vanskelig å presentere.

For å presentere en sammenlagt rangering basert på data fra alle brukertestene gjennomført, blir "Condorcet-metoden" brukt. Dette er en metode vanligvis brukt for å velge vinnere av politiske valgkamper, der hver stemmer rangerer listen av kandidater fra høyest til lavest preferanse [26]. Siden rangering av autentiseringsmetoder tilsvarer en slik avstemning, vil denne metoden fungere godt for å vise hvilken av metodene som rangerer høyest.

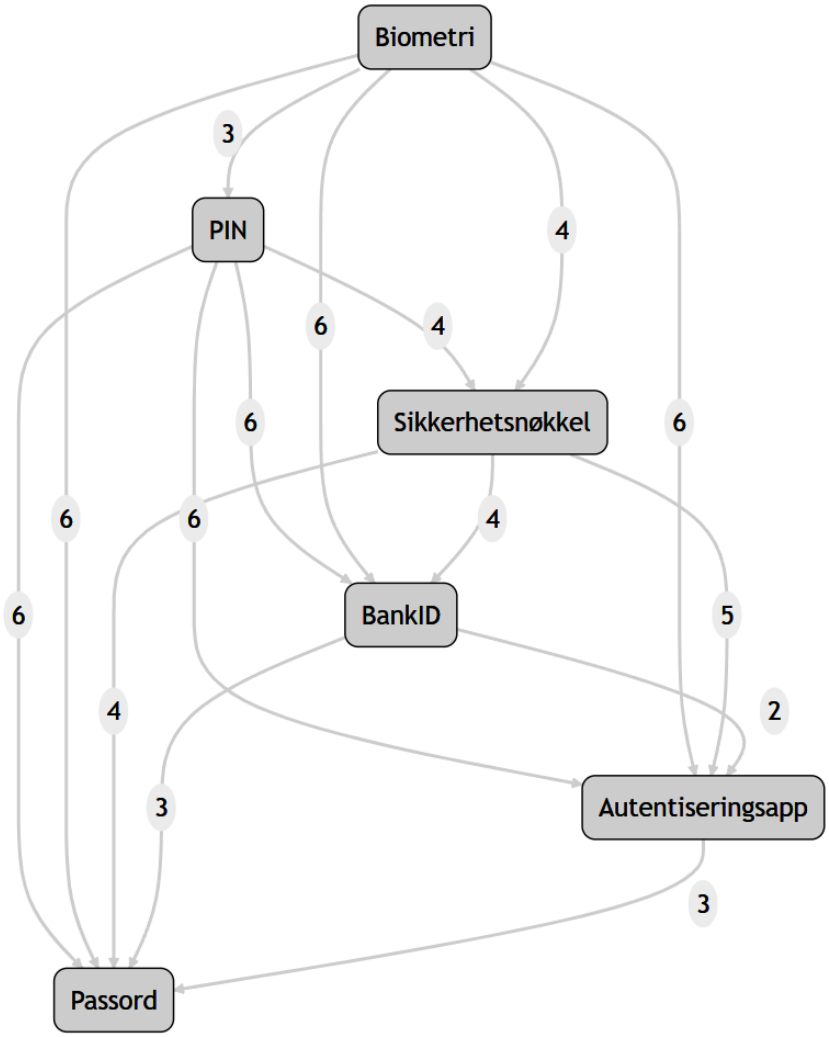
Condorcet-metoden er basert på parvis sammenligning av hver enkelt kandidat. I brukertesten sammenlignes alle de ulike autentiseringsmetodene med hverandre. Man teller hvor mange ganger metode A ble rangert høyere enn metode B, hvor mange ganger metode B ble rangert høyere enn metode A, hvor mange ganger metode A ble rangert høyere enn metode C, og så videre. Dette gjøres for alle metodene. Med seks forskjellige metoder ble det gjennomført totalt 30 forskjellige sammenligninger.

Sammenligning *x*>*y*	**Antall tilfeller *x* var høyere rangert enn *y***
Sikkerhetsnøkkel>Passord	4
Sikkerhetsnøkkel>Pin	1
Sikkerhetsnøkkel>Biometri	0
Sikkerhetsnøkkel>BankID	4
Sikkerhetsnøkkel>App	5
Passord>Sikkerhetsnøkkel	1
Passord>Pin	0
Passord>Biometri	0
Passord>BankID	1
Passord>App	2
Pin>Sikkerhetsnøkkel	4
Pin>Passord	6
Pin>Biometri	1
Pin>BankID	6
Pin>App	6
Biometri>Sikkerhetsnøkkel	4
Biometri>Passord	6
Biometri>Pin	3
Biometri>BankID	6
Biometri>App	6
BankID>Sikkerhetsnøkkel	1
BankID>Passord	3
BankID>Pin	0
BankID>Biometri	0
BankID>App	2
App>Sikkerhetsnøkkel	1
App>Passord	3
App>Pin	0
App>Biometri	0
App>BankID	2

Tabell 3.2: Parvis sammenligning av autentiseringsmetoder

Neste steg er å omgjøre de parvise dataene til en graf. I denne grafen vil hver metode representeres som en node, og hver sammenligning vil representeres som en vektet kant. Retningen på kanten indikerer hvilken metode som vant den parvise sammenligningen, der noden med den innkommende kanten er taperen. For eksempel, hvis sikkerhetsnøkkel ble vurdert høyere enn PIN-kode i ett tilfelle, mens PIN-kode ble vurdert høyere enn sikkerhetsnøkkel i fire tilfeller, vil kanten mellom disse nodene gå fra PIN-kode til sikkerhetsnøkkel og ha en vekt på fire. På denne

måten konstrueres grafen ut fra datasettet. Mens grafen konstrueres, er det viktig å se etter og eliminere eventuelle løkker når de oppstår. I dette tilfellet ble det ikke funnet slike løkker.



Figur 3.1: Condorcet graf

Når grafen er konstruert, kan man identifisere noden uten innkommende kanter. Denne noden representerer autentiseringsmetoden som aldri tapte en parvis sammenligning, og kan dermed betegnes som "Condorcet-vinneren". I tillegg kan vi rangere nodene fra færrest til flest innkommende kanter for å generere en rangert

Node	Ant. innkommende kanter
Biometri	0
Pin-kode	1
Sikkerhetsnøkkel	2
BankID	3
Autentiseringsapp	4
Passord	5

Tabell 3.3: Autentiseringsmetoder rangert basert på innkommende kanter

liste over metodene. Færre innkommende kanter tilsvarer en høyere rangering og dermed et bedre resultat.

3.4.2 Punktdiagram for sammenligning av autentiseringsmetoder

Punktdiagrammene brukt for å sammenligne autentiserings-faktorer basert på egenskapene sikkerhet, brukervennlighet, dekning, kostnad og implementasjon tar utgangspunkt i de kvantitative verdiene satt for hver autentiseringsfaktor.

For å presentere disse dataene, brukes det hovedsaklig to varianter. Den første er en sammenligning av brukervennlighet og sikkerhet, de to viktigste egenskapene i følge oppdragsigver, se møtereferat 29. jan, vedlegg N. Disse egenskapene blir representert av de to aksene i punkt-diagrammet, mens de resterende egenskapene blir utelatt.

Den andre metoden brukes for å gi et helhetsbilde av autentiseringsmetoden, hvor alle egenskaper tas med i beregningen. For å oppnå dette, deles egenskapene inn i to forskjellige grupper, som plasseres på hver sin akse i et punktdiagram. Den første gruppen kalles “input”. Denne gruppen representerer alle egenskaper knyttet til negative konsekvenser ved å ta i bruk autentiseringsfaktoren, som er *kostnad* og *implementasjon*. Den andre gruppen kalles “output” og representerer egenskapene som gir fordeler ved å bruke metoden, som er *sikkerhet*, *brukervennlighet* og *dekning*.

For sikkerhet/brukervennlighet-sammenligningene er det ikke nødvendig med vekting, ettersom det kun er en faktor på hver akse. For sammenligningene av “input” og “output”, har det blitt tatt i bruk vekting av egenskapene for å produsere en visuell og forklarende graf. Denne vektingen utføres basert på prioriteringen av egenskaper som forklart av oppdragsgiver, samt egne vektinger basert på interne beslutninger i gruppen.

Vekting av egenskaper for input/output graf

Prioriteringen fra oppdragsgiver er som følger(se vedlegg N.3.2):

1. Sikkerhet
2. Brukervennlighet
3. Kostnad for kunde
4. Kostnad av implementering

Denne rangeringen ble gitt tidlig i prosjektet, og følger dermed en litt annen kategorisering enn det som ble fulgt videre. *Kostnaden for kunde* og *kostnad for implementering* blir omgjort til *kostnad* og *implementering*. I tillegg legges "dekning" til som en egenskap.

Rangeringen med de nye egenskapene er som følger:

1. Sikkerhet
2. Brukervennlighet
3. Dekning - *Satt som n3 ettersom dårlig dekning antagelig vil medføre kostnad for kunde*
4. Kostnad
5. Implementering

For vektingen av punkt-diagrammene er dermed faktorene vektet med disse verdiene: Output:

Sikkerhet: 3

Brukervennlighet: 2

Dekning: 1

Input: (*vektet til 3/2 forhånd ettersom 2/1 førte til en over-representasjon av kostnadseffektive metoder)*

Kostnad: 3

Implementasjon: 2

Eksempel: Om en autentiseringsmetode har sikkerhet 3, brukervennlighet 4 og dekning 5, vil disse verdiene multipliseres med de relevante vektene, slik at sikkerhet blir 9, brukervennlighet 8 og dekning 5. Disse legges da sammen til 22, og

deles på antall "multiplikasjoner" tatt med i beregningen. I dette tilfellet er det 3, 2 og 1, for en total av 6. Siden 22 delt på 6 er 3.6, vil dette være "output"-verdien for denne autentiseringsfaktoren. Uten vektingen ville gjennomsnittet av disse blitt 4, men da sikkerhet er viktigere enn de to andre verdiene, hjelper vektingen å trekke ned resultatet for å reflektere dette.

Kapittel 4

Utvikling

I dette kapitlet gjennomgås prosessen for utvikling av de tekniske produktene. Selv om oppgaven opprinnelig ikke krevde produktutvikling, verken i del 1 eller del 2, ble det besluttet å utvikle en demonstrasjon eller et *proof of concept* for en av de mest lovende autentiseringsløsningene. Dette muliggjør en grundigere brukertesting av autentiseringsmetoden samt gir teknisk innsikt i dens funksjonalitet. Brukertesting er en svært viktig del av produktdesignprosessen [25, kap. 2]. Ved å gjennomføre tester tidlig og kontinuerlig gjennom hele utviklingsløpet, reduseres risikoen for at produktet inneholder feil eller ikke oppnår ønsket brukervennlighet.

For pasientmodulen var målet å designe en ny modul for pasienthåndtering. Det ble besluttet at en interaktiv web-demo ville gi mer nøyaktige og nyttige resultater fra brukertesting sammenlignet med en enkel wireframe. Siden oppgaven ikke inkluderte noen kravspesifikasjon fra oppdragsgiver for utviklingen av disse to demoene", har gruppen selv definert interne kravspesifikasjoner for produktene.

4.1 Utvikling av demo for WebAuthn autentisering

4.1.1 Interne kravspesifikasjoner

Dette konseptbeviset skal demonstrere bruk av autentiseringsmetodene som ble vurdert som de mest lovende. Som nevnt i introduksjonen til dette kapitlet, så er ingen kravspesifikasjoner bestemt fra oppdragsgiver sin side. Interne kravspesifikasjoner ble dermed bestemt, og er listet opp under:

1. Produktet vil i sin helhet være en innloggings-portal til Omhu. Pasientmodulen utviklet i dette prosjektet legges bak innloggings-løsningen.
2. Produktet skal være en nettside kompatibel med Google Chrome nettleser for Android og Apple IOS våren 2024.
3. Produktet skal utvikles med en mobile-first approach, eller mobil-først tilnærming.
4. Produktet skal ha et fungerende brukergrensesnitt for prosessen av både innlogging og registrering av ny bruker.
5. Produktet skal utnytte WebAuthn / FIDO2 protokollene for å autentisere brukeren opp mot en autentiserings-server.
6. Produktet skal kreve to-faktor autentisering for å logge inn, der platformautentisering i form av ansiktsgjenkjenning, fingeravtrykk eller pin kode skal utnyttes som første faktor, og sikkerhetsnøkkel over USB-C eller NFC skal utnyttes som andre faktor.

4.1.2 Valg av teknologier og verktøy

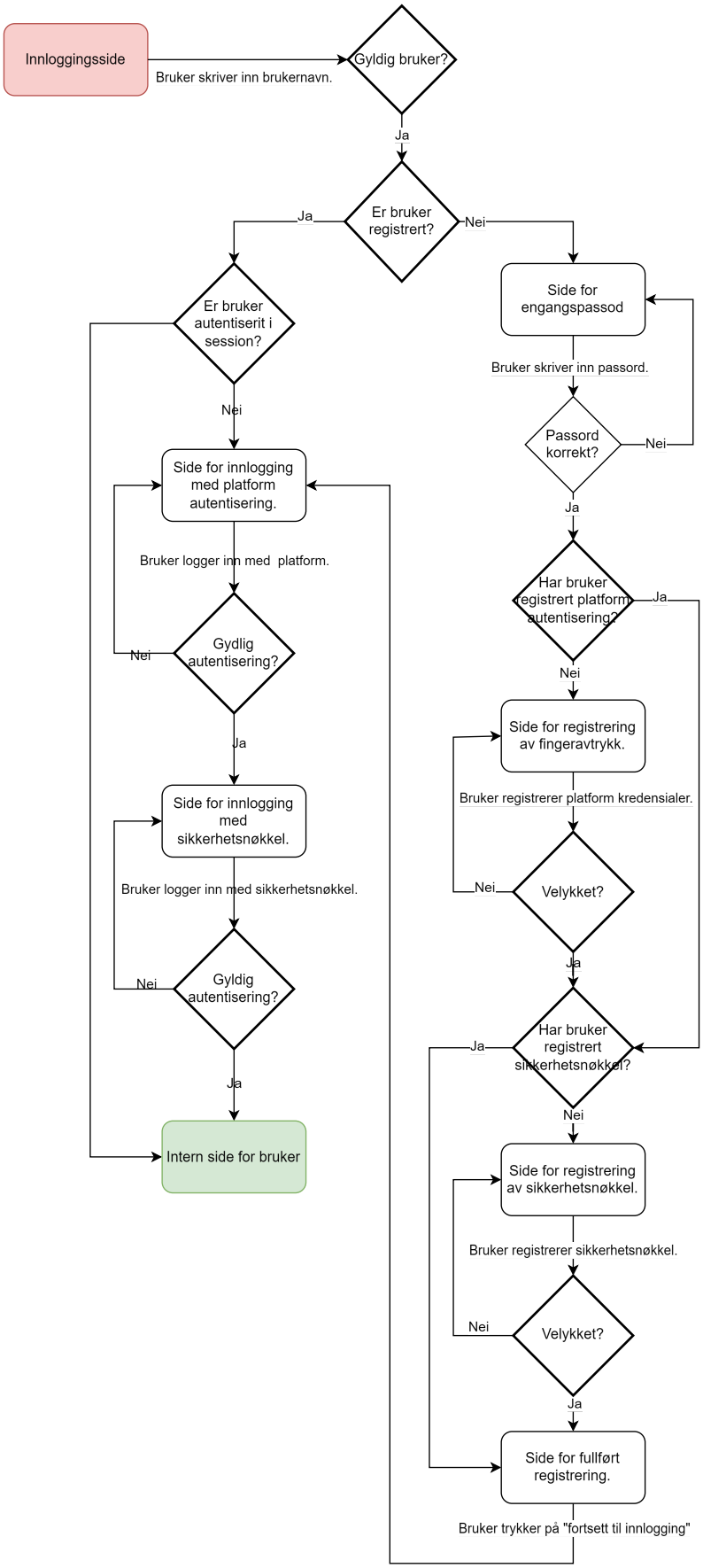
For å utvikle autentiserings-demonstrasjonen, ble følgende verktøy brukt:

1. **Golang** - for utvikling av backend.
    a. Standard bibliotek.
    b. **WebAuthn** - Offisiell pakke hentet fra github. Brukt for å forenkle operasjoner relatert til håndtering av WebAuthn-standarden.
    c. **Gorilla** - tredjeparts pakke brukt for håndtering av sessions. Hentet fra github.
2. **Javascript/CSS/HTML** - for utvikling av generell frontend.
    a. **jQuery** - Bibliotek utnyttet for å gjøre kontakt med API raskere, samt simplifisere bruk av animasjoner. Hentet fra jquery.
    b. **crypto-js** - Ble brukt i liten grad for å generere hash av engangspassord. Hentet fra npmjs.

4.1.3 Design

Informasjons-modell

Grensesnittet for demoen hadde som formål å være så enkel som mulig, for å effektivt demonstrere hvordan en slik autentisering kan bli gjennomført. Til å begynne med, ble det designet et svært enkelt prosess-flyt diagram for hvordan en bruker skulle kunne gjennomføre forskjellige handlinger på nettsiden.



Figur 4.1: Prosessflytdiagram for webauthn demo

Som vist i figur 4.1, skal nettsiden kun ha støtte for at brukeren kan registrere seg, samt autentisere seg. I en reell implementasjon ville det vært et krav om å kunne endre legitimasjon(eng. credentials, passord, fingeravtrykk osv.). Siden dette er en enkel demo, har slike egenskaper blitt utelatt for å spare tid og ressurser.

Grensesnitt

Grensesnittet for autentiserings-demoen ble bygd for å være så enkel som mulig. Brukeren vil bli tatt gjennom en serie med bokser. Hver boks skal ha følgende detaljer:

1. **Overskrift** - hva skal brukeren skrive inn.
2. **Input felt eller knapp** - her kan bruker skrive inn passord, brukernavn, eller trykke for å aktivete en funksjon.
3. **Fremgangs måler** - her vil brukeren se hva som har blitt gjort, og hva som gjenstår å gjøre.
4. **Error felt** - her kommer feilmeldinger som forteller brukeren hva som eventuelt har gått galt.

Hvert avrundete rektangel på prosessflyt-diagrammet, er en side med den samme oppbygning. Med dette som utgangspunkt ble det besluttet å ikke produsere en digital wireframe, grunnet manglende tidsressurser. Det ble derimot skissert design fysisk under denne delen av utviklingsprosessen. En gjennomgang av demo-en med lysbilder kan bli funnet i vedlegg G.

Grensesnittet består dermed av følgende elementer, for to ulike prosesser. En prosess for registrering, etterfulgt av en prosess for autentisering.

For registreringsdel er det følgende sider:

1. Innskriving av brukernavn
2. Innskriving av engangspassord
3. Registrering av platform-legitimasjon
4. Registrering av sikkerhetsnøkkel
5. Sluttside, med link til innlogging

Autentiseringsdelen begynner når brukeren trykker på knappen på side 5, *sluttside*, eller når brukeren skriver inn brukernavnet sitt på side 1, *innskriving av brukernavn*, men allerede har registrert autentisering:

1. Autentisering med platform-legitimasjon(pin-kode, fingeravtrykk, ansikts-

gjenkjenning)
2. Autentisering med sikkerhetsnøkkel
3. Sluttside med link til intern nettside

Siden demoen skal benyttes til brukertesting, er det viktig å fokusere på et enkelt og "simplistisk" design. Brukeren blir presentert en egen side for hvert steg gjennom både registrering- og autentiserings-prosessen. Dette er for å begrense mengden valgmuligheter, for å tydeliggjøre det neste steget i prosessen. Teknikken med å begrense informasjonsmengden på en nettside for å forbedre brukervennligheten, er en god praksis, spesielt mtp. brukere som har kognitive utfordringer og lese- og skrive-vansker [27, Guideline 2].

Det vises også en fremgangs-måler på bunnen av siden, der brukeren hele tiden kan se hvilket steg av autentisering eller registrering de er på. De forskjellige stegene viser sin status gjennom en serie med animasjoner. En "loading" animasjon betyr at prosessen utføres for øyeblikket. En grønn "hake" viser at steget er ferdig, og rødt kryss viser at steget mislyktes. En blank sirkel viser at dette trinnet ikke er behandlet enda, og ikke behandles for øyeblikket. Bruk av såkalte "breadcrumbs" for å orientere brukeren, er også anbefalt ved generelt design, men spesielt i design for brukere med lese/skrive-vansker [27, Guideline G8].

Teknisk

Demonstrasjonen er bygd opp av flere komponenter, som i sin helhet lar brukeren autentisere seg hos tjenesten. Bruk av WebAuthn/FIDO2 krever en grunnleggende "mal" for dataflyten i designet, som det er forventet at utviklere skal ta utgangspunkt i ved utvikling av applikasjoner som skal bruke WebAuthn/FIDO2. Av denne årsaken har også denne demostrasjonen blitt utviklet utifra samme "mal". For mer informasjon om WebAuthn/FIDO2, se kapittel 2.1.4. En vanlig WebAuthn autentiseringsapplikasjon består av følgende komponenter:

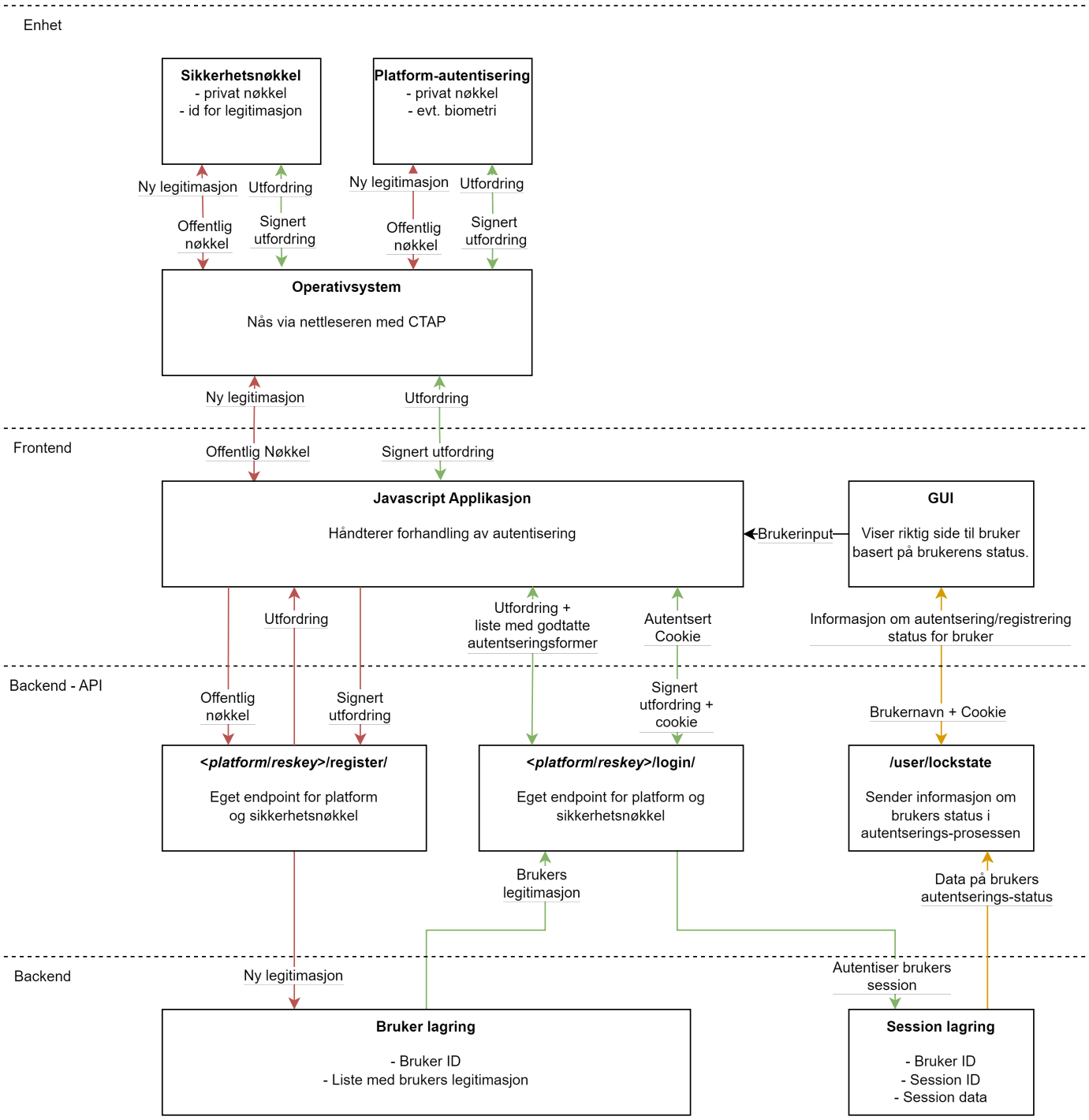
1. Relying party
2. Klient
3. Autentiserings-enhet

På et lavere nivå er applikasjonen bygd opp av følgende elementer:

1. Backend API
2. Fil-server
3. Javascript applikasjon i glsfrontend
4. Nettleser

5. Operativsystem m/platform autentiserings-enhet
6. Ekstern autentiserings-enhet

Dataflyten i applikasjonen følger stort sett samme struktur som vist i figur 2.1. Nedenfor er en forenklet domene-modell av dataflyten i programmet.



Figur 4.2: Domenemodell

Programmets interne design utgjør en liten forskjell fra standard-oppsettet med

at det meste av FIDO2 systemene er kodet "dobbelt opp". Dette er gjort for å håndtere de to autentiserings-faktorene som er krevet for å gjennomføre en autentisering. Dette inkluderer egne API endepunkt for registrering og innlogging, med platform-autentisering(biometri, pin-kode) og sikkerhetsnøkkel. Endepunktene for disse handlingene er dermed delt opp i to grupper, identifisert av begynnelsen på stien. Programmet autentiserer altså hver autentiserings-faktor som en separat prosess, som er logisk separert fra den andre autentiseringen.

Endepunkter for autentisering:

```
/api/v1/reskey/register/new
/api/v1/reskey/register/complete
/api/v1/reskey/login/init
/api/v1/reskey/login/complete
/api/v1/platform/register/new
/api/v1/platform/register/complete
/api/v1/platform/login/init
/api/v1/platform/login/complete
```

Bruk av cookie Programmet utnytter en kryptert cookie til å lagre informasjon om pågående autentiseringer, samt for å identifisere brukeren. Denne cookien kommer ikke frem i domenemodellen, men blir opprettet så snart brukeren har sendt et brukernavn til serveren for første gang, og beholdes frem til cookien ikke har blitt hentet på en time. Cookien slettes fra frontend når nettleseren lukkes, men varer ellers uendelig. Denne cookien identifiserer brukeren, og er knyttet til en lagret status for autentisering på serveren. For hver eksisterende cookie lagrer serveren et sant/usant flagg for begge faktorene, som brukeren må autentisere seg for. Disse flaggene vil deretter bli "hevet" hver for seg, ettersom brukeren autentiserer den gjeldene faktor ovenfor serveren. Forespørsler mot interne endepunkt vil kun være tilgjengelig om den tilknyttede cookien er registrert til at begge faktorene er satt til "sann".

4.1.4 Utviklingsprosess

Utviklingsprosessen for autentiserings-demostrasjonen var svært enkel. I begynnelsen ble det holdt et gruppemøte der et omtrentlig grensesnitt ble besluttet, og etter dette ble programmet utviklet ganske raskt. Det ble ikke gjort eksterne brukertester for programmet i løpet av utviklingen, og programmet gikk ikke gjennom store endringer som skilte seg fra planen før slutten av prosjektet. Da ble deler av

brukergrensesnittet endret til å bedre samsvare med pasientmodulen. Dette innebar endring av farger og generelt utseende.

Kvalitetssikring av programvaren ble utført ved hjelp av fagfellevurderinger fra gruppemedlemmene. Dette ble gjort som en del av utformingen av Kanban-tavlen beskrevet i kapittel 1.6. I tillegg ble testing ved hjelp av Golang's test-rammeverk implementert mot slutten av prosjektet.

Testing

Testing bidrar til å isolere deler av koden tilknyttet spesifikke funksjoner, og kan avdekke mindre problemer som kan eskalere til større, mer komplekse utfordringer. I dette tilfellet ble koden under utils- og session-mappene testet. Testing av handlers ble utelatt, siden httptest ble ekskludert på grunn av at backend ikke er hovedfokus for oppgaven. De gjennomførte testene dekket over 70% av koden. Testingen ble utført med Golang's innebygde testing-bibliotek og testify-biblioteket. Under er et eksempel på test av SetConfig-funksjonen:

```
package utils_test

import (
"testing"
"omhuDemo/utils"
"github.com/stretchr/testify/assert"
"github.com/go-webauthn/webauthn/protocol"
)

func TestSetConfig(t *testing.T) {
// Call the SetConfig function
err := utils.SetConfig()

// Check if there are no errors
assert.NoError(t, err, "SetConfig should not return an error")

// Check if the WebAuthn object is initialized
assert.NotNil(t, utils.WebAuthn, "WebAuthn should be initialized after calling SetConfig")

// Check if the SessionStore object is initialized
assert.NotNil(t, utils.SessionStore, "SessionStore should be initialized after calling SetConfig")
}
```

Denne testfunksjonen validerer at SetConfig-funksjonen i utils-pakken fungerer som den skal. Testen inneholder tre hovedsjekker:

- Ingen feil: Testen bekrefter at SetConfig ikke returnerer noen feil, noe som

indikerer at funksjonen kjører problemfritt.
- WebAuthn initialisert: Den sjekker om WebAuthn-objektet, som er sentralt i autentiseringsprosessen, er riktig initialisert og ikke null.
- SessionStore initialisert: På samme måte sikrer testen at SessionStore, som kan være ansvarlig for håndtering av brukersesjoner, også er korrekt initialisert.

Disse sjekkene er essensielle for å sikre at kritiske systemkomponenter er operative og feilfrie, noe som bidrar til kodens pålitelighet.

4.1.5 Challenge-respons autentisering med WebAuthn

Dette avsnittet er en teorietisk gjennomgang av en challenge-respons autentisering, som blir utført i blant annet WebAuthn.

Prosessen begynner med at nettsiden mottar og lagrer en offentlig nøkkel generert i autentiseringsenheten. Denne brukes til å kryptere en lang, tilfeldig streng av bokstaver og tall kalt en "utfordring"[13]. Den krypterte utfordringen sendes deretter fra serveren til den lokale nettsiden på brukerens enhet, som bruker WebAuthn API for å videreformidle utfordringen til autentiseringsenheten gjennom operativsystemet, for eksempel fingeravtrykk, PIN-kode, ansiktsgjenkjenning eller sikkerhetsnøkkel[28]. Autentiseringsenheten autentiserer brukeren på sin egen måte, dersom autentiseringen er vellykket, blir utfordringen"signert". Dette betyr at den dekrypteres med den private nøkkelen som er plassert i autentiseringsenheten. Den signerte utfordringen sendes tilbake til serveren, der den sammenlignes med den opprinnelige utfordringen før kryptering. Hvis den ukrypterte utfordringen er identisk med den signerte utfordringen som sendes tilbake fra autentiseringsenheten, var autentiseringen vellykket [29].

4.1.6 Implementasjon

For å implementere webauthn autentisering ble programmet utviklet basert på en fremgangsmåte skrevet av Herbie Bolimovsky, programutvikler og tidligere ansatt for Apple. Nettsiden kan bli funnet under følgende kilde [30].

Enkelte deler av koden, spesifikt delen innenfor `/pub/auth/relyingparty.js`, samt `/handler/register.go` og `/handler/login.go` er basert på kode-eksempelene gitt i denne fremgangsmåten. Enkelte beslutninger, som det å bruke jQuery, ble også gjort som en følge av Bolimovsky's blogg-innlegg.

Programmet er som tidligere nevnt bygd opp ved bruk av go-WebAuthn biblioteket i golang, samt gorilla til design av cookies. I frontend utnyttes WebAuthn til å gjennomføre autentiserings-handlinger. Nedenfor er et utvalg av kode-eksempeler på de kritiske delene av programmets utførelse:

Registrering

Det første kritiske steget i autentiserings-prosessen begynner ved at brukeren kontakter serveren og forespør skapelsen av en ny legitimasjon. jQuery brukes for å sende en GET forespørsel mot serveren. Ettersom brukeren ikke har registrert WebAuthn-autentisering ennå, benyttes et

Om den midlertidige legitimasjonen er gyldig, vil serveren sende tilbake en datastruktur med innstillinger nødvendig for skapelsen av en ny legitimasjon. Denne datastrukturen er definert i WebAuthn som "*publicKeyCredentialCreationOptions*", og inneholder informasjon på f.eks hva slags type autentisering som skal brukes, hvem som forespør m.m. Dette objektet sendes videre gjennom WebAuthn API'et med funksjonen `navigator.credentials.create()`. Fra dette tidspunktet vil nettleseren kommunisere med operativsystemet, og håndtere resten av opprettelsen av en ny legitimasjon på autentiseringsenheten.

```
$.get(
    createApiUrl(
        "api/v1/" + authType + "/register/new?username=" + username + "&hash=" + hashedPassword
    ),
    null,
    function (data) { return data; },
    'json'
).then((credentialCreationOptions) => {
    credentialCreationOptions.publicKey.challenge = bufferDecode(
        credentialCreationOptions.publicKey.challenge
    );
    credentialCreationOptions.publicKey.user.id = bufferDecode(
        credentialCreationOptions.publicKey.user.id
    );

    return navigator.credentials.create({ publicKey: credentialCreationOptions.publicKey });
})
```

Frontend - Fullføring av registrering. WebAuthn-funksjonen vil returnere et nytt objekt, som sendes tilbake til serveren med en POST forespørsel:

```
.then((credential) => {
```

```
    let attestationObject = credential.response.attestationObject;
    let clientDataJSON = credential.response.clientDataJSON;
    let rawId = credential.rawId;

    $.post(
        "/api/v1/" + authType + "/register/complete?username=" +
        username + "&hash=" + hashedPassword,
        JSON.stringify({
            id: credential.id,
            rawId: bufferEncode(rawId),
            type: credential.type,
            response: {
                attestationObject: bufferEncode(attestationObject),
                clientDataJSON: bufferEncode(clientDataJSON),
            }
        }),
        function (data) { return data; },
        'json'
    ).then((success) => {
        resolve(true);
    })
})
```

På backend håndteres de mer komplekse operasjonene lettvint av WebAuthn biblioteket.

Backend - Begynnelse av registrering. Etter at serveren mottar en forespørsel om å operette ny legitimasjon, hentes de relevante konfigurasjons-objekter og pakkes inn til et *publicKeyCredentialCreationOptions* objekt, som sendes tilbake til klienten(ikke inkludert i kode-snipp). Session-data om den pågående registreringsprosessen lagres i en session store, og en samsvarende cookie sendes til klienten som del av retur-pakken. I golang er variabelen *r* den innkommende forespørselen, og *w* det utgående svaret til klienten (*request* og *responseWriter*).

```
// generate PublicKeyCredentialCreationOptions and session data for user
options, sessionData, err := webAuthn.BeginRegistration(
    user,
    //Set type of authentication with config provided as parameter
    webauthn.WithAuthenticatorSelection(config),
)

// store session data as marshaled JSON
err = sessionStore.SaveWebauthnSession(sessionKey, sessionData, r, w)
```

Backend - Fullføring av registrering. Etter at serveren mottar en offentlig nøkkel fra klienten, lagres denne enkelt i *WebAuthn* objektet, som er en del av We-

bAuthn biblioteket. Session påbegynt i forrige steg hentes ut med hjelp av cookien festet til forespørselen.

```
//Complete registration of new credential
credential, err := webAuthn.FinishRegistration(user, sessionData, r)

// load data from the previous step of the registration
sessionData, err := sessionStore.GetWebauthnSession(sessionKey, r)

//save credential to user
user.AddPlatformCredential(*credential)
```

4.1.7 Innlogging

Koden som håndterer innlogging(autentisering), er strukturelt bygd opp nokså lik som registrering, men med mindre variasjoner i hva som blir sendt. I likhet med registrering, består prosessen av to frem-og-tilbake kommunikasjoner mellom front-end og back-end.

Frontend - Begynnelse av innlogging. Det første steget for klienten, er å forespørre en autentisering fra serveren. Dette gjøres med en GET forespørsel. Her er det ikke nødvendig å autentisere brukeren med passord, slik som med registrering, så alle kan i prinsippet initialisere en autentisering med en hvilken som helst bruker. Etter at forespørselen er sendt, vil serveren svare med et *credentialRequestOptions* objekt, som inneholder en utfordring, samt en liste med de gyldige legitimasjonene som kan benyttes til å signere utfordringen.

Denne listen hentes fra brukerens kontoinformasjon i serveren. Om ingenting er registrert, vil dette feile ettersom det ikke er noe å hente. I denne implementasjonen sendes kun ID'ene til de autentiserings-enhetene som samsvarer med faktoren som skal autentiseres for. Med andre ord; Dersom brukeren forsøker å logge inn med fingeravtrykk, vil ikke deres registrerte sikkerhetsnøkler sendes på dette tidspunktet.

Etter at klienten mottar innstillingene, kan de sendes videre til operativsystemet gjennom WebAuthn API'en bygget inn i javascript med metoden: `navigator.credentials.get();`. Herfra tar nettleseren og operativsystemet over, og kommuniserer innstillingene til den rette autentiserings-enheten utifra hva som var inkludert på listen over gyldige enheter.

```
$.get(
```

```
        createApiUrl('api/v1/' + authType + '/login/init?username=' + username),
        null,
        function (data) {
            return data;
        },
        'json'
    ).then((credentialRequestOptions) => {
        credentialRequestOptions.publicKey.challenge = bufferDecode(
            credentialRequestOptions.publicKey.challenge
        );
        credentialRequestOptions.publicKey.allowCredentials.forEach(function (listItem) {
            listItem.id = bufferDecode(listItem.id);
        });
        return navigator.credentials.get({
            publicKey: credentialRequestOptions.publicKey
        });
    })
```

Backend - Begynnelse av innlogging. På backenden håndteres det første steget med å hente alle lovlige autentiserings-enheter som brukeren har registrert. Parameteret `sessionKey` spesifiserer om det skal hentes ID'er av typen sikkerhetsnøkkel eller platform-autentisering. Disse enhetene pakkes deretter inn i et objekt `credentialDescriptors`, og kjøres gjennom WebAuthn-objektets metode for å registrere begynnelsen på et autentiserings-forsøk. Dette vil returnere innstillingene som skal sendes til brukeren, samt en ny session som lagres på serveren og knyttes til en cookie som sendes tilbake.

```
//get allowed credentials for user
credentials = user.WebAuthnCredentialsByKey(sessionKey)

// Convert the credentials to credential descriptors
credentialDescriptors := make([]protocol.CredentialDescriptor, len(credentials))
for i, cred := range credentials {
    credentialDescriptors[i] = protocol.CredentialDescriptor{
        Type: protocol.PublicKeyCredentialType,
        CredentialID: cred.ID,
    }
}

// generate PublicKeyCredentialRequestOptions, session data
options, sessionData, err := webAuthn.BeginLogin(
    user,
    webauthn.WithAllowedCredentials(credentialDescriptors)
)

// store session data as marshaled JSON
err = sessionStore.SaveWebauthnSession(sessionKey, sessionData, r, w)

//Return options to client
utils.JsonResponse(w, options, http.StatusOK)
```

Frontend - Fullføring av innlogging. Når den offentlige nøkkelen er sendt til klienten's operativsystem via WebAuthn API, vil operativsystemet, ved vellykket autentisering, returnere et objekt kalt *assertion*. Dette objektet inneholder blant annet den signerte utfordringen. Deretter pakkes dette objektet inn og sendes tilbake til serveren.

```
.then((assertion) => {

    //Variables
    let authData = assertion.response.authenticatorData;
    let clientDataJSON = assertion.response.clientDataJSON;
    let rawId = assertion.rawId;
    let sig = assertion.response.signature;
    let userHandle = assertion.response.userHandle;

    //Post request to server
    $.post(
        'api/v1/' + authType + '/login/complete?username=' + username,
        JSON.stringify({
            id: assertion.id,
            rawId: bufferEncode(rawId),
            type: assertion.type,
            response: {
                authenticatorData: bufferEncode(authData),
                clientDataJSON: bufferEncode(clientDataJSON),
                signature: bufferEncode(sig),
                userHandle: bufferEncode(userHandle),
            },
        }),
        function (data) {
            return data;
        },
        'json'
    ).then((success) => {
        resolve(true); // Resolve with true if login is successful
    }).catch((error) => {
        reject(false); // Reject with false if login fails
    });
})
```

Backend - Fullføring av innlogging. Serveren mottar *assertion*-objektet fra klienten og verifiserer signaturen mot den lagrede offentlige nøkkelen ved hjelp av *WebAuthn*-objektet. Ved vellykket autentisering oppdateres cookiene for å markere brukerens session som autentisert.

```
// load the session data
sessionData, err := sessionStore.GetWebauthnSession(sessionKey, r)

// Check credential
```

```
_, err = webAuthn.FinishLogin(user, sessionData, r)
if err != nil { //Send error message if authentication was not successful
    return utils.WrapError(err,http.StatusUnauthorized,"Autentisering mislykkes.",0,"Authentication failed.")
}

//Create new authentication data to be stored in session
newAuthData := ...
..
..

// Save new authentication data to users session
sessionStore.SaveAuthSession(newAuthData,r,w);

//Return OK
utils.JsonResponse(w, newAuthData, http.StatusOK)
```

Overnevnte kode-snipper er de mest kritiske delene av hele autentiserings-prosessen.

4.1.8 Installasjon

For å kjøre applikasjonen ble det besluttet å bruke NTNU's egen skytjeneste, "SkyHigh"[1], ettersom det her var mulig å få tildelt ressurser til bruk i faglig sammenheng. En global IP-adresse ble også utdelt, som demoen nå er knyttet til.

Siden alle WebAuthn JavaScript-funksjoner krever HTTPS for å fungere, var det nødvendig å implementere SSL i demonstrasjonen. For å oppnå dette ble det anskaffet et domene, som deretter ble sertifisert ved hjelp av *certbot*[2].

Det ble vurdert å ta i bruk continuous integration and continuous delivery/deployment (CI/CD), for å kontinuerlig "pushe" endringer i koden ut i produksjon, altså til den virtuelle maskinen i SkyHigh. Grunnet tidsbegrensninger ble dette ikke gjennomført. Det ble i stedet benyttet et script for å automatisk trekke ned git-repoet, og kjøre koden med en kommando på den virtuelle maskinen i SkyHigh. Dette ble et enklere, men akseptabelt alternativ til CI/CD-metodikker.

Administrator-grensesnitt

For opprettelse av nye brukere ble det implementert et administratorgrensesnitt som del av API'et til autentiserings-demoen. Her er det mulig å opprette brukere,

[1] SkyHigh, NTNU's egen skytjeneste basert på Openstack https://www.ntnu.no/wiki/display/skyhigh

[2] Dokumentasjonen for denne prosessen er tilgjengelig på https://certbot.eff.org

samt se informasjonen til eksisterende brukere. Merk at denne funksjonaliteten ikke reflekterer en reell implementasjon, og kun er til stede for praktiske formål relatert til demoen.

For å opprette en bruker til demoen brukes følgende endepunkt:

```
https://omhu.raphaelstorm.no/api/v1/admin/createuser?username=<brukernavn>
```

Dette vil opprette en bruker med et valgfritt brukernavn, og deretter returnere et JSON objekt med informasjon om kontoen, inkludert engangspassordet nødvendig for å registrere brukeren. Engangspassordet ligger under *FirstlogonPass* og vil se noe ut som dette `"FirstlogonPass": "BJ762F5S",`.

For å vise informasjon om en eksisterende bruker, kan en bruke følgende endepunkt:

```
https://omhu.raphaelstorm.no/api/v1/admin/viewuser?username=<brukernavn>.
```

4.2 Utvikling av prototype for pasientmodul

Dette kapittelet omhandler prosessen rundt utviklingen av en prototype for et nytt design av Omhu. Dette designet skal basere seg på den allerede eksisterende web-applikasjonen, men skal være tilpasset målgruppen. I dette kapittelet skal krav, utførelse og teknologi-valg design-valg for grensesnittet, samt teknisk design for prototypen, bli gjennomgått. Ettersom oppgaven fokuserer på brukervennlighet, er dette noe som blir vektlagt gjennom utvilings-prosessen.

4.2.1 Kravspesifikasjon

I oppgavebeskrivelsen star det at gruppen skal kartlegge og designe en pasient-modul av Omhu. MVP er kort for "Minimum Viable Product", som kan oversettes til "minste brukbare produkt". Etter samtaler med oppdragsgiver kom det frem at en "prototype" er et mer passelig begrep for oppgaven, ettersom dette ikke krever et resultat bestående av et funksjonelt produkt, men heller en tidlig utgave med det formål å teste forskjellige design-konsepter på. Dette var mer i tråd med oppdragsgiver' ønske.

Utrykket "pasientmodul" blir også brukt i oppgaveteksten. I denne oppgaven har dette blitt definert som **et sett med inkluderte funksjonaliteter, samt det tilhørende grafiske grensesnittet for å benytte seg av disse funksjonalitetene**.

Den grunnleggende kravspesifikasjonen som lagt frem av oppgavebeskrivelsen er som følger:

1. Designe en pasientmodul av Omhu som inkluderer følgende funksjonalitet:
    a. Side for "dashbord' som viser en sluttbrukers dags-plan og fremtidige aktiviteter.
    b. Side for "aktivitets-plan" der brukere kan opprette nye aktiviteter og se ansattes tilgjengelighets-status. Maler kan utnyttes for å raskt lage aktiviteter.
2. Funksjonalitetene tilbudt i pasientmodulen skal være lette og venne seg til, og lett å bli benyttet av pasienter med forskjellige forutsetninger. Som nevnt i kapittel 2.4, er målgruppen mennesker med lettere psykiske funksjonshemninger.

Denne kravspesifikasjonen er bevisst utformet for å være fleksibel, slik at gruppen får større frihet i valg av utførelse. Minstekravet kan oppfylles med en enkel wireframe. I dette prosjektet er det imidlertid ønsket å gjennomføre brukertes-

ter for å få et målbart resultat på designkvaliteten, noe som er utfordrende med kun en wireframe. Derfor ble det besluttet å produsere designet som et interaktivt grensesnitt i form av en nettside. Målet er at en slik prototype skal ligge nærmere et potensielt ekte produkt, og dermed gi bedre og mer pålitelige data.

Ettersom det ble bestemt at pasientmodulen skal være interaktiv, ble kravspesifikasjonen utvidet til å inkludere tekniske krav for nettsiden. Støtten for bruk av maler, ble utvidet fra å kun være mulig å lese, til å også kunne bli opprettet og redigert.

1. Et interaktivt brukergrensesnitt som kan navigeres av brukeren uten direkte innflytelse fra en test-moderator(*Som f.eks når en manuelt må bytte vinduer på en papir-wireframe*).
2. Pasientmodulen skal være tilgjengelig som en nettside i Google Chrome nettleser for Android og IOS (Vår 2024).
3. Pasientmodulen skal være designet med en mobil-først tilnærming.
4. Pasientmodulen skal ha følgene funksjonalitet utover det spesifisert i minimumskravet:
    a. Mulighet for å opprette aktivitets-maler
    b. Mulighet for å rapportere manglende eller dårlig utførelse av en aktivitet

4.2.2 Valg av teknologier og verktøy

Valgene av teknologier og verktøy for utviklingen ble besluttet på grunnlag av kravspesifikasjonen lagt frem fra oppdragsgiver, samt de interne ønskene satt i prosjektet. Nedenfor er en liste med de teknologiene som ble brukt til formålet:

HTML, CSS, JS Den grunnleggende kombinasjonen for web-utvikling.

jQuery Et populært tredjeparts bibliotek for javascript med mange forskjellige funksjonaliteter. I dette prosjektet var det hovedsaklig de lettvinte animasjonene som ble utnyttet fra denne pakken.

golang Golang ble brukt for å "hoste" filserveren der nettsiden var plassert.

Teknologivalgene er dermed nokså grunnleggende. Ettersom utvikling av pasientmodulen fokuserte på å undersøke brukeropplevelsen, i motseting til autentiseringsdemoen der målet var å demonstrere tekniske konsepter, var det naturlig å velge en tidsbesparende løsning.

Tidligere i prosjektet ble det vurdert å utnytte rammeverket **Svelte** for denne delen av prosjektet, ettersom WeissTech selv planlegger å bytte til dette rammeverket i fremtiden (se vedlegg N). Det ble vurdert som unødvendig å bruke tid på å lære et nytt rammeverk for en enkel prototype, som ikke skal direkte ut i produksjon.

4.2.3 Utviklingsprosess

1. **Identifikasjon av problemområde** - Hva skal designet løse?
2. **Forslag til høy-level design** - Brainstorming og produksjon av wireframes.
3. **Utvikling av førsteutkast** - Produksjon av nettsiden basert på wireframe.
4. **Testing** - Brukertesting for å avdekke feil og mangler
5. **Forbedring** - Endring av design, legge til og fjerne funksjonalitet basert på resultat av brukertester.
6. *Tilbake til steg 4. Fortsett med iterasjoner og testing om mulig.*

Utviklingsprosessen er basert på en SDLC prosess av kontinuerlig testing og forbedring, men uten delene knyttet til drift og vedlikehold. Det ble planlagt minst to iterasjoner, noe som ble gjennomført. Versjonene ble lagret i egne grener i git-repoet under V1, V2 og V3. Alle oppgaver relatert til koding, design og informasjonssamling ble gjort med Kanban, som nevnt i kapittel 1.6.

4.2.4 Design

I dette underkapittelet vil det ferdige designet, versjon 3, bli gjennomgått. Neste seksjon vil gjennomgå tidligere iterasjoner av pasientmodulen og endringene gjort mellom iterasjonene.

Grensesnittet er utviklet basert på retningslinjene fra WCAG, "Design of Everyday Things" av Don Norman og "The elements of user experience" av Jesse James Garrett. For kilder mer skreddersydd for målgruppen benyttes grunnprinsippene utarbeidet i "Interface design guidelines for low literature users: a literature review" publisert i ACM i 2023 [27].

De viktigste beslutningene angående design vi har gjort i pasientmodulen, har tatt utgangpspunkt i de fem elementene av design, beskrevet i boka "The elements of user experience" [31].

Elementene av design:

1. *Strategy plane*, referert til som *strategi plan*.
2. *Scope plane*, refert til som *ramme-plan*.
3. *Structure plane*, referert til som *strukturelt plan*.
4. *Skeleton plane*, referert til som *skjelett plan*.
5. *Surface plane*, referert til som *overfladisk plan*.

Strategi- og ramme-plan: Valg av funksjonalitet

Ifølge Garrett er det øverste "planet" av design, strategi-planet. Dette omhandler formålet med nettsiden, og hva brukerene av siden ønsker å oppnå. Dette planet er irrelevant i denne oppgaven, ettersom Omhu allerede er en etablert tjeneste med formål og kundebase. Design-valget i dette planet er derfor kravspesifikasjonen og innledningen til denne rapporten.

Ramme-planet, som er det neste planet, omhandler hvilke funksjonaliteter som skal være på nettsiden, og hvordan de passer sammen. De grunnleggende egenskapene til pasientmodulen er allerede definert i kravspesifikasjonen og den allerede eksisterende Omhu. For å se hvordan Omhu for ansatte ser ut per dags dato (se vedlegg J).

Funksjonalitet i eksisterende Omhu:

1. Kalendervisning av fremtidige aktiviteter
2. Sammenligne timeplaner mellom ansatte og brukere.
3. Opprette nye aktiviteter med ansatt, bruker, tidspunkt og andre detaljer som medisiner og lignende.
4. Opprette og bruke maler for aktiviteter for å effektivisere bruk av applikasjonen.

Dette er de grunnleggende egenskapene innenfor rammene til den originale Omhu, som per dags dato blir brukt av ansatte i helsesektoren. Målgruppa som vil benytte pasientmodulen har derimot andre behov og begrensninger.

Derfor har det blitt gjort følgende endringer i rammene av pasientmodulen:

Kalendervisning Dashbordet i Omhu som viser dagens aktiviteter har blitt omgjort til "Oversikt" i denne pasientmodulen. Kalenderen er erstattet med en mer kompakt liste av kommende aktiviteter for å vise flere hendelser samtidig og lengre frem i tid uten behov for blarbevegelser. Målet er å gi brukeren en bedre oversikt over fremtidige hendelser uten å fokusere på timevisning, basert på antakelsen om at sluttbrukere ikke trenger en detaljert timeplan

som de ansatte. Denne tilnærmingen reduserer mengden informasjon som vises for å forbedre brukervennligheten [27, G2].

Sammenligning: Ettersom Omhu per dags dato er et organiseringsverktøy for ansatte, har de nå mulighet til å sammenligne timeplan mellom kollegaer og pasienter. Det er derimot problematisk å gi pasienter full tilgang på de ansattes timeplan (se vedlegg L). Derfor vil rammene for pasientmodulen gi tilgang til en binær status for hver ansatt, som kun sier om vedkommede er tilgjengelig eller ikke. Funksjonen vil integreres i aktivitetsredigeringsverktøyet samt kalendersiden.

Opprette ny aktivitet: Målet er at sluttbrukere fortsatt skal være i stand til å opprette nye aktiviteter på egen hånd. Sensitive detaljer som f.eks medisiner kan derimot ikke integreres i pasientmodulen grunnet applikasjonens sikkerhetsnivå. Det har også kommet frem at å la pasientene velge en ansatt som de ønsker skal være med på en aktivitet, ikke alltid vil la seg gjøre pga. digitale turnus-system (se vedlegg L).

Opprettelse av maler: Maler vil fortsatt være tilgjengelig for sluttbrukere, men igjen i en enklere form. Systemet for maler har vist seg å være en utfordrende del av designet, noe som blir næremere diskutert på et lavere plan.

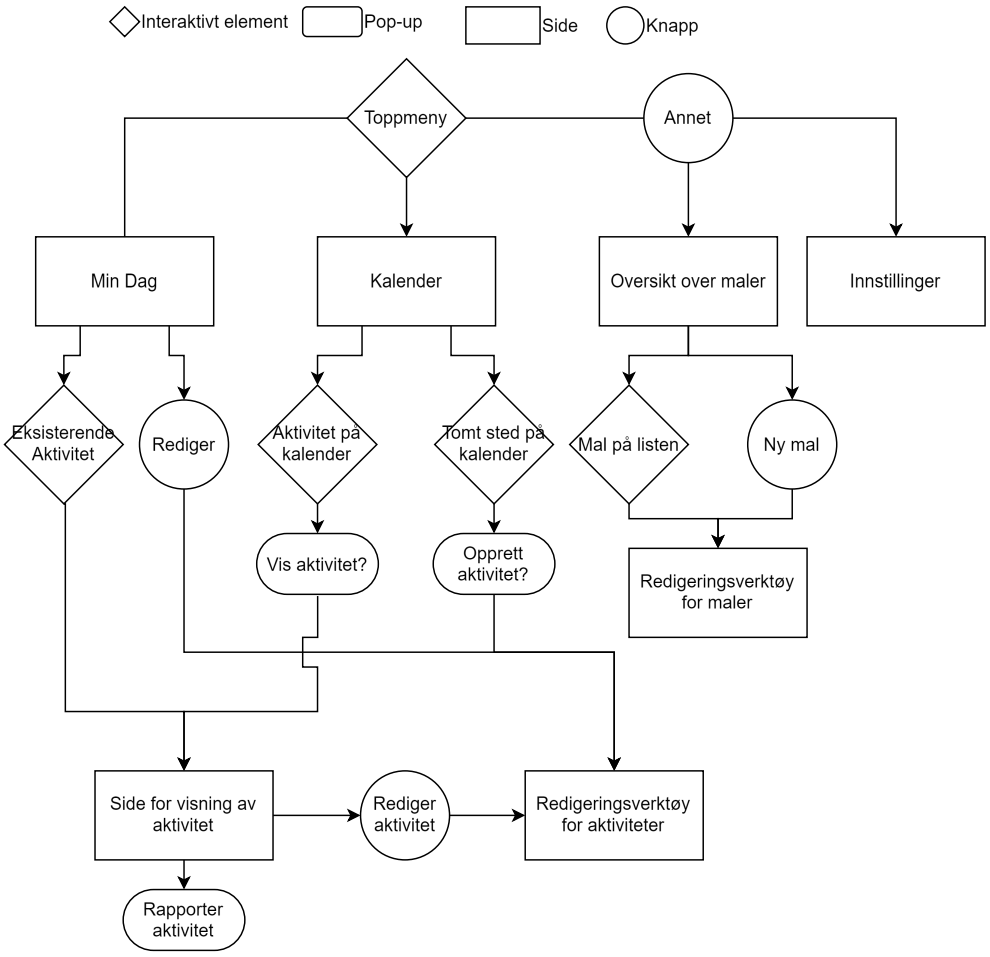
Det ble også inkludert ny funksjonalitet som ikke eksisterer i den nåværende versjonen av Omhu:

Rapportering av aktiviteter: Et av målene for dette prosjektet var å gi sluttbrukerene av BPA-ordninger, muligheten til egenrapportering. Dette innebærer at pasientene kan gi tilbakemelding på dårlig utført jobb eller uønskede hendelser. For å oppnå dette målet vil pasientmodulen inneholde funksjonalitet for å rapportere aktiviteter, og på denne måten senke terskelen for rapportering av problemer.

Strukturelt plan: Navigasjon og informasjonsmodell

Det strukturelle planet omhandler en nettsides mulighet for navigasjon, og om sammenhengen mellom forskjellige sider i applikasjonen [31]. Utgangspunktet for denne delen av designet er lånt fra den eksisterende Omhu, med to hovedsider: en for dashbord og en for "arbeidsplan". Designet av pasientmodulen har tatt utgangspunkt i disse.

Figur 4.3 inneholder et "sitemap", altså en oversikt over pasientmodulens sider og oppkoblingene mellom dem. Videre i denne seksjonen vil det gjøres en gjennomgang av viktige sider og funksjonaliteter implementert på det strukturelle planet.



Figur 4.3: Sitemap for pasientmodul versjon 3

Hovedsider: "Oversikt" er det som før var dashbord, og "kalender" er det som før var arbeidsplanen. Disse to sidene gir begge muligheter til å observere, inspisere og opprette aktiviteter, på ulike måter. Kalenderen er mer skreddersydd for opprettelse og planlegging av aktiviteter, mens "Min dag" er rettet mot observasjon og oversikt av alle fremtidige aktiviteter.

Vis aktivitet: Det ble også laget en ny side for visning av spesifikke aktiviteter. Denne siden inneholder mer detaljert informasjon om aktiviteten, samt knapper for å redigere aktiviteten eller rapportere den om den ikke ble gjennomført som forventet.

Redigeringsverktøy: Via flere av disse sidene er det mulig å navigere inn på redigeringsverktøyet for aktiviteter. Denne siden brukes for å opprette nye aktiviteter med tidspunkt, beskrivelse, tittel og valg av ansatte(om dette er

muliggjort). Her er det også mulig å raskt fylle ut informasjonen om aktiviteten basert på en mal brukeren kan lage selv.

Maler: Merk at under detaljene av tidligere versjoner i kapittel 4.2.5 kan det merkes at det tidligere var mulig å opprette nye maler i det samme redigeringsverktøyet, som en bruker til opprettelse av aktiviteter. Denne funksjonaliteten ble derimot flyttet til en egen side, da test-deltagere hadde vanskeligheter med å forstå to-i-en systemet i redigeringssiden (se kapittel 5.2.2 for resultater).

For å få plass til redigeringsverktøy for maler, ble det opprettet en ny side tilgjengelig via en ny knapp i toppnavigerings-menyen. Denne knappen, "annet", viser en nedtrekksmeny som lar brukeren navigere til oversikten av maler, eller innstillingene. Fra siden med oversikt av maler kan brukeren igjen trykke seg inn på en mal, eller opprette en ny fra bunnen av for å se redigerings-siden for maler.

Den ekstra siden dedikert til behandling av maler medfører at det kommer en ekstra knapp i hovednavigasjonsmenyen. Selv om dette gjør strukturen av pasientmodulen kompleks, er det verdt det for å forenkle redigeringssiden for aktiviteter, som vil bli brukt vesentlig mer enn siden for redigering av mal. Denne beslutningen støttes av både G1 og G2 som forklart i "Interface design guidelines for low literature users"[27]: 1) "*Hold designet minimalistisk*" og 2) "*Kun vis den informasjonen som er nødvendig*". Spesielt for brukere som sliter med lesing og skriving, er det fordelaktig å fordele informasjonen over flere sider, heller enn å minimere mengden sider.

Toppmeny: Toppmenyen i pasientmodulen er hovedverktøyet som vil bli benyttet til å navigere på nettsiden. Personer med skrive/lesevansker foretrekker navigasjonsmenyer der alt informasjonen vises på skjermen samtidig, uten bruk av undermenyer[27]. De to hovedsidene har dermed beholdt en posisjon direkte i toppmenyen, mens diverse andre sider som "behandling av maler" og "innstillinger", er plassert i en drop-down meny plassert under knappen "annet" i topp-navigasjonsmenyen.

Bruken av en nedtrekksmeny i toppnavigasjonsmenyen er et bevisst designvalg, selv om det er direkte motstridene til kilden som nettopp ble brukt. Tanken bak bruken av en slik meny er at funksjonaliteten på disse sidene antageligvis er utenfor mestringsnivået for flesteparten av sluttbrukerene, og at det dermed er mest brukervennlig å hjemme de vekk, slik at brukere ikke navigerer dit med et uhell. I denne situasjonen er den beste muligheten å fjerne disse sidene i sin helhet, men dette ble besluttet til å være urealistisk, da funksjonene for behandling av maler og innstillinger for siden er en viktig del av applikasjonen. Om sluttbrukeren trenger en funksjon som er tilgjengelig på en av disse sidene, vil en ansatt antageligvis ikke ha problem med å navigere gjennom menyen for å hjelpe sluttbrukeren. Ettersom disse

egenskapene er vesentlig mindre brukt enn de andre sidene i pasientmodulen, vil ikke dette være et stort problem ved bruk av applikasjonen.

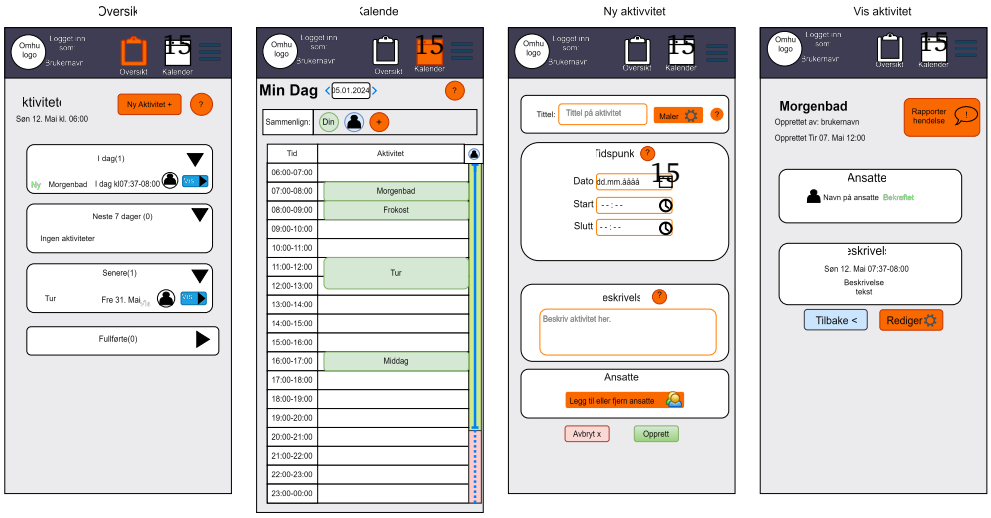
Breadcrumbs: "Interface design guidelines for low literature users" spesifiserer at det er viktig og alltid gi brukeren en pekepin på hvor de befinner seg i applikasjonen. Dette gjøres vanligvis med såkalte "breadcrumbs", eller "brødsmuler"[27]. Dette er en meny på siden som viser historikken av navigasjonen utført. Brødsmuler har typisk følgende format: `/hjem/min side/profilbilde`. For pasientmodulen har denne egenskapen derimot ikke blitt implementert. Dette valget ble gjort da pasientmodulen ikke har nok "dybde" til å rettferdiggjøre å legge til mer informasjon på siden. Det ble ikke avdekket noen problemer med navigasjonen på siden under brukertestingen, og det kan dermed sies at brødsmuler er unødvendig for modulens bruk.

Angring: Det blir påpekt at det allid er viktig å presentere brukeren med muligheter for å angre eller navigere tilbake til forrige side [27]. Dette prinsippet er implementert i pasientmodulen med bruk av "avbryt" eller "tilbake" knapper plassert på alle sider som er dypere enn øverste lag av strukturen.

Skjelettplan: Sideoppsett

Skjelettplanet omhandler plassering av konkrete elementer, samt hvordan det totale sideoppsettet er strukturert [31]. Design-valgene tatt her, er i høy grad påvirket av hvordan informasjonen og interaktive elementer kan presenteres på en mest mulig ryddig og oversiktlig måte. I denne seksjonen blir det ikke henvist til konkrete eksempler, men prinsipper som har blitt brukt i utviklingen.

En av de viktigste faktorene som kan påvirke designvalg på dette planet er hvilken plattform nettsiden skal bli brukt på. I henhold til kravspesifikasjonen skal pasientmodulen utvikles med en mobile-first approach. Designet skal dermed først og fremst bygges for å passe til en vertikal, liten skjerm, og å tilpasse og integrere touch-egenskaper på best mulig vis. Utviklingen av nettsiden har blitt fullført fra start til slutt med disse prinsippene i sentrum. Denne tilnærmingen til utvikling spiller størst rolle når skjelettplanet skal designes.



Figur 4.4: Wireframe for V3 - Del 2

Sideoppsett: Skjermen på en mobiltelefon er langt mindre, og har en annen høyde/bredde forhold enn en tradisjonell datamaskin, noe som begrenser hvor mye informasjon som kan få plass på skjermen uten at det blir uoversiktlig. Dette hviste seg å ikke være et så stort problem, ettersom retningslinjene i "Interface design guidelines for low literature users" går godt sammen med egenskapene til en mobiltelefon. I artikkelen blir det beskrevet at nettsider for personer med lese/skrivevansker burde være designet med en minimalistisk tilnærming, og at informasjon på en side burde begrenses til det absolutt minimum. Informasjonen burde presenteres fra topp til bunn, i en sekvensiell stil der det viktigste på siden blir presentert først. Artikkelen fraråder også bruk av design med mye informasjon plassert horisontalt ovenfor hverandre, ettersom slike brukere ofte kan mangle den intuitive evnen til å "scanne" en side. For å implementere dette prinsippet inn i designet er hver side i pasientmodulen bestående av en enkel kolonne, der den viktigste informasjonen er presentert på toppen.

Tomrom og bokser: Gjennom designet er det også blitt benyttet flere midler for å kommunisere separasjon og relasjon mellom elementer på skjermen. Tilhørende elementer er innrammet i felles bokser. De separerte boksene bidrar til å tydeliggjøre hvilken elementer det er som samhandler med hverandre, og definerer en ramme som brukeren kan fokusere på. Den samme studien beskriver også hvordan det er viktig å separere elementer for å ikke overvelde brukeren[27].

Toppmeny: Hovedmenyen på den eksisterende Omhu er plassert til høyre på siden i en vertikal konfigurasjon. Det ble tidlig besluttet at denne menyen skulle flyttes til toppen av skjermen i en horisontal konfigurasjon, for å best

utnytte plassen på mobilskjermer, som vanligvis brukes i en horisontal retning. Topp-menyen på siden er et konstant element som aldri forsvinner, uansett hvor brukeren befinner seg i pasientmodulen. Dette gir brukeren mulighet til å når som helst navigere seg tilbake til en av hovedsidene.

Pop-up sider: Det blir også benyttet "pop-up" sider i designet av pasientmodulen. Disse sidene dekker ikke hele skjermen, og lar den tidligere siden være synlig i en uskarp tilstand bak pop-up elementet. Pop-up'sene gjør det mulig å plassere innhold som ikke passer seg direkte på siden. Dette tiltaket bidrar til å rydde opp pasientmodulen, noe som er spesielt viktig for denne målgruppen [27].

Overfladisk plan: Feilmeldinger og fargekoding

Det overfladiske planet omhandler spesifikke elementer på siden, og designvalg rundt farger, utsende, tekst og animasjon [31]. Det er ofte dette planet som er mest avgjørende for brukeropplevelsen.

Fargekoding: Farger er brukt som virkemiddel i pasientmodulen. Ved å knytte farger opp til korresponderende konsepter, kan en underbevist lede brukeren gjennom designet. I pasientmodulen brukes fargene oransje, rød, grønn og blå for å kommunisere forskjellige egenskaper av elementer.

- **Rød** er en farge som kan assosieres med negativitet[32], og brukes for feilmeldinger og avbrytende handlinger. Fargen brukes i tekst og rammer rundt feilmeldinger, samt bakgrunnsfargen i "avbryt" knapper. Rød brukes også for å vise at en ansatt ikke er tilgjengelig i sammenligningsfunksjonen. Se figur 4.5a for demonstrasjon av fargen rød til statusmeldinger og avbryt-knapper.
- **Grønn** er en farge som assosieres med positivitet[32], og brukes for bekreftende handlinger. I pasientmodulen brukes grønnfargen i bakgrunnen av knapper som resulterer i at noe blir opprettet eller lagret, samt tilbakemeldinger om vellykkede operasjoner til brukeren, som når en aktivitet har blitt lagret. Grønn brukes også for å vise at en ansatt er tilgjengelig. Se figur 4.5a for demonstrasjon av fargen grønn til bekreftende knapper og for å kommunisere tilgjengelighet.
- **Oransje** er en energisk farge, ofte brukt til å frembringe en "hasterespons", altså å frembringe en handling fra brukeren, ofte brukt i klassisk kommersielt design[32]. I pasientmodulen brukes denne fargen for å signalisere at en endring er mulig. Se figur 4.5a for demonstrasjon av fargen oransje for handlings-knapper.
- **Blå** er en beroligende, men ellers nøytral farge. I pasientmodulen brukes blå farge for å vise muligheter for interaksjon som ikke har en va-

rende eller endrende effekt på innholdet, dette er typisk navigasjonsknapper. Knapper for "tilbake", og "vis side for aktivitet" og lignende farges blått. Se figur 4.5a for demonstrasjon av fargen blå for navigasjons knapper som ikke utøver en endring på siden.

Knapper: Som beskrevet ovenfor, er knappene i pasientmodulen alltid fargekodet utifra funksjon. Den kraftige fargen hjelper brukeren å skjønne at den er et interaktivt element. Det blir også brukt en egen skrift-type for teksten på knappene. En fagperson, vedlegg L, anbefalte bruk av piktogrammer, for at brukeren lettere skal forstå betydningen av et element. Derfor er det også ikon på knappene, som skal ytterligere vise knappens formål. Disse valgene er felles for alle knappene, og skaper en intern konsistens i designet som brukeren vil gjenkjenne. Siden av pasientmodulen vist i figur 4.5a inkluderer alle typene knapper brukt i pasientmodulen. Det brukes også en subtil animasjon for å vise at en knapp har blitt aktivert, da den vil bli "trykket ned" raskt, for så og heve seg sakte opp igjen, slik som en fysisk knapp kunne oppført seg.

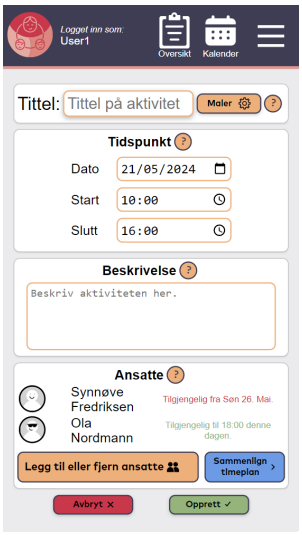
Tekstfelt: Tekstfelt i pasientmodulen bruker også fargekoding for å signalisere brukeren om at det er muligheter for interaksjon. Dette gjøres med en oransje ramme rundt boksen som matcher den oransje fargen brukt for alle lignende interaksjoner på siden. Det vises også en grå "stedfortredende" tekst i tekstbokser, før brukeren har gitt tekstinput. Se 4.5a for side av pasientmodulen med tekst-felt.

Feilmeldinger: Feilmeldinger i pasientmodulen er implementert som en designert boks på siden, der feilmeldinger kan vises. Denne boksen er i utgangspunktet skjult, frem til brukeren gjør en feil som trigger meldingen. Feilmeldingsboksene har en kraftig rød ramme, samt stor rød tekst som dominerer siden. Attpåtil vil boksen bli "ristet" for å trekke brukerens oppmerksomhet. Bevegelsen sikrer at det skjer en synlig endring på skjermen hver gang brukeren trykker på knappen, slik at de observerer at deres input har en funksjon, og at applikasjonen ikke har hengt seg opp. I figur 4.5b vises siden for redigering av aktivitet etter at brukeren har forsøkt å lagre aktiviten uten å fylle inn en tittel.

På enkelte sider i pasientmodulen*(redigering av aktiviteter og rapportering av aktivitet)*, er det lagt inn et ekstra signal for å veilede brukeren til å rette opp feil som har oppstått. Etter at feilmeldingen er aktivert, vil tekst-feltet som inneholder årsaken til feilen begynne å pulsere i rødt. Dette støtter opp feilmeldingen med en mer visuell forklaring på problemet, som er nyttig dersom brukeren skjønner at noe har gått galt, men mangler leseferdighetene til å forstå tekstinnholdet av feilmeldingen. Dette tiltaket er spesielt nyttig gitt at en stor andel av målgruppen har vanskeligheter med lesing og skriving (Se vedlegg N). Figur 4.5b viser den pulserende effekten rundt tekst-feltet som den ser ut på sitt sterkeste.

Bekreftende meldinger: Pasientmodulen bruker bekreftende tilbakemeldinger til brukeren for å kommunisere en vellykket operasjon. Meldingene opptrer som bokser, "flytende" ned fra toppen av skjermen. Disse meldingene har grønn bakgrunn, noe som utnytter den interne konsistensen og gir en respons til brukeren etter at brukeren har gjennomført en handling, f. eks. å lagre en redigert aktivitet. Disse meldingene er et tiltak for å gi brukeren synlige tilbakemeldinger for alle handlinger gjennomført på siden. Se 4.5c for et eksempel fra pasientmodulen der brukeren nettopp har trykket på knappen for "Opprett aktivitet" i redigeringsverktøyet med alle velter riktig fylt ut.

Estetiske valg: De konkrete fargene og estetiske valgene tatt i design-prosessen, er hovedsakelig basert på Omhu's egen hjemmeside[3]. Fonter og fargekoder er hentet fra en design pakke sent fra oppdragsgiver.



(a) Side for redigering av aktivitet i pasientmodulen

(b) Feilmelding og markering av årsak for feil

(c) Bekreftende melding etter opprettelse av aktivitet

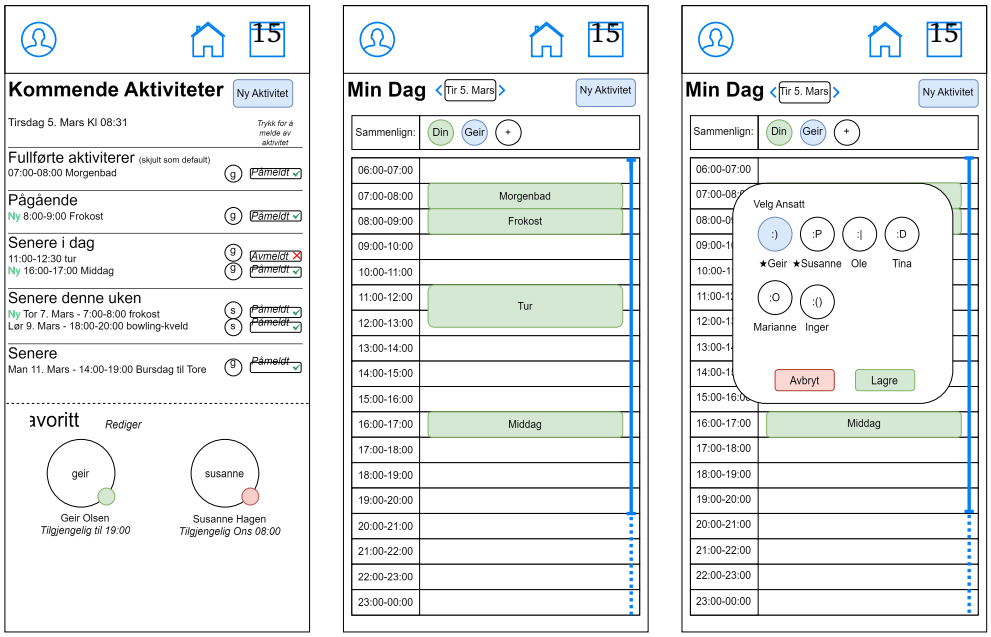
4.2.5 Tidligere iterasjoner

Utviklingen av pasientmodulen gikk gjennom tre iterasjoner av programvare, samt en iterasjon av wireframe. Endringene gjort mellom iterasjonene er gjort på bakgrunn av data og erfaringer samlet fra brukertester, og erfaringer gjort med intern testing av modulen.

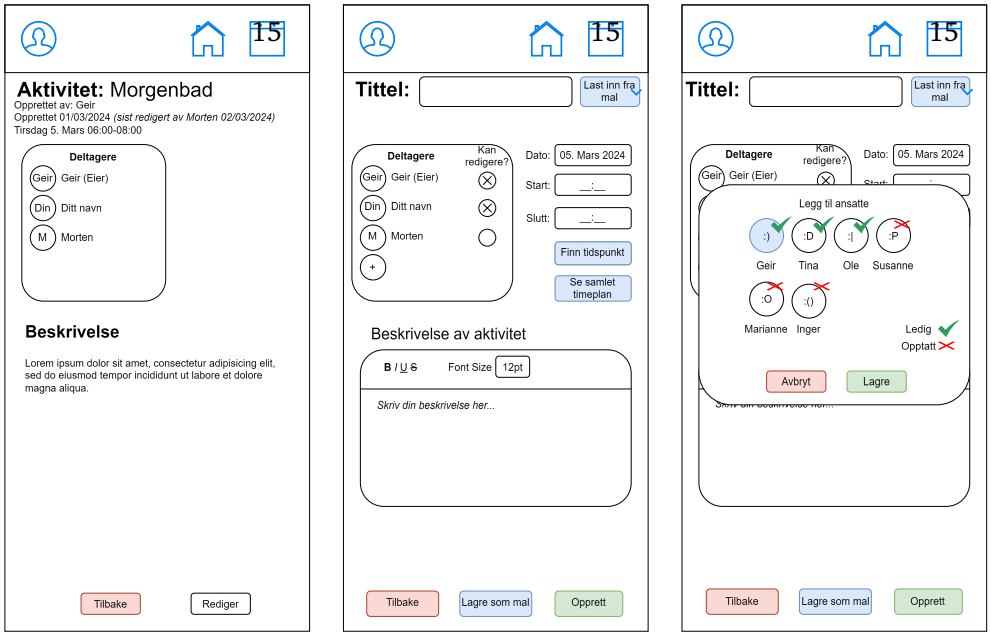
[3]Hjemmesiden til Omhu kan sees her: https://omhuapp.no

Wireframe

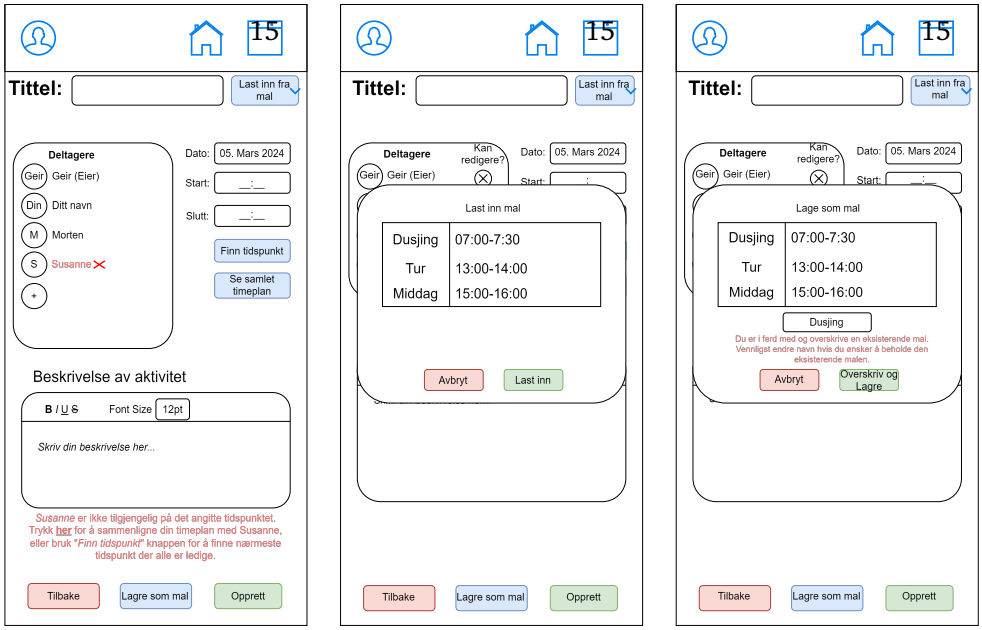
Det første konkrete designet av pasientmodulen var en wireframe med det grunnleggende designet og strukturen til nettsiden.



Figur 4.6: Wireframe for iterasjon 0 - Del 1



Figur 4.7: Wireframe for iterasjon 0 - Del 2



Figur 4.8: Wireframe for iterasjon 0 - Del 3

Nedover følger en liste med funksjonalitet skissert i wireframen:

1. Mulighet til å se aktiviteter i liste-format. Her kan en trykke seg inn på aktiviteter med å trykke på "vis aktivitet".
2. Mulighet til å favorisere en ansatt, og vise deres tilgjengelighets-status på forsiden.
3. Side med kalender-visning av dagen, med aktiviteter vist som firkantede "blokker" i kalenderen.
4. Mulighet for å legge til ansatte på kalender-visningen, der deres status skal bli representert som en fast linje gjennom tilgjengelige timer, og en stiplet linje gjennom utilgjengelige timer.
5. Mulighet for å inspisere aktivitet. Her kan en se ansatt og beskrivelse, samt redigere denne aktiviteten.
6. Redigerings-side for aktiviteter. Her kan brukeren legge til tittel, beskrivelse, tidspunkt og ansatt.
7. Seleksjon av ansatte gjøres i en pop-up meny som også viser hver av de ansattes status på det nåværende tidspunkt. Favoriserte ansatte er på toppen av listen.
8. Ansatte lagt til vil vise en tilbakemelding om de er tilgjengelige i det valgte tidsrommet.
9. Knapp i redigeringsverktøy for å automatisk finne et tidspunkt der alle ansatte er ledig.
10. Knapp i redigeringsverktøy for automatisk åpning av kalender-siden med alle selekterte ansatte, som er valgt for sammenligning.
11. Innlasting og lagring av mal direkte i redigerings-verktøyet.

Iterasjon 1

Versjon 1 av pasientmodulen er en omtrentlig gjennomføring fra wireframen i versjon 0. Mindre endringer ble gjort ettersom implementasjonen som vist i wireframe ikke lot seg gjøre, eller hadde et opplagt bedre alternativ.

1. Funksjonaliteten for å favorisere ansatt ble fjernet, dette for å redusere kompleksitet og spare ressurser.
2. I redigeringsverktøyet for aktiviteter ble skjelettet på siden endret til et enkelt-kolonne design. Dette var for å bedre utnytte plass på mobilskjermen, samt forenkle brukervennligheten [27].
3. Funksjonalitet for å "finne tidspunkt" ble fjernet, ettersom det gjorde siden veldig komplisert.

Iterasjon 2

De følgende endringene ble gjennomført utifra resultatene fra brukertest for versjon 1 av pasientmodulen, se vedlegg A. De implementerte endringene er konkrete løsninger, trekket fra et utvalg av foreslåtte tiltak gjenomgått i resultatene fra denne.

1. Forbedret visuelt hierarki på dashbordet:
    - Økt avstand mellom aktivitetene.
    - Økte tekststørrelsen.
    - Gråfarget mindre viktig tekst for å fremheve aktivitetstitlene.
    - Plasserte kategoriene i bokser.
    - Lagt til ny tidskategori: “Neste 7 dager”.
    - Fjernet seksjonen “Fullført” fra dashbordet.
    - Endret visning av aktiviteter som skjer i morgen til å vise “I morgen” i stedet for datoen.
2. Lagt til ikoner på alle knapper: pil for blå navigasjonsknapper, tannhjul eller pluss-tegn for oransje handlingsknapper, et sjekkmerke for grønne «bekreft»-knapper, og et kryss for røde «avbryt»-knapper.
3. Lagt til ny side for visning av maler, med en knapp på dashbordet for å navigere til denne siden.
4. Introdusert en ny editor for å redigere maler.
5. Utvidet malenes egenskaper til å inkludere tidspunkt, ansatte og ukedag i tillegg til tittel og beskrivelse, hvor de førstnevnte egenskapene er valgfrie.
6. Fjernet muligheten til å lagre maler i aktivitetseditoren.
7. Redusert visningen av statusmeldinger i «velg ansatt»-menyen når ingen tidspunkt er valgt.
8. Forenklet statusmeldingene i «velg ansatt»-menyen for å ikke overvelde brukeren.

Iterasjon 3

De følgende endringene ble gjort på bakgrunn av funn gjort i brukertesten for versjon 2 av pasientmodulen. Listen med potensielle tiltak gjennomgås i kap 5.2.2. Planen og resultatene for brukertesten kan du se i B, de behandlede dataene er i kap 5.2.2.

1. Introduserte funksjonalitet for å legge til aktiviteter ved å trykke på kalenderen.
2. Implementerte funksjonalitet for å inspisere aktiviteter ved å trykke på dem

i kalenderen.
3. Forbedret feilmeldinger i redigeringsverktøyet ved å legge til ny boks med statisk feilmeldinger samt rød omramming rundt relevante elementer.
4. La til funksjonalitet for å rapportere aktiviteter.
5. Lagt til side for innstillinger.
    a. Valg for å skjule sammenlign i timeplanknappen i redigeringsverktøyet.
    b. Valg for å fjerne muligheten til å velge egen ansatt i aktivitetsredigeringsmodus.
    c. Valg for å deaktivere malbasert system i aktivitetsredigeringsmodus.
6. Oppdaterte ikoner og knappetekst i toppmenyen.
7. Lagt til en ny knapp i toppmenyen for "annetsom åpner en rullegardinmeny med innstillinger og malbehandling.
8. Implementerte hjelpeknapper flere steder for å gi brukervennlig dokumentasjon om avanserte funksjoner.
9. Oppdaterte ikoner for knapper relatert til ansatte.
10. Forenklet tekst på flere knapper.
11. La til knapper flere steder i pasientmodulen for dokumentasjon av funksjonalitet. Disse knappene er markert med spørsmålstegn.

4.2.6 Implementasjon

Formålet ved å omdefinere pasientmodulen til en prototype i stedet for en MVP, var for å spare tid, ettersom en MVP krever at produktet skal være funksjonelt, men ikke nødvendigvis brukervennlig eller godt designet. Oppdragsgiver ønsket heller at design og brukervennlighet skulle prioriteres, fremfor ren funksjonalitet.

Utviklingen av pasientmodulen ble dermed gjennomført uten oppkobling til en backend server, med unntak av den initielle hentingen av filer fra filserveren. Pasientmodulen er dermed et offline program, med hardkoda verdier lagt inn i minnet. For å “simulere” en backend ble all data som modulen trengte, definert i et eget javascript dokument som en rekke JSON stringer.

Med denne ordningen ble resten av nettsiden koblet opp mot denne lokale datakilden, og ikke direkte hardkodet. Det var viktig for test-formål at nettsiden var interaktiv, noe som innebærer at bruker-input bør registreres og ivaretas av nettsiden enten midlertidig eller varig. En tilnærming med total hardkoding av alle verdier, som egentlig er dynamiske, ville motvirket formålet med å utvikle nettsiden i utgangspunktet.

Koden for pasientmodulen ligger under mappen `/omhu-demo/public/site` i github-repoet vårt.

4.2.7 Installasjon

Som nevnt, er pasientmodulen designet for å være offline-vennlig. Modulen kan kjøres lokalt ved å åpne `/omhu-demo/public/site/index.html` i en nettleser. Filene nødvendig for kjøring av pasientmodulen er inkludert i tilleggsmaterialet. For å skape en sammenknytning til demostrasjonen for WebAuthn-autentisering, ble likevel pasientmodulen bygget inn i samme golang-program som WebAuthn demo'en. Se kapittel 4.1.8 for oppsett av infrastruktur for å besøke nettsiden. Pasientmodulen ligger under `/site/` mappen i filserveren vertet i SkyHigh. Det er dermed mulig å besøke modulen via url https://omhu.raphaelstorm.no/pub/site/ vår og tidlig sommer 2024.

4.3 WCAG suksesskriterier

Som nevnt i kapittel 2.3.3, finnes det lovpålagte suksesskriterer i WCAG 2.1, som skal sørge for at alle kan ta i bruk en web-applikasjon, uavhengig av syn, hørsel, motorikk og kognisjon. Testprosedyrer for å sjekke om alle suksesskriteriene i WCAG 2.1 er implementert, er under arbeid og eksisterer ikke per dags dato. Testprosedyrer for WCAG 2.0 er derimot utarbeidet av Tilsynet for universell utforming av ikt(uutilsynet), og er et godt verktøy for å sjekke om en web-applikasjon tilfredsstiller en del av WCAG 2.1, siden WCAG 2.1 bygger videre på WCAG 2.0 [33].

Alle testprosedyrene kan finnes på hjemmesiden til uutilsynet, og er brukt for å sjekke om autentiseringsdemoen og pasientmodulen tilfredsstiller WCAG 2.0. Pga. at demoene ikke skal ut i produksjon, er suksesskriterier som gjelder HTML-koden i seg selv, som riktig merking av HTML-elementer, ikke vurdert. Det er kun kriterier som kan bli merket av brukeren, som har blitt vurdert. Det er de siste versjonene av begge demoene som har blitt vurdert.

Suksesskriterie	Testregel	Informasjon
2.1.1 *	Det er mulig å nå innhold og bruke funksjonalitet med tastatur	Ettersom begge demoene ble utviklet for bruk av mobil, og vi ikke har hatt nok tid, så er ingen av demoene "tastatur-vennlige".
2.2.2	Det er mulig å pause, stoppe eller skjule innhold som beveger seg, blinker eller ruller.	I autentiseringsdemoen er det en "loading-button" som ruller kontinuerlig, mellom startfasen og sluttfasen av både registreringsdelen og autentiseringsdelen. Denne bør bli satt til å slutte å rulle innen 5 sekunder.
3.3.2	Skjemaelement er identifiserte ved hjelp av instruksjoner eller ledetekster.	Alle skjemaelement er identifiserte med ledetekster, men ingen er merka som obligatoriske, selv om de er det. Samtlige skjemaelement bør merkes som obligatorisk, der merkingen blir forklart på forhånd.

Tabell 4.1: WCAG 2.0 - suksesskriterier som ikke er oppfylt

* Siden dette suksesskriteriet ikke er oppfylt, er heller ingen av de andre kriteriene som gjelder tastatur oppfylt. Disse kriteriene er som følger; 2.1.2, 2.4.3, 2.4.7, 3.2.1 og 3.2.2.

Kapittel 5

Resultat

I dette kapittelet skal vi gjennomgå resultatene fra de forskjellige brukertestene som ble gjennomført. For kartleggingen av autentisering vil resultatene brukes til å sette kvantitative verdier på de forskjellige egenskapene til autentiseringsmetoder.

5.1 Undersøkelse & brukertest av flere autentiseringsmetoder

Denne brukertesten gikk ut på å innhente kvantitative verdier for ulike autentiseringsmetoder til sammenligning. Hele brukertesten og resultatene av testen kan sees i vedlegg D. Ettersom WeissTech ønsker at det skal være mulig å registrere seg på Omhu hjemme, og uten hjelp av eksterne personer og hjelpemidler, er det ønskelig at registreringen skal være enkel nok til at brukerene kan gjøre dette selv. Det er også ønskelig at autentiseringsmetoden skal være lett å lære, og skal kunne ta så liten tid som mulig å gjennomføre i hverdagen. Derfor ble både registrering av autentiseringsmetode, og selve autentiseringen per metode, testet. Dette for å kunne sammenligne både hvor lett hver enkel autentiseringsmetode er å registrere ved førstegangsbruk, i tillegg til hvor enkel autentiseringsmetoden er å bruke i hverdagen.

Fire ulike autentiseringsmetoder ble testet. Sikkerhetsnøkkel, passord og brukernavn med og uten autentiseringsapplikasjon, og biometri. I tillegg ble kvalitative data for BankID innhentet. Grunnen til at kvalitative data ble innhentet for BankID, var fordi det kan være aktuelt for noen i målgruppa, som har tilgang til BankID.

I tillegg til sikkerhetsnøkkel og passord med/uten autentiseringsapplikasjon, ble også biometri testet. Siden biometri er en sensitiv personopplysning, ble det valgt å ikke teste registrering av biometri i testen. Dette er fordi vi ikke kunne vite på forhånd om brukerene hadde mulighet til å registrere biometri på sin egen mobil, og det ikke ville vært passende å få brukerene til å registrere en biometrisk autentiseringsmetode på en låne-mobil. Biometrisk autentisering ble testet dersom brukeren hadde dette på mobilen, og også hadde mobilen tilgjengelig. Kvalitativ data ble innhentet for både registrering og autentisering av biometri.

For å unngå bias, ble autentiseringsmetodene testet før selve registreringen. Dette er fordi registrering av autentiseringsmetodene er antatt å være mer krevende og vanskelig enn å autentisere seg. Derfor ble autentiseringen per metode testet først, før brukerene ble satt til å registrere autentiseringsmetodene.

Seks personer deltok i brukertesten. Deltagerne ble plukket ut spesifikt for å gi et så realistisk resultat som mulig. Grunnet problemer med å skaffe nok deltagere i målgruppen, ble personer som ikke er i målgruppen, men som likevel kan gi et realistisk resultat, plukket ut. Alle deltagerne i denne brukertesten var over 40 år, bortsett fra en som var 25 år. Ingen hadde bedre IT-ferdigheter enn gjennomsnittspersonen. Tre av seks av deltagerne hadde ME, noe som kan gi kognitive symptomer som svekket hukommelse, redusert konsentrasjonsevne, langsom informasjonsbearbeiding, dårlig korttidsminne m.m. [34]. Dette er symptomer som også personer med funksjonsnedsettelse kan oppleve, og resultatene fra brukertestene er derfor sammenlignbare med resultater vi hadde fått ved å teste personer i målgruppen.

Under er de kvantitative resultatene vist i hvert sitt delkapittel.

5.1.1 Autentiseringsdel

I tabellen under er kvantitative data fra autentiseringsgsdelen av brukertesten vist. Gjennomsnittlig tidsbruk er regnet ut ved å ta hver brukers siste forsøk, altså de forsøkene som endte med suksess, og finne gjennomsnittet av tidsbruken på dette. I de tilfellene der brukeren ikke fikk et suksessfullt forsøk, ble ikke resultatet fra respektive bruker tatt med i beregningen. Fullføringsrate beskriver hvor mange av deltagerne i testen som etter x antall forsøk fikk et suksessfullt resultat.

Autentiseringsmetode	Gjennomsnittlig tidsbruk	Fullføringsrate
Sikkerhetsnøkkel	49.1 sek	6 av 6 - 100%
Passord og brukernavn med autentiseringsapp	40 sek	4 av 6 - 66%
Biometri	1.4 sek	5 av 6 deltagere i brukerundersøkelsen brukte fingeravtrykk eller ansiktsgjenkjenning på mobilen

Tabell 5.1: Autentisering - kvantitative verdier

5.1.2 Registreringsdel

I tabellen under er kvantitative data fra registreringsdelen av brukertesten vist. Gjennomsnittlig tidsbruk er regnet ut ved å ta hver brukers siste forsøk, altså de forsøkene som endte med suksess, og finne gjennomsnittet av tidsbruken på dette. I de tilfellene der brukeren ikke fikk et suksessfullt forsøk, ble ikke resultatet fra respektive bruker tatt med i beregningen. Fullføringsrate beskriver hvor mange av deltagerne i testen som etter x antall forsøk fikk et suksessfullt resultat.

Autentiseringsmetode	Gjennomsnittlig tidsbruk	Fullføringsrate
Sikkerhetsnøkkel	70.2 sek	5 av 6 - 83%
Passord og brukernavn uten autentiseringsapp	40 sek	6 av 6 - 100%
Passord og brukernavn med autentiseringsapp	100 sek	5 av 6 - 83%

Tabell 5.2: Registrering av autentiseringsmetoder - kvantitative verdier

5.1.3 Sammenligning

Under testen ble det inkludert segmenter der brukeren fikk en liste med autentiseringsmetodene som de hadde fått prøve under testen, samt andre metoder de hadde opplyst om å bruke tidligere. Brukerene ble da bedt om å rangere metodene utifra hvor enkelt de syntes de er å bruke. Denne rangeringen ble gjennomført både for registrering og autentisering.

Da deltagerene var tillatt å rangere forskjellige metoder på likt nivå, uten kategorisering å feste rangeringen til, er dataen noe vanskelig å tyde. For å vise dataen

på en måte som gjør sammenligningen klar, sammtidig som at modellen ikke misrepresenterer data, brukes condorcet metoden for å rangere autentiseringsfaktorene. Det står mer om denne metoden i kapittel 3.4.1. Resultatet under gjelder for de seks brukertestene gjennomført.

1. Fingeravtrykk/Ansiktsgjenkjenning
2. Pin-kode
3. Sikkerhetsnøkkel
4. BankId
5. Autentiseringsapp
6. Passord

5.1.4 Kvalitative data

I tillegg til kvantitative verdier, ble kvalitative data innhentet. Dette for å finne ut hva som kan være problematiske aspekter ved de ulike autentiseringsmetodene. I tillegg er det også ønskelig å finne brukerenes preferanser og meninger om de ulike metodene. Selv om en metode har høy gjennimsnittstid, kan det likevel vise seg at denne metoden er den som er preferert blant flest brukere. Følgende resultater kan oppsummeres fra de kvalitative dataene:

- **Sikkerhetsnøkkel - autentisering**: Alle fikk til å autentisere seg med sikkerhetsnøkkel. Noen hadde problemer med at de ikke skjønte hvor på mobilen sikkerhetsnøkkelen skulle plasserest. Med NFC teknologi så må sikkerhetsnøkkelen helt inntil mobilen, og ikke en cm ifra.
- **Passord og brukernavn - registrering**: Ingen syntes denne testen var vanskelig, og alle fikk det til på første forsøk. Fikk tilbakemeldinger på at 12 tegn, som var minstekravet, er utrulig mye å huske. En person mente også at passordet hen lagde ikke er sikkert, siden det var et ganske enkelt passord.
- **Passord og brukernavn med registreringsapplikasjon - autentisering**: To av deltagerne fikk ikke til dette. Av de som fikk det til, var det noen som syntes det var enkelt og heilt greitt. Noen hadde problemer med tidsbegrensningen på 30 sekunder i appen. Noen visste ikke om muligheter for "klipp og lim" på mobilen, så de matte gå inn og ut mellom appene og pugge tallene som skulle skrivest inn. Dette gav de inntrykk for var krevende og lite effektivt.
- **Bimoetri - autentisering**: En av testpersonene brukte ikke biometri på mobilen. De andre deltagerene var alle fornøgde med autentisering vha. biometri. Både fingeravtrykk og ansiktsgjenkjenning var representert i brukertesten.
- **Sikkerhetsnøkkel - registrering**: Fem av testpersonene fikk til å registrere sikkerhetsnøkkel. Noen deltagere syntes det var litt krevende når de gjor-

de det, men i ettertid syntes de at det ikke vår så vanskelig likevel. En av testdeltagerne opplevde tekniske problemer med sikkerhetsnøkkelen, ved at den ikke registrerte seg selv om brukeren gjorde alt rett. Dette gjorde det vanskelig for brukeren å vite om hen gjorde noe feil eller ikke.

- **Passord og brukernavn med autentiseringsapplikasjon - registrering**: Det ble litt forskjellige tilbakemeldinger i denne testen. Fem av brukerene fikk det til, men noen påpekte at de ikke hadde klart det uten hjelp eller opplæring. Flere mente at dette er en "knotete" måte å autensiere seg på, iallefall i forhold til andre alternativ, som biometri. En av brukerene misforstod hva hen skulle gjøre, noe som både kan skyldest hvordan testen var satt opp, men også manglende kunnskap om hvordan autentiseringsapplikasjoner egentlig fungerer. Årsaken kan også være dårlig brukergrensesnitt på testnettsiden. Det er også mulig at autentiseringsapplikasjonen i8 seg selv er problemet, grunnet brukergrensesnitt eller andre faktorer som ikke er tatt høyde for i brukertesten. En bruker påpekte at hen ikke hadde fått til dette selv, mens en annen syntes det gikk helt greitt uten hjelp.
- **Biometri - registrering**: Dette var en av to tester som ikke var mulig å observere, og dermed heller ikke mulig å samle inn kvantitative verdier. Fem av deltagerne brukte biometri for å låse opp mobilen. Tre av deltagerne klarte å registrere dette selv. En av deltagerne fikk hjelp første gang, men klarte det selv ved en senere anledning. Alt i alt positive tilbakemeldinger.
- **BankID - registrering**: Tre av testpersonene satt opp BankID selv. De andre fikk hjelp, enten av et familiemedlem, eller i banken.

Mer utfyllende informasjon kan finnes i vedlegg D.

5.2 Brukertest av pasientmodul

Denne seksjonen vil omhandle resultatene fra brukertestene gjort for pasientmodulen. Utviklingen av pasientmodulen dokumenteres i kapittel 4.2.

Gjennom hele prosessen ble det gjennomført totalt fire brukertester for pasient modulen, med to forskjellige varianter av testen. Variantene er omtalt som brukertest v1 og v2, og samsvarer med versjonen av pasientmodulen testen gjennomføres for. Det vil si at brukertest v1 var brukt til å teste pasientmodul v1, og tilsvarende med v2.

Brukertestene er destignet basert på prinsippene gjennomgått i boken "Handbook of usability testing" av Jeffrey Rubin [25].

5.2.1 Brukertest pasientmodul v1 - Deltagere utenfor målgruppen

Versjon 1 av brukertesten ble gjennomført på versjon 1 av pasientmodulen. Det ble gjennomført totalt to brukertester av denne varianten. Resultatene fra disse brukertestene dokumenteres i denne seksjonen. Planen for denne testen er dokumentert i vedlegg A og omhandler mål, gjennomføring, manus og oppgaver for testen.

For å repetere fra testplanen, er test-spørsmålene for denne testen som følger:

1. Er top-menyen intuitiv til bruksområdene av fanene?
2. Forstår brukeren hva som som kan interageres med?
3. Hvor vanskelig er det for brukeren å se når en ansatt er ledig?
4. Forstår brukeren hvordan de vertikale og horisontale navigasjons-elementene fungerer?
5. Klarer brukere å rette opp fra feiltrinn raskt?
6. Er nettsiden oversiktlig?

Deltagere

Deltagerne som gjennomførte denne testen består av venner og familie til gruppemedlemmer i prosjektet. Utvalget av deltagere faller dermed ikke under målgruppen pasientmodulen er ment for, noe som kan svekke vekten av resultatene for denne testen. Resultatene hentet fra testen er fortsatt nyttige for utviklingen av pasientmodulen, men kan ikke brukes som en erstatning med en reell bruker. Se versjon 2 av testen for gjennomføring med deltagere innenfor målgruppa.

Vurderende test

I tabell 5.7 er et sammendrag av resultatene for de vurderende oppgavene i testen. Verdiene vist er en kombinasjon av begge gjennomføringene av brukertesten, der det mest negative utfallet av de to testene er plukket ut for hver oppgave. Dette vil gjøre at resultatet vist er noe verre en en gjennomsnittlig gjennomføring. Dette valget er tatt for å vise svakhetene med designet.

Oppgave	Beskrivelse	Fullførings-nivå	Antall Feil-trinn
1	Med å bruke nettsiden, fortell meg hva klokka er.	1/1 - 100%	0
2	Når på dagen skal du på kino neste uke?	3/3 - 100%	0
3	Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.	4/5 - 80%	1
4	Du fikk hjelp til å lage middag av en ny ansatt i går. Finn navnet til denne ansatte.	3/3 - 100%	0
5	Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.	4/5 - 80%	2
6	Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.	6/7 - 86%	1
7	Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Du liker ikke fisk, og dette er aldri inkludert i aktivitets-beskrivelsen for middag. Kan du redigere malen for middag for å spesifisere at du ikke liker fisk, for så og lagre denne malen?	1/5 - 20%	2
8	Du pleier ofte å gå tur, og er lei av å skrive inn på nytt vær gang. Finn en måte å lage en ny mal med dine tur-preferanser.	2/5 - 40%	1
9	Du har lyst til å rydde leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.	0/5 - 0%	2

Tabell 5.3: Data for vurderende test v1

Spørreskjema

Spørreskjema-et gjennomgått mot slutten av testen bestod av en rekke påstander om nettsiden, som deltagerene besvarte med en skala fra 1-5 på hvor enige de var med påstanden basert på deres erfaringer. Deltagerene var også oppmuntret til å dele meninger relatert til spørsmålet. Tabellen nedenfor viser et utdrag av tilbakemeldingene fra de to brukertestene. De mer negative tilbakemeldingene er igjen blitt prioritert, så resultatet kan virke noe mer negativt en det er i realiteten. De kvalitative tilbakemeldingene er samlet senere i seksjonen.

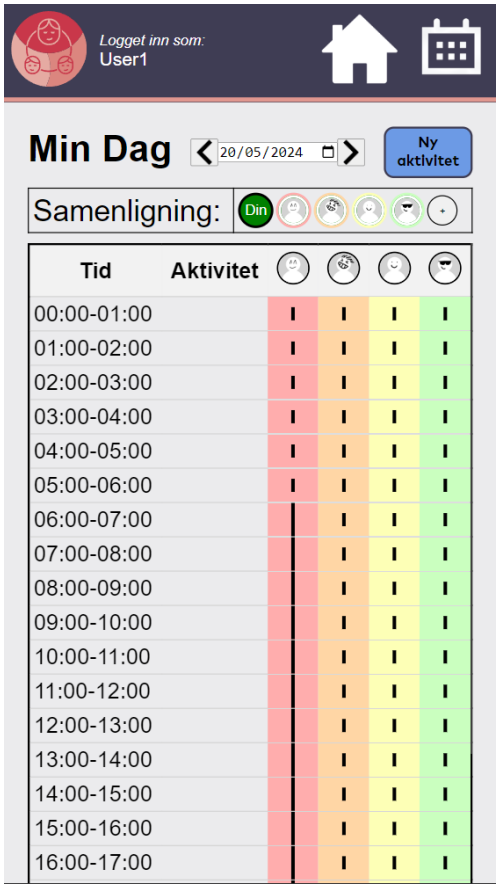
#	Påstand	Kvantitativ besvarelse
1	Det er enkelt å forstå hvor man skal trykke for å bytte mellom siden for dashbord og siden for "min dag".	3 - litt enig
2	Skriften på nettsiden var passe stor.	2 - uenig
3	Det er enkelt å gå tilbake til den forrige siden man var på.	4 - enig
4	Hjemsiden var oversiktelig.	2 - uenig
5	Det er enkelt å forstå hva de forskjellige knappene gjør før man trykker på de.	4 - enig
6	Det er enkelt å forstå hvor man kan skrive inn tekst.	5 - helt enig
7	Det er enkelt å forstå om det jeg har skrevet har blitt lagret.	3 - litt enig
8	Det er tydelig når en ansatt er ledig, og når de er opptatt på kalender-siden.	1 - helt uenig
9	Det er tydelig om en ansatt er ledig eller ikke når man oppretter en aktivitet.	2 - uenig
10	Det er tilfredstillende å bruke nettsiden.	3 - litt enig

Tabell 5.4: Data for vurderende test v1 - Spørreskjema

Kommentarer og preferansedata

Gjennom både vurderingstesten samt post-test spørreskjema-et ble deltagerene oppmuntret til å dele deres meninger om pasientmodulen. Et utdrag av kommentarene og meningene uttrykt av deltagerene er presentert i listen nedenfor. Dette er et behandlet utdrag basert på en subjektiv vurdering av deltagerenes meninger, og bør ikke tolkes som sitater. Ubehandlede data for brukerenes tilbakemeldinger ligger i testplanen i vedlegg A.

1. Editoren krever innskrevet dato felt med opprettelse av mal, selv om denne verdien ikke brukes. *Dette kan betraktes som en bug.*
2. Fanen for lagring av mal lukkes ikke automatisk med lagring, som gir intrykk av at ingenting har skjedd. Dette er forvirrende.
3. Pop-up menyene for valg av ansatt med sammenligning av ansatte gir alt for mye informasjon. Forvirrer og distraherer med det egentlige formålet med menyen.
    - Menyen som er grunnlag for klagen har som formål å la brukeren velge en eller flere ansatte som skal sammenlignes. Menyen er i formatet av en pop-up, og krever at brukeren trykker på en "OK" knapp før de ansatte lastes inn i sammenligningen. Men hver ansatt hadde også en tekstreng som beskrev deres neste ledige tidspunkt, ment til å være en hjelp for å finne ledig tidspunkt raskere. Det var denne teksten som distraherte brukerene, og foråsaket tilbakelemdingen.
4. En deltager forsto ikke formålet med "strekene" ment til å symbolisere en ansattes tilgjengelighet. Se 5.1 for bilde. Brukeren korrelerte fargen rødt til "ikke tilgjengelig", men forsto ikke hvorfor forskjellige ansatte hadde forskjellige farger.
    - På versjonen av pasientmodulen som ble testet for, var alle ansattes "tilgjengelighets-streker" farget i forskjellige farger for å klarere separere dem.
5. Hjemsiden oppleves som litt rotete. Det er lite som hjelper å gruppere tekst på siden, og teksten kan være liten på enkelte plass. Kategorieren "fullført" er unyttig, og bidrar til å rote til siden.
6. Savnet input felt for egne typer informasjon i aktivitets editor. F.eks eget "middags" felt for å skrive inn måltid.
7. Savnet mulighet for å ha ansatte som del av aktivitets-mal.
8. Knappene i toppmenyen er litt utydelige med hvor de tar brukeren. Deltagere forventer ikke at start-siden for testen er samme side som hjemsiden(ikon med hus).
9. Funksjonalitet for å behandle maler ble forventet å ha på forsiden.
10. For aktiviteter var det en viss forventing om at det var input felt spesifikke for typer aktiviteter. F.eks "matrett" felt på aktiviteter relatert til middag eller måltider.
11. Muligheten for å legge til faste tidspunkt i maler er lurt å ha, ettersom mange som jobber innen feltet har veldig "skjema" i hverdagen.



Figur 5.1: Sammenligning av ansatte i v1 av pasientmodul.

Siden for sammenligning av ansatt vist i figur 5.1 gjelder versjon 1 av pasientmodulen og har siden blitt forbedret. Se figur H.8 for samme side i versjon 3 av pasientmodul.

Identifiserte problemer og forslag til tiltak

Brukertesten genererte mye data som hjalp sette lys på problemer med pasientmodulen. I denne seksjonen listes de viktigste problemene som ble identifisert gjennom brukertesten, samt forslag til tiltak som kan mitigere det gjeldende problemet. Merk at tiltak i denne listen ikke er garantert til å bli implementert i neste iterasjon. Se kapittel 4.2.5 for liste med implementerte endringer.

Problem	Tiltak
Det er forvirrende for brukere at verktøyet for å redigere og opprette maler er den samme siden som aktivitets-redigeringsverktøyet.	Flytte behandling av maler til en ny dedikert side. Dette vil frigjøre plass i aktivitets-regieringsverktøyet, samt gjøre det tydeligere hva funksjonen til hver side er. Denne siden kan attpåtil knyttes opp til en knapp på dashbordet for å gjøre navigasjonen til denne siden enklere.
Forskjellige grupper av tekst er vanskelig å skille fra hverandre på forsiden. Dette fører til en rotete forside.	Implementasjon av bokser og justering av skriftstørrelser og farger på dashbord kan gjøre siden lettere å lese.
Knappene i topp navigasjonsmenyen bruker kun ikoner. Dette gir ikke brukeren nok informasjon til å forstå funksjonen av disse knappene.	Legge til tekst ved ikonene i topp-navigasjonsmenyen vil gi enda en indikator på knappens formål, og gjøre det enklere å navigere på siden.
Navigasjonen via toppmenyen er ikke helt klar, da det ikke er noen form for "breadcrumbs" for å vise brukeren hvilken side de befinner seg på. Dermed trodde brukere at knappen for hjem førte de til en annen side, selv om de allerede befinner seg på denne siden.	Implementering av fargeskifte for ikoner i toppmeny om brukeren er inne på den sammsvarende siden i pasientmodulen. Dette vil gjøre det enklere å orientere seg på siden, da brukeren kan vite hvor de er til et hvert tidspunkt.
Manglende mulighet for å inkludere ansatte i mal.	Utvidelse av mal-inneholdet med tidspunkt, ukedag og ansatt kan gir større fleksibilitet med malene, og lar den brukes i flere situasjoner.
Pop-up menyene for å velge ansatt viser alt for mye informasjon. Denne menyen viser om den ansatte er ledig på et gitt tidspunkt. Da denne informasjonen blir gitt direkte i valg-menyen, forsøker ikke brukere å legge ansatte da de allerede har fått informasjonen de leter etter. Dette fører til at de ikke får brukt sammenlignings-skjemaet til sitt fulle potensiale.	Fjerning av "status" meldinger for ansatte i seleksjonsmenyen med sammenligning av timeplan. Reduksjon av de samme status-meldingene i den samme menyen når den brukes for valg av ansatte til aktivitet eller mal. Med å redusere denne informasjonen til et minimum kan brukeren bedre fokusere på sidens funksjonalitet. Skriften i mange menyer for liten, og mengden informasjon på disse sidene er ofte for høy.
Metoden for sammenligning av ansattes timeplan er ikke tydelig. Det er ikke klart hva strekene betyr i stiplet eller solid form, og fargene brukt for å skille de ansatte følger ingen tidligere satt standard. Behovet for en slik egenskap er også vanskelig for brukerene å se for seg, da de foretrekker å prøve og feile seg frem til et passende tidspunkt. Fenomenet av prøving og feiling oppstår trolig p.g.a. neste punkt.	Farge-koding av "status-strekene" for ansatte med sammenligning av timeplan. I stedet for at hver ansatt har en egen farge, vil de stiplete "utilgjengelig" strekene nå alltid være røde, uavhengig av hvilken ansatt det tilhører. På samme måte vil de faste "tilgjengelig" strekene alltid være grønne. Betydningen av disse fargene er allerede definert på flere steder i pasientmodulen. Dette tiltaket vil styrke den interne konsistensen[31, p. 143] og gjøre sammenligningsverktøyet enklere å tolke og lese.

Tabell 5.5: Tiltak basert på resultater av brukertest v1

5.2.2 Brukertest pasientmodul v2 - Deltagere innenfor målgruppen

Versjon 2 av brukertesten er for det meste identisk til versjon 1, men med visse endringer i testens plan og gjennomføring for å bedre passe med endringene av pasientmodulen implementert i versjon 2, som er versjonen denne testen er ment for. Planen for testen ligger i vedlegg B og inkluderer testoppsett, testspørsmål, manus, oppgaver og ubehandlede resultater.

Denne brukertesten ble gjennomført i samarbeid med et omsorgsenter innenfor feltet der Omhu har sin nisje. Deltagerene som ble testet som del av dette samarbeidet faller innenfor målgruppen, og vil da gi mer relevant data enn versjon en av testen.

Vurderende test

Den vurderende testen har samme oppgavesett som på versjon 1 utenom oppgave fire, som er fjernet da funksjonaliteten som skulle testes i denne oppgaven ble fjernet siden forrige versjon. På andre oppgaver har kriteriene for sukksess blitt endret. Resultatene fra denne testen vises på samme måte som tidligere, med at det "dårligste" datapunktet av de to testene blir tatt med.

I tabellen er det ikke registrert data for oppgave 6 og 7. Dette kommer av at oppgavene var kansellert underveis i testen da testmoderator bedømte at det ikke var nytteverdi i å gjennomføre dem, da det var tydelig at test-deltagere manglet kunnskap om fundamentale konsepter kritiske for fullføring av oppgaven. Dette gjaldt begge gjennomføringene av testen.

Oppgave	Beskrivelse	Fullførings-nivå	Antall Feil-trinn
1	Med å bruke nettsiden, fortell meg hva klokka er.	1/1 - 100%	0
2	Når på dagen skal du på kino neste uke?	3/3 - 100%	2
3	Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.	2/4 - 50%	0
4	Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.	1/4 - 25%	3
5	Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.	3/7 - 42%	1
6	Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Du liker ikke fisk, og dette er aldri inkludert i aktivitets-beskrivelsen for middag. Kan du redigere malen for middag for å spesifisere at du ikke liker fisk, for så og lagre denne malen?	*Ingen data.*	*Ingen data.*
7	Du pleier ofte å gå tur, og er lei av å skrive inn på nytt vær gang. Finn en måte å lage en ny mal med dine tur-preferanser.	*Ingen data.*	*Ingen data.*
8	Du har lyst til å rydde leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.	0/4 - 0%	1

Tabell 5.6: Data for vurderende test v2

Spørreskjema

#	Påstand	Kvantitativ besvarelse
1	Det er enkelt å forstå hvor man skal trykke for å bytte mellom siden for dashbord og siden for "min dag".	4 - Enig
2	Skriften på nettsiden var passe stor.	4 - Enig
3	Det er enkelt å gå tilbake til den forrige siden man var på.	5 - Helt enig
4	Hjemsiden var oversiktelig.	3 - Litt enig
5	Det er enkelt å forstå hva de forskjellige knappene gjør før man trykker på de.	5 - Helt enig
6	Det er enkelt å forstå hvor man kan skrive inn tekst.	5 - Helt enig
7	Det er enkelt å forstå om det jeg har skrevet har blitt lagret.	*Ingen data*
8	Det er tydelig når en ansatt er ledig, og når de er opptatt på kalender-siden.	*Ingen data*
9	Det er tydelig om en ansatt er ledig eller ikke når man oppretter en aktivitet.	4 - Enig
10	Det er tilfredstillende å bruke nettsiden.	4 - Enig

Tabell 5.7: Data for vurderende test v2 - Spørreskjema

Kommentarer og preferansedata

Denne seksjonen er lik den funnet i resultatene for versjon 1. Et utvalg av kommentarer og tilbakemelding fra deltagerene legges her. Igjen, så er ikke disse kommentarene ment til å tolkes som sitater, men heller en omformulering og sammendrag av ideene deltagerene har gitt utrykk for gjennom deres kommentarer.

1. Deltager utrykket frustrasjon over tilbakemelding fra siden “Vennligst fyll inn obligatorisk informasjon” da deltageren mente at hen allerede hadde gjort dette.
    - Kommentaren ble gitt i redigerings-verktøyet for aktiviteter, der input feltet for tittel ikke var fylt ut.
2. Deltager hadde en forventing om at hen skulle kunne trykke på kalenderen for å legge til en aktivitet. Deltager ga utrykk for forvirring da dette ikke gikk an.
3. Deltager syntes at “vis” knappene på dashbordet var enkle og forstå.

4. Deltager forstår at grønn skriftfarge betyr ledig, og rød betyr ikke ledig.
5. Deltager syntes skriften i menyer for å velge ansatt er litt for liten, men at det ellers er leselig.

Identifiserte problemer og forslag til tiltak

Tabell 5.8 inneholder en oversikt over de viktigste problemene identifisert under brukertestene, samt et forslag til tiltak for å mitigere problemet. Denne listen er mer overordnet, og tilsvarer ikke de implementerte tiltakene for versjon 3 av pasientmodulen, som ligger i kapittel 4.2.5.

Problem	**Tiltak**
Nettsiden bruker hovedsaklig tekst for å kommunisere med brukeren. Dette ble et problem da begge deltagerene hadde lese/skrive-vansker.	En mer utbredt implementasjon av ikoner over hele pasientmodulen. Ikoner er vist til å være effektive for brukere med dysleksi[35] og vil antageligvis være effektivt for målgruppen på samme måte.
Det var enkelte ord på nettsiden som deltagerene ikke forsto da de var for tekniske/avanserte. F.eks "redigere".	1. Disse ordene kan endres til mer forståelige varianter. "Redigere" kan f.eks. skrives som "Endre"[27, G5]. 2. Bruk av ikoner der det er relevant kan også hjelpe å kommunisere betydningen av ordet[35]. 3. Lett-tilgjengelig dokumentasjon i form av "hjelpe knapper" som forklarer funksjonen av enkelte ord og konsepter på siden[27, G12].
Deler av funksjonaliteten i nettsiden var for avanserte til at deltagerene klarte å bruke de til sitt formål. Hovedsaklig egenskaper rundt mal-systemet i pasientmodulen var vanskelig å bruke. Det virket ikke som konseptet eller formålet med å bruke en aktivitetsmal slo gjennom.	Dette er et vanskelig problem å løse med et enkelt tiltak i pasientmodulen. 1. Medhørende dokumentasjon som forklarer bruken av funksjonaliteten[27, G12]. Her er det mulig å ta i bruk "smarte" måter for dokumentasjon, slik som video og lydklipp. 2. Simplifisere funksjonalitet med kun la sluttbrukere bruke maler, ikke lage eller redigere disse. Funksjonen for å redigere og opprette maler kan inkluderes i pasientmodul, men gjemmes bak en form for "avanserte funksjoner".
Deltagerne savnet funksjonalitet for å trykke på kalenderen for å legge til aktiviteter. Antageligvis da dette er implementert i den ekte Omhu, samt andre kalender applikasjoner som Google kalender.	Implementere funksjonaliteten i pasientmodulen.
Deltagere klarte ikke å bruke verktøyet for sammenligning av timeplan. Dette kommer av to hovedårsaker årsaker: 1. Deltager så ikke knappen for å legge til ansatte, dette kom av tidligere nevnte problem med for mye tekst og dårlig bruk av ikoner. 2. Deltager forstår ikke konseptet eller formålet av å sammenligne timeplaner. Det er mulig at oppgaven var for kompleks, og at brukeren hadde fått det til i et enklere scenario. Det virket ikke som deltagere så poenget med et slikt verktøy.	1. Tydeligere teksting og bedre bruk av ikoner kan gjøre det mer intuitivt hvor brukeren skal trykke for å sammenligne ansatte. 2. Hjelpedokumentasjon som forklarer hvordan sammenligningen funker[27, G12]. Her kan det også være nødvendig å bruke video for å få noe merkbar effekt. 3. Revisjon av hele systemet for sammenligning. Formålet med systemet er å vise brukeren når en ansatt er ledig på lang sikt. Dette kan trolig oppnås på langt enklere måter som er mer brukervennlige.
Feilmeldinger dukker opp og forsvinner for raskt til at brukeren kan lese disse.	Forbedret visning av feilmeldinger i statiske bokser, slik at brukeren får lenger tid til å lese og tolke meldingen.

Tabell 5.8: Tiltak basert på resultater av brukertest v1

5.2.3 Helhetlig resultat av pasientmodul

Utviklingen av pasientmodulen for Omhu har gjennom flere iterasjoner funnet feil og mangler i designet, og sluttresultatet er en pasientmodul med et godt sett med funksjonalitet, som er rimelig brukervennlig. Gjennom brukertestingen ble det funnet at enkelte deler av designet fungerte godt, mens andre deler var mindre velykket.

Deler av designet som fungerte godt:

Navigasjon: Navigasjonen på nettsiden er designet for å være så enkel som mulig, med få lag og minimalistiske menyer. I brukertestene har dette vært velykket, da (med unntak av problemer med knapper) strukturen til pasientmodulen ikke har vært noe problem for noen av brukerene som har testet den. Bruk av knapper for navigasjon og handlinger har vært hovedsaklig velykket, med gode tilbakemeldinger fra deltagere, spesielt i de siste brukertestene. Dette gjelder også angring og feil-rettende handlinger på siden, som de deltagere har gitt god tilbakemelding på.

Aktivitets editor: Kanskje noe overaskende, så har redigerings-verktøyet for aktiviteter fungert meget godt gjennom alle testene. Det har vært problemer relatert til designet av denne siden, hovedsaklig realtert til at brukere overså feilmeldinger, og vanskeligheter med å tolke ansatt-seleksjonsmenyen. Kjernefunksjonen av å legge til den obligatoriske informasjonen av en aktivitet, for så og lagre denne har vært forstått og gjennomført av alle testdeltagere. Redigering av eksisterende aktiviteter var også jevnt over velykket. Innskriving av informasjon i input-felt har gått svært bra.

Valg av ansatt: Funksjonaliteten for å velge ansatt til en aktivitet har vært noe vrient å få til, men etter flere iterasjoner har det blitt landet på et design som fungerer godt til formålet. Selv om det er noe tvilsomt om en integrasjon med turnus-plan er mulig for Omhu, så har testene vist at brukerene klarer å velge ansatt basert på hvorvidt de er ledige. Brukerene responderte godt på bruk av fargekoding for å vise en ansattes status.

Deler av designet som ikke har fungert like godt:

Innlasting og redigering av maler: Systemet for bruk av maler har vært mindre velykket i implementasjonen. Tidlig i utviklingsfasen var systemet noe forvirrende for test-deltagere da malene ble behandlet i samme redigeringsverktøy som aktiviteter. Dermed ble redigering av maler flyttet til sin egen side. Dette hjalp derimot lite da deltagerne på versjon to av testen ikke så

ut til å forstå formålet med en mal, selv etter grundig forklaring. Disse deltagerene ble heller ikke videre testet for redigering og oppretting av slike maler, og virket å være fornøyde med å skrive inn detaljene av aktiviteten manuelt. Det er godt mulig at disse egenskapene kunne blitt velykket med bedre dokumentasjon og/eller opplæring, men kjerneproblemet med denne funksjonaliteten virker i grunn til å være et mangel på behov fra brukerenes side. På grunn av dette var valget å gjemme denne egenskapen vekk i siste versjon av pasientmodulen, da det antageligvis kun er avanserte brukere og assistenter som vil ta bruk av dette verktøyet uansett.

Sammenligning av ansatte: Siden for sammenligning av ansatte har vært utsatt for mange av de samme problemene som systemet for maler. Fremstillingen av ansattes timeplan som "'linjer" ble implementert for å ivareta assistentener og andre sluttbrukeres personvern i pasientmodulen. Men dette ble ikke presentert på en tydelig måte, og fremstillingen virket fremmed for deltagerene av de tidlige brukertestene.

I de senere brukertestene, med et forbedret design, gikk problemet mer ut på at deltagerene ikke forsto formålet med enten oppgaven, eller funksjonen. Igjen kan det rett og slett virke som at denne egenskapen av pasientmodulen er i overkant avansert, og over-leverer på hva brukerene egentlig trenger. Alternative løsninger for denne egenskapen vil bli videre diskutert i kap 6.2.

5.3 Brukertest autentiseringsdemo - Deltagere innenfor målgruppen

Til slutt, etter flere brukertester på personer utenfor målgruppen, ble det gjennomført brukertester på to personer med lettere psykisk utviklingshemming. Disse brukertestene ble gjennomført i Halden kommune, som et ledd av et samarbeid mellom denne kommunen og WeissTech. Av WeissTech's kunder og samarbeidspartnere, var det Halden kommune som var best egnet til brukertesting. Her var det to personer i målgruppen, som hadde hatt tilgang til Omhu en viss tid. Denne tilgangen var en begrenset versjon av Omhu for ansatte, hvor de kunne se dagens plan og dagens assistent. Denne begrensa versjonen ble veldig lite brukt av den ene brukeren, men den andre brukte den av og til. Grensesnittet var ikke laget for mobil, så for å logge inn på Omhu, var det nødvendig å brukte pc. Begge brukerene hadde dermed en viss kjennskap til Omhu, og kommunen er svært positive til å ta i bruk en fremtidig app spesifikt for målgruppen.

Det ble gjennomført to ulike brukertester med ulike målsetninger. I den første brukertesten ble autentiseringsdemoen brukt. Dette var for å teste alternativet med å bruke biometri sammen med en sikkerhetsnøkkel som autentiseringsmetode. Grunnen til at biometri og sikkerhetsnøkkel ble valgt, var fordi dette var de

to mest lovende alternativene mtp. resultater fra tidligere brukertester. Hele brukertesten kan sees i vedlegg C. De to instruksjonsheftene, vedlegg E og vedlegg F, hører også med til brukertesten.

Både kvantitative og kvalitative data ble innhentet frå denne brukertesten. Grunnet brukertestens "think aloud" protokoll, som går ut på at testdeltageren skal si høyt det hen mener og tenker under testen, ble ikke den konkrete tidsbruken målt. En tidsbegrensning på hva som regnet som et suksessfullt forsøk ble satt til henholdsvis 3 og 5 minutter. 5 minutter for registreringsdel, og 3 minutter for autentiseringsdel. De to kvantitative dataene innhentet i denne brukertesten var av binær type, altså det to mulige verdiene kunne være *ja* eller *nei*. De to kvantitative verdiene innsamlet er som følger:

- Oppnådde brukeren et suksessfullt forsøk uten hjelp av testmoderator?
- Oppnådde brukeren et suksessfullt forsøk innenfor tidsrammene på 3/5 minutt?

Under viser de kvantitative resultatene for begge brukerene samlet. De forskjellige oppgavene er delt inn i undergrupper, altså oppgave 1.1 til oppgave 1.5 er fem forskjellige oppgaver, men tilhører samme undergruppe av brukertesten.

Kvantitative resultater - registreringsdel demo

Oppgavenr	**Uten hjelp?**	**Innen 5 minutt?**	**Notater**
1.1 - 1.5	7 av 10 - ja 3 av 10 - nei	7 av 10 - ja 3 av 10 - nei	Var litt forvirring rundt forskjeller i grensesnitt og utseende mellom screenshotene i instruksjonsheftet, og brukerens egen mobil.
2.1 - 2.5	5 av 9 - ja 4 av 9 - nei	5 av 9 - ja 4 av 9 - nei	Tekniske problemer med den ene brukerens mobil, mobilen's biometri fungerte ikke sammen med demoen. Fikk ikke testet biometri på den ene. Sikkerhetsnøkkel fikk den ene til, men den andre måtte ha hjelp. Biometri fungerte fint på den andre brukerens mobil.

Tabell 5.9: Registreringsdel - kvantitative verdier

Kvantitative resultater - autentseringsdel demo

Oppgavenr	Uten hjelp?	Innen 3 minutt?	Notater
1.1 - 1.4	6 av 7 - ja 1 av 7 - nei	7 av 7 - ja 0 av 7 - nei	Biometri ble kun testet på en av brukerene, grunnet tekniske problemer på den ene brukerens mobil. Den ene brukeren gjorde en "slurvefeil" ved autentisering med sikkerhetsnøkkel, ellers ingen problemer.

Tabell 5.10: Autentiseringsdel - kvantitative verdier

Kvalitative data kan oppsummeres slik:

- Den ene testdeltageren fikk hovedsakelig ikke hjelp av testmoderator, men fikk støttende "feedback" fra assistenten som var tilstede gjennom hele testen. Deltageren fikk gjennom hele testen hint og tips på hva hen skulle gjøre av assistenten. Det var tydelig at brukeren ikke hadde klart de fleste av oppgavene hvis det ikke var for denne støtten. Testmoderator aksepterte dette, ettersom i en reell situasjon, er det usannsynlig at brukerene er nødt til å registrere seg på Omhu-appen uten noen form for hjelp og støtte fra en assistent eller et familiemedlem. Det ble dessuten tydelig under testen at det ikke er realistisk å anta at brukerene skal klare å registrere seg helt alene, uten hjelp fra andre. Den andre testdeltageren fikk ikke hint og støtte fra assistenten i like stor grad, noe som resulterte i at testmoderater måtte vise hen hvordan hen skulle løse oppgaven ved mange flere anledninger, i forhold til den første testdeltageren.
- Den første testpersonen fikk til nesten alle punktene under test av registreringsdelen. Det var tekniske problemer under biometri-delen, og demoen fungerte ikke på testpersonens egen mobil. Selv om brukeren brukte biometri som opplåsning på mobilen, så fungerte det altså ikke på demoen. Bruk av biometri som autentiseringsfaktor var vellykket på den andre testpersonens mobil.
- Den ene testdeltakeren slet med å bruke sikkerhetsnøkkelen riktig. Hen måtte bli vist tre ganger hvordan hen skulle gjøre det. Dette var samme deltaker som fikk mye hjelp og støtte fra assistenten, og assistenten skjønte heller ikke hvordan de skulle løse dette. Grunnen var at bruk av sikkerhetsnøkkel krever en viss "teknikk", som testdeltakeren slet med. Den andre testdeltakeren opplevde tekniske problemer, men når problemene ble fjernet av testmoderator, klarte deltakeren å registrere sikkerhetsnøkkelen på første forsøk.

Etter overnevnte brukertest, ble prototypen til pasientmodulen testet. Etter dette ble et kort, kvalitativt intervju gjennomført på testdeltakerne. Se vedlegg D. Intervjuet ble gjennomført for å innhente preferanser og meninger, samt for å få et overblikk over målgruppas ferdigheter og holdninger til mobilbruk, sosiale medier og appbruk generelt.

Resultatene fra intervjuet kan oppsummeres slik:

- Begge testdeltagerne bruker ansiktsgjenkjenning på mobilen.
- Begge er på alle "vanlige" sosiale medier, som facebook og Snapchat. Ingen av de logger inn på sosiale medier noen gang, fordi de aldri logger ut, og får hjelp av andre dersom de får ny mobil eller lignende.
- Begge liker biometri godt som autentiseringsmetode. Den ene liker ansiktsgjenkjenning bedre enn passord.
- Den ene testdeltageren liker sikkerhetsnøkkel som autentisering veldig godt, dette var den samme deltageren som ikke hadde problemer med å bruke den. Den andre deltageren likte sikkerhetsnøkkel mye bedre enn passord, men ville helst brukt biometri fremfor sikkerhetsnøkkel.
- Ingen av de har noe problem med å bruke en fysisk gjenstand som autentiseringsfaktor, men den ene får hjelp av assistenter til å passe på gjenstander når hen er ute.
- Ingen av de kunne tenkt seg å bruke passord, begge glemmer passord lett, og må skrive det ned i en bok.
- Begge har god kontroll på mobilen, og mister den aldri eller sjeldent.
- En av testdeltagerne har tilgang til BankID, i motsetning til mange i målgruppa, og får til å bruke denne. Hen påpeker at det er irriterende med push-varslinger og dette med å gå "inn og ut" av appen når hen skal autentisere seg.

5.4 Kvantifisering av egenskaper for autentiseringsmetoder

Som autentiseringsmetode ble det vurdert og analysert flere ulike alternativ. Tofaktor autentisering ble tidlig bestemt at er et krav, grunnet Omhu-appens krav til sikkerhetsnivå *betydelig*, se kapittel 2.1.3.

I dette underkapitlet vil forskjellige autentiseringsfaktorer bli beskrevet, og deretter kvantifisert. Kvantifisering av verdiene *brukervennlighet, sikkerhet, implementasjon og kostnad* har blitt gjort for å lettere kunne sammenligne de ulike autentiseringsfaktorene.

5.4.1 Tradisjonelle autentiseringsfaktorer - *noe en vet*

Tradisjonelle autentiseringsfaktorer er en av de mest brukte autentiseringsmetodene gjennom tidene, og de utgjør en kritisk del av sikkerhetsinfrastrukturen for både individuelle brukere og organisasjoner. Denne formen for autentisering er basert på noe en enkelt person vet, og det er vanligvis representert av et passord eller en PIN-kode. Denne enkle, men effektive tilnærmingen til autentisering har dominert landskapet for digital sikkerhet i årevis, og den har vært fundamentet for adgangskontroll til alt fra personlige datamaskiner til globale bedriftsnettverk.

Mens tradisjonelle autentiseringsfaktorer har tjent sitt formål godt, har de også blitt gjenstand for kritikk og utfordringer. For eksempel er passord ofte sårbare for hacking, spesielt hvis de er svake eller gjenbrukes på tvers av ulike kontoer. I tillegg kan brukere glemme eller miste passordene sine, noe som kan føre til frustrasjon og behov for omfattende gjenopprettingsprosesser.

Dette kapittelet vil utforske tradisjonelle autentiseringsmetoder som kan være relevante som innloggingsløsninger.

Passord

Bakgrunn Passord som autentiseringsfaktor har vært blant de mest brukte autentiseringsfaktorene. Tradisjonelt har passord vært en av de mest brukte metodene for digital autentiserig, men har hatt en avtagende popularitet de siste årene pga. større fokus rundt digital sikkerhet. Når brukeren lager et passord, blir det så lagret på autentiseringstjenestens database, vanligvis kryptert. Selv om populariteten er avtagende, er likevel passord som autentiseringsalternativ ennå en av de mest brukte enkeltfaktorene i digitale løsninger [36]. Det er dermed ingen tvil om at passord er en av det mest populære autentiseringsmetodene per dags dato, og kommer til å være det i mange år fremover.

Sikkerhet Sikkerheten til bruk av passord varierer veldig. Et avansert passord med små og store bokstaver, tall og spesialtegn er mye mer sikkert enn et enkelt ord. Dette er pga. at lengre og mer komplekse passord er vanskeligere å "brute force", eller å gjette seg til. Sluttbrukere har dessuten en tendens til å bruke samme passord flere steder, noe som påvirker sikkerheten betraktelig. Dersom det skjer et databasebrudd på en server hvor passord kommer på avveie, går det også ut over andre kontoer som er beskyttet med det samme passordet. Hvordan passordet blir lagret er også en sårbarhetsfaktor. I en godt beskyttet database, der passordene er kryptert med sikre algoritmer, er passordet mye sikrere mot å komme på avveie, enn i en dårlig beskyttet database som ikke har kryptert passordene, men hvor passordene

ligger i "plaintext". Avanserte passord er dessuten noe som er lett å glemme, og krever som oftest å bli notert ned ett sted. Hvor sikkert passordet blir oppbevart, er helt opp til brukeren, og dermed utenfor applikasjonens kontroll. Alle har hørt om den klassiske "post-it lapp på dataskjerm" snarveien mange brukere har tatt opp gjennom. Om passord er sikkert å bruke som autentiseringsfaktor varierer dermed fra "veldig usikkert" til "veldig sikkert" avhengig av gjennomføringsevenen til brukeren. Dette kan forbedres med utfyllende opplæring på god passordhygiene og / eller hardkoda retningslinjer for passord, som f.eks tvinger brukere til å bruke minst 12 tegn. På grunn av passordets mange sårbarheter samt den manglende evnen for håndheving av sikkerhetsrutiner får passordet sikkerhetsvurdering *moderat*.

Brukervennlighet Passord er veldig intuitivt, men er middels brukervennlig pga. behovet for kompleksitet. Et passord bør være av en viss lengde og kompleksitet for å være sikkert nok, noe som påvirker brukervennligheten negativt. Komplekse passord er vanskelige å huske, og kan dermed kreve at en noterer det ned og plasserer det på et trygt oppbevaringssted, enten fysisk eller digitalt. Dette gjør det litt vanskeligere å få tak i når en trenger det. Om passord er brukervennlig eller ikke, avhenger derfor av brukerens evne til memorering av passord. I breddetesten av autentiseringtyper (se kap 5.1 og vedlegg D) var det ingen brukere som hadde problemer med passord, men det ble gitt kommentarer på at lengde-kravet på 12 tegn gjorde det vanskelig å huske. I den videre sammenligningstesten rangerte passord lavest av alle testede autentiseringsmetoder. Dette var noe overaskende, men kan være grunnet deltagerene sin erfaring med misnøyen av å måtte memorere flere passord til en hver tid. I motsetning til mange andre autentiseringsmetoder, vil passord bli vanskeligere å huske jo flere av dem en bruker. Grunnet det strenge kravet for memorering og misnøyen vist i brukertestene, blir passord dermed gitt en vurdering av *krevende* brukervennlighet.

Kostnad Svært billig å implementere. Utover den grunnleggende kostnaden for databaser og eventuelt servere, som vi i denne kartleggingen ikke regner med i kostnaden, krever ikke implementasjonen av passord autentisering noen ekstra utgifter. Tvert i mot, kan en påstå at passord er den mest grunnleggende, og også billigste formen for autentisering som er realistisk å bruke. Dermed får passord kosntad's vurderingen *ubetydelig*.

Implemententasjon Implementeringen av passordsikkerhet er relativt enkel, da det finnes et bredt utvalg av eksisterende dokumentasjon og løsninger som veileder i å sikre passord på best mulig måte. Med den omfattende dokumentasjonen tilgjengelig er det enkelt å implementere en løsning basert på beste praksis. Dette inkluderer hash-kryptering av passord i databasen, implementering av passordpolicyer og fastsettelse av utløpsdatoer for passord. Ettersom de fleste andre autentiseringsmetoder ofte bygger på passordsystemet, kan dette betraktes som grunnleggende nivå for selvutviklede auten-

tiseringsløsninger.

Fra et organisatorisk perspektiv innebærer passord som innlogging at ansatte trolig må hjelpe brukere huske eller skrive ned passord.

Utifra den grunnleggende implementasjonen samt minimale påvirkning på arbeidsrutiner passord vurderingen "enkelt".

Dekning For at en bruker skal kunne utnytte passord for innlogging, er det ingen krav for enhet, da passord kan brukes på bortimot alle digitale enheter laget de siste 20 årene. Dekningen for passord er dermed vurdert til "optimal".

5.4.2 Biometriske autentiseringsfaktorer - *noe en er*

I moderne tid har biometriske autentiseringsfaktorer blitt stadig mer populære, spesielt blant mobilbrukere, og de representerer en betydelig utvikling innen sikkerhetsteknologi. Denne autentiseringsmetoden er basert på noe en person er, og den bruker unike fysiske eller atferdsmessige egenskaper for å verifisere identiteten til en individuell bruker.

Det som gjør biometriske autentiseringsfaktorer så populære, er den høye graden av unikhet og sikkerhet de tilbyr. Hvert individ har unike biometriske egenskaper, og dette reduserer sjansene for at uautoriserte personer kan få tilgang ved å bruke en annen persons biometriske data. For eksempel er det svært usannsynlig at to personer har identiske fingeravtrykk, noe som gjør fingeravtrykksautentisering til en pålitelig og sikker autentiseringsmetode.

I tillegg til fingeravtrykk inkluderer biometriske autentiseringsfaktorer også andre metoder som ansiktsgjenkjenning, irisavlesning, stemmegjenkjenning og selv adferdsbiometri som gjenkjenner mønstre i en persons tastatur- eller skrivestil.

Selv om biometriske autentiseringsfaktorer har mange fordeler, møter de også en rekke utfordringer som må håndteres for å sikre deres effektivitet og pålitelighet. En av de største utfordringene er personvernsbekymringer. Fordi biometriske data er knyttet direkte til en persons unike identitet, er det en risiko for at disse dataene kan bli misbrukt eller kompromittert. Hvis biometriske data blir stjålet eller lekket, kan det være vanskelig eller umulig å erstatte dem, noe som gjør dem potensielt sårbare for misbruk i lang tid.

En annen utfordring er nøyaktigheten og påliteligheten til biometriske sensorer og algoritmer. Selv om biometriske autentiseringsmetoder som fingeravtrykksavlesning og ansiktsgjenkjenning har blitt stadig mer avanserte, er det fortsatt muligheter for feilaktig identifikasjon eller avvisning av legitime brukere. Dette kan føre til frustrasjon og redusert brukertillit, spesielt hvis autentiseringsprosessen blir for plagsom eller upålitelig. ¨

Dette kapittelet vil utforske noen biometiske autentiseringsmetoder som kan være relevante som innloggingsløsninger.

Iris-scanning

Bakgrunn Å bruke iris som biometrisk autentisering blir regnet som den sikreste biometriske autentiseringsmetoden. Iris, som er den fargelagde delen av øyet, er unikt for hver person, og endrer seg typisk ikke med tiden. Dette gjør

iris til en ideell biometrisk faktor, som er en autentiseringsfaktor i kategorien *noe man er*.

Sikkerhet Iris-gjenkjenning har den høyeste nøyaktigheten av alle biometriske faktorer. False acceptance rate (se false acceptance rate (FAR) i ordbok) er regnet til 1 per 10 millioner scanninger, noe som innebærer at en falsk positiv er ekstremt sjeldent [37]. For å spoofe en denne formen for autentisering med en god sjanse for å lyktes ville det krevet avansert 3D printing, fysisk tvang av irisen's eier eller avanserte former for sosial manipulasjon. Denne eksreme sikkerheten gir iris-scanning lett en status som *svært sterk*.

Brukervennlighet Sammenlignet med andre biometriske autentiseringsmetoder er ikke iris-skanning den mest brukervennlige. For å autentisere seg med iris-skanning må brukeren løfte kameraet på mobilen helt opp mot øyet, noe som kan oppleves som ubehagelig og/eller tungvindt. Det samme problemet oppstår under registrering, da brukeren må gjennom en engangsprosess for å fange øyet på et høykvalitets infrarødt kamera. Siden det er lite sannsynlig at sluttbrukeren allerede har et slikt kamera, vil dette kreve en reise til en ekstern operatør for å utføre skanningen [38]. Denne prosessen vil være oppnåelig for en enkeltperson, men har åpenbare utfordringer dersom man velger å implementere dette systemet for en større brukerbase innenfor en institusjon. Det har ikke blitt samlet data på brukervenligheten av iris-scanning i denne studien, men grunnet den lange prosedyren for registrering av legitimasjon, samt stegene krevet for å gjennomføre hver enkelt autentisering, vil iris-scanning rangeres som "krevende".

Kostnad Å implementere irisgjenkjenning krever tilgang til et spesialkamera designet for å skanne iris. Dette bildet fungerer som en mal for hvordan hver enkelt iris skal se ut, og det er dette bildet alle senere iris-skanninger blir sammenlignet med i en database. Slike kamera koster vanligvis rundt 5000 kroner.

For å skanne iris for autentisering, må brukeren også ha en mobiltelefon med et kamera som har implementert IR-blaster. Per dags dato har svært få mobiler denne funksjonen. Kun noen få Android-mobiler, som for eksempel Samsung Galaxy S8, har dette. Ingen iPhones har slike kameraer ennå, og veldig få bærbare datamaskiner har det per dags dato.

Som det utdypes om i neste avsnitt, vil denne formen for autentisering pådra seg enda mer kostnader i form av software-as-a-service programvare som en plugger inn i systemet. Dette gjør at iris-scanning, alt i alt, er en av de mer kostbare formene for autentisering. Denne formen for autentisering rangeres som *svært kostbar*.

Implementasjon Implementasjon av iris-skanning behøver ikke nødvendigvis være svært avansert. Det finnes flere selskaper som tilbyr iris-skanning som en tjeneste. Selv om det medfører kostnader å anskaffe slike tjenester, blir det

mindre utfordrende å implementere programvare og databaser selv. Aware er for eksempel en leverandør som tilbyr implementering av iris-skanning for autentisering [39]. Men, som nevt i avsnittet om kostnad, kommer de fleste problemene med denne formen for autentisering fra den markante logistikken som må til for gjennomføring. Prosessen av å implementere egne mobiler for brukere med den nødvendige kamerateknologien, samt et system for registrering av legitimasjoner med IR-kamera, fører til store orginistaoriske og logistiske utfordringer, noe som setter implementasjoen til iris-scanning i kategorien *svært krevende*.

Dekning Som nevnt tidligre i denne seksjonen, krever iris-scanning teknologier som hittil (V2024) ikke er utbredt til vanlige mobiltelefoner. Grunnet den relativt sjelne forekomsten av mobiler som støtter denne autentiseringsformen, er dekningen vurdert til "svært dårlig".

Geolokasjon

Bakgrunn Geolokasjon er en måte å la web-applikasjonen se hvor enheten, og dermed brukeren som prøver å logge seg på, befinner seg i verden. Av personvernshensyn blir brukeren spurt om tillatelse av applikasjonen til å dele posisjonen sin på forhånd, noe brukeren må tillate for at geolokasjon skal funke. Geolokasjon kan hindre at brukere som ikke befinner seg utenfor et gitt geografisk område, kan logge seg inn. Det er også mulig å overvåke tidsintervallet mellom to ulike påloginger, slik at påloginger i ulike steder av verden som krever en "umulig reise" for brukeren, ikke skal bli godkjent. Dette vil forhindre at uvedkommede utenfor et gitt område ikke kan logge seg inn, selv om vedkommede hadde klart å fått tak i de to andre faktorene, som SMS-kode og passord. Dette gjør geolokasjon til en god tredje faktor i innlogging på en brukerkonto, ettersom geolokasjon ikke er sikkert nok til å være faktor en eller faktor to, men fungerer som en ekstra sikkerhetsfaktor i applikasjonen.

Sikkerhet Som nevnt i innledningen, er ikke geolokasjon sikkert nok som en hovedfaktor i autentiseringen. Dette pga det er relativt enkelt å bruke VPN eller andre verktøy for å manipulere enheten til å vise en annen lokasjon enn den faktiske lokasjonen. Det er mange måter å implementere geolokasjon på, deriblandt kan en bruke enhetens innebygde GPS med svært høy presisjon, eller man kan bruke IP-basert geolokasjon [40]. IP-basert geolokasjon er den vanligste måten å finne enhetens lokasjon på, og baserer seg på at applikasjonen ser på enhetens IP-adresse for å bestemme hvor i verden den befinner seg. Dette er den minst nøyaktige måten å finne lokasjon på, og samtidig den letteste måten for uvelkommede å manipulere enheten til å vise en annen lokasjon enn enheten faktisk er. Slik manipulasjon er lett gjennomførbart for personer uten teknisk kompetanse, det er derfor aldri

anbefalt å bruke denne metoden som en første eller andre faktor. Grunnet den ekstremt lave terskelen for spoofing av denne autentiseringsfaktoren, er den rangert som *svært svak*.

Brukervennlighet Geolokasjon er svært brukervennlig. Når brukeren først logger inn på applikasjonen, må hen trykke "tillat", slik at applikasjonen kan se hvor enheten befinner seg. Dette vil variere mellom ulike måter å implementere på. Bortsett fra dette, kommer ikke brukeren til å merke at geolokasjon er implementert. Det er imidlertig et personvernhensyn å ta, ettersom webapplikasjonen vil ha tilgang til brukerens omtrentlige lokasjon hver gang brukeren logger inn og har applikasjonen åpen. Denne metoden er ikke testet, men ut i fra dens natur med bare null/en interaksjon med brukeren, kan denne enkelt klassifiseres som *svært enkel* å bruke.

Kostnader Innebygde API-er i JavaScript gir kostnadsfri tilgang til både IP- og GPS-basert geolokasjon. Ønsker man svært nøyaktig GPS-posisjon, kan det være nødvendig å utvikle en egen applikasjon for å få tilgang til denne funksjonen på mobiltelefonen, noe som vil øke kostnadene til den grad at geolokasjon ikke lenger er verdt og utnytte. Men dersom man ikke har behov for ekstrem nøyaktighet i GPS-lokasjonen, vil løsningen presentert i HTML5 være tilstrekkelig. Kostnadene her er dermed neglisjerbare og blir kategorisert som *ubetydelig*.

Implementasjon Implementasjonen av geolokasjon kan være relativt enkel hvis man velger den raskeste løsningen. Brukerens lokasjon kan hentes ut ved hjelp av noen få funksjoner i et innebygd JavaScript API. Både Google og Mozilla tilbyr grundig dokumentasjon om hvordan man implementerer geolokasjon i JavaScript [41, 42]. Implementasjon av geolokasjon som autentisering er dermed "enkelt".

Ansiktsautentisering

Bakgrunn Ansiktsautentisering, "face authentication", er metoden for å gjenkjenne et individ som prøver å autentisere seg på det gitte systemet eller applikasjonen. Metoden bruker ansiktet som autentiseringsfaktor, og er dermed en biometrisk faktor. Ansiktsautentisering skiller seg fra ansiktsgjenkjenning, "facial recognition", ved at ansiktsgjenkjenning baserer seg på å finne et spesifikt individ i en gruppe med mennesker. Ansiktsautentisering skal verifisere at det gitte ansiktet som prøver å autentisere seg, faktisk er den korrekte personen [43].

Prosessen ved ansiktsautentisering starter ved at ansiktstrekkene blir kartlagt, enten fra et bilde eller i virkeligheten. Algoritmer regner ut ansiktets egenskaper, som avstanden fra pannen til haken, eller vidden på munnen.

Dette blir til en digital kode, også kalla et "faceprint", og vil fungere som en mal for ansiktet [43]. Det er denne malen som senere ansiktsautentiseringer vil bli sammenlignet med.

For å implementere ansiktsautentisering, finnes det flere måter å gjøre det på. Avhengig av hvilken metode som blir implementert, vil vanskelighetsgraden i implementasjon, dekning i brukerbasen og kostnaden knyttet til løsningen variere. De to ulike metodene skissert i dette kapitlet, er å bruke mobile enheter's innebygde ansiktsgjenkjenning, som Apple's FaceID, eller å bruke Azure AI Face service, levert av Microsoft.

Metode 1 - Bruk av mobile enheters innebygde ansiktsgjenkjenning
Blant mobiler, har både Android- og iPhone-enheter implementert ansiktsautentisering, i utgangspunktet blir det brukt for å ha en alternativ måte å låse opp mobilen uten bruk av passord/kode. Denne teknologien er i stadig utvikling, og begynner å bli mer utbredt på nyere bærbare datamaskiner. Ettersom mange moderne enheter, spesielt mobiler, allerede har ansiktsgjenkjenningsteknologi innebygd i operativsystemet, er det fordelaktig å utnytte denne muligheten i stedet for å kjøpe dyre lisenser og implementere avanserte systemer. Denne formen for ansiktsgjenkjenning kan nås gjennom WebAuthn/FIDO2 rammeverket i Javascript.

Metode 2 - Bruk av Microsoft Azure AI Face service
Microsoft's Azure AI Face service, er en software basert på kunstig intelligens. Den kunstige intelligensen er i stand til å oppdage, kjenne igjen og analysere ansikter i et bilde, enten i et statisk 2D bilde, eller i sanntidsvideo der personen blir kjent igjen og autentisert i sanntid. Servicen har en rekke ulike bruksområder, blant annet å kjenne igjen ulike mennesker på et bilde, til å kjenne igjen mennesker som bruker briller, eller å verifisere personer i en autentiseringssammenheng.

Sikkerhet Ifølge Apple har Face ID en False Acceptance Rate (FAR) på 1:1 000 000, betydelig bedre enn 1:50 000 for TouchID [44]. Dette er en av hovedårsakene til at Apple faser ut fingeravtrykksteknologien til fordel for FaceID. Sanntidsvideo benyttes hyppig i ansiktsautentiseringsteknologi for å motvirke spoofing, altså forsøk på å lure programmet til å tro at personen som prøver å autentisere seg faktisk er den rette personen, f. eks. ved hjelp av et bilde. Gjennom sanntidsvideo kan algoritmen observere livligheten i ansiktet som ikke hadde vært synlig gjennom et statisk bilde.

Det er viktig å merke seg at teknologien for ansiktsautentisering varierer mellom leverandører, noe som naturligvis medfører variasjoner i sikkerhetsnivået. Algoritmene som brukes varierer, og noen implementerer også kunstig intelligens (AI) i prosessen.

Grunnet de omfattende tiltakene som må til for å spoofe ansiktsgjenkjenning og den smale angrepsflaten trusselaktører har å jobbe med, vurderes ansiktsgjenkjenning som *sterkt*.

Brukervennlighet Ansiktsgjenkjenning er jevnt over en svært brukervennlig form for autentisering som for det meste går av seg selv. Brukeren som autentiserer seg behøver kun vise ansiktet for kamera i noe grei belysning, og autentiseringen vil gjennomføres. Hastigheten for ansiktsgjenkjenning ble demonstrert i brukerundersøkelsen(se kap 5.1) da den gjennomsnittlige tiden brukt for en autentiseringen var på under to sekunder. Denne tiden kom fra både fingeravtrykk og ansiktsgjenkjenning, men da begge autentiseringsfaktorene hadde omtrentlig samme hastighet, er dette tallet representativt. Testen viste også ansiktsgjenkjenning og fingeravtrykk som den soleklare vinneren, da det var disse metdoene som deltagerene samlet mente var mest brukervennlig(se kap 5.1.3).

Det kan oppstå problemer med bruk av hatt, maske, briller eller andre hodeplagg. Samt at personer med raskt endrende utsende, f.eks barn, regelmessig må oppdatere autentiseringen for at den skal fortsette å fungere.

Disse problemene er derimot marginale til brukervennligheten av ansiktsgjenkjenning. Grunnet den høye hastigheten, lave kompleksiteten og ikkeeksisterende krav til brukerens hukommelse kategoriseres ansiktsgjenkjenning som *svært enkelt*.

Kostnad Om en går utifra at alle brukere har tilgang på ansiktsgjenkjenning med sin mobil, kan FIDO2/webauthn brukes for å implementere ansiktsautentisering uten ekstra kostnader utover utvikling og standard driftsavgifter. Dermed vil kostnaden for ansiktsgjenkjenning kategoriseres som *ubetydelig*.

Implementasjon Implementasjonen av ansiktsgjenkjenning kan gjennomføres rimelig enkelt med hjelp av FIDO2/webauthn som dokumentert i 4.1. Webauthn er grundig dokumentert, og med rette kode-biblioteker vil den største delen av arbeidet allerede være gjennomført for utviklerene. Ansiktsgjenkjenning er også en svært sømløs autentiseringsmetode å utnytte, da den ikke medfører noe ekstra arbeid for ansatte eller brukere av institusjoner. Utifra den relativt milde kravet for teknisk implementasjon, vil ansiktsgjenkjenning kategoriseres som *enkelt* å implementere.

Dekning Ansiktsgjenkjenning er en utbredt teknologi som finnes i de fleste mobiler, og dermed kan nås gjennom webauthn. I 2022 rapporterte Cisco at 81% av mobiler utnytter biometrisk innlogging [45]. Dette estimatet er derimot trolig lavt, da data fra Telia viser at de mest solgte brukte mobilene i Norge Q4 2023 var dominert av nyere iPhone modeller [46], som alle har tilgang på ansiktsgjenkjenning. Det er dermed trykt å anta at i minimum 80% av brukere vil ha tilgang på ansiktsgjenkjenning gjennom sin mobil, selv om dette tallet antageligvis er høyere. Dekningen rangeres dermed som *god*.

Autentisering ved bruk av fingeravtrykk

Bakgrunn Scanning av fingeravtrykk er en form for biometrisk autentisering som tar utgangspunkt i hver persons unike fingeravtrykk for å identifisere brukeren. Biometri med fingeravtrykk har eksistert lenge, men ble popularisert for mobil-autentisering med lanseringen av Apple iPhone 5S i 2013 [47, 48]. I dag er ikke fingeravtrykk en veldig utbredt form for mobil-autentisering. Apple har faset ut fingeravtrykk til fordel for ansiktsgjenkjenning (se kap. 5.4.2). Scanning av fingeravtrykk er derimot en rask og sikker form for autentisering med meget god brukervennlighet.

Sikkerhet Når man diskuterer autentisering ved bruk av fingeravtrykk, kan metodene deles inn i to kategorier: Apple Touch-ID og Androids tilsvarende. Som spesifisert på side 12, kategoriserer Android sikkerheten for biometriske sensorer i tre klasser. Hvis vi antar at Omhu implementerer web-applikasjonen på en måte som tillater bare klasse 3 fingeravtrykk, vil autentiseringen ha relativt god sikkerhet. Android krever at autentiseringen skal ha en spoof acceptance rate"(se “” i ordbok) under 7% for PAI-species A, 20% for PAI-species B, og 40% for PAI-species C [16]. Se presentation attack instrument (PAI) i ordbok for beskrivelse av de ulike nivåene for “presentation attack instrument”. Med mindre en av Omhus sluttbrukere er en offisiell person av særdeles høy status, er det svært usannsynlig at et angrep høyere enn nivå A vil forekomme. Med et målrettet angrep kan man forvente at 7% av disse angrepene vil være vellykket. Selv om denne figuren virker høy, er det med et såpass høyt sikkerhetsnivå sannsynlig at angripere vil rette seg mot et annet, svakere punkt i sikkerhetssystemet dersom de har motivasjon til å få uautorisert tilgang til systemet.

Angrep med fingeravtrykk-spoofing inkluderer vanligvis å løfte målets fingeravtrykk fra en overflate av glass, for eksempel et bord eller mobilens skjerm. Dette krever fysisk tilstedeværelse for å utføres, noe som begrenser angrepsflaten dramatisk og dermed unngår opportunistiske trusselaktører som opererer gjennom nettet. Den største trusselen med tanke på fingeravtrykk vil i all hovedsak være ansatte som jobber på institusjonene Omhu har som kunde, da disse personene vil ha rikelig med muligheter for å løfte fingeravtrykk, og samtidig ha relativ enkel tilgang til sluttbrukerens enhet.

Android krever at klasse 3 biometri oppfyller kravet om en false acceptance rate"(se “FAR” i ordbok) mindre enn 1/50 000 forsøk [16]. Sammenlignet med andre former for biometri er dette ikke det beste som finnes, men det regnes som tilstrekkelig med tanke på at mobilen bytter tilbake til tradisjonell autentisering etter tre mislykkede forsøk. Samtidig krever Android at falske negativer ikke kan forekomme i mer enn én av ti innloggingsforsøk [16].

Apple sin Touch ID har ikke like mye informasjon ute som Android. Likevel kan den vise til lignende rater for falske positiver som Android sin klasse 3

fingeravtrykk. Ifølge Apple rapporteres det at Touch ID har en FAR på 1/50 000, men denne raten kan øke til cirka 1/10 000 etter hvert som brukeren legger til flere fingeravtrykk på enheten [44]. Apple har ikke delt informasjon om spoof acceptance rates, men det kan antas at deres verdier er sammenlignbare med standardene til Android.

Ettersom spoofing av fingeravtrykk krever at trusselaktøren har fysisk tilgang til brukerens fingeravtrykk, f. eks. ved å kopiere fingeravtrykket fra en overflate, krever det målrettet planlegging og fysisk tilstedeværelse. I motsetning til passord er det svært lite sannsynlig at en trusselaktør kunne ha skaffet en persons fingeravtrykk med phising eller lignende, ikke fysiske angrep. Derfor er sikkerhetsnivået rangert som *sterk* sikkerhet.

Brukervennlighet Årsaken til at fingeravtrykk ble tatt i bruk, er blant annet dens kombinasjon av sikkerhet og praktisk bruk. Når et fingeravtrykk først er registrert på en enhet, blir det svært enkelt å benytte. Autentiseringen aktiveres når brukeren utfører en handling som krever autentisering; da vil det dukke opp en pop-uppå mobilen. Brukeren trykker fingeren mot sensoren, som registrerer fingeravtrykket og gir brukeren tilgang. Autentiseringsprosessen ved bruk av fingeravtrykk er svært rask. Dette gjør den ideell som erstatning for lav-nivå passordløsninger som pin-koder, som er relativt enkle å avlese eller stjele basert på hvor ofte man låser opp mobilen.

Fingeravtrykk kunne vært en lovende metode da den er utrolig enkel å bruke og gir tilstrekkelig sikkerhet i kombinasjon med andre faktorer. I Omhus implementasjon vil brukeren skrive inn sitt brukernavn og trykke Logg inn". Deretter vil det dukke opp en forespørsel om fingeravtrykk, som brukeren svarer på ved å skanne sin finger. Etter dette vil Omhu gå videre til neste form for autentisering før brukeren blir logget inn.

Brukertesten gjennomført for å sammenligne brukervennligheten til autentiseringsmetoder (se kap 5.1 og vedlegg D) viste at deltagerene i snitt brukte under to sekunder på å gjennomføre en autentisering med biometri, der ansiktsgjenkjenning og fingeravtrykk viste lignende ytelse. Også i senere tester gjennomført på webauthn demostrasjonen dokumentert i kapittel4.1 skjedde det aldri at en deltager hadde problemer med å forstå eller gjennomføre autentisering med fingeravtrykk.

Begrunnet høy hastighet og lav kompleksitet er autentisering med fingeravtrykk rangert som *enkelt*. Årsaken til at metoden unngår rangeringen som "svært enkelt" er kravet om å presse fingeren mot mobilen, som muligens må forklares med førstegangsbruk. Dette er derimot ubetydelig ettersom brukeren venner seg til autentiseringen.

Kostnad I utviklingsfasen påløper det ingen ekstra kostnader knyttet til bruk av fingeravtrykk for autentisering, ettersom hele autentiseringsløsningen allerede er integrert i mobilens operativsystem og primært utføres på klientens side med hjelp av webauth/FIDO2. I motsetning til f. eks. Azure Face API,

er det ingen ekstra tjeneste involvert for at systemet skal fungere. Dette gjør fingeravtrykks-autentisering økonomisk gunstig, og kostnaden knyttet til fingeravtrykk er derfor rangert som *ubetydelig*.

Implementasjon Implementasjonen av fingeravtrykk som autentiseringsfaktor er i utgangspunktet enkelt å gjennomføre for en gjennomsnittlig utvikler.

Dette skyldes at Google WebAuthn-rammeverket som er integrert i JavaScript kan brukes. Ved hjelp av dette rammeverket får utvikleren tilgang til en API for brukerens smarttelefon, som fullfører autentiseringen lokalt på enheten i en isolert modul dedikert til biometrisk autentisering [49]. Sett fra utviklerens perspektiv fungerer autentiseringen som en standard "challenge-responseautentisering. Google Developers har en utmerket kodelab funnet under

Fingeravtrykk har heller ingen negative orginisatoriske konsekvenser for ansatte med kundene av Omhu.

Grunnet den utbredte dokumentasjonen og enhets-støtten for teknologien, samt den sømløse integrasjonen i kundens arbeidsrutine, rangeres fingeravtrykk som *enkel* å implementere.

Dekning Antall brukere som har mulighet til å bruke denne faktoren er begrenset. De fleste nyere iPhone-modeller har ikke TouchID implementert. Ettersom ca. 56% av norske smarttelefon-brukere bruker iPhone [50], er det mange som ikke har mulighet til å bruke dette alternativet. Dessuten har de aller fleste bærbare pcer eller nettbrett ikke denne funksjonen implementert, og dekningen blir derfor vurdert som *dårlig*.

5.4.3 Fysiske autentiseringsfaktorer - *noe en har*

Fysiske autentiseringsfaktorer representerer en annen viktig kategori innenfor autentiseringsteknologien. Disse autentiseringsfaktorene er basert på noe en person har, og de omfatter fysiske gjenstander eller enheter som brukes til å bekrefte identiteten til en bruker. Eksempler på fysiske autentiseringsfaktorer inkluderer smartkort, nøkkelkort, USB-token, og fysiske nøkler.

Denne autentiseringsmetoden har blitt utbredt i både bedriftsmiljøer og personlig bruk på grunn av sin pålitelighet og brukervennlighet. Fysiske autentiseringsfaktorer gir en ekstra lag med sikkerhet ved å kreve at brukeren fysisk har tilgang til den fysiske enheten eller gjenstanden for å få tilgang til systemer eller data. Dette gjør det vanskeligere for uautoriserte brukere å få tilgang til systemer selv om de har fått tak i brukerens legitimasjon, for eksempel brukernavn og passord.

Mens fysiske autentiseringsfaktorer har mange fordeler, møter de også visse utfordringer og begrensninger. En av utfordringene er risikoen for tap eller tyveri

av de fysiske enhetene. Hvis en bruker mister sitt smartkort eller nøkkelkort, kan det potensielt gi uautoriserte personer tilgang til systemer eller fasiliteter som er beskyttet av autentisering basert på disse enhetene.

En annen utfordring er kostnaden og kompleksiteten knyttet til implementering og vedlikehold av fysiske autentiseringsfaktorer. Produksjon og distribusjon av smartkort eller nøkkelkort kan være kostbart, spesielt for store organisasjoner med mange ansatte. I tillegg krever administrasjon av disse enhetene nøye håndtering for å sikre at de ikke blir misbrukt eller kompromittert.

Dette kapittelet vil utforske noen fysiske autentiseringsmetoder som kan være relevante som innloggingsløsninger.

Sikkerhetsnøkkel

Bakgrunn YubiKey er en sikkerhetsnøkkel produsert av Yubico. En sikkerhetsnøkkel, også kjent som en sikkerhetstoken, er en fysisk enhet ment for å bli brukt til multi-faktor autentisering. Enheten har gjerne form og størrelse som en minnepinne, noe som gjør den enkel å transportere. Forskjellige sikkerhetsnøkler tilbyr forskjellige tilkoblingsmuligheter, typisk USB-C eller NFC. Den konkrete YubiKey-en skissert i denne rapporten, Yubico Security Key C NFC, støtter tilkobling med begge disse metodene.

Sikkerhet Sikkerhetsnøkler tilbyr en pålitelig faktor i autentiseringsprosessen og regnes som et svært sikkert alternativ for tofaktorautentisering (2FA). De er motstandsdyktige mot både tradisjonelle og digitale hackerangrep, samt mot phishing og metoder knyttet til sosial manipulasjon. Imidlertid innebærer det fysiske aspektet ved nøkkelen en potensiell risiko for tap eller tyveri fra brukeren selv [51]. I tilfelle at en bruker mister sin sikkerhetsnøkkel til en potensiell trusselaktør, kan den likevel ikke brukes som eneste autentiseringsfaktor for pålogging til applikasjonen. Dette skyldes at sikkerhetsnøkkelen alltid må kombineres med en annen faktor, for eksempel et passord. Dette gir brukeren tid til å deaktivere nøkkelen og skaffe en ny.

YubiKey benytter sikre protokoller som WebAuthn/FIDO2, FIDO U2F, engangspassord (OTP), OpenPGP 3, og smartkortautentisering for å fullføre transaksjoner i autentiseringsprosessen [52]. Nøkkelen som er beskrevet i denne rapporten støtter imidlertid kun FIDO2/WebAuthn- og FIDO U2F-autentiseringsprotokoller.

Sikkerhetsnøkler er svært resistant mot phising og sosial manipulasjon, samt tekniske angrep, da den private nøkkelen aldri forlater enheten. For å forbipassere sikkerheten gitt av en sikkerhetsnøkkel vil en angriper være nødt til å gå til svært drastiske tiltak. Derfor er sikkerhetsnøkkel vurdert som *svært sikker*.

Brukervennlighet Når YubiKey-en først er satt opp på en enhet, er den nokså enkel å bruke. Når brukeren logger inn på Omhu, får de muligheten til å plugge nøkkelen inn i mobilens USB-C inngang eller bruke NFC for å skanne brikken med en sensor vanligvis plassert på mobilens bakside, hvis enheten støtter dette. Hvis mobilen ikke har en USB-C kontakt, kan man bruke en adapter for å koble den til alternative innganger som Micro-USB eller Apple's Lightning kontakt.

Utifra brukertestene gjennomført med sikkerhetsnøkkelen(se kap 5.1 og vedlegg D), var ikke denne metoden uten problemer. Brukere hadde ofte problemer med å få sikkerhetsnøkkelens NFC til å registrere. Menyene i operativsystemet en bruker for å selektere sikkerhetsnøkkelen var også et problem på flere tidspunkt, da brukere hadde vanskeligheter med å finne riktig knapp og trykke på. Dette kommer antageligvis av at sikkerhetsnøkkelen er en ny teknologi, som ingen av deltagerene hadde testet fra før. Likevel var de fleste deltagerene stort sett fornøyde med sikkerhetsnøkkelen. I delen av brukertesten der deltagerene fikk i oppgave å sammenligne autentiseringsmetodene, var sikkerhetsnøkkelen rangert som nummer tre av seks (se kap 5.1.3). Det samlede resultatet viser at kun de mest praktiske metodene som pin-kode og biometri var mer brukervennlig enn sikkerhetsnøkkel. Dette resultatet vise bety at nøkkelen er vanskelig å lære, men enkel å bruke etter at en har blitt vant til den.

Alt i alt er sikkerhetsnøkkelen noe kronglete, men fortsatt mulig å lære for brukerene. Grunnet de relativt komplekse stegene for både autentisering og registrering, samt den minimale mengden memorering nødvendig for å passe på et fysisk objekt, er sikkerhetsnøkkelens brukervennlighet vurdert som *moderat*.

Kostnad For selve YubiKey-en ligger de fleste modeller i prisklassen mellom 500 kr og 1000 kr per enhet. I denne rapporten er den rimeligste modellen, Yubico Security Key C NFC, valgt for testing. Nøkkelen koster omtrent 375 kr, inkludert frakt. Dette utgjør en engangskostnad, med mindre brukeren mister eller ødelegger nøkkelen. Skalert opp til eksempel-brukerbasen for Omhu på 2000 brukere vil sikkerhetsnøkkelen innebære en engangskostnad på 750 000kr, samt mindre summer for å dekke erstaning av mistede enheter. Utifra denne verdien vurderes sikkerhetsnøkkel som *kostbart*.

Implementasjon Sikkerhetsnøkkelen "YubiKey", har som tidligere nevnt støtte for FIDO2/webauthnn protokollen. Denne protokollen funker med å simplifisere implementasjonen av trygg autentisering, og gjør bruk av sikkerhetsnøkkel som autentisering svært enkelt fra en teknisk side. For mer om implementasjon av sikkerhetsnøkkel se kapittel 4.1.

Fra en organisatorisk synspunkt er implementasjonen noe mer komplisert, da det fysiske aspektet med sikkerhetsnøkkelen krever en viss innsats fra kundens side for å organisere og gjennomføre. Handlingene kundens an-

satte må gjennomføre innebærer deaktivering og erstatning av tapte sikkerhetsnøkkler, samt assistanse for sluttbrukere å holde styr på hvor sikkerhetsnøkkelen er lagt. Mer eller mindre av denne prosessen kan håndteres av Omhu.

Fra et teknisk synspunkt er sikkerhetsnøkkelen enkel å implementere, men grunnet de ekstra organisatoriske ressursene nødvendig å realisere denne formen for autentisering vil implementasjonen bli vurdert som *moderat*.

Dekning Sikkerhetsnøklen kan kobles til mobilen via USB-C eller NFC, samt andre kontakter om adaptere tas i bruk. Gitt fleksibiliteten til sikkerhetsnøklen vil bortimot alle mobiler være i stand til å utnytte denne autentiseringsmetoden. Dermed er sikkerhetsnøkkel vurdert til *optimal* dekning.

Autentiserings-applikasjon på mobil

Bakgrunn Mobilautentisering er i dag en svært vanlig løsning for to-faktor autentisering, og det er en effektiv måte å styrke innloggingsikkerheten på. Det finnes mange ulike autentiseringsapplikasjoner, og de fleste er gratis. Felles for de fleste er at de benytter TOTP (Time-based one-time password) for å generere engangskoder. Når brukeren logger inn på en applikasjon eller en nettside med brukernavn og passord, må de i tillegg oppgi den korrekte engangskoden fra autentiseringsapplikasjonen som en andre faktor.

De fleste autentiseringsapplikasjoner tilbyr også "number matching" som et enklere alternativ til engangskoder. Dette innebærer at et tallnummer genereres når brukeren forsøker å logge inn på den aktuelle kontoen. Dette tallnummeret er typisk et tosifret tall og må legges inn i autentiseringsapplikasjonen som en andre faktor. Dette skiller seg fra det tidligere nevnte engangspassordet via TOTP, da denne løsningen krever kommunikasjon med autentiseringsserveren og dermed nødvendiggjør internettilkobling.

Mobilautentisering har en betydelig grad av tilgjengelighet, gitt at de fleste i dag eier smarttelefoner. Dette gjør det lettere å integrere i folks daglige liv, og tilgjengeligheten til mobilautentisering er nesten konstant. Mange selskaper, inkludert store aktører som Google, Microsoft og Cisco, tilbyr løsninger for mobilautentisering. Dette understreker populariteten og pålitteligheten til denne sikkerhetstilnærmingen.

Sikkerhet Mobilautentisering er sikrere enn andre tradisjonelle metoder for to-faktor autentisering, slik som engangskoder via SMS eller e-post. Autentisering på mobil er sikker, da den lagrer koden for innlogging lokalt på enheten. Den eneste måten for en trusselaktør å få tilgang til koden på, er ved å infisere brukerens enhet med skadelig programvare. For eksempel kan malware forsøke å stjele koden ved å registrere tastetrykk eller manipulere mobilapplikasjonen. Normalt genererer appen en ny kode hvert 30 til 60 sekund. Denne dynamiske koden må deretter tastes inn på det aktuelle stedet du ønsker å logge inn. Den begrensede levetiden for koden gir et ekstra lag med sikkerhet, da en potensiell trusselaktør har betydelig mindre tid til å misbruke koden før den ikke lenger fungerer som autentisering [53]. Å bruke en autentiseringsapplikasjon er en av de mest brukte metodene for MFA, og samtidig en av de mest sikre metodene [54]. Koden blir derimot skrevet ut i plaintekst, og åpner dermed for muligheten av at angripere kan manipulere brukeren til å gi fra seg koden, for eksempel mens de utgir seg for å være kundeservice eller lignende. Å forbipassere en slik sikkerhetsbarriære krever altså en dedikert angriper som har motivasjon og kunnskap til å manipulere brukeren til å gi fra seg koden. Grunnet den smale angrepsflaten i kontrollerte omgivelser kategoriseres sikkerheten for denne metoden som *sterk*.

Brukervennlighet Når det gjelder brukervennlighet, kan mobilautentisering være en utfordring for vår målgruppe. Brukerne må potensielt navigere mellom innloggingsfanen på web-applikasjonen og autentiseringsapplikasjonen når de logger seg inn på mobilen. Prosessen forenkles noe ved pålogging via PC da brukeren ikke trenger å navigere gjennom flere faner på mobilen. Videre forutsetter mobilautentisering at brukeren logger inn med en dedikert konto på de fleste applikasjoner. Selv om denne konto-oppsettprosessen er en engangstrinn, innebærer den et ekstra steg for brukeren å fullføre for å kunne dra nytte av denne autentiseringsformen. Vanskelighetsgraden varierer også mellom ulike applikasjoner; noen bruker for eksempel et seks-sifret tall for autentisering, mens andre benytter "number matching", der brukeren må skrive inn et tilsvarende tall. Totalt utgjør denne formen for autentisering mange operasjoner med en tidsbegrensning, som kan oppleves som vanskelig for uerfarne brukere.

I brukertesten(se kap 5.1 og vedlegg D) gjennomførte deltagere både registrering og autentisering med autentiseringsapp av typen TOTP. Denne autentiseringsformen tok i snitt mest tid av alle de testede metodene, både for registrering og autentisering. Da ingen av deltagerne visste at det var mulig å kopiere koden, var dem i stedet nødt til å memorisere den eller skrive den ned. Dette resulterte i at deltagerene navigerte flere ganger mellom autentiseringsappen og innloggings-portalen før de fikk overført koden. I flere tilfeller ble autentiseringen deretter mislykket, da en kode kun er gyldig 30 sekunder. Dette førte til en suksessrate på brukertesten på bare fire av seks.

Autentiseringsappen var generelt mislikt av test-deltagerene. I den samlede vurderingen fra sammenlignings-oppgaven for autentisering falt autentiseringsapp på nest siste plass (se kap 5.1.3.

I forsvar av autentiseringsappen, rangerte en bruker denne som nr 2, da etter å ha blitt fortalt hvordan kopiering av tekst fungerer. Det kan være at denne appen vil score langt bedre om opplæring var inkludert i testen.

Autentiseringsappen er er tvilstilfelle når det kommer til brukervennlighet. Grunnet de mange stegene nødvendig for å bruke auteniseringsappen, samt det høye konsentrasjonsbehoved, krav om memorering og tidspress, er denne metoden vurdert som *krevende*.

Dette er til tross for at den var mer likt enn passord, i utgangspunktet virker enklere å bruke med langt færre steg og mindre tidspress. Dette skyldes antageligvis mengden passord en bruker er forventet å huske. Selv om autentiseringsappen er mer krevende å bruke, vil det fortsatt være grunn til å foretrekke denne over passord, da vanskelighetsgraden av autentiseringsapp ikke øker med antall legitimasjoner i bruk, slik som gjøres med passord.

Kostnad Kostnaden av å bruke autentiseringsapper varierer mellom ulike leverandører, men I utgangspunktet er de fleste applikasjonene gratis å laste

ned for brukeren. Det krever ingen lisenser eller lignende å implementere TOTP, så kostnad er derfor vurdert som *ubetydelig*.

Implementasjon De fleste produkter som benytter mobilautentisering har mye dokumentasjon om hvordan man kan implementere autentiseringen i sin egen web-applikasjon. Det finnes også rikelig med video-guider man kan følge når man implementerer denne sikkerhetsløsningen. For eksempel har Duo Security, utviklet av Cisco, god video-dokumentasjon som viser ulike måter å implementere produktet på [55]. De fleste plattformer for mobilautentisering tilbyr også API-er som man kan bruke for å integrere autentisering i sin egen applikasjon. Uansett er de fleste autentiseringsapper bygget opp på det samme konseptet og har mange likheter.

Valget mellom de forskjellige leverandørene vil hovedsakelig avgjøres av hvilken programvare og infrastruktur bedriften allerede benytter. Dette skyldes at de fleste autentiseringsapplikasjoner er utviklet av store teknologiselskaper som Google, Microsoft eller Cisco, og er ment å samhandle best mulig med deres egne produkter. Å implementere bruk av en ekstern autentiseringsapplikasjon er en nokså rett frem prosedyre som en gjennomsnittlig utvikler fint kan fullføre. Det er ikke en direkte "plug-in" implementasjon, men er helt standard for denne typen funksjonalitet.

Bruken av TOTP koder vil heller ikke pådra noen ekstra orginisatoriske konsekvenser, med unntak av at alle brukere må innstallere autentiseringsapplikasjonen på sin egen mobil.

TOTP er allerede godt utbredt og dokumentert, men mangler et universalt rammeverk slik som finnes med webauthn. Grunnet den minimale innvirkningen på kunden, samt tekniske krav fra utvikler er autenitseringsapp vurdert som *moderat*.

Dekning For å bruke denne autentiseringsfaktoren, trenger brukeren en smarttelefon. Det er ingen krav til spesielle funksjoner på mobilen, da autentiseringsapper pleier å være svært enkle. Ettersom de aller fleste nordmenn har en egen smarttelefon , er dekning kategorisert som *optimal*.

QR som autentiseringsfaktor

Bakgrunn Autentisering med QR-kort er et semi-originalt konsept gruppen har utviklet, der et fysisk ID-kort brukes til å lagre brukerens autentisering i en QR-kode som trykkes på kortet. For å lese av QR-koden og autentisere brukeren, scanner sluttbrukeren koden med hjelp av en kamerafunksjon i webgrensesnittet, altså et mobilkamera eller lignende. Ettersom Omhus' kundebase vanligvis består av relativt små bedrifter, vil det være praktisk å la hver kunde skrive ut og administrere QR-kort for sine egne sluttbrukere. Kortet vil ha omtrent samme størrelse som et vanlig ID-kort og inneholde personens navn, QR-kode, trykkedato, utløpsdato, logo, bilde, og andre relevante elementer.

For å registrere en ny bruker går sluttbrukeren gjennom registreringsprosessen på nettleseren. Når dette er ferdig, vil de få beskjed om at brukeren deres er opprettet, men låst, og at de må gå til IT-avdelingen/resepsjonen for å hente nøkkelkortet sitt. I resepsjonen vil en administrator ha et grensesnitt med alle brukere og deres registrerte nøkkelkort. Når en ny bruker registreres, kommer det en notifikasjon, og administratoren vil få muligheten til å generere et nøkkelkort til den nye brukeren. En PDF av kortet blir generert og lastet ned av administratoren, som deretter printer ut kortet og gir det til sluttbrukeren.

Sikkerhet Et QR-kort er en autentiseringsløsning med både fordeler og ulemper når det gjelder sikkerhet. Med utgangspunkt i de tre autentiseringskategoriene, er QR-kortet *noe du har*. Kortet konkurrerer dermed med andre fysiske autentiseringsenheter, som sikkerhetsnøkler. En sikkerhetsnøkkel er betydelig sikrere enn et QR-kort. Både sikkerhetsnøkler og QR-kort er fysiske objekter som inneholder et autentiseringsbevis. Sikkerhetsnøkler bærer beviset i digital form, og kan ikke kopierest av å f. eks. bli tatt bilde av. QR-kortet kan bli tatt bilde av, og har dermed større potensial av å bli misbrukt.

Det fremste problemet med et QR-kort er dets sårbarhet for tyveri dersom en potensiell trusselaktør er villig til å fysisk bryte seg inn hos kunden. Trusselaktøren kan enten stjele kortet eller enkelt "skuldersurfe" brukeren mens vedkommende bruker koden. Ved å filme koden i løpet av få millisekunder, kan et kamera lese av koden for bruk av trusselaktøren. For å adressere dette, anbefales det å skaffe et etui for å oppbevare kortet, slik at det ikke eksponeres for offentligheten unødvendig, kun når det skal brukes.

Utenom problemet med skuldersurfing, tilbyr et QR-kort en sikkerhet som tilsvarer et ekstremt langt og komplekst passord; nærmest umulig å "brute force". Denne metoden kan deretter kombineres med fingeravtrykkskanning for å oppnå tilstrekkelig sikker to-faktor-autentisering uten å kreve at brukeren husker passord eller lignende.

En kan alternativt utnytte QR kort som alternativ for fysisk kodebrikke som

f.eks bankID brikke. I motsetning til en kodebrikke, vil ikke koden på QR-kortet endre seg, men til gjengjeld vil det være enklere å bruke. Et sikkert passord sammen med et QR-kort kan også være tilstrekkelig autentisering.

Alt i alt tilbyr QR kort et sikkerhetsnivå på linje med passord, men har fordelen av den ekstra sikkerhetslaget fra den fysiske naturen av koden. QR-kort rangeres dermed som *sterk* sikkerhet.

Brukervennlighet Et QR-kortsystem vil i prinsippet være både enkelt å bruke og enkelt å sette opp. Ved innlogging må brukeren trykke på en logg-inn-knapp i webgrensesnittet. Deretter må de akseptere en pop-up når nettleseren ber om tillatelse til å bruke kameraet (hvis det er første gang de bruker enheten til Omhu) og deretter fange QR-koden gjennom mobilkameraet.

QR-kortet har ikke blitt testet som en del av denne studien, men sammenlignet med andre former for autentisering med lignende sikkerhet (for eksempel autentiseringsapp eller fysisk kodebrikke) vil QR-kortet antageligvis være vesentlig enklere å bruke. Dette skyldes at det ikke krever at brukeren må memorisere informasjon for å transportere autentiseringsmediumet mellom enheter eller applikasjoner. Det er også betraktelig mindre "krongling" en med sikkerhetsnøkkel, som ofte krever en viss presisjon for å gjennomføre.

Et fysisk nøkkelkort vil også oppleves mer som en verdigjenstand på lik linje med lommebok og husnøkler, noe som kan få brukere til å forstå viktigheten av å holde god kontroll på kortet. Dette kan være positivt i et sikkerhetsperspektiv, da brukere blir mindre sannsynlige til å gi fra seg kortet til personer som ikke skal ha tilgang til det.

Grunnet den enkle fremgangsmåten for bruk av QR kortet, vurderes dette som *enkelt* å bruke.

Kostnad Når man vurderer kombinasjonen av sikkerhet og brukervennlighet som QR-kort gir, fremstår denne løsningen som et svært kostnadseffektivt alternativ der man får mye verdi for pengene. I utgangspunktet forutsetter dette systemet at kunden eier en kortprinter. Prisen for en slik maskin varierer, men ligger generelt mellom 3000 og 20000 kr. Selv om mange bedrifter allerede har en slik maskin, representerer dette kun et engangskjøp. Deretter vil hvert kort koste omtrent 1-2 kr. Som et fysisk sikkerhetsalternativ er dette betydelig rimeligere sammenlignet med kodebrikker eller sikkerhetsnøkler, som kan koste opptil 700 kr per nøkkel. Ved å finne en rimelig standardisert maskin, for eksempel "IDP Smart 21,som for tiden selges for 3295 DKK [56], vil det ikke ta mange kortutskrifter før dette systemet blir vesentlig billigere enn andre systemer for fysisk to-faktorautentisering.

Kostnaden vurderes dermed som *svært rimelig*.

Implementasjon Implementasjonen av et system for generering og autentisering vil være relativt rett frem, da en QR-kode i essens er en streng med tekst.

Den tekniske utfordringen ligger hovedsaklig i å tillate brukeren å lese inn QR-koden i frontend ved hjelp av kameraet på mobilen. Det finnes imidlertid forhåndslagede biblioteker i JavaScript som kan brukes til dette formålet, men dette medfører risiko i form av tredjeparts kode. Systemet trenger også et system for å generere QR-koder, noe som også er tilgjengelig for både GoLang (som gruppen ønsker å benytte til demoen) og .NET-rammeverket, som brukes av Weisstech.

Et system basert på denne løsningen ville også kreve utvikling av et grafisk administratorgrensesnitt der en administrator hos kunden har oversikt over eksisterende brukere og nøkkelkort som eventuelt er koblet til deres konto. Her skal administratoren kunne se hvilke kort som nærmer seg utløpsdatoen og ha oversikt over hvor i verden dette kortet er blitt brukt til å logge inn.

Bortsett fra moduler relatert til generering og skanning av QR-koder, kan systemet bygges i et relativt standard format, som man ville gjort med et passord-autentisert system.

Dersom det er tilgjengelige ressurser, ville det være lurt å vurdere en metode for å lage et etui for QR-kortet, slik at QR-koden normalt sett skjules. Et slikt etui ville selvfølgelig øke kostnadene for løsningen betydelig, så hvis det finnes et forhåndseksisterende alternativ, kan dette være å foretrekke.

Fra et orginisatorisk perspektiv vil QR-kort kreve justering fra kundens side. I likhet med andre fysiske autentiseringsmetoder vil implementasjonen kreve logistikk for erstatning og de-aktivering av tapte kort, samt et system for registrering av nye brukere. Ansatte vil også måtte passe på at sluttbrukere ivaretar qr-kortet på en forsvarlig måte.

Grunnet at QR kort er et nytt konsept, vil den tekniske implementasjonen bli over snittet vanskelig. De individuelle komponentene sav systemet er godt dokumentert, men sammensetningen av disse til et fungerende system er ikke utbredt, og medfører en høyere sjanse for sikkerhetsbrister grunnet uforutsette feil. Dette kombinert med de mindre organisatoriske konsekvensene gjør at QR kort er vurdert til *moderat*.

Dekning For at en bruker skal kunne utnytte QR kort, trenger dem en mobiltelefon med kamera og nettleser kompatibel med “capture” funksjonen i HTML 5, som er den vanligste metoden for å bruke kamera på nettsider. Denne funksjonen ble implementert i Chrome Android i 2013 som del av versjon 25 [57]. Det er dermed høyst antagelig at over 95% av brukere har tilgang på dette i dag. Dekningen rangeres dermed som *optimal*.

Figur 5.2: Skisse av QR-kort

Kodebrikke

Bakgrunn Kodebrikker er en fysisk brikke som genererer engangskoder. Det mest typiske eksempelet på kodebrikker i Norge er å bruke kodebrikke sammen med BankID. Kodebrikken er unikt programmert slik at den samsvarer med en autentiseringstjeneste for applikasjonen den skal autentisere for. Brikken og tjenesten inneholder derfor samme algoritme og samme input, typisk en personlig id og forrige engangskode eller et sekvensnummer. Ettersom både autentiseringstjenesten og brikken har samme informasjon, vil autentiseringstjenesten vite hvilken kode som kommer til å bli generert ved neste innlogging. Typisk vil tjenesten tolerere et avvik i sekvensen fra forrige engangskode, for å forhindre at en ubrukt engangskode ikke gjør kodebrikken ubrukelig [58]. På denne måten vil autentiseringstjenesten oppdage dersom engangskoden ikke stemmer med forventet input og sekvensnummer, og brikken vil ikke kunne autentisere brukeren.

Sikkerhet Når kodebrikken genererer en engangskode, vil koden typisk kun være gyldig i 30 til 60 sekunder, og kan ikke brukes til autentisering etter at tiden har gått ut [59]. Dette gjør bruk av kodebrikke til autentisering som svært resistant mot phishing og social engineering. En cyberkriminell kan ikke stjele en engangskode for så og bruke den senere, da den er ugyldig etter de første 30 sekundene. I motsetning til passord, kan ikke uvedkommede få tilgang til koden, med mindre de har fått tak i den fysiske kodebrikka. Som ved bruk av andre fysiske autentiseringsfaktorer, er en kodebrikke sårbar for fysisk skade, og kan bli stjålet eller mistet. Derfor er en kodebrikke kun aktuell som en av flere faktorer i en autentiseringsløsning.

Kodebrikker har sammenlignbar sikkerhet med autentiseringsapp, med en ekstra buffer da den er en fysisk gjenstand. Til tross for tidsbegrensingen, forblir brikken sårbar for sosial manipulasjon og tyveri. Grunnet den smale angrepsflaten og tilretteleggingen nødvendig for å forbipassere en slik kode, vurderes den som *sikker*.

Brukervennlighet En kodebrikke blir regnet som svært brukervennlig. Kodebrikken har en knapp som brukeren trykker på, og har dermed 30 til 60 sekunder på seg til å skrive engangskoden inn i nettløsningen. Det er samme vanskelighetsgrad om brukeren logger seg inn på en pc eller en mobil, og en kodebrikke er dermed en god løsning for både pc- og mobilbrukere. Kodebrikke er ikke blandt de testede metodene i denne studien, men da den fungerer på lignende vis som autentiseringsapp, vil resultatene være noe sammenlignbare.

Med autentiseringsapp gikk derimot mye av tiden og frustrasjonene til testdeltagerne ut på og navigere mellom innloggingsportalen og autentiseringsappen, et trinn som ikke er med for kodebrikken.

Dette vil antageligvis gjøre kodebrikken vesentlig mer brukervennlig. Basert

på resultatet av autentiseringsappen på brukertesten, med hensyn tatt for simplifiseringen av prosessen i tilfellet av kodebrikken, vurderes kodebrikken som *moderat* brukervennlighet.

Kostnad Prisene for kodebrikker avhenger mye av hvilken form for implmentasjon blir valgt. En kodebrikke i seg selv koster rundt 150-300kr per stykk. Informasjon om kodebrikker er derimot noe vanskelig å finne, da det ikke ser ut til å være et særlig marked for "selvstendige" brikker som ikke er koblet opp mot en større tjeneste. Om en tar utgangspunkt i f.eks DUO security, vil dette pådra en ekstra kostnad på omtrent 720 000kr i året for en brukerbase med 2000 brukere, gitt DUO sin kostnad på 3$ per bruker per måned [60].

Dersom Omhu velger å implementere teknolgien uten hjelp av tredjeparter, vil integrasjonen ikke pådra noen ekstra kostnad. Men gitt prisen på omtrentlig 150kr per kodebrikke, med antagelsen om 2000 brukere vil kostnaden ligge på rundt 300 000kr. Sammenlagt med kostnaden for duo-security vil kostbarheten for kodebrikke vurderes til å være *svært kostbar*.

Implementasjon Implentasjonen av kodebrikke er med første øyekast ikke særlig utbredt. Det virker ikke som det er noe utbredt løsning for "selvstendig" implementering av kodebrikke, da alle populære løsninger er koblet opp mot et abonnement en må kjøpe som software as a service (SaaS) løsning. Om en velger å bruke software as a service (SaaS) løsningen tilbudt av Duo Security, kan den tekniske implementasjonen oppnås gjennom API'et de tilbyr som del av tjenesten [61]. Denne løsningen vil også inkludere implementasjonshjelp, og være relativt lett på utviklingssiden.

PÅ et organisatorisk nivå vil kodebrikken ha samme konsekvenser som andre fyiske autentiseringsfaktorer. Dette innebærer logistikk for erstatning og deaktivering av tapte kodebrikker, samt at de ansatte må gjøre mindre justeringer for å passe på at brukerene ikke mister sine kodebrikker.

Selv om den tekniske implementasjonen er svært lettvint som del av software as a service (SaaS) pakke, vil de orginistatoriske konsekvensene for kunden medføre at kodebrikke rangeres som *enkelt* å implementere.

Dekning: Da en slik kodebrikke ikke vil være knyttet til noen spesifike krav for mobil enhet, kan denne enkelt rangeres som "optimal" dekning.

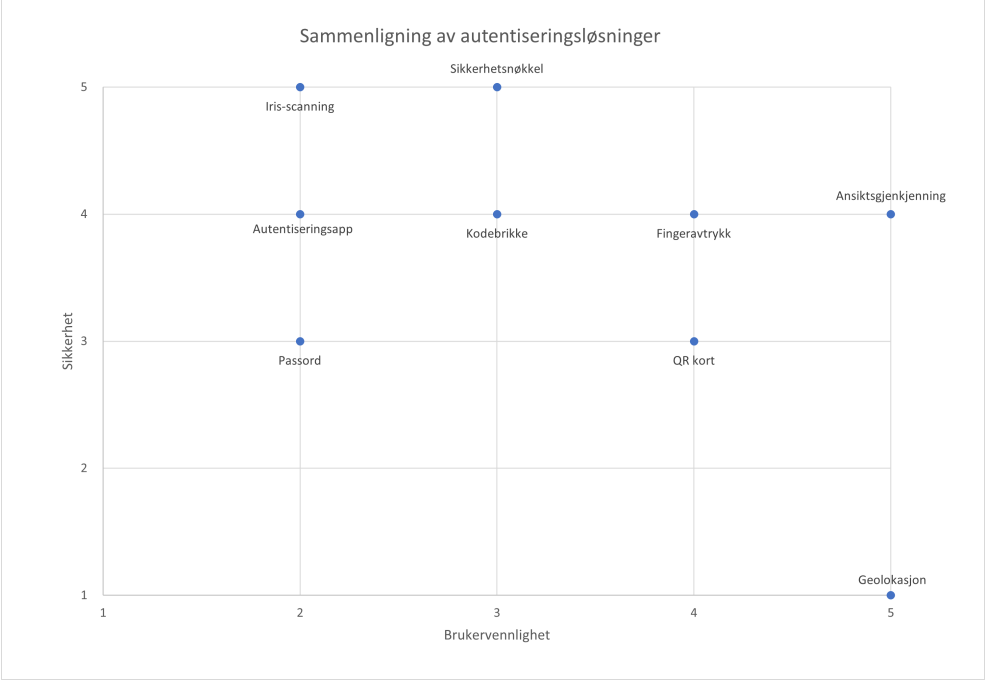
Oppsummering av enkelt-faktorer

I denne seksjonen vises oversikt og resultater for enkelt faktorer, der alle faktorene vurdert hittil sammenlignes basert på vurderingene gitt. Tabell 5.11 viser alle vurderingene gjort til nå, omgjort til numeriske verdier der 1 er dårligst, og 5 er best.

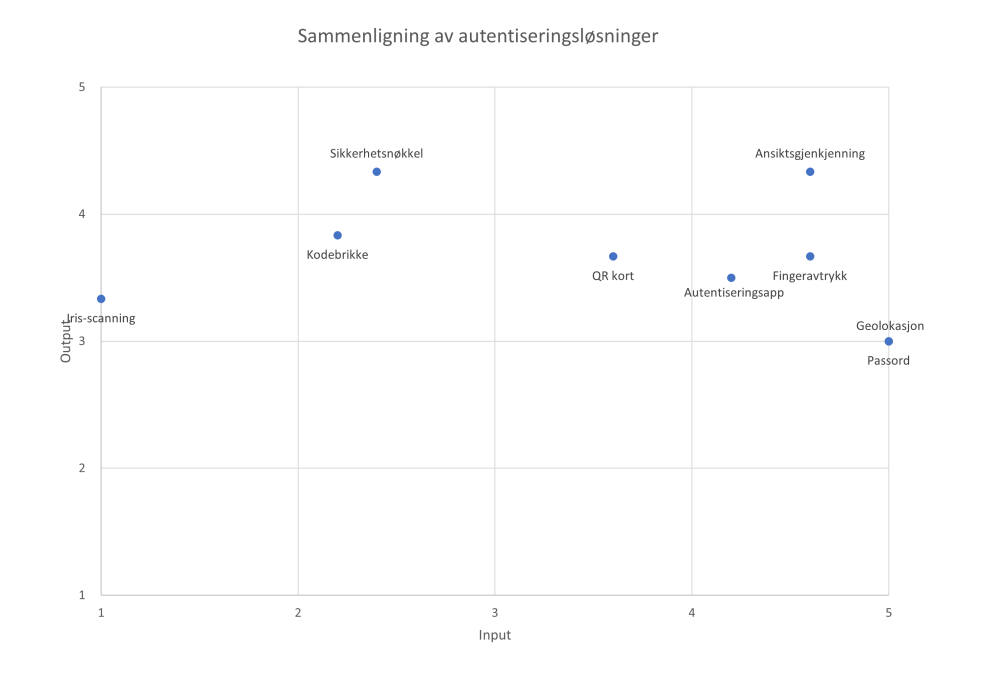
Figur 5.4 viser de forskjellige faktorene sammenlignet utifra deres "input", et vektet gjennomsnitt av egenskapene knyttet til investering og negative konsekvenser av å bruke metoden: kostnad og implementasjon. På x aksen vises "output", et vektet gjennomsnitt av positive egenskaper som gir utbytte for investeringen. Disse egenskapene er sikkerhet, brukervennlighet og dekning. Mer om vektingen av scorene i data beskrives i kapittel 3.4.2. Figur 5.3 viser forholdet mellom sikkerhet og brukervennlighet, som er de høyest prioriterte egenskapene.

Faktor	**Sikkerhet**	**Bruker-vennlighet**	**Dekning**	**Kostnad**	**Implemen-tasjon**
Passord	3	2	5	5	5
Iris-scanning	5	2	1	1	1
Geolokasjon	1	5	5	5	5
Ansiktsgjenkjenning	4	5	4	5	4
Fingeravtrykk	4	4	2	5	4
Autentiseringsapp	4	2	5	5	3
Sikkerhetsnøkkel	5	3	5	2	3
QR Kort	3	4	5	4	3
Kodebrikke	4	3	5	1	4

Tabell 5.11: Verdier fra enkelt-faktorer



Figur 5.3: Enkeltfakor brukervennlighet / sikkerhet



Figur 5.4: Enkeltfaktor input / output

Utifra figurene er det tydelig at biometriske løsninger som ansiktsgjenkjenning og fingeravtrykk viser den beste balansen mellom sikkerhet og brukervennlighet, samtidig som de også scorer godt med de andre faktorene tatt med i betraktning også. Sikkerhetsnøkkel scorer også høyt på output siden, grunnet dens utmerkede sikkerhet og greie brukervennlighet, den er derimot noe svakere når det kommer til input, da denne metoden krever mye tilrettelegging og investering for å kunne tas i bruk på kryss av en hel organisasjon. QR-kort og autentiseringsapp faller også inn under området med en helt grei balanse av investering og resultat. Andre metoder som kodebrikke og iris-scanning ser ikke ut til å være aktuelle da det finnes like gode metoder som er langt enklere å implementere.

5.4.4 Ferdige løsnigner for MFA

Google Identity Platform med passord og sms

Bakgrunn Google Identity Platform er tjeneste som inkluderer en fullstendig innloggingsportal og verktøy for identitets-styring som kan utnyttes for autentisering med bruk av en lang rekke kontoer, deriblant google konto. Denne tilnærmingen eliminerer behovet for å opprette og huske separat påloggingsinformasjon for hver enkel webapplikasjon, ettersom brukeren kan bruke sitt eksisterende Google-passord og brukernavn for tilgang. Dette er et godt alternativ dersom de fleste i målgruppa allerede har en Google-konto.

Sikkerhet Den grunnleggende sikkerheten ved Google login er god til å være en enkel-faktor autentiseringsmetode. Denne metoden kan betraktes som sikrere en tradisjonell passord/brukernavn innlogging da det benytter seg av OAuth-protokollen. Denne protokollen gir en trygg autentiseringsflyt, uten å eksponere brukerens faktiske påloggings-informasjon til tjenesten. Tredjepartsautentiseringen mottar begrenset tilgang til brukerens Google-data basert på brukerens samtykke [62].

Google tilbyr mange metoder å legge til tofaktor, fra sikkerhetsnøkkel til autentiseringsapp eller en egen push-varslings app en kan ha på mobilen. De tilbyr også 2fa gjennom sms som den mest grunnleggende metoden. Det er denne metoden som vurderes i denne kartleggingen. Med implementasjonen av dette er det viktig å tvinge brukere til å utnytte 2fa, da dette er skrudd av som standard [63].

Google login i seg selv er en form for passord-innlogging, så vurderingen gitt til passord brukes som utgangspunkt for vurderingen av sikkerhet. Denne verdien er “moderat”. Den ekstra sikkerheten tilbudt av 2fa for sms øker sikkerheten betraktelig, da en potensiell angriper nå trenger tilgang til brukerens sms-meldinger samtidig som passordet må anskaffes. Så langt som to faktor går, er dette derimot ikke det vanskeligste sikkerhetstiltaket å forbipassere. Koden som sendes på sms kan “enkelt” anskaffes av en trusselaktør med som utnytter sosial mainipulasjon. Om trusselaktøren er villig til å gå enda lenger, finnes det flere kjente sikkerhetsnhull i SMS infrastrukturen som lar trusselaktører utføre man in the middle (MitM) angrep for å anskaffe brukeres sms-kommunikasjon [64, p. 12].

Den ekstra beskyttelsen fra 2fa senker angrepsflaten betraktelig, men viser fortsatt sårbarheter oppnåelig for en dedikert angriper og utnytte. Dermed rangeres Google Oauth’s sikkerhet som *sterk*.

Brukervennlighet Brukervennligheten for Google Oauth er sammenlignbar med den av passord. Dette setter den allerede på en vurdering som “krevende”.

SMS koden brukeren får må også hentes fra en annen applikasjon på mobilen, noe brukertesten gjennomført for autentiserignsapp viste var vanskelig for mange brukere. Disse ekstra stegene viser en økning av steg brukerne må gjennomføre for å autentisere seg, men er ikke tilstrekkelig for å senke nivået for brukervennlighet noe lavere enn grunnverdiene. Dermed vurderes Google Oauth med SMS som *krevende*.

Kostnad Implementasjonen av google Identity Platform gjøres gjennom deres tjenetse Google Identity Platform. Denne tjenesten er i utgangspunktet gratis så lenge en ligger under 50 000 aktive brukere i måneden [65]. Bruk av SMS som tofaktor pådrar derimot en ekstra kostnad på $0.07 per SMS sent(0,75kr per nåværende kurs), med unntak av de 10 første hver dag. Med en hypotetisk brukerbase på 2000 brukere som autentiserer i snitt tre ganger hver dag, vil dette koste i overkant av 1 600 000kr i løpet av et år. For selve API'et vil det derimot ikke være tilstrekkelig med brukere for å overstige betalingsgrensen denne grensen. Kostnaden av Google Oauth er dermed vurdert som *svært kostbar*.

Implementasjon For å implementere Google Login i en webapplikasjon må en sette opp den nødvendige infrastrukturen i Google Identity Platoform. Dette gjøres gjennom egne grensesnitt, og har utfyllende dokumentasjon og tilgang på kundeservice. Google Identity Platform selges som en komplett platform for autentisering og identitetskontroll, og bør dermed være lettvint å implementere på et teknisk nivå. Google Identity platform kommer også med mange andre funksjonaliteter for å berike innloggings-systemet ytterligere.

Fra et organisatorisk nivå vil denne formen for autentisering ikke gi noen ekstra arbeidsbelastning for kundene av Omhu.

Grunnet "authentication as a service" konseptet av google identity platoform og dens sømløse integrasjon hos kunden vurderes Google Identity Platform som *svært enkelt*.

Dekning Autentisering med denne metoden krever en google konto, samt en enhet i stand til å utnytte SMS. I 2023 rapporterte statistisk sentralbyrå (SSB) at 98% av nordmenn eide en mobiltelefon [66]. Utira denne statistikken vurderes dekningen på Google Identity Platform til *optimal*.

MinID

Bakgrunn MinID representerer en personlig elektronisk ID (eID) som gir deg tilgang til offentlige tjenester via ID-porten. Dette utgjør en komplett tofaktor autentiseringsløsning, der passord utgjør den første faktoren, mens den andre kan være en engangskode levert via SMS eller et push-varsel i

MinID-appen [67]. Altinn klassifiserer MinID som en autentiseringsmetode på sikkerhetsnivå 3 (se kap 2.1.3). Dette sikkerhetsnivået tilfredsstiller målgruppens behov, ettersom sluttbrukerene ikke skal ha tilgang til sensitive personopplysninger, f. eks. helseopplysninger, som krever sikkerhetsnivå 4.

Sikkerhet MinID inkluderer allerede en fullverdig to-faktors autentiseringsløsning, som gjør implementeringen enklere sammenlignet med alternative løsninger med lignende sikkerhet. Brukerens tjenestepassord er selvvalgt, og sikkerheten avhenger av passordets styrke. Derfor er det fornuftig å anbefale og eventuelt veilede brukerne i å lage gode, sikre passord. Passord-delen av MinID er dermed rangert likt som passord, og blir vurdert til "moderat" sikkerhet.

Den andre faktoren kan være SMS eller dedikert app for MinId.

For MinID med sms faller under den samme vurderingen som Google Identity Service, og vurderes til å ha *sterk* sikkerhet grunnet den drastisk minimerte angrepsflaten.

For MinID med applikasjon vurderes annerledes fra SMS grunnet mangelen på svakhetene funnet i SMS infrastrukturen. Denne metoden er sterkere enn med SMS, men ikke til slik grad at vurderingen økes vidre. Det er fortsatt mulig å forbipassere denne faktoren gitt tilstrekkelig sosial manipulasjon. Dermed vurderes MinID med app fortsatt til å ha *sterk* sikkerhet.

Brukervennlighet MinID er designet med brukervennlighet i fokus og er tilpasset brukere helt ned til tretten år. Brukernavnet er brukerens fødselsnummer, kombinert med et selvvalgt passord for pålogging. I tillegg kreves det enten en engangskode fra SMS, eller som et push-varsel fra MinID-applikasjonen der du må logge inn med enten mobilens egen pinkode, fingeravtrykk eller ansiktsgjenkjennelse. Den eneste potensielle utfordringen kan være å navigere mellom SMS/MinID-applikasjon og web-applikasjonen for pålogging. Brukertesten gjennomført for å sammenligne autentiseringsmetoder (se kapittel 5.1). Her var deriblant en av faktorene BankID, som bærer mange likheter med MinID's autentiseringsapp. BankID var her generelt negativt omtalt, og rangerte som nest laveste autentiseringsmetode, like over passord. Årsakene gitt av brukerene misliker BankID er at de må navigere inn på appen, og deretter skrive inn passordet for BankID, noe en også må for MinID med tilsvarende passord.

Grunnet flere steg og navigasjon mellom forskjellige faner på mobilen og memorering av passord vurderes brukervennligheten av MinID som *krevende*.

Kostnad MinID blir tilbudt av IDportalen som en gratis tjeneste så lenge antallet transaksjoner ikke overstiger 200 000 i året. Med en hypotetisk brukerbase på 2000 brukere som autentiserer tre ganger om dagen vil det genereres i

overkant av 2 millioner transaksjoner i året. Dette overstiger grensen med 1,8 millioner transaksjoner. IDportalen opplyser på sin nettside at deres tjenester kostet 0,46 kr per transaksjon inkludert merverdiavgift (MVA) for året 2022-2023 [68]. Med 1,8 millioner betalte transaksjoner vil MinID dermed koste 828,000kr per år inkludert merverdiavgift (MVA). Basert på dette tallet vurderes kostnaden for MinID som *kostbart*.

Implementasjon MinID er utstedt og driftet av digitaliseringsdirektoratet. Ettersom ID-porten allerede er implementert i Omhu, vil det være enkelt å implementere MinID som en autentiseringsløsning. ID-porten har god dokumentasjon på hvordan implementere autentiseringen på deres nettside [69]. Grunnet at Weisstech allerede utnytter IDportalen, vil implementasjonen av MinID trolig være trivielt, og rangeres dermed som *svært enkelt*.

Dekning Vurderingen for dekning av MinID har de samme premissene som for Google Identity Platoform, og kan dermed også vurderes til *optimal* uten videre gransking.

5.4.5 Relevante multi-faktor løsninger

Flere av de diskuterte faktorene har utmerket sikkerhet. Likevel er de alle sårbare, da kun ett ledd må brytes for å omgå autentiseringen. Derfor anbefales det alltid å kombinere to faktorer for å oppnå tilstrekkelig sikkerhetsnivå. Selv to svake sikkerhetsformer kan være betydelig kraftigere enn bare en sterk sikkerhetsfaktor alene. I denne delen av kartleggingen sammenlignes sammensetninger av to-faktorautentisering (2FA) for å identifisere svakheter og styrker ved dem.

Ikke-aktuelle faktorer

Noen faktorer blir ikke vurdert videre i denne delen av kartleggingen. Dette skyldes ikke nødvendigvis at metodene er vurdert som usikre eller dårlige, men heller at de ikke utgjør et praktisk alternativ sammenlignet med andre faktorer som undersøkes i denne rapporten.

Geolokasjon: Denne teknologien kan anvendes som en bakgrunnsprosess for å avdekke mistenkelige innloggingsforsøk. Teknologien vurderest likevel til å ha for svak sikkerhet til å være en av to faktorer i en autentiseringsprosess.

Iris-skanning: Dette er en imponerende teknologi som utvilsomt vil bli et nyttig verktøy i nær fremtid. For øyeblikket er imidlertid teknologien ikke moden nok til å være anvendelig, da den er kompleks, krever spesialisert utstyr fra både kunder og sluttbrukere, og mangler tilstrekkelig dokumentasjon for effektiv implementering.

Kodebrikke: Denne metoden har vist seg veldig effektiv, som demonstrert i BankID. På grunn av et begrenset marked og dokumentasjon for slike brikker, fremstår dette imidlertid som et mindre attraktivt valg. Når de få produktene som er mulig å anskaffe er i samme prisklasse som fullverdige sikkerhetsnøkler, er det å velge en sikkerhetsnøkkel over kodebrikke et åpenbart valg.

Oversikt

Metodene som vil bli kartlagt videre er som følger:

- Google Identity Platform med kode på sms
- MinID med SMS-kode eller applikasjon
- Platform-autentisering(fingeravtrykk eller ansiktsautentisering) med sikkerhetsnøkkel

- Platform-autentisering(fingeravtrykk eller ansiktsautentisering) med qr-kort
- Passord og autentiseringsapplikasjon
- Microsoft's Azure Face API med sikkerhetsnøkkel

5.4.6 Vurdering av sammensatte MFA løsninger

Google Identity Platform med kode på sms

Denne løsningen er allerede i utgangspunktet en multi-faktor, og er dermed ikke endret siden delkapittelet om autentiseringsløsningen. Metoden beholder derfor den samme vurderingen. Se side 119 for begrunnelse av vurderingen.

Attributt	**Nr**	**Kvalitativ Score**
Sikkerhet	4	Sterk
Kostnad	1	Svært kostbar
Brukervennlighet	2	Krevende
Dekning	5	Optimal
Implementasjon	5	Svært enkelt

MinID

MinID kommer som en komplett løsning for multi-faktor autentisering i utgangspunktet, og har dermed ikke endret vurdering siden den opprinnelige drøftingen. Se side 120 for begrunnelse av vurderingen. MinID behodler samme vurdering uavhengig av om app eller SMS blir brukt, selv om bruk av app vil innebære en mild forbedring av sikkerhetg.

Attributt	**Nr**	**Kvalitativ Score**
Sikkerhet	4	Sterk
Kostnad	2	Kostbart
Brukervennlighet	2	Krevende
Dekning	5	Optimal
Implementasjon	5	Svært enkelt

Platform-autentisering med sikkerhetsnøkkel

Denne 2FA-løsningen forener to sterke, moderne og brukervennlige autentiseringsfaktorer for å skape en ideell passordfri autentisering. Platform-sikkerhet

referer her til autentiseringsformene funnet lokalt på brukerens enhet, og inkluderer hovedsaklig pin kode, fingeravtrykk og ansiktsgjenkjenning. Alle disse metodene implementeres under samme paraply, da webauthn ikke gjør forskjell på slike autentiseringsmetoder fra et teknisk perspektiv. Sikkerhetsvurderingen forblir "Svært sterk", ettersom sikkerhetsnøkkelen allerede har en rangering på nivå 5, mens både fingeravtrykk og ansiktsautentisering ligger på nivå 4. I denne løsningen gir vi brukerne muligheten til å velge mellom fingeravtrykk eller ansiktsautentisering, noe som øker dekningsgraden betraktelig. Mange mobile enheter mangler enten fingeravtrykks- eller ansiktsgjenkjenningsfunksjoner, men de fleste har minst en av teknologiene implementert. De som ikke har noen av delene kan fortsatt ta i bruk pin kode, som selvfølgelig er mye svakere. De fleste operativsystemer prioriterer derimot å utnytte biometri hvis dette er tilgjengelig for brukeren. Med untaket av pin-koden som vil gjelde for de ferreste av brukerene, vil denne løsningen være fullstendig passordfri. Den opprettholder dermed brukervennlighetsvurdering på "Moderat" da sikkerhetsnøkkelen forblir den vanskeligste faktoren å bruke blandt alternativene. Vurderingen for kostnad og implementasjon arves også fra sikkerhetsnøkkel da det er denne som holder de laveste verdiene for disse egenskapene.

Attributt	**Nr**	**Kvalitativ Score**
Sikkerhet	5	Svært sterk
Kostnad	1	Svært kostbart
Brukervennlighet	3	Moderat
Dekning	5	Optimal
Implementasjon	3	Moderat

Platform-autentisering med qr-kort

Denne løsningen benytter, i likhet med *Platform-autentisering med sikkerhetsnøkkel*, webauthn/FIDO2 rammeverket for å utnytte den innebygde autentiseringen i mobilen for å markant forbedre dekningsgraden, samtidig som sikkerheten forblir høy i de aller fleste tilfeller. Den består også av både en fysisk og en biometrisk komponent, noe som resulterer i en passordløs tilnærming for brukere med biometri tilgjengelig. Den skiller seg imidlertid fra overnevnte løsning, ved at den fysiske faktoren er et QR-kort, som har betydelig lavere sikkerhetsnivå sammenlignet med sikkerhetsnøkkelen. Kostnadene vil derimot også være betydelig lavere. Sikkerhetsnivået forblir på nivå 4, ettersom QR-kortet ikke gir tilstrekkelig økning i sikkerhet for å rettferdiggjøre en høyere sikkerhetsvurdering. Dette er derimot kun om alle brukere utnytter biometri for autentisering. Dette kravet kan ikke administreres gjennom webauthn, og må dermed gjøres på et organisatorisk nivå. Dermed justeres også verdien for implementasjon ned til *krevende*. Løsningen opprettholder derimot den gode brukervennligheten og dekningen fra begge

komponentene. Grunnet kravet om ikke bruke pin-kode, selv om dette er eneste alternativ får ikke denne metoden økning til "optimal" dekning slik som forrige metode fikk.

Attributt	**Nr**	**Kvalitativ Score**
Sikkerhet	4	Sterk
Kostnad	3	Rimelig
Brukervennlighet	4	Enkelt
Dekning	4	Optimal
Implementasjon	2	Krevende

Passord og autentiseringsapplikasjon

Denne løsningen er svært utbredt, og kan regnes som den mest grunnleggende 2FA kombinasjonen. Sikkerheten og enkelheten av implementasjonen gjør den effektiv å implementere for rask, god sikkerhet. Sikkerheten forblir dermed "sterk", basert metodenes felles sårbarhet for sosial manipulasjon. Brukervennligheten kan imidlertid være utfordrende, ettersom den krever at brukeren husker et komplekst passord i samsvar med retningslinjene for passord. I tillegg må brukeren håndtere en autentiseringsapplikasjon, noe som oppleves som krevende av mange brukere. Brukeren må huske en kode innenfor ett kort tidsintervall, samtidig som de navigerer mellom autentiseringsapplikasjonen og webapplikasjonen på mobilen, gitt at mobiltelefon blir brukt for å logg inn på Omhu. Dersom brukeren logger inn på en annen enhet enn mobiltelefonen, f. eks. nettbrett, blir brukervennligheten lettere, ettersom det da ikke er nødvendig å navigere mellom programmer på den samme enheten. Autentiseringsapplikasjoner er vanligvis lasta ned på mobiltelefonen.

Denne autentiseringsløsningen ligner på metoder allerede implementert i Omhu, som BankID og Buypass, sett fra brukerens perspektiv. Dette gjør muligens integrasjonsprosessen noe enklere. Brukertestene gjennomført i denne studien viser derimot at både passord og autentiseringsapp er generelt mislikt blant deltagerene(se kap 5.1.3). Grunnet kombinasjonen av disse to vanskelige faktorene, vurderes denne metoden til å være "svært krevende" for brukervennlighet.

Denne tilnærmingen ligner på metoden brukt i BankID, men den er implementert uavhengig av fra IDPortalens's systemer. Dette fører til betydelig lavere kostnader, ettersom det ikke er nødvendig å betale for API-tilgang når antallet systemkall overskrider de 200 000 gratis systemkallene per år. Kostnaden forblir dermed ubetydelig.

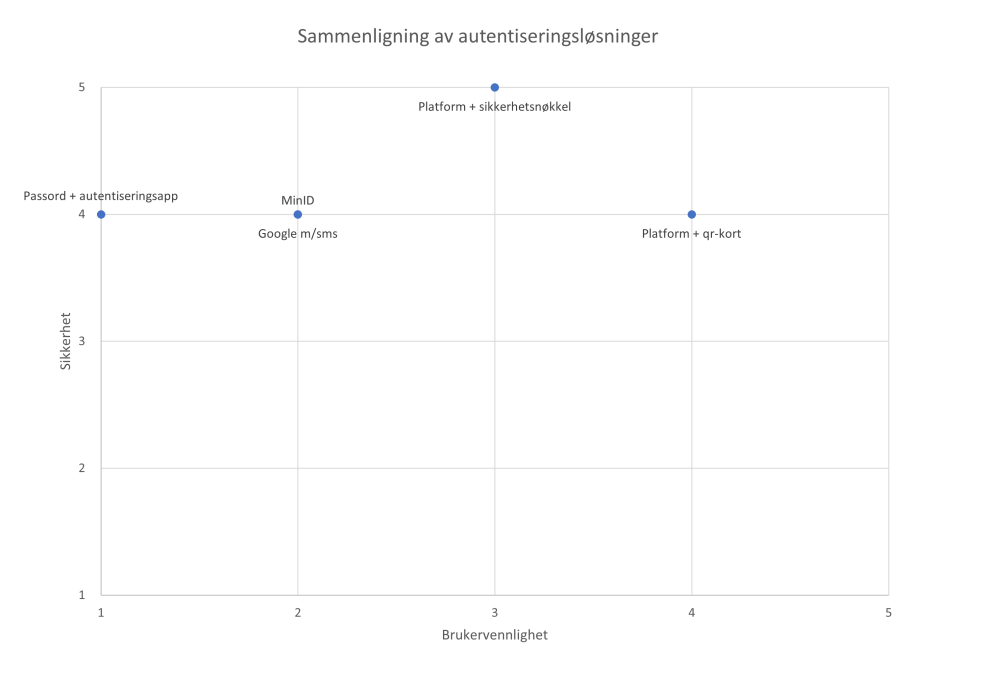
De resterende verdiene av dekning og implementasjon arves fra autentiseringsap-

pen, som hadde den verste verdien for implementasjon.

Attributt	**Nr**	**Kvalitativ Score**
Sikkerhet	4	Sterk
Kostnad	5	Ubetydelig
Brukervennlighet	1	Svært krevende
Dekning	5	Optimal
Implementasjon	3	Moderat

Sammenligning basert på sikkerhet og brukervennlighet

For å evaluere de ulike løsningene, benyttes de kvantitative vurderingene gitt til hver løsning for å visualisere dem i en punktgraf. Først vurderes de to mest betydningsfulle egenskapene: sikkerhet og brukervennlighet. Sikkerhet representeres langs X-aksen, mens brukervennlighet langs Y-aksen. Løsninger som ligger lengre opp mot det høyre hjørnet anses som bedre. Det bør bemerkes at dataene er basert på omtrentlige verdier og er hovedsakelig produsert for sammenligning heller enn å gi konkrete datapunkter. Resultatene fra ulike metoder vil variere avhengig av situasjonen.



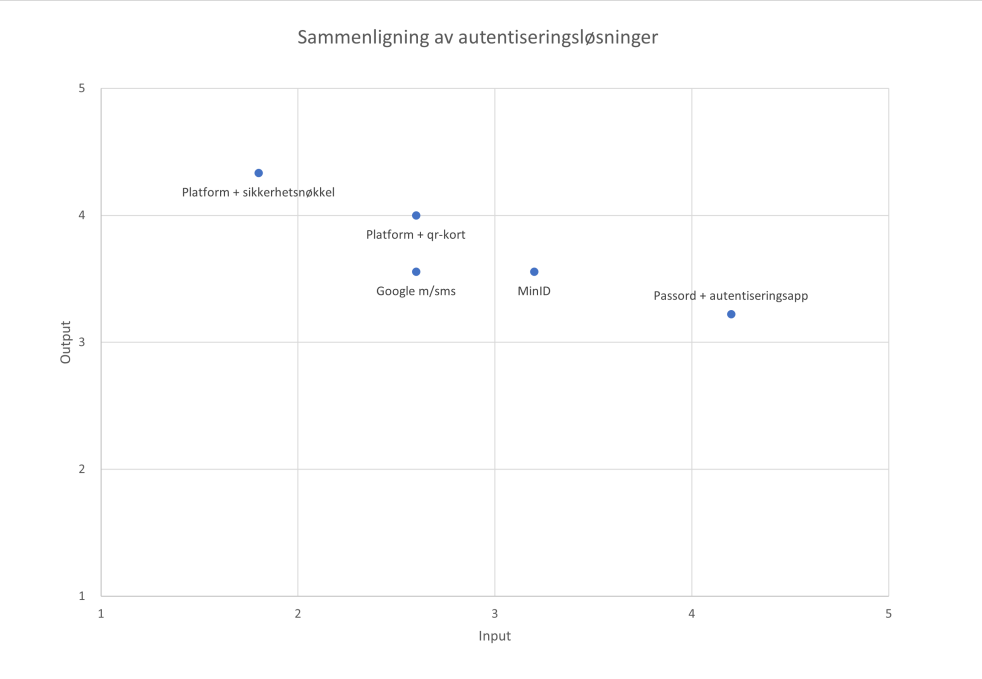
Figur 5.5: Sammenligning av løsninger for 2fa - Brukervennlighet / Sikkerhet

Grafen indikerer at kombinasjonen av platform-autentisering og sikkerhetsnøkkel presterer best på sikkerhet, og nest-best på brukervennlighet. Platform-autentisering med bruk av QR-kode er heller ikke et dårlig alternativ, da det scorer høyere på brukervennlighet sammtidig som det opprethholder sammenlignbar sikkerhet som de resterende metodene. Imidlertid kan noen alternativer avvises basert på denne analysen. Google-login, MinID og passord+app presterer alle dårlig når det gjelder brukervennlighet. I lys av de andre alternativene på grafen, kan man hevde at passord og autentiseringsapplikasjon er relativt unødvendige. Dersom man kun

vurderer disse egenskapene, fremstår platform-autentisering og sikkerhetsnøkkel samt qr-kort og platform-autentisering som de mest optimale metodene.

Sammenligning basert på input/output

For å gi en klar oversikt over alle løsningene inkludert de resterende egenskapene, benyttes et vektet gjennomsnitt der egenskapene av autentiseringen er delt inn i gruppen "input", altså ressurskrevende egenskaper, eller "output", avkastingsgivende egenskaper. Metoden for konstrueringen av dette diagrammet forklares i kapittel 3.4.2.



Figur 5.6: Sammenligning av løsninger for 2fa - Output / Input

Biometri med sikkerhetsnøkkel Grafen illustrerer at det ikke finnes en ideell løsning, da forbedring av produktet ofte medfører større vanskeligheter med å bruke metoden. Metoden med platform-sikkerhet og sikkerhetsnøkkel skiller seg klart som metoden med best avkastning, grunnet den gode kombinasjonen av sikkerhet og brukervennlighet. Disse løsningene er imidlertid utfordrende å

implementere på grunn av de høye kostnadene knyttet til anskaffelse av sikkerhetsnøkler, og logistikken rundt den praktiske implementasjonen av disse. Den høye kostnaden gir derimot en meget god avkastning, og kan dermed anbefales om ressursene for å implementere dette er tilgjengelig.

Biometri med QR-kort Lenger ned på grafen finner vi muligheten for mobilbiometri med QR-kode. Denne løsningen representerer et kompromiss mellom input og output, da den gir opp sikkerheten fra sikkerhetsnøkler til fordel for det mindre sikre, men mer kostnadseffektive QR-kortet. Denne metoden innebærer derimot en risiko som ikke vises på diagrammet i form av usikkerhet rundt effektiviteten av metoden. Dette er en ubrukt metode for autentisering, og mangler støtten og veiledningen tilgjengelig for alle andre autentiseringsmetoder. Derfor kan heller ikke denne metoden anbefales, med mindre kostnad er en høy prioriterting, men at en fysisk autentiseringsfaktor fortatt er ønsket.

MinID Lenger ned kurven finner man MinID med bruk av applikasjon og SMS. Kostnadene knyttet til denne løsningen er fortsatt betydelige, samt at den gir akseptabel sikkerhet og brukervennlighet. Denne metoden representerer kanskje den mest realistiske løsningen, grunnet dens gode balanse av praktikalitet og ytelse, samt Weisstech's tidligre erfaring med IDportalen.

Passord Passord og autentiseringsapp bryter noe med den ellers lineære grafen da den scorer svært bra i input gruppen. Utbyttet er derimot ikke like bra, grunnet den svært dårlige brukeropplevelsen. Likevel ligger den ikke langt bak MinID på output. Det unike med denne løsningen er dens uforholdsmessig gode outputverdi i forhold til dens meget gode inputverdi. Passord og autentiseringsapplikasjon er en utbredt og testet løsning, og dermed en av de minst krevende metodene for tofaktor autentisering å implementere. Denne løsningen gir utmerket verdi i forhold til ressursene krevet for å implementere den, og kan anbefales som en "billig" metode om kostaden blir prioritert høyere i fremtiden.

Google Identity Platform med SMS Løsningen med den laveste kvaliteten på sluttproduktet er Google-innlogging med kode på sms. Dette skyldes den relativt middelmådige brukervennligheten og sikkerheten sammenlignet med andre løsninger på listen, kombinert med den høye kostnaden knyttet til bruk av tjenesten. Det er imidlertid tydelig at denne løsningen er blant de minst kompliserte autentiseringsmetodene å implementere, ettersom det er en ferdigpakke som enkelt kan integreres i eksisterende systemer. Dette kan være et nyttig valg dersom ressursene er begrensede. Men ellers anbefales det å bruke MinID ovenfor Google Identity

Platform, da dette er en billigere variant av det Google tilbyr. Denne løsningen har derimot mer fleksibilitet og valgmuligheter med platformen.

Kapittel 6

Diskusjon

I dette kapitlet vil det bli reflektert rundt resultatene funnet i denne studien. Dette innebærer diskusjon rundt de viktigste resultatene, feil og mangler i resultatet samt forslag til videre arbeid for autentiserings-kartlegging og utvikling av pasientmodul.

6.1 Kartlegging av autentiseringsmetoder - hovedfunn

Gjennom prosjektet har gruppen kartlagt og testet ulike løsninger for autentisering i Omhu. Testingen inkluderte en test for å sammenligne forskjellige autentiseringsfaktorer opp mot hverandre, samt avdekke problemer og mangler, og å samle preferansedata på disse metodene (se kap 5.1). Denne brukertesten, kombinert med fag-litteratur og personlige erfaringer utgjorde en kvantitativ vurdering av hver aktuelle autentiserings-metode's sikkerhet, brukervennlighet, kostnad, dekning og implementasjon. Disse verdiene ble sammenlignet opp mot hverandre.

6.1.1 Mest lovende metode ifølge brukertestene

Den mest brukervennlige autentiseringsmetoden identifisert gjennom brukertestene, er sikkerhetsnøkkel sammen med platform-autentisering. Dette er en multifaktor kombinasjon, som under brukertesting alt i alt fikk et godt resultat. Sikkerhetsnøkkelen autentiserer brukeren for "noe man har", mens platformsikkerheten benytter "noe man er" med fingeravtrykk eller ansiktsgjenkjenning. Dersom enheten ikke har biometri registrert, blir PIN-kode brukt som erstatning, som er "noe man vet".

Grunnet den passordløse tilnærmingen, har denne metoden best sikkerhet av alle metodene testet. Dessuten er implementasjons-prosessen gjennom FIDO2 rammeverket nokså lettvint. Plattform-autentiseringen, som oftest ansiktsgjenkjenning, fingeravtrykk eller PIN-kode, scorer alle høyt på brukervennlighet, ifølge brukertestingen som er gjennomført. Sikkerhetsnøkkelen scorer ikke så bra på brukervennlighet som plattform-autentiseringen, men scorer høyere enn autentiseringsapplikasjon, som også går under kategorien "noe man har".

Brukertestingen av autentiseringsdemoen med WebAuthn, underbygd av kvalitative intervjuer, viser at en stor andel sluttbrukere er meget fornøyd med å bruke ansiktgsgjenkjenning eller fingeravtrykk. Flere opplevde at sikkerhetsnøkkelen var krevende å bruke, men rangerte likevel sikkerhetsnøkkel som bedre å bruke enn flere alternativ. Det kan tenkes at de fleste brukere er i stand til å bruke sikkerhetsnøkkel uten problemer, gitt introduserende opplæring.

Denne metoden medfører dermed en moderat engangskostnad for innkjøp av sikkerhetsnøkler, men vil fortsatt være rimeligere enn andre alternativer, ettersom kostnaden for API'er ofte overstiger kostnaden av sikkerhetsnøkler over tid.

6.2 Pasientmodul hovedfunn

Pasientmodulen ble utviklet gjennom tre iterasjoner, for å få et mest mulig brukervennlig resultat som samtidig tilfredsstiller målgruppen's behov. Flere av pasientmodulens hovedfunksjoner har vært vellykkede sett fra et brukervennlighetsperspektiv. Andre funksjonaliteter har vært mindre vellykkede pga. alt for stor kompleksitet.

Strukturen, det visuelle designet og den grunnleggende handlings-flyten kan sies å ha vært en sukksess. Brukertesten gjennomført med deltagere fra målgruppa viste at brukerene forstod konseptene av pasientmodulen, og etter litt prøving og feiling, var i stand til å opprette egne aktiviteter og legge til ansatte basert på deres tilgjengelighet. Vi fikk tilbakemelding fra en ansatt i omsorgs-sektoren, at sammenligningsfunksjonen der brukerene kan se tilgjengelighet og velge ansatte fra en timplan, er en god ide, men vanskelig å implementere grunnet digitale turnusordninger (vedlegg L). Det er nødvendig å integrere støtte for at Omhu kan hente turnusplanen til de ansatte fra en ekstern virksomhet, for at funksjonen lar seg gjøre.

Oppdragsgiver har også gitt uttrykk for at enkelte tjenesteytere, spesielt i offentlig sektor, ønsker mulighet til å administrere brukerenes tilgang til opprettelse og redigering av aktiviteter. Dette er pga. at mange i målgruppen ikke er vant til en så stor grad av selvbestemmelse, og det er ønskelig med en gradvis tilvenning av

slike funksjoner. Resultatet fra brukertesten av målgruppen, viste at alt relatert til "lesing" av aktiviteter, som å sjekke klokkeslett og beskrivelse av aktiviteten, fungerte svært bra.

Som nevnt i kapittel 5, var det flere deler av pasientmodulen som i løpet av brukertesting, viste seg å ikke fungere optimalt. Dette gjelder funksjonalitet relatert til aktivitets-maler, og funksjonalitet for sammenligning av de ansatte sin timeplan. Utifra brukertestene er det tydelig at bruk av aktivitets-maler vil kreve dedikert opplæring av sluttbrukerene. Redigering og opprettelse av nye maler kan regnes å være utenfor evnenivået til mange i målgruppen.

Dette gjelder også sammenlignings-funksjonen. Ut i fra brukertestingen på målgruppen, har problemet antageligvis ikke noe med designet i seg selv å gjøre, men heller at funksjonaliteten er "overflødig", og gir brukerene funksjonalitet som de ikke trenger eller ønsker seg. Under testen, klarte ikke testmoderator eller testdeltagernes assistent, å forklare konseptet "mal" til deltageren. Testdeltageren skjønte med andre ord ikke hva en "mal" er, og heller ikke hva den brukes til. Dette gjør en slik funksjonalitet i Omhu overflødig. Oppdragsgiver har også nevnt at maler ikke trenger å være en del av applikasjonen til målgruppen (vedlegg møtereferat, 22.04, N).

Grunnet utbredelsen av lese- og skrive-vansker innad i målgruppen [70], er det antagelig at et system for aktivitets-maler, kan være en fordel. Utfordringen er å finne en bedre metode for å få brukerene til å lettere skjønne konseptet, og å skjønne fordelene ved en slik funksjon. Mal-funksjonen har dermed blitt bevart til den siste iterasjonen av pasientmodulen, med mulighet for å skru av denne funksjonen på sidens innstillinger. Funksjonaliteten for redigering og opprettelse av maler har i tillegg blitt skjult bak en "'hamburger-meny", ment som en "avansert" egenskap som forblir tilgjengelige for brukere som ønsker denne funksjonen.

6.3 Videre arbeid

Dette kapittelet beskriver videre arbeid som kan gjøres, både mtp. autentisering og design av pasientmodulen.

6.3.1 Videre arbeid for kartlegging av autentisering

Kartleggingen av autentiseringsmetoder gjennført i denne studien har vært basert på kilder fra tjenesteytere, faglitteratur og brukertesting. Det finnes derimot svært få kilder som gjennomfører sammenligninger av autentiseringsmetoder, og enda

mindre som omhandler den konkrete brukergruppa.

Brukertestene gjennomført for autentisering har vært svært verdifulle, men det er fortsatt mange aspekter som vi ikke har undersøkt pga. tidsmangel. For videre arbeid kan det tenkes at flere brukertester av forskjellige typer er fordelaktig. De ulike typene er beskrevet nedenfor. Selv om vi brukertestet 8 personer til sammen i autentiseringsdelen, var det kun 2 stk som er i målgruppen. Dette er en målgruppe som det ikke er så enkelt å få kontakt med, og derfor var vi nødt til å også finne testpersoner utenfor målgruppen. I videre arbeid er det derfor anbefalt at flere personer i målgruppen blir testet, for å få et representativt resultat.

Validerings-testing av komplette løsninger

Det kan med fordel teste to eller flere komplette løsninger opp mot hverandre mot en forhåndsdefinert standard, i en *valideringstest*. En slik test er egnet til å bekrefte eller avkrefte vurderingene/resultatene fått i dette prosjektet. Ved å ha flere "komplette" innloggingsløsninger for 2-faktor autentisering, kan mer nøyaktig, kvantitativ data brukes for å måle metodene opp mot hverandre. For at en slik test skal være legitim, bør en benytte et større antall testdeltagere.

Testing av autentiseringsmetoder med opplæring

Grunnet at testdeltagerne allerede hadde erfaring med noen autentiseringsmetoder, kan det også tenkes at enkelte autentiseringsfaktorer fikk "urettferdig" dårlig score under brukertestene. F. eks. sikkerhetsnøkkel hadde ingen erfaring med på forhånd, men alle var vant til å bruke passord, og mange brukte biometri som autentiseringsfaktor daglig. Under det kvalitative intervjuet under den første brukertesten (vedlegg D), kom det dessuten frem at flere testdeltagere mente at rangeringen de gav de ulike faktorene var "urettferdig", ettersom noen faktorer var de mye mer kjent med enn andre.

Det kan derfor antas at enkelte autentiseringsfaktorer var vanskelige, pga. at de var ukjente, og at brukerene ikke hviste hvordan de skulle bruke den ved førstegangsbruk. Ved å gi opplæring på alle autentiseringsmetodene på forhånd, for så å brukerteste etter en viss tid, kan man få bedre sammenligninger med autentiseringsfaktorer som "alle" er kjent med fra før, som biometri og passord.

MinID

MinID er et autentiseringsalternativ via IDporten, som ikke har blitt brukertestet i oppgaven. Dette er et offentlig, sikkerhetsnivå 3 alternativ, som kan vurderes i fremtiden.

6.3.2 Videre arbeid for nytt grensesnitt

Pasientmodulen utviklet i oppgaven har gjennomgått tre iterasjoner med testing og forbedring. Testene gjennomført har derimot ikke vært fullstendige, og det har enda ikke blitt gjort testing for den siste versjonen av grensesnittet. Mye av det videre arbeidet med pasientmodulen vil da være videre testing, for å validere at løsningene implementert fungerer som ønsket. Deretter er det også forslag til ny funksjonalitet som kunne ha forbedret brukeropplevelsen ytterligere.

Testing av rapporterings-funksjon

Etter møte med fagpersoner fra Halden kommune ble det diskutert nødvendigheten for å la brukere rapportere uønskede hendelser med de ansatte, f. eks. tilbakemelding om dårlig utført jobb. Denne funksjonen ble ikke implementert i iteration 3 av pasientmodulen, og dermed ennå ikke brukertestet. Dette er en viktig funksjon som bør bli implementert, og deretter brukertestet i fremtiden. Denne brukertestingen, kan utføres med fokus på scenarioer med sluttbrukere, for å se hvilke hypotetiske situasjoner som de prioriterer å melde fra om eller ikke.

Testing av pasientmodul med opplæring av brukere

Som med autentiserings-kartleggingen, hadde det vært ønskelig å gjennomføre brukertester av pasientmodulen der brukerene først får en gjennomgang av hvordan applikasjonen fungerer. Brukertestene gjennomført for pasientmodulen viste at brukere i målgruppen har store problemer med å forstå formålet og utførelsen av enkelte deler av applikasjonen. Det hadde vært en fordel å kunne ha gjennomført tester på disse delene, etter at opplæring har blitt utført. Dette vil vise om disse elementene av pasientmodulen er verdt å ta med videre, eller om de er overflødige.

Video-dokumentasjon og video-elementer i aktiviteter

Bruk av video i pasientmodulen med det formål av å forbedre brukervennligheten har vært vurdert i dette prosjektet. Video kan brukes i pasientmodulen som virkemiddel for å forklare sluttbrukere mer komplekse begreper som ville vært uoverkommelig med tekst. For eks. å legge til video-guider på alle hjelpe-popups plassert på siden, tilgjengelig via de runde knappene med spørsmålstegn. For øyeblikket viser disse hjelpe-sidene kun tekst, men som forklart både fra våre brukertester og eksterne kilder, hadde brukere med lese-skrivevansker problemer med å lese lange avsnitt med dokumentasjon.

Et annet forslag for bruk av video kan være dens implementasjon som et element av aktiviteter. Brukere og ansatte ville kunne laste opp video til nettsiden, som deretter vises når en inspiserer en aktivitet. En slik egenskap vil forbedre nytteverdien av hele platformen, da dette åpner for muligheten til å ha fremgangsmåter og "guider" integrert i aktiviteter i Omhu, som sluttbrukerene deretter kan følge på egenhånd. For eksempel, i en aktivitet kalt "Pusse tenner", kunne det ha vært en video brukeren kan spille av, som tydelig viser en film eller animasjon der verten forklarer alle stegene nødvendig for å pusse tennene ordentlig. Brukeren kan deretter kopiere stegene vist i videoen for å gjennomføre handlingen selv. Dette vil ytterligere øke autonomien til sluttbrukerene av Omhu, og dermed effektivisere løsningen for både brukere og ansatte.

6.4 Bærekraft

Som nevnt i introduksjonen til denne oppgaven, slår FN fast at mennesker med utviklingshemming, både er i stand til og skal bestemme over eget liv. De har også en rett til å gjøre nettopp dette. Det er likevel grunner som gjør at disse menneskene ikke får praktisere selvbestemmelse i stor nok grad i forhold til funksjonsevnene deres. Ifølge stortingsmeldingen [3] og intervjuer vi har gjort med fagpersoner, se vedlegg L, er tydelig at et system som kan tilrettelegge for dette rundt om i Norge's kommuner, er enten fraværende, eller svært vanskelige å bruke på en effektiv måte.

Oppgavens formål var å kartlegge alternative innloggingsløsninger (autentiseringsmetoder) som i større grad tilgjengeliggjør Omhu for pasientene, samtidig som personvernet blir ivaretatt på en tilfredsstillende måte. I tillegg skulle vi designe en pasientmodul som er brukervennlig, og enkel å benytte for pasienter med forskjellige forutsetninger. For hele oppgaveteksten, se vedlegg R

Mangelen på gode systemer i helsesektoren, gjør det dermed vanskeligere å sikre

at mennesker med utviklingshemming, får i stor nok grad et rettferdig og anstendig liv, på lik linje med samfunnet forøvrig. Omhu tar i bruk den økte digitaliseringen og tilgjengeligheten som mobile enheter og internett har muliggjort, og utnytter dette med mål om å effektivisere og gjøre samarbeidet mellom pasienten selv, og tjenesteyterene enklere. Oppgaven har bidratt til å realisere WeissTech sine ambisjoner om en web-app, som spesifikt er rettet mot å gjøre hverdagen til målgruppen og arbeidslivet til assistentene, bedre og enklere. På denne måten kan man konkludere med at bacheloroppgaven har bidratt til en bærekraftig utvikling, ved å bidra til å designe teknologiske system som har et stort potensial for å forbedre brukerenes selvbestemmelse og autonomi.

6.5 Kritikk av oppgaven

Dette kapittelet reflekterer rundt feil og mangler, samt konstruktiv kritikk til tilærmingen av oppgaven.

6.5.1 Manglende datamateriale for vurderinger

For kartleggingen av autentiseringsmetoder var målet å skape et resultat som kunne være nyttig for Weisstech i deres fremtidige valg av autentiseringsløsning, når Omhu skulle utvides til den nye målgruppen. Av denne grunn ble autentiseringsmetodene vurdert ut fra fem egenskaper som til sammen skulle gi et realistisk bilde av metodene.

Det oppsto imidlertid utfordringer med å anskaffe enkelte av de nødvendige verdiene for å kunne evaluere metodene. På grunn av mangel på eksisterende undersøkelser på temaet, ble noen vurderinger basert på logiske slutninger fremfor empiriske data. Slike slutninger medfører antagelser om produktene basert på teoretiske beskrivelser, som ikke nødvendigvis er korrekte i praktisk implementasjon.

Vurderingen av "brukervennlighet" for de forskjellige metodene, viste seg å være spesielt utfordrende. Derfor ble det besluttet å gjennomføre en brukertest for å verifisere de tidligere vurderingene av brukervennlighet, basert på offentlig tilgjengelig informasjon om produktene. I flere tilfeller viste denne brukertestingen at produktene var vanskeligere eller enklere å bruke enn først antatt. Det er positivt at disse feilvurderingene ble avdekket, men det gjenstår fortsatt vurderinger i studien som ikke har gjennomgått samme behandling. Dette svekker kredibiliteten til noen av resultatene i kartleggingen.

6.5.2 Bredde over dybde - Spredt fokusområde

Denne oppgaven er todelt, med den ene delen fokusert på kartleggingen av autentiseringsmetoder, mens andre halvdel omhandler designet av brukergrensesnittet. Denne formen for oppgave førte til at ressursene ble noe tynt fordelt utover prosjektet. Om gruppen hadde besluttet å kutte vekk enten del 1 eller del 2, ville det vært mer tid til å gå i dybden av de respektive temaene.

Pasientmodulens design kunne ha blitt mer skreddersydd, dersom vi fikk testet elementer som er mer spesifikke for bruksområdet. F. eks. bruk av instruksjonvideoer i pasientmodulen, for å sjekke hvordan målgruppen hadde respondert til dette. Dette hadde vært mulig, om tidsressursene hadde latt oss gjøre en eller to iterasjoner til. På samme måte kunne kartleggingen av autentisering blitt forbedet med mer tid.

Oppgavens todeling gjorde det med andre ord vanskelig å få et godt resultat av både del 1 og del 2 av oppgaven. I stedet for å gå i dybden på enten autentisering eller web-design, fikk vi kun bevege oss mer i overflaten av begge fagområdene. Den røde tråden mellom oppgavene er brukervennlighet med fokus på målgruppen, men sett bort i fra dette kunne det like så godt vært to separate oppgaver.

6.5.3 Feil i brukertest av flere autentiseringsmetoder

Ved brukertest for forskjellige autentiseringsmetoder (se kapittel 5.1) ble brukerene spurt om de hadde erfaring med BankID appen eller kodebrikken som autentiseringsmetode. For dette spørsmålet svarte de fleste av deltagerene “ja”. I testen var formålet å la brukerne sammenligne forskjellige faktorer hver for seg, slik som at “passord” og “autentiseringsapp” ble rangert som to seperate metoder, selv om de var testet i samme test. I etterkant av testen ble det trukket oppmerksomhet til det faktum at BankID var rangert så lavt, og at flere brukere klagde på at “de måtte skrive inn passord likevel”. Utifra dette er det mulig at disse deltagerene vurderte hele prosessen for bruk av BankID, inkludert personummer og passord når de ga rangeringen, og ikke bare autentiseringsappen. Dette var selvfølgelig en forklaringsfeil fra gruppens side, men gjør at BankID i grunn ble vurdert som en 2-faktor autentisering løsning opp mot alle de andre metodene, som var 1-faktor. Resultatet viser derfor potensielt BankID i et dårligere lys enn det som hadde vært riktigt.

6.6 Evaluering av gruppens arbeid

I begynnelsen av prosjektet satte gruppen et sett med felles prosess-mål, som skulle omhandle hvordan gruppen målsatte seg å arbeide gjennom prosjektet for å oppnå det ønskede resultatet.

1. Holde en effektiv og god arbeidsflyt innad i gruppen gjennom hele prosjektet
2. Ha en løpende og tett kommunikasjon med oppdragsgiver og veiledere
3. Jobbe etter Scrum metodikken
4. Dokumentere og loggføre fremgangen av arbeid

Målene er oppnådd, men i varierende grad. Organiseringen av arbeid i gruppen har generelt vært god, der alle har hatt god oversikt over fremtidige mål og fremtdrift gjennom Scrum-sprintene. Det har likevel vært sprinter der mindre har blitt gjort, og sprinter der mer har blitt gjort. Arbeidsflyten har dermed ikke vært kontinuerlig, men fulgt en "bølge"-effekt, gjennom sprintene.

Kommunikasjon med oppdragsgiver og veiledere har vært svært god.

Arbeidet har gått etter scrum metodikken gjennom hele prosjektet, der sprinter og Kanban Board har vært godt brukt for å organisere og spore fremgang av arbeidsoppgaver.

Gode møtereferat og skrifltig dokumentasjon på fremgang har blitt godt dokumentert. Det som ikke dokumenteres i møtereferat, har blitt dokumentert som GitHub issues gjennom prosjektet.

6.7 Bruk av KI

Gjennom prosjektet har KI språkmodeller blitt utnyttet til følgende formål:

Rettskriving og tekst-pynting: KI ble brukt for å gjennomføre rettskriving, samt pynte på setningsoppbygning i enkelte avsnitt i rapporten. Teksten som KI modellen returnerte hadde omtrentlig lik lengde som teksten den fikk i utgangspunktet. I denne studien har KI aldri blitt benyttet til å generere nye avsnitt eller komme med påstander som ikke var i den opprinnelige inputteksten. De brukte modellene er ChatGTP 3.5 og ChatGTP 4o.

Koding: Programutviklingen gjort i dette prosjektet ble gjennomført med bruk av KI for skriving av isolerte funksjoner, identifisering av feil i kode samt

kommentering av kode. KI har ikke blitt brukt for å ta beslutninger relatert til overordnet dataflyt, valg av teknologier, eller andre interne mekanismer i koden utover det isolert i enkelt-funksjoner. De brukte modellene er ChatGTP 3.5 og Github Copilot.

Kapittel 7

Konklusjon

I dette prosjektet har gruppen samarbeidet med WeissTech AS for å fullføre følgende oppgaver:

1. Komme med forslag til ny pasientmodul av Omhu, spesielt tilpasset sluttbrukerene i målgruppen.
2. Kartlegge alternative autentiseringsmetoder til BankID, som ivaretar sikkerhet for brukere innen målgruppen på en brukervennlig måte.

Både kartleggingen av autentisering og utviklingen av pasientmodulen gjennomføres som forberedelse på en fremtidig ekspansjon av Omhu, et journal-verktøy utviklet av WeissTech ment for å brukes av ansatte innen brukerstyrt personlig assistanse (BPA). Ekspansjonen har som mål å la sluttbrukerene av BPA benytte seg av Omhu slik som kun ansatte har kunnet gjøre til nå. Med dette skal sluttbrukerene oppnå en høyere grad av autonomi i sin egen hverdag. Målgruppen for prosjektet består av personer med behov for personlig assistanse grunnet lettere psykisk utviklingshemming.

Pasientmodul For den andre delen av oppgaven har det blitt utviklet et forslag til design av pasientmodulen. Dette designet innebærer funksjonalitet for å la brukere se fremtidige aktiviteter i både liste og kalender visning, opprette aktiviteter der de selv kan legge til ønske om spesifikk ansatt utifra hvem som er tilgjengelig for dem på et gitt tidspunkt. Brukerene kan også se en begrenset utgave av ansattes timeplan for bedre planlegge når dem er tilgjengelig. Det er også mulighet for å opprette aktiviteter basert på maler, samt redigere og opprette maler selv.

Gjennom prosjektet testet vi pasientmodulen i to omganger, der vi implementerte endringer etter begge omgangene for totalt tre iterasjoner. Testene viste at kjerne-

funksjonaliteten av navigasjon, lesing, opprettelse og redigering av aktiviteter fungerte bra, mens egenskapene for behandling av aktivitets-maler og sammenligning av ansatte i kalenderen fungerte dårligere(se kap 5.2.3). Mye av vanskelighetene kom fra feil i lav-nivå designet, der det ofte var for mye informasjon per side og et u-intuitivt sideoppsett. Det er også antagelig at enkelt av funksjonaliteten i pasientmodulen er for avansert for målgruppen. Det virker derfor usannsynlig at sluttbrukerene vil kunne utnytte tjenesten utover det mest grunnleggende med mindre opplæring blir gitt.

Kartlegging av autentiseringsfaktorer Denne delen av oppgaven kommer som et resultat av at mange personer innenfor målgruppen mangler tilgang på BankID.

I dette prosjektet har det blitt identifisert flere lovende, og en del ikke-lovende, autentiseringsmetoder som eksisterer i dag. Disse metodene blir vurdert basert på deres sikkerhet, brukervennlighet, dekning(andel sluttbrukerene som har tilgang på metoden), kostnad og implementasjon (vanskelighetsgrad av teknisk implementasjon samt organisatoriske konsekvenser, målestokk på hvor "'realistisk" løsningen er.). Hver egenskap for hver metode ble vurdert med en verdi fra en til fem. For å begrunne verdiene satt, ble faglitteratur brukt, teknisk dokumentasjon lest og brukertester gjort. De ulike autentiseringsfaktorene ble først vurdert for seg selv, før de ble vurdert sammen med andre faktorer, for komplette multi-faktor løsninger.

En av de mer lovende metodene identifisert tidlig i prosjektet er *sikkerhetsnøkkel* kombinert med *fingeravtrykk/ansiktsgjenkjenning* som et passordløst innloggingsalternativ. Ved å bruke FIDO2/WebAuthn standarden, ble det utviklet en komplett teknisk demo for denne metoden, som også ble brukt i brukertesting.

Brukertestingen viste at biometri er er godt alternativ som autentiseringsfaktor, ettersom de fleste testdeltagerene i de forskjellige brukertestene var fornøyd med dette. I tillegg er det meget sikkert, og ved hjelp av plattform-autentisering, blir ingen biometrisk informasjon sendt ut av enheten. Sikkerhetsnøkkel ble godt likt av den ene testdeltageren fra målgruppen, men ikke av den andre. Sikkerhetsnøkkel som autentiseringsfaktor nummer 2, må derfor vurderes nøyere som et alternativ i fremtiden. Sikkerhetsnøkkel er likevel mye bedre enn passord og autentiseringsappkikasjon. Begge disse faktorene ble ikke vurdert som brukervennlige av de fleste testdeltagerene.

Bibliografi

[1] G. Lawton. «near-field communication (NFC).» (2022), adresse: https://www.techtarget.com/searchmobilecomputing/definition/Near-Field-Communication (sjekket 24.01.2024).

[2] NAKU - Nasjonalt kompetansemiljø om utviklingshemming. «Utviklingshemming – Mennesket og diagnosen.» (2024), adresse: https://naku.no/utviklingshemming-%E2%80%93-mennesket-og-diagnosen (sjekket 09.05.2024).

[3] *Menneskerettigheter for personer med utviklingshemming*, Stortingsmelding, Kultur- og likestillingsdepartementet, 2023. adresse: https://www.regjeringen.no/contentassets/49e90a1d80dd4b4bbe6ef117d548262c/no/pdfs/meldst8_lettlest.pdf.

[4] «Sikkerhetsnivå,» Altinn. (2024), adresse: https://info.altinn.no/hjelp/innlogging/diverse-om-innlogging/hva-er-sikkerhetsniva/. besøkt: 29.01.2024.

[5] T. H. Nätt og S. J. Knapskog. «autentisering.» (2022), adresse: https://snl.no/autentisering (sjekket 23.01.2024).

[6] «Biometri,» Datatilsynet. (2019), adresse: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/ (sjekket 11.05.2024).

[7] A. Jain, R. Bolle og S. Pankanti, *Biometrics: Personal Identification in Networked Society*. Springer Science+Business Media, 1996.

[8] «Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor,» Digdir. (2024), adresse: https://www.digdir.no/digital-samhandling/veileder-identifikasjon-og-sporbarhet-i-elektronisk-kommunikasjon-med-og-i-offentlig-sektor/2992#definisjon_av_sikkerhetsniver_for_identifikasjon (sjekket 29.01.2024).

[9] «Regler og krav for bruk av eID,» Digdir. (2024), adresse: https://www.digdir.no/digital-identitet/regler-og-krav-bruk-av-eid/4702 (sjekket 29.01.2024).

[10] «Ulike sikkerhetsnivå,» Difi. (2024), adresse: https://eid.difi.no/nb/sikkerhet-og-personvern/ulike-sikkerhetsniva (sjekket 29.01.2024). besøkt: 29.01.2024.

[11] «What is FIDO?» FIDO Alliance. (2024), adresse: https://fidoalliance.org/what-is-fido/ (sjekket 11.05.2024).

[12] «User Authentication Specifications Overview,» FIDO Alliance. (2024), adresse: https://fidoalliance.org/specifications/ (sjekket 24.01.2024).

[13] «WebAuthn: A better alternative for securing our sensitive information online,» Duo Security. (2024), adresse: https://webauthn.guide/ (sjekket 04.05.2024).

[14] «WebAuthn Introduction,» Yubico. (2024), adresse: https://developers.yubico.com/WebAuthn/ (sjekket 04.05.2024).

[15] «Android is for everyone,» Google LLC. (2024), adresse: https://www.android.com/everyone/ (sjekket 29.01.2024).

[16] «Measuring Biometric Unlock Security,» Google LLC. (2024), adresse: https://source.android.com/docs/security/features/biometric/measure (sjekket 29.01.2024).

[17] «Vi kan digital sikkerhet,» Commfides Norge AS. (2024), adresse: https://www.commfides.com/ (sjekket 02.02.2024).

[18] F. E. Sandnes, *Universell utforming av IKT-systemer - brukergrensesnitt for alle*. Universitetsforlaget, 2022.

[19] T. Tullis og B. Albert, *Measuring the User Experience - Collecting, Analyzing, and Presenting Usability Metrics*. Elsevier Inc., 2013.

[20] «WCAG 101: Understanding the Web Content Accessibility Guidelines,» WCAG. (2021), adresse: https://wcag.com/resource/what-is-wcag/ (sjekket 02.05.2024).

[21] «What's New in WCAG 2.2,» W3C. (2023), adresse: https://www.w3.org/WAI/standards-guidelines/wcag/new-in-22/ (sjekket 02.05.2024).

[22] «Hvorfor universell utforming av IKT?» Tilsynet for universell utforming av ikt. (2024), adresse: https://www.uutilsynet.no/veiledning/kvifor-universell-utforming-av-ikt/240 (sjekket 02.05.2024).

[23] I. M. Lid. «gap-modellen i Store norske leksikon.» (2022), adresse: https://snl.no/gap-modellen (sjekket 30.04.2024).

[24] «Menneskerettigheter for personer med utviklingshemming,» Regjeringen. (2023), adresse: https://www.regjeringen.no/no/dokumenter/menneskerettigheter-for-personer-med-utviklingshemming/id2966435/?ch=4 (sjekket 17.05.2024).

[25] J. Rubin, D. Chisnell og J. Spool, *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*, 2. utg. Wiley Publishing, Inc., 2008.

[26] R. B. Darlington, *Are Condorcet and minimax voting systems the best?* 2022. arXiv: 1807.01366 [physics.soc-ph].

[27] L. Guimarães, N. Martins, E. Penedos-Santiago, L. Pereira og D. Brandão, «Interface design guidelines for low literature users: a literature review,» *ACM*, 2022. DOI: https://doi.org/10.1145/3578837.3578842.

[28] D. Balfanz, A. Czeskis, J. Hodges, J. Jones, M. Jones, A. Kumar, A. Liao, R. Lindemann og E. Lundberg, «Web Authentication: An API for accessing Public Key Credentials Level 1,» i W3C, 2019, kap. 1.

[29] D. Balfanz, A. Czeskis, J. Hodges, J. Jones, M. Jones, A. Kumar, A. Liao, R. Lindemann og E. Lundberg, «Web Authentication: An API for accessing Public Key Credentials Level 1,» i Authenticator, W3C, 2019, kap. 4.

[30] H. Bolimovsky. «WebAuthn Basic Web Client/Server.» (2019), adresse: https://www.herbie.dev/blog/webauthn-basic-web-client-server/ (sjekket 08.05.2024).

[31] J. J. Garett, *The Elements of User Experience: User-Centered Design for the Web and Beyond, Second Edition*, 2. utg. New Riders Publishing, 2011.

[32] N. Britton. «the psychology of color in web design and how to use it.» (2023), adresse: https://thrive.design/color-psychology-web-design/ (sjekket 18.05.2024).

[33] «Testprosedyrar for nettstader og appar,» Tilsynet for universell utforming av ikt. (2024), adresse: https://www.uutilsynet.no/regelverk/testprosedyrar-nettstader-og-appar/709 (sjekket 17.05.2024).

[34] «Kronisk utmattelsessyndrom – CFS/ME,» Helsedirektoratet. (2023), adresse: https://www.helsenorge.no/sykdom/skader-og-sykdommer-i-hjernen/cfs-me/ (sjekket 12.05.2024).

[35] V. F. de Santana, R. de Oliveira, L. D. A. Almeida og M. C. C. Baranauskas, «Web accessibility and people with dyslexia: a survey on techniques and guidelines,» *ACM*, 2012. DOI: https://doi.org/10.1145/2207016.2207047.

[36] «What is Password-Based Authentication?» Descope. (2023), adresse: https://www.descope.com/learn/post/password-authentication (sjekket 01.02.2024).

[37] «Unlocking the Mystery of Iris Recognition,» Aratek. (2023), adresse: https://www.aratek.co/news/what-is-iris-recognition (sjekket 30.01.2024).

[38] «Iris Recognition Technology,» Innovatrics. (2024), adresse: https://www.innovatrics.com/iris-recognition-technology/ (sjekket 30.01.2024).

[39] «Biometrics Simplified,» Aware. (2024), adresse: https://www.aware.com/ (sjekket 30.01.2024).

[40] «Geolocation,» Khan Academy. (2024), adresse: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:user-data-tracking/a/geolocation (sjekket 31.01.2024).

[41] «Geolocation: Displaying User or Device Position on Maps,» Google. (2024), adresse: https://developers.google.com/maps/documentation/javascript/geolocation#maps_map_geolocation-javascript (sjekket 31.01.2024).

[42] «Geolocation API,» Mozilla. (2023), adresse: https://developer.mozilla.org/en-US/docs/Web/API/Geolocation_API (sjekket 31.01.2024).

[43] «Face Authentication,» Innovatrics. (2024), adresse: https://www.innovatrics.com/glossary/face-authentication/ (sjekket 02.02.2024).

[44] «Face ID, Touch ID, koder og passord,» Apple Inc. (2022), adresse: https://support.apple.com/no-no/guide/security/sec9479035f1/web (sjekket 31.01.2024).

[45] «The 2022 Duo Trusted Access Report,» Cisco Duo. (2022), adresse: https://duo.com/resources/ebooks/the-2022-duo-trusted-access-report#anchor (sjekket 16.05.2024).

[46] «Telias salg av brukte mobiler fjerde kvartal og hele 2023: Apple iPhone 11 forblir favoritten,» Telia. (2023), adresse: https://presse.telia.no/pressreleases/telias-salg-av-brukte-mobiler-fjerde-kvartal-og-hele-2023-apple-iphone-11-forblir-favoritten-3298890 (sjekket 16.05.2024).

[47] «iPhone5S iPhone 5s - Tekniske spesifikasjoner,» Apple Inc. (2024), adresse: https://support.apple.com/kb/SP685?locale=nb_NO&viewlocale=no_NO (sjekket 29.01.2024).

[48] J. Chuck. «Apple's iPhone 5s 1 Worldwide Smartphone And Quadruples Chinese Share.» (2013), adresse: https://www.forbes.com/sites/chuckjones/2013/12/11/apples-iphone-5s-1-worldwide-smartphone-and-quadruples-chinese-share/?sh=7568b5d252d5 (sjekket 29.01.2024).

[49] «Build your first WebAuthn app,» Kitamura Eiji. (2022), adresse: https://developers.google.com/codelabs/webauthn-reauth#0 (sjekket 31.01.2024).

[50] «Hvor mange mennesker har smarttelefoner i Norden?» MyTrendyPhone. (2024), adresse: https://www.mytrendyphone.no/shop/cms-rapport-smarttelefonbruk-i-norden.html (sjekket 02.02.2024).

[51] «A Comprehensive Guide to Security Keys and Terms: Key Concepts You Need to Know,» Kensington Computer Products Group. (2023), adresse: https://www.kensington.com/news/security-blog/key-concepts-you-need-to-know-about-security-keys/ (sjekket 24.01.2024).

[52] «How the YubiKey works,» Yubico. (2024), adresse: https://www.yubico.com/products/how-the-yubikey-works/ (sjekket 24.01.2024).

[53] A. Trevino. «What Are Authenticator Apps and How Do They Work?» (2023), adresse: https://www.keepersecurity.com/blog/2023/07/20/what-are-authenticator-apps-and-how-do-they-work/ (sjekket 24.01.2024).

[54] A. Trevino. «Types of Multi-Factor Authentication (MFA).» (2023), adresse: https://www.keepersecurity.com/blog/2023/06/27/types-of-multi-factor-authentication-mfa/#:~:text=Time%2DBased%20One%2DTime%20Password%20(TOTP)&text=After%20entering%20their%20password%20to,protected%20and%20difficult%20to%20intercept (sjekket 24.01.2024).

[55] «Technical Setup Archive,» Cisco system Inc. (2024), adresse: https://duo.com/resources/videos/archive/technical-setup (sjekket 25.01.2024).

[56] «Kortskriver Smart-21 tilbud - Inkl. programvare og tilbehørspakke for både Windows og MAC,» NORDANO. (2024), adresse: https://nordano.com/no/index.php/vare/smart-21s-nordano/ (sjekket 24.01.2024).

[57] «HTML attribute: capture,» Mozilla. (2023), adresse: https://developer.mozilla.org/en-US/docs/Web/HTML/Attributes/capture (sjekket 17.05.2024).

[58] T. H. Nätt. «kodebrikke i Store norske leksikon.» (2022), adresse: https://snl.no/kodebrikke (sjekket 25.01.2024).

[59] R. Awati og D. Hwang. «What is a key fob?» (2021), adresse: https://www.techtarget.com/searchsecurity/definition/key-fob (sjekket 25.01.2024).

[60] «Editions Pricing,» Duo. (2024), adresse: https://duo.com/editions-and-pricing (sjekket 18.05.2024).

[61] «Duo Auth API,» Duo. (2024), adresse: https://duo.com/docs/authapi (sjekket 18.05.2024).

[62] «Introduction to OAuth 2.0,» Google. (2024), adresse: https://cloud.google.com/apigee/docs/api-platform/security/oauth/oauth-introduction (sjekket 26.01.2024).

[63] «Enforce 2-Step Verification (2SV),» Google. (2023), adresse: https://knowledge.workspace.google.com/kb/enforce-2-step-verification-000008884 (sjekket 18.05.2024).

[64] H. K. R. Garder, L.-M. Kristiansen og S. H. Bae, «Sikkerhet i mobilinfrastruktur/autentisering,» *NTNU Open*, 2018. adresse: http://hdl.handle.net/11250/2562059.

[65] «Identity Platform pricing.» (2024), adresse: https://cloud.google.com/identity-platform/pricing (sjekket 18.05.2024).

[66] «Fakta om Internett og mobiltelefon.» (2023), adresse: https://www.ssb.no/teknologi-og-innovasjon/faktaside/internett-og-mobil (sjekket 18.05.2024).

[67] «MinID,» MinID. (2024), adresse: https://eid.difi.no/nb/minid (sjekket 29.01.2024).

[68] «Kostnadsmodell for ID-porten.» (2023), adresse: https://samarbeid.digdir.no/id-porten/kostnadsmodell-id-porten/66 (sjekket 18.05.2024).

[69] «Ta i bruk ID-porten,» Samarbeidsportalen. (2024), adresse: https://samarbeid.digdir.no/id-porten/ta-i-bruk-id-porten/94 (sjekket 30.01.2024).

[70] NAKU - Nasjonalt kompetansemiljø om utviklingshemming. «Den medisinske diagnosen psykisk utviklingshemming.» (2024), adresse: https://naku.no/kunnskapsbanken/diagnose-psykisk-utviklingshemming-icd-10 (sjekket 09.05.2024).

Figurer

Tabeller

Kodelister

Vedlegg A

Brukertest for pasientmodul v1

Bachelor Gruppe 120 - Vår 2024

Dato: 30/03/2024

Test objekt: Omhu pasient modul versjon 1.0

A.1 Mål for test

Hva ønskes å finne ut av gjennom testen?

1. Er top-menyen intuitiv til bruksområdene av fanene?
2. Forstår brukeren hva som som kan interageres med?
3. Hvor vanskelig er det for brukeren å se når en ansatt er ledig?
4. Forstår brukeren hvordan de vertikale og horisontale navigasjons-elementene fungerer?
5. Klarer brukere å rette opp fra feiltrinn raskt?
6. Er nettsiden oversiktlig?

A.2 Oversikt over test

Testen er strukturert som følger:

1. Introduksjon
2. Pre-test spørreskjema
3. Utforskende test
4. Oppgave 1: Top-nav meny
5. Oppsummerende test
    a. Klokkeslett
    b. Inspiser aktivitet
    c. Rediger aktivitet
    d. Inspiser fullført aktivitet
    e. Last inn mal
    f. Rediger mal
    g. Opprett ny mal
    h. Sammenlign ansatte
6. Post-test spørreskjema

A.3 Testdeltakere

For denne testen er det ikke satt noen spesifikke krav for testdeltakerne, men det er ønskelig å teste med personer som betraktes å ha lavere kompetanse i bruk av nettsider på smarttelefoner enn gjennomsnittsnordmannen.

Som nevnt er det ingen strenge begrensninger for hvem som kan delta i testen, men det vil bli gjennomført minst en test med en deltaker som oppfyller beskrivelsen ovenfor. Resultatene fra denne testen vil også bli vektlagt høyere i konklusjonen av testen.

For å kartlegge deltakernes ferdigheter brukes et kort spørreskjema, som gis til deltakerne før testen starter. Skjemaet finnes under kapittel A.8.2.

For å avgjøre om deltakeren tilhører den ønskede gruppen, baserer vi oss hovedsakelig på deltakerens egen beskrivelse av sine tekniske ferdigheter. Hvis de svarer "lav" eller "svært lav", tilhører de gruppen. Det andre spørsmålet om deres mobilbruksvaner kan brukes til å vurdere tvilstilfeller der deltakernes ferdigheter ikke samsvarer med deres egen vurdering av ekspertise.

Spørreskjema'et inneholder også beskrivelser av de ulike ferdighetsnivåene.

A.4 Metodologi

De valgte metodene som er utnyttet til testen er basert på metodene funnet i boken "Handbook of usability testing" skrevet av Jeffrey Rubin og Dana Chisnell. Da denne boken er skrevet i kontekst av brukertesting innad i en større bedrift, brukes kun elementer av boken som anses som relevant til brukertesting på en mindre skala.

A.4.1 Utforskende test

Om metoden

Brukertesten er en hybrid av forskjellige former for tester. Det vil først bli gjennomført en svært kort "oppsummerende test". En slik test er kvalitativ, har en høy mengde interaksjon med test-moderatoren, og brukes ofte tidlig i designprosessen for å finne åpenbare feil og mangler. I denne testen utnytter vi denne metoden for å spørre deltageren om hva de forvanter skal skje når de gjør visse handlinger på siden.

Metode for data-innsamling

Denne metoden generer kvalitativ data i form av tilbakemeldinger fra deltageren. Om det er mange tilbakemeldinger som går igjen vil det tyde på at dette er et stort problem. Om en tilbakemelding kun tas opp av en enkel deltager kan det vurderes om dette er et særtilfelle.

A.4.2 Oppsummerende test

Om metoden

I motsetning til en utforskende test, er en oppsummerende test mindre "fri", og følger i større grad et planlagt sett med oppgaver. Kommunikasjonen mellom deltageren og moderator er også mindre under slike tester. Oppsummernede tester fungerer met at brukeren får et scenario der de er en sluttbruker med et problem eller mål, og at de da må bruke produktet for å oppnå dette målet med hjelp av produktet. Gjennom selve testen vil det ikke være noe kommunikasjon mellom deltager og moderator.

Metode for datainnsamling

Denne metoden er bedre egnet for å samle kvantitative data, og vil derfor bli utført i tillegg til innsamling av støttende kvalitative datapunkter. Følgende data vil bli målt under oppgavene:

1. Antall horisontale feiltrinn.
2. Antall vertikale feiltrinn.
3. Kommentarer og uttrykk for frustrasjon, samt om de er positive eller negative.
4. Tid brukt på å rette opp feil.
5. Grad av fullføring i henhold til de spesifikke kriteriene for suksess i oppgaven.

Hver forekomst av disse hendelsene dokumenteres, inkludert hvor på nettsiden hendelsen oppstod og årsaken til hendelsen. Dette gjøres gjennom en spørsmålsrunde etter hver oppgave, der deltakeren blir bedt om å beskrive tankene og intensjonene sine i øyeblikket feilen oppstod. På denne måten har hvert datapunkt en tilknyttet skriftlig forklaring på hvorfor hendelsen fant sted. Dette gjør det mulig å bruke hver hendelse som et kvantitativt datapunkt, samtidig som kvantitative begrunnelser blir samlet inn.

A.4.3 Post-test spørreskjema

Metodebeskrivelse

Etter gjennomføringen av oppgavene vil deltakerne bli bedt om å fylle ut et muntlig spørreskjema sammen med moderator. Hensikten med dette spørreskjemaet er å samle preferansedata, det vil si deltakernes meninger og tilbakemeldinger om produktet.

Datainnsamlingsmetode

Hvert element i skjemaet består av en påstand som deltakerne kan svare på ved hjelp av skalaen: *Svært uenig -> Uenig -> Litt enig -> Enig -> Svært enig*. I tillegg vil deltakerne bli bedt om å gi en begrunnelse for valget sitt. Dette gjør at spørreskjemaet genererer både kvalitativ og kvantitativ data som kan analyseres.

A.4.4 Verktøy for datainnsamling

All data samles inn ved hjelp av et Excel-dokument, der tabeller brukes til å registrere dataforekomster og tilhørende årsaks-forklaringer. Resultatene fra pre- og post-test spørreskjemaene vil også bli lagret her.

A.5 Test oppsett

Testen er utformet på en enkel måte for rask implementering på ulike steder. Deltakeren er plassert ved et bord med mobiltelefonen foran seg. Moderator sitter ved siden av for å observere skjermen. En eventuell sekretær sitter på den motsatte siden av bordet, overfor moderatoren.

A.6 Konfigurasjon av utstyr

- Brukertesten utføres på en OnePlus Nord smart-telefon med skjermstørrelse på 6,44 tommer og oppløsning på 1080 x 2400 pikseler.
- Brukertesten utføres i Google Chrome nettleser.
- Brukertesten utføres på den interaktive prototypen for pasientmodulen, versjon *1.0*.
- Brukertesten begynner på hjemsiden, altså på *dashboard* fanen.
- Brukertesten tar utgangspunkt i følgene sample data:
    1. Det er tre ansatte lagt til i systemet. De to første ansatte har skift annenhver dag fra kl07:00-23:00. Den tredje ansatte har skift lørdag-søndag fra kl07:00-23:00.
        - Åse Haug Løseth, Man-ons-fre
        - Trond Gjestad, Tirs-tors-Lør
        - Synnøve Fredriksen: Søn, Natt.
    2. Det er lagt til fire aktiviteter fra før. Tre av aktivitetene skjer på samme dag som brukertesten utføres.
        - Middag, i går.
        - Middag, i dag.
        - Middag, i morgen.
        - Kino, neste uke.

A.7 Oppgaver

A.7.1 Utforskende test

1. Hva forventer du skal dukke opp når du trykker på knappen her? *Vis knapp for kalender.*

A.7.2 Oppsummerende test

1 Finn klokkeslett

Spørsmål: Med å bruke nettsiden, fortell meg hva klokka er.
Krever fullført oppgave: Ingen
Kriterie for suksess:

1. Brukeren oppgir korrekt klokkeslett.

2 Inspiser aktivitet

Spørsmål: Når på dagen skal du på kino neste uke?
Krever fullført oppgave: Ingen
Kriterie for suksess:

1. Brukeren identifiserer den riktige aktiviteten på dashboard.
2. Brukeren inspiserer den riktige aktiviteten.
3. Bruker oppgir klokkeslettet til den riktige aktiviteten.

3 Redigere aktivitet

Spørsmål: Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.
Krever fullført oppgave: 2
Kriterie for suksess:

1. Brukeren finner aktiviteten på dashboard.
2. Brukeren inspiserer aktiviteten.

3. Bruker går inn på redigerings-siden for aktiviteten.
4. Bruker redigerer beskrivelsen for å skrive inn endringen i fritekst.
5. Brukeren lagrer den redigerte aktiviteten.

4 Innspiser fullført aktivitet

Spørsmål: Du fikk hjelp til å lage middag av en ny ansatt i går. Finn navnet til denne ansatte.
Krever fullført oppgave: 2
Kriterie for suksess:

1. Brukeren expander oversikten over ferdige aktiviteter.
2. Brukeren inspiserer aktiviteten.
3. Brukeren oppgir navnet til den ansatte.

5 Opprett ny aktivitet

Spørsmål: Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.
Krever fullført oppgave: 2,3
Kriterie for suksess:

1. Brukeren kommer inn på siden for å opprette en ny aktivitet.
2. Brukeren legger til alle obligatoriske felter med informasjon.
3. Brukeren legger til Trond som ansatt.
4. Hvis Trond ikke er ledig, trykker brukeren på sammenlign timeplan".
5. Hvis sammenligner timeplan: brukeren blar frem og tilbake til de finner en dag som passer.
6. Hvis sammenligner timeplan: brukeren trykker tilbake til redigeringetterpå.
7. Brukeren lagrer aktiviteten.

6 Last inn mal

Spørsmål: Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.

Krever fullført oppgave: 2,3,5
Kriterie for suksess:

1. Brukeren opretter en ny aktivitet.
2. Brukeren trykker på last inn fra mal".
3. Brukeren velger malen som heter "middag".
4. Brukeren laster inn malen i editoren.
5. Brukeren legger til dato på aktiviteten.
6. Brukeren legger til ansatt på aktiviteten.
7. Brukeren lagrer aktiviteten.

7 Rediger Mal

Spørsmål: Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Du liker ikke fisk, og dette er aldri inkludert i aktivitets-beskrivelsen for middag. Kan du redigere malen for middag for å spesifisere at du ikke liker fisk, for så og lagre denne malen?
Krever fullført oppgave: 2,3,5,6
Kriterie for suksess:

1. Brukeren navigerer til editor for aktivitet.
2. Bruker laster inn mal "middag".
3. Bruker endrer inneholdet.
4. Bruker lagrer malen under samme navn.
5. Bruker returnerer til dashboard uten å opprette en ny aktivitet.

8 Opprett ny mal

Spørsmål: Du pleier ofte å gå tur, og er lei av å skrive inn på nytt vær gang. Finn en måte å lage en ny mal med dine tur-preferanser.
Krever fullført oppgave: 2,3,5,6
Kriterie for suksess:

1. Brukeren navigerer til editor for aktivitet.
2. Brukeren skriver inn tidspunkt, beskrivelse og tittel.
3. Bruker trykker på lagre som mal".
4. Bruker lagrer malen.
5. Brukeren går tilbake til dashboard uten å opprette en ny aktivitet.

9 Sammenlign ansatte

Spørsmål: Du har lyst til å rydde leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.
Krever fullført oppgave: Ingen
Kriterie for suksess:

1. Brukeren navigerer til "min dagside.
2. Bruker velger de ansatte de ønsker å ha med sammenlignings-funksjonen.
3. Brukeren går fremover i tid og ser på ulike dager.
4. Brukeren finner et tidspunkt der to ansatte er ledige sammtidig.

A.8 Test-materiale

A.8.1 Introduksjon

Den følgende teksten skal leses nesten ordrett for test-subjektet før testen begynner:

Bakgrunn

1. Hei, jeg er ____, takk for at du vil delta på denne brukertesten.
2. Gjennom denne testen kommer jeg til å lese høyt fra et manus, så om det høres litt hakkete ut er det sannsynligvis derfor.
3. Vi er studenter med NTNU linje for cybersikkerhet og digital infrastruktur, der vi holder på og skrive vår bachelor-oppgave.
4. Vi skriver oppgaven for et firma som utvikler en nettside som brukes av helse-personale innenfor BPA, eller brukerstyrt personlig assistanse.
5. BPA er en bransje der personer som av forskjellige grunner ikke er i stand til å leve selvstendig, og derfor trenger hjelp av assistenter til å fullføre daglige gjøremål. BPA spesifikt har et mål om å la brukeren styre mest mulig av assistansen de får.
6. Nettsiden fungerer som et sammenslått planleggings-verktøy og pasient-journal der de ansatte kan holde styr på aktiviteter, brukere, og deres informasjon.
7. Utgiveren ønsker nå og utvide web-appen til ikke bare å fungere for ansatte, men også brukerene selv. Dette er da for å gi de mer kontroll over egen hverdag.
8. Oppgaven vår er å komme med en idee til en ny nettside, som er skreddersydd for behovene til sluttbrukerene, ikke de ansatte.
9. Kjernefunksjonen til nettsiden er det samme som før. Altså å planlegge assistanse mellom de ansatte og sluttbrukerene. Bare at versjonen vi lager, er spesifikt for at sluttbrukerene skal kunne bruke det.
10. Vi har nå laget et første-utkast av nettsiden, som vi ønsker å teste for å se hvor enkel den er å bruke, slik at vi kan forbedre den. Dette er det vi skal gjøre i dag.

Hvordan testen fungerer

1. Testen begynner med at vi fyller ut et lite skjema med litt bakgrunns-informasjon.

2. Deretter vil jeg stille deg noen åpne spørsmål om nettsiden, som du da besvarer muntlig.
3. Selve testen fungerer slik at jeg ber deg om å bruke nettsiden til å gjøre noen forskjellige oppgaver som en typisk sluttbruker ville ha gjort. Jeg kommer til å observere hvordan du oppnår eller ikke oppnår målet med oppgaven. Etter hver oppgave kan det hende jeg stiller noen spørsmål om det du gjorde for å bedre forstå tankegangen din. Jeg kan ikke hjelpe deg under testen, men kommer til å stoppe deg når du har fullført oppgaven. Om du sitter fast kan du også si i fra, så avslutter vi testen da. Om du lurer på noe teknisk om hvordan testen fungerer, kan vi selvfølgelig hjelpe deg med dette.
4. Til slutt skal jeg stille deg spørsmål om hva du syntes om nettsiden. Jeg gir deg svar-alternativer, og så kan du utdype fritt for begrunnelsen av ditt valgte svar.

Annen informasjon om testen

1. Jeg kommer til å gjøre opptak av mobilskjermen under testen, men ingenting annet blir gjort opptak av. Data'en vi samler er ikke sensitiv, men vil likevel bli lagret anonymt. Navnet ditt blir aldri skrevet ned.
2. Jeg vil også spesifisere at det overhodet ikke er du som blir testa her, det er nettsiden selv som vi ønsker å teste. Om noe skjærer seg, er det på grunn av at det er et problem med nettsiden.
3. Vi ønsker å bruke data fra denne testen for å forbedre nettsiden, og har derfor ikke noe insentiv om å få gode eller dårlige tilbakemeldinger. Så vær så ærlig som mulig når du gir tilbakemelding og svarer på spørsmål om på nettsiden.
4. Vi ønsker også at du "tenker høyt" gjennom testen.
5. Denne økta vil ta omtrent xx minutter. Gjerne still spørsmål underveis om det er noe du lurer på.
6. Har du noen spørsmål før vi begynner? [*Svar på spørsmål.*]

A.8.2 Pre-test spørreskjema

Det følgende skjema skal gjennomåes muntlig med test deltageren. Om deltager har spørsmål om spørsmålene, skal disse besvares av moderator etter beste evne.

Hva er din alder?

1. <13

2. 13-20
3. 21-30
4. 31-40
5. 41-50
6. 51-60
7. 61-70

Omtrentlig hvor ofte besøker du nettsider med smart-telefon eller nettbrett?

1. Mindre enn 1 gang i året.
2. 1-11 ganger i året.
3. 1-3 ganger i måneden.
4. 1-6 ganger i uka.
5. 1-2 ganger om dagen.
6. Mer enn tre ganger om dagen.

Hvordan vil du beskrive dine ferdigheter med bruk av smart-telefon?

1. Svært lav kompetanse. *Trenger hjelp med nesten alt. Ingen teknisk innsikt.*
2. Lav kompetanse. *Trenger hjelp med alt utenom rutine-oppgaver. Ingen teknisk innsikt.*
3. Moderat kompetanse. *Kan gjennomføre rutine-oppgaver og andre enklere oppgaver med applikasjoner du har trening i. Trenger hjelp for oppgaver du ikke har gjort før. Minimalt med teknisk innsikt.*
4. God kompetanse. *Trenger svært sjeldent hjelp med bruk av mobiltelefon. Klarer vanligvis å oppnå nye oppgaver uten hjelp. Kan behøve hjelp med særskilte problemer. Moderat teknisk innsikt.*
5. Svært god kompetanse. *Trenger nesten aldri hjelp. Kan gjennomføre alle oppgaver som kreves på mobilen, og fikser ofte problemer selv. God teknisk innsikt.*

A.9 Resultat fra brukertest

A.9.1 Subjekt 1

Aldersgruppe:21-30
Mobil-Kompetanse: God kompetanse
Hyppighet av mobilbruk: Mer enn tre ganger daglig.
Merknad: Ingen

Oppgave 1

Med å bruke nettsiden, fortell meg hva klokka er.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren oppgir korrekt klokkeslett.	Ja	

Tabell A.1: Subjekt 1 - Oppgave 1 - Kriterie for suksess

Oppgave 2

Når på dagen skal du på kino neste uke?

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren identifiserer den riktige aktiviteten på dashboard.	Ja	
Brukeren inspiserer den riktige aktiviteten.	Ja	
Bruker oppgir klokkeslettet til den riktige aktiviteten.	Ja	

Tabell A.2: Subjekt 1 - Oppgave 2 - Kriterie for suksess

Oppgave 3

Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren expander oversikten over ferdige aktiviteter.	Ja	
Brukeren inspiserer aktiviteten.	Ja	
Brukeren oppgir navnet til den ansatte.	Ja	

Tabell A.3: Subjekt 1 - Oppgave 3 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
Kollapset kategori-boks på dashboard	Deltageren kom borti pilen for å kollapse boksen.	Raskt, noen få sekunder.

Tabell A.4: Subjekt 1 - Oppgave 3 - Feiltrinn

Kontekst av kommentar	**Kommentar**	**Utdypning**
Lette etter sted å skrive inn pølser.	Gjerne ha spesifike felter for informasjon. Mer håndhålding. Litt vel åpent.	Test subjektet så etter et spesifikt felt for middags-ønske.

Tabell A.5: Subjekt 1 - Oppgave 3 - Kommentarer fra bruker

Oppgave 4

Du fikk hjelp til å lage middag av en ny ansatt i går. Finn navnet til denne ansatte..

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren inspiserer aktiviteten.	Ja	
Brukeren oppgir navnet til den ansatte.	Ja	

Tabell A.6: Subjekt 1 - Oppgave 4 - Kriterie for suksess

Oppgave 5

Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren kommer inn på siden for å opprette en ny aktivitet.	Ja	
Brukeren legger til alle obligatoriske felter med informasjon.	Ja	
Hvis Trond ikke er ledig, trykker brukeren på ss-ammenlign timeplan".	Nei	inkludert
Hvis sammenligner timeplan: brukeren blar frem og tilbake til de finner en dag som passer.	-	gikk ikke inn på sammenlign
Hvis sammenligner timeplan: brukeren trykker tilbake til redigeringetterpå.	-	gikk ikke inn på sammenlign
Brukeren lagrer aktiviteten.	Ja	

Tabell A.7: Subjekt 1 - Oppgave 5 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
La til trond uten at han var tilgjengelig.	La merke til rød skrift, gadd ikke lese. Liten skrift, mye informasjon..	-
Ignorerte advarsel om utilgjengelig ansatt.	-	-

Tabell A.8: Subjekt 1 - Oppgave 5 - Feiltrinn

Oppgave 6

Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren opretter en ny aktivitet.	Ja	
Brukeren trykker på last inn fra mal".	Ja	
Brukeren velger malen som heter "middag".	Ja	
Brukeren laster inn malen i editoren.	Ja	
Brukeren legger til dato på aktiviteten.	Ja	
Brukeren legger til ansatt på aktiviteten.	Nei	
Brukeren lagrer aktiviteten.	Nei	-

Tabell A.9: Subjekt 1 - Oppgave 6 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
La ikke til ansatt	Forslag til favoritt ansatt, prioriterings liste.	Raskt

Tabell A.10: Subjekt 1 - Oppgave 6 - Feiltrinn

Oppgave 7

Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Du liker ikke fisk, og dette er aldri inkludert i aktivitets-beskrivelsen for middag. Kan du redigere malen for middag for å spesifisere at du ikke liker fisk, for så og lagre denne malen?

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Bruker laster inn mal "middag".	Ja	
Bruker endrer innholdet.	Ja	
Bruker lagrer malen under samme navn.	Ja	
Bruker returnerer til dashboard uten å opprette en ny aktivitet.	Ja	

Tabell A.11: Subjekt 1 - Oppgave 7 - Kriterie for suksess

Oppgave 8

Du pleier ofte å gå tur, og er lei av å skrive inn på nytt vær gang. Finn en måte å lage en ny mal med dine tur-preferanser.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren navigerer til editor for aktivitet.	Ja	
Brukeren skriver inn tidspunkt, beskrivelse og tittel.	Ja	
Bruker trykker på lagre som mal".	Ja	
Bruker lagrer malen.	Ja	
Brukeren går tilbake til dashboard uten å opprette en ny aktivitet.	Ja	

Tabell A.12: Subjekt 1 - Oppgave 8 - Kriterie for suksess

Kontekst av kommentar	**Kommentar**	**Utdypning**
Velger dato.	Ikke relevant med dato.	
Lagrer al.	Fanen for lagring av mal lukkes ikke etter at malen blir lagret.	

Tabell A.13: Subjekt 1 - Oppgave 8 - Kommentarer fra bruker

Oppgave 9

Du har lyst til å rydde leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren navigerer til "min dagside..	N/A	
Bruker velger de ansatte de ønsker å ha med sammenligningsfunksjonen.	Ja/Nei	Tror at informasjonen blir gitt ut med en gang, i select menyen.
Brukeren går fremover i tid og ser på ulike dager.	Nei	Skjønner ikke at man må selecte ansatte først, så se når de er ledige.
Brukeren finner et tidspunkt der to ansatte er ledige sammtidig.	Nei	Fortår ikke hva streker betyr.

Tabell A.14: Subjekt 1 - Oppgave 9 - Kriterie for suksess

Kontekst av kommentar	Kommentar	Utdypning
	Ingen ansatte er tilgjengelig.	
	Alt er i røtt.	
Ser gjennom sammenligning.	Hva betyr disse strekane? Utydelig med hva strekene betyr. Korrelerer rødt til “ikke tid”. Samme farge hadde vært bedre.	
	Jeg har ikke peiling på hva disse strekene betyr.	

Tabell A.15: Subjekt 1 - Oppgave 9 - Kommentarer fra bruker

A.9.2 Subjekt 2

Aldersgruppe:
Mobil-Kompetanse:
Hyppighet av mobilbruk:

Merknad:

Oppgave 1

Med å bruke nettsiden, fortell meg hva klokka er.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren oppgir korrekt klokkeslett.	Ja	

Tabell A.16: Subjekt 2 - Oppgave 1 - Kriterie for suksess

Oppgave 2

Når på dagen skal du på kino neste uke?

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren identifiserer den riktige aktiviteten på dashboard.	Ja	
Brukeren inspiserer den riktige aktiviteten.	Ja	
Bruker oppgir klokkeslettet til den riktige aktiviteten.	Ja	

Tabell A.17: Subjekt 2 - Oppgave 2 - Kriterie for suksess

Oppgave 3

Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren finner aktiviteten på dashboard.	Nei	Bruker gikk inn på feil aktivitet. Bedre å skrive dagen og datoen på ssenere I dag".
Brukeren inspiserer aktiviteten.	Ja	
Bruker går inn på redigerings-siden for aktiviteten.	Ja	
Bruker redigerer beskrivelsen for å skrive inn endringen i fritekst.	Ja	
Brukeren lagrer den redigerte aktiviteten.	Ja	

Tabell A.18: Subjekt 2 - Oppgave 3 - Kriterie for suksess

Oppgave 4

Du fikk hjelp til å lage middag av en ny ansatt i går. Finn navnet til denne ansatte.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren expander oversikten over ferdige aktiviteter.	Ja	
Brukeren inspiserer aktiviteten.	Ja	
Brukeren oppgir navnet til den ansatte.	Ja	

Tabell A.19: Subjekt 2 - Oppgave 4 - Kriterie for suksess

Oppgave 5

Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren kommer inn på siden for å opprette en ny aktivitet.	Ja	
Brukeren legger til alle obligatoriske felter med informasjon.	Ja	
Hvis Trond ikke er ledig, trykker brukeren på ss-ammenlign timeplan".	Nei	Byttet dag i stedet for å bruke funksjonen.
Brukeren lagrer aktiviteten.	Ja	

Tabell A.20: Subjekt 2 - Oppgave 5 - Kriterie for suksess

Oppgave 6

Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivitet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren opretter en ny aktivitet.	Ja	
Brukeren trykker på last inn fra mal".	Ja	
Brukeren velger malen som heter "middag".	Ja	
Brukeren laster inn malen i editoren.	Ja	
Brukeren legger til dato på aktiviteten.	Ja	
Brukeren legger til ansatt på aktiviteten.	Nei	Det burde ha vært advarsel når det ikke er ansatt lagt til.
Brukeren lagrer aktiviteten.	Nei	Glemt å legge til ansatt før lagring.

Tabell A.21: Subjekt 2 - Oppgave 6 - Kriterie for suksess

Oppgave 7

Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Du liker ikke fisk, og dette er aldri inkludert i aktivitets-beskrivelsen for middag. Kan du redigere malen for middag for å spesifisere at du ikke liker fisk, for så og lagre denne malen?

Kriterie for suksess	Grad av fullføring	Begrunnelse
Bruker laster inn mal "middag".	Ja	
Bruker endrer innholdet for å ekskludere fisk.	Ja	
Bruker lagrer malen under samme navn.	Ja	

Tabell A.22: Subjekt 2 - Oppgave 7 - Kriterie for suksess

Oppgave 8

Du pleier ofte å gå tur, og er lei av å skrive inn på nytt hver gang. Finn en måte å lage en ny mal med dine tur-preferanser.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren navigerer til editor for aktivitet.	Ja	
Brukeren skriver inn tidspunkt, beskrivelse og tittel.	Ja	
Bruker trykker på lagre som mal".	Ja	Forstår ikke at knappen er der. Eller forstår ikke hva knappen gjør. Det er ikke intuitivt.
Bruker lagrer malen.	Ja	

Tabell A.23: Subjekt 2 - Oppgave 8 - Kriterie for suksess

Oppgave 9

Du har lyst til å rydde leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren navigerer til "min dagside.	Nei	Kom aldri på og trykke der. Fant ikke feature.
Bruker velger de ansatte de ønsker å ha med sammenligningsfunksjonen.	Nei	Tre som er rød og en som er grønn, hvorfor det?
Brukeren går fremover i tid og ser på ulike dager.	Nei	Skjønner ikke at man må selecte ansatte først, så se når de er ledige.
Brukeren finner et tidspunkt der to ansatte er ledige samtidig.	Nei	Forstår ikke hva strekene betyr.

Tabell A.24: Subjekt 2 - Oppgave 9 - Kriterie for suksess

A.9.3 Post-test spørreskjema

Dette spørreskjema'et skal gjennomgås muntlig med deltageren i etterkant av de utforskende og oppsummerende testene. Om deltageren har spørsmål, skal moderator besvare disse etter beste evne for å unngå tvetydighet rundt svaret.

Hver påstand nedenfor skal besvares med følgende skala:
Svært uenig -> Uenig -> Litt enig -> Enig -> Svært enig

Etter at deltageren har gitt et svar på skalaen, skal de spørres om å utdype svaret sitt. Dette noteres sammen med svaret.

Generelt

1. Det er vanskelig å vite hvor man skal trykke for å bytte mellom siden for dashbord og siden for "min dag".
2. Det er vanskelig å gå tilbake til den forrige siden man var på.
3. Skriften på nettsiden var for liten.
4. Hjemsiden var uoversiktlig.
5. Det er utydelig hva de forskjellige knappene gjør før man trykker på de.

Editor

1. Det er vanskelig å vite om det jeg har skrevet har blitt lagret.
2. Det er vanskelig å vite hvor man kan skrive inn tekst.

Min-dag

1. Det er vanskelig å forstå når en ansatt er ledig, og når de er opptatt på kalender-siden.

Editor

1. Det er vanskelig å forstå om en ansatt er ledig eller ikke når man oppretter en aktivitet.

A.10 Resultat fra brukertest

Deltager 1

Test gjennomført 31/03/2024

Profil:

Aldersgruppe: 21-30

Kompetanse for mobilbruk: God kompetanse

Hyppighet av besøk til nettsider: 3+ ganger daglig.

Definisjoner av svaralternativer ligger i test-plan under vedlegg A.8.2.

Deltager 2

Vedlegg B

Brukertest for pasientmodul v2

Bachelor Gruppe 120 - Vår 2024

Dato: 09/04/2024

Test objekt: Omhu pasient modul versjon V2

B.1 Endringslogg fra v1

1. Fjernet utforskende del av test pga tidsbegrensing.
2. Speilet spørsmål i skjema for preferansedata til å være positive i stedet for negative.

Mål for test

Hva ønskes å finne ut av gjennom testen?

1. Er top-menyen intuitiv til bruksområdene av fanene?
2. Forstår brukeren hva som som kan interageres med?
3. Hvor vanskelig er det for brukeren å se når en ansatt er ledig?
4. Forstår brukeren hvordan de vertikale og horisontale navigasjons-elementene fungerer?
5. Klarer brukere å rette opp fra feiltrinn raskt?
6. Er nettsiden oversiktlig?

Oversikt over test

Testen er strukturert som følger:

1. Introduksjon
2. Pre-test spørreskjema
3. Utforskende test
4. Oppgave 1: Top-nav meny
5. Oppsummerende test
    a. Klokkeslett
    b. Inspiser aktivitet
    c. Rediger aktivitet
    d. Inspiser fullført aktivitet
    e. Last inn mal
    f. Rediger mal
    g. Opprett ny mal
    h. Sammenlign ansatte
6. Post-test spørreskjema

B.2 Testdeltakere

For denne testen er det ikke satt noen spesifikke krav for testdeltakerne, men det er ønskelig å teste med personer som betraktes å ha lavere kompetanse i bruk av nettsider på smarttelefoner enn gjennomsnittsnordmannen.

Som nevnt er det ingen strenge begrensninger for hvem som kan delta i testen, men det vil bli gjennomført minst fire tester med deltakere som oppfyller beskrivelsen ovenfor. Resultatene fra disse testene vil også bli vektlagt høyere i konklusjonen av testen.

For å kartlegge deltakernes ferdigheter brukes et kort spørreskjema, som gis til deltakerne før testen starter. Skjemaet finnes under kapittel B.7.2.

For å avgjøre om deltakeren tilhører den ønskede gruppen, baserer vi oss hovedsakelig på deltakerens egen beskrivelse av sine tekniske ferdigheter. Hvis de svarer "lav" eller "svært lav", tilhører de gruppen. Det andre spørsmålet om deres mobilbruksvaner kan brukes til å vurdere tvilstilfeller der deltakernes ferdigheter ikke samsvarer med deres egen vurdering av ekspertise.

Spørreskjemaet inneholder også beskrivelser av de ulike ferdighetsnivåene.

B.3 Metodologi

De valgte metodene som er utnyttet til testen er basert på metodene funnet i boken "Handbook of usability testing" skrevet av Jeffrey Rubin og Dana Chisnell. Da denne boken er skrevet i kontekst av brukertesting innad i en større bedrift, brukes kun elementer av boken som anses som relevant til brukertesting på en mindre skala.

B.3.1 Utforskende test

Om metoden

Brukertesten er en hybrid av forskjellige former for tester. Det vil først bli gjennomført en svært kort "vurderende test". En slik test er kvalitativ, har en høy mengde interaksjon med test-moderatoren, og brukes ofte tidlig i design-prosessen for å finne åpenbare feil og mangler. I denne testen utnytter vi denne metoden for å spørre deltageren om hva de forvanter skal skje når de gjør visse handlinger på siden.

Metode for data-innsamling

Denne metoden generer kvalitativ data i form av tilbakemeldinger fra deltageren. Om det er mange tilbakemeldinger som går igjen vil det tyde på at dette er et stort problem. Om en tilbakemelding kun tas opp av en enkel deltager kan det vurderes om dette er et særtilfelle.

B.3.2 Oppsummerende test

Om metoden

I motsetning til en utforskende test, er en oppsummerende test mindre "fri", og følger i større grad et planlagt sett med oppgaver. Kommunikasjonen mellom deltageren og moderator er også mindre under slike tester. Oppsummernede tester fungerer met at brukeren får et scenario der de er en sluttbruker med et problem eller mål, og at de da må bruke produktet for å oppnå dette målet med hjelp av produktet. Gjennom selve testen vil det ikke være noe kommunikasjon mellom deltager og moderator.

Metode for datainnsamling

Denne metoden er bedre egnet for å samle kvantitative data, og vil derfor bli utført i tillegg til innsamling av støttende kvalitative datapunkter. Følgende data vil bli målt under oppgavene:

1. Antall horisontale feiltrinn.
2. Antall vertikale feiltrinn.
3. Kommentarer og uttrykk for frustrasjon, samt om de er positive eller negative.
4. Tid brukt på å rette opp feil.
5. Grad av fullføring i henhold til de spesifikke kriteriene for suksess i oppgaven.

Hver forekomst av disse hendelsene dokumenteres, inkludert hvor på nettsiden hendelsen oppstod og årsaken til hendelsen. Dette gjøres gjennom en spørsmålsrunde etter hver oppgave, der deltakeren blir bedt om å beskrive tankene og intensjonene sine i øyeblikket feilen oppstod. På denne måten har hvert datapunkt en tilknyttet skriftlig forklaring på hvorfor hendelsen fant sted. Dette gjør det mulig å bruke hver hendelse som et kvantitativt datapunkt, samtidig som kvantitative begrunnelser blir samlet inn.

B.3.3 Post-test spørreskjema

Metodebeskrivelse

Etter gjennomføringen av oppgavene vil deltakerne bli bedt om å fylle ut et muntlig spørreskjema sammen med moderator. Hensikten med dette spørreskjemaet er å samle preferansedata, det vil si deltakernes meninger og tilbakemeldinger om produktet.

Datainnsamlingsmetode

Hvert element i skjemaet består av en påstand som deltakerne kan svare på ved hjelp av skalaen: *Svært uenig -> Uenig -> Litt enig -> Enig -> Svært enig*. I tillegg vil deltakerne bli bedt om å gi en begrunnelse for valget sitt. Dette gjør at spørreskjemaet genererer både kvalitativ og kvantitativ data som kan analyseres.

B.3.4 Verktøy for datainnsamling

All data samles inn ved hjelp av et Excel-dokument, der tabeller brukes til å registrere dataforekomster og tilhørende årsaks-forklaringer. Resultatene fra pre- og post-test spørreskjemaene vil også bli lagret her.

B.4 Test oppsett

Testen er utformet på en enkel måte for rask implementering på ulike steder. Deltakeren er plassert ved et bord med mobiltelefonen foran seg. Moderator sitter ved siden av for å observere skjermen. En eventuell sekretær sitter på den motsatte siden av bordet, overfor moderatoren.

B.5 Konfigurasjon av utstyr

- Brukertesten utføres på en OnePlus Nord smart-telefon med skjermstørrelse på 6,44 tommer og oppløsning på 1080 x 2400 pikseler.
- Brukertesten utføres i Google Chrome nettleser.
- Brukertesten utføres på den interaktive prototypen for pasientmodulen, versjon *2*.
- Brukertesten begynner på hjemsiden, altså på *dashboard* fanen.
- Brukertesten tar utgangspunkt i følgene sample data:
    1. Det er tre ansatte lagt til i systemet. De to første ansatte har skift annenhver dag fra kl07:00-23:00. Den tredje ansatte har skift lørdag-søndag fra kl07:00-23:00.
        - Åse Haug Løseth, Man-ons-fre
        - Trond Gjestad, Tirs-tors-Lør
        - Synnøve Fredriksen: Søn, Natt.
    2. Det er lagt til fire aktiviteter fra før. Tre av aktivitetene skjer på samme dag som brukertesten utføres.
        - Middag, i går.
        - Middag, i dag.
        - Middag, i morgen.
        - Kino, neste uke.

B.6 Oppgaver

1 Finn klokkeslett

Spørsmål: Med å bruke nettsiden, fortell meg hva klokka er.
Krever fullført oppgave: Ingen
Kriterie for suksess:

1. Brukeren oppgir korrekt klokkeslett.

2 Inspiser aktivitet

Spørsmål: Når på dagen skal du på kino neste uke?
Krever fullført oppgave: Ingen
Kriterie for suksess:

1. Brukeren identifiserer den riktige aktiviteten på dashboard.
2. Brukeren inspiserer den riktige aktiviteten.
3. Bruker oppgir klokkeslettet til den riktige aktiviteten.

3 Redigere aktivitet

Spørsmål: Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.
Krever fullført oppgave: 2
Kriterie for suksess:

1. Brukeren finner aktiviteten på dashboard.
2. Brukeren inspiserer aktiviteten.
3. Bruker går inn på redigerings-siden for aktiviteten.
4. Bruker redigerer beskrivelsen for å skrive inn endringen i fritekst.
5. Brukeren lagrer den redigerte aktiviteten.

4 Innspiser fullført aktivitet

Spørsmål: Du fikk hjelp til å lage middag av en ny ansatt i går. Finn navnet til denne ansatte.
Krever fullført oppgave: 2
Kriterie for suksess:

1. Brukeren expander oversikten over ferdige aktiviteter.
2. Brukeren inspiserer aktiviteten.
3. Brukeren oppgir navnet til den ansatte.

5 Opprett ny aktivitet

Spørsmål: Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.
Krever fullført oppgave: 2,3
Kriterie for suksess:

1. Brukeren kommer inn på siden for å opprette en ny aktivitet.
2. Brukeren legger til alle obligatoriske felter med informasjon.
3. Brukeren legger til Trond som ansatt.
4. Hvis Trond ikke er ledig, trykker brukeren på sammenlign timeplan".
5. Hvis sammenligner timeplan: brukeren blar frem og tilbake til de finner en dag som passer.
6. Hvis sammenligner timeplan: brukeren trykker tilbake til redigeringetterpå.
7. Brukeren lagrer aktiviteten.

6 Last inn mal

Spørsmål: Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.
Krever fullført oppgave: 2,3,5
Kriterie for suksess:

1. Brukeren opretter en ny aktivitet.
2. Brukeren trykker på last inn fra mal".
3. Brukeren velger malen som heter "middag".

4. Brukeren laster inn malen i editoren.
5. Brukeren legger til dato på aktiviteten.
6. Brukeren legger til ansatt på aktiviteten.
7. Brukeren lagrer aktiviteten.

7 Rediger Mal

Spørsmål: Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Du liker ikke fisk, og dette er aldri inkludert i aktivitets-beskrivelsen for middag. Kan du redigere malen for middag for å spesifisere at du ikke liker fisk, for så og lagre denne malen?
Krever fullført oppgave: 2,3,5,6
Kriterie for suksess:

1. Brukeren navigerer til editor for aktivitet.
2. Bruker laster inn mal "middag".
3. Bruker endrer inneholdet.
4. Bruker lagrer malen under samme navn.
5. Bruker returnerer til dashboard uten å opprette en ny aktivitet.

8 Opprett ny mal

Spørsmål: Du pleier ofte å gå tur, og er lei av å skrive inn på nytt vær gang. Finn en måte å lage en ny mal med dine tur-preferanser.
Krever fullført oppgave: 2,3,5,6
Kriterie for suksess:

1. Brukeren navigerer til editor for aktivitet.
2. Brukeren skriver inn tidspunkt, beskrivelse og tittel.
3. Bruker trykker på lagre som mal".
4. Bruker lagrer malen.
5. Brukeren går tilbake til dashboard uten å opprette en ny aktivitet.

9 Sammenlign ansatte

Spørsmål: Du har lyst til å rydde leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.

Krever fullført oppgave: Ingen
Kriterie for suksess:

1. Brukeren navigerer til "min dagside.
2. Bruker velger de ansatte de ønsker å ha med sammenlignings-funksjonen.
3. Brukeren går fremover i tid og ser på ulike dager.
4. Brukeren finner et tidspunkt der to ansatte er ledige sammtidig.

B.7 Test-materiale

B.7.1 Introduksjon

Den følgende teksten skal leses nesten ordrett for test-subjektet før testen begynner:

Bakgrunn

1. Hei, jeg er ____, takk for at du vil delta på denne brukertesten.
2. Gjennom denne testen kommer jeg til å lese høyt fra et manus, så om det høres litt hakkete ut er det sannsynligvis derfor.
3. Vi er studenter med NTNU linje for cybersikkerhet og digital infrastruktur, der vi holder på og skrive vår bachelor-oppgave.
4. Vi skriver oppgaven for et firma som utvikler en nettside som brukes av helse-personale innenfor BPA, eller brukerstyrt personlig assistanse.
5. BPA er en bransje der personer som av forskjellige grunner ikke er i stand til å leve selvstendig, og derfor trenger hjelp av assistenter til å fullføre daglige gjøremål. BPA spesifikt har et mål om å la brukeren styre mest mulig av assistansen de får.
6. Nettsiden fungerer som et sammenslått planleggings-verktøy og pasient-journal der de ansatte kan holde styr på aktiviteter, brukere, og deres informasjon.
7. Utgiveren ønsker nå og utvide web-appen til ikke bare å fungere for ansatte, men også brukerene selv. Dette er da for å gi de mer kontroll over egen hverdag.
8. Oppgaven vår er å komme med en idee til en ny nettside, som er skreddersydd for behovene til sluttbrukerene, ikke de ansatte.
9. Kjernefunksjonen til nettsiden er det samme som før. Altså å planlegge assistanse mellom de ansatte og sluttbrukerene. Bare at versjonen vi lager, er spesifikt for at sluttbrukerene skal kunne bruke det.
10. Vi har nå laget et første-utkast av nettsiden, som vi ønsker å teste for å se hvor enkel den er å bruke, slik at vi kan forbedre den. Dette er det vi skal gjøre i dag.

Hvordan testen fungerer

1. Testen begynner med at vi fyller ut et lite skjema med litt bakgrunns-informasjon.

2. Deretter vil jeg stille deg noen åpne spørsmål om nettsiden, som du da besvarer muntlig.
3. Selve testen fungerer slik at jeg ber deg om å bruke nettsiden til å gjøre noen forskjellige oppgaver som en typisk sluttbruker ville ha gjort. Jeg kommer til å observere hvordan du oppnår eller ikke oppnår målet med oppgaven. Etter hver oppgave kan det hende jeg stiller noen spørsmål om det du gjorde for å bedre forstå tankegangen din. Jeg kan ikke hjelpe deg under testen, men kommer til å stoppe deg når du har fullført oppgaven. Om du sitter fast kan du også si i fra, så avslutter vi testen da. Om du lurer på noe teknisk om hvordan testen fungerer, kan vi selvfølgelig hjelpe deg med dette.
4. Til slutt skal jeg stille deg spørsmål om hva du syntes om nettsiden. Jeg gir deg svar-alternativer, og så kan du utdype fritt for begrunnelsen av ditt valgte svar.

Annen informasjon om testen

1. Jeg kommer til å gjøre opptak av mobilskjermen under testen, men ingenting annet blir gjort opptak av. Data'en vi samler er ikke sensitiv, men vil likevel bli lagret anonymt. Navnet ditt blir aldri skrevet ned.
2. Jeg vil også spesifisere at det overhodet ikke er du som blir testa her, det er nettsiden selv som vi ønsker å teste. Om noe skjærer seg, er det på grunn av at det er et problem med nettsiden.
3. Vi ønsker å bruke data fra denne testen for å forbedre nettsiden, og har derfor ikke noe insentiv om å få gode eller dårlige tilbakemeldinger. Så vær så ærlig som mulig når du gir tilbakemelding og svarer på spørsmål om på nettsiden.
4. Vi ønsker også at du "tenker høyt" gjennom testen.
5. Denne økta vil ta omtrent xx minutter. Gjerne still spørsmål underveis om det er noe du lurer på.
6. Har du noen spørsmål før vi begynner? [*Svar på spørsmål.*]

B.7.2 Pre-test spørreskjema

Det følgende skjema skal gjennomåes muntlig med test deltageren. Om deltager har spørsmål om spørsmålene, skal disse besvares av moderator etter beste evne.

Hva er din alder?

1. <13

2. 13-20
3. 21-30
4. 31-40
5. 41-50
6. 51-60
7. 61-70

Omtrentlig hvor ofte besøker du nettsider med smart-telefon eller nettbrett?

1. Mindre enn 1 gang i året.
2. 1-11 ganger i året.
3. 1-3 ganger i måneden.
4. 1-6 ganger i uka.
5. 1-2 ganger om dagen.
6. Mer enn tre ganger om dagen.

Hvordan vil du beskrive dine ferdigheter med bruk av smart-telefon?

1. Svært lav kompetanse. *Trenger hjelp med nesten alt. Ingen teknisk innsikt.*
2. Lav kompetanse. *Trenger hjelp med alt utenom rutine-oppgaver. Ingen teknisk innsikt.*
3. Moderat kompetanse. *Kan gjennomføre rutine-oppgaver og andre enklere oppgaver med applikasjoner du har trening i. Trenger hjelp for oppgaver du ikke har gjort før. Minimalt med teknisk innsikt.*
4. God kompetanse. *Trenger svært sjeldent hjelp med bruk av mobiltelefon. Klarer vanligvis å oppnå nye oppgaver uten hjelp. Kan behøve hjelp med særskilte problemer. Moderat teknisk innsikt.*
5. Svært god kompetanse. *Trenger nesten aldri hjelp. Kan gjennomføre alle oppgaver som kreves på mobilen, og fikser ofte problemer selv. God teknisk innsikt.*

B.7.3 Post-test spørreskjema

Dette spørreskjema'et skal gjennomgås muntlig med deltageren i etterkant av de utforskende og oppsummerende testene. Om deltageren har spørsmål, skal moderator besvare disse etter beste evne for å unngå tvetydighet rundt svaret.

Hver påstand nedenfor skal besvares med følgende skala:
Svært uenig -> Uenig -> Litt enig -> Enig -> Svært enig

Etter at deltageren har gitt et svar på skalaen, skal de spørres om å utdype svaret sitt. Dette noteres sammen med svaret.

Generelt

1. Det er vanskelig å vite hvor man skal trykke for å bytte mellom siden for dashbord og siden for "min dag".
2. Det er vanskelig å gå tilbake til den forrige siden man var på.
3. Skriften på nettsiden var for liten.
4. Hjemsiden var uoversiktlig.
5. Det er utydelig hva de forskjellige knappene gjør før man trykker på de.

Editor

1. Det er vanskelig å vite om det jeg har skrevet har blitt lagret.
2. Det er vanskelig å vite hvor man kan skrive inn tekst.

Min-dag

1. Det er vanskelig å forstå når en ansatt er ledig, og når de er opptatt på kalender-siden.

Editor

1. Det er vanskelig å forstå om en ansatt er ledig eller ikke når man oppretter en aktivitet.

B.8 Resultat fra brukertest

B.8.1 Subjekt 1

Aldersgruppe: 41-50
Mobil-Kompetanse: Lav

Hyppighet av mobilbruk: 3+ ganger om dagen
Merknad: Subjekt har bruker med Facebook, Instagram og Snapchat, og bruker disse applikasjonene hyppig.

Oppgave 1

Med å bruke nettsiden, fortell meg hva klokka er.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren oppgir korrekt klokkeslett.	Ikke fullført	Deltager kan ikke digital klokke. Hen fant i stedet posisjonen der klokkeslettet var, og pekte på dette.

Tabell B.1: Subjekt 1 - Oppgave 1 - Kriterie for suksess

Oppgave 2

Når på dagen skal du på kino neste uke?

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren identifiserer den riktige aktiviteten på dashboard.	Ja	
Brukeren inspiserer den riktige aktiviteten.	Ja	
Bruker oppgir klokkeslettet til den riktige aktiviteten.	Ja	

Tabell B.2: Subjekt 1 - Oppgave 2 - Kriterie for suksess

Kontekst av feiltrinn	Årsak til feiltrinn	Tid for å gjenopprette
Kollapset kategori-boks på dashboard	Raskt, noen få sekunder.	Deltageren kom borti pilen for å kollapse boksen.

Tabell B.3: Subjekt 1 - Oppgave 2 - Feiltrinn

Oppgave 3

Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren finner aktiviteten på dashboard.	Ja	
Brukeren inspiserer aktiviteten.	Ja	
Bruker går inn på redigerings-siden for aktiviteten.	Nei	Brukeren forsto ikke order “redigere”, men etter å bli forklart at dette betyr “endre” forsto hen dette.
Bruker redigerer beskrivelsen for å skrive inn endringer i fritekst.	Nei	Deltageren fant ikke tekstboksen, eller forsto ikke at hen måtte skrive inn her. Moderator spurte ut om hen så etter et annet sted å legge til informasjonen, men fikk ikke noe klart svar. Etter å bli vist hvordan det fungerte, forsto deltageren funskjonen av beskrivelses-boksen, og brukte den til god effekt med å fylle ut informasjon om middags-ønske. Deltager la også til annen relevant informasjon som i utgangspunktet var utenfor oppgavebeskrivelsen.
Brukeren lagrer den redigerte aktiviteten.	Ja	

Tabell B.4: Subjekt 1 - Oppgave 3 - Kriterie for suksess

Oppgave 4

Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren kommer inn på siden for å opprette en ny aktivitet.	Nei	Deltageren ble distrahert av et annet sted på siden. Trengte hjelp med å finne knappen for å opprette en ny aktivitet.
Brukeren legger til alle obligatoriske felter med informasjon.	Nei	Deltager la til tidspunkt, dato og beskrivelse, men ikke tittel. En feilmelding ble vist, men den burde ha vært mer spesifikk for å si at det var tittel som manglet.
Brukeren legger til Trond som ansatt.	Nei	
Hvis Trond ikke er ledig, trykker brukeren på ssammenlign timeplan".	-	
Hvis sammenligner timeplan: brukeren blar frem og tilbake til de finner en dag som passer.	-	
Hvis sammenligner timeplan: brukeren trykker tilbake til redigeringetterpå.	-	
Brukeren lagrer aktiviteten.	Ja	

Tabell B.5: Subjekt 1 - Oppgave 4 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
Brukeren skulle lage en ny aktivitet, men gikk i stedet inn på kalenderen.	Lang, trengte hjelp med å komme tilbake.	

Tabell B.6: Subjekt 1 - Oppgave 4 - Feiltrinn

Kontekst av kommentar	**Kommentar**	**Utdypelse**
Deltager prøver å legge til en aktivitet med å trykke på kalenderen.	"Det går ikke"	Bruker er muligens vant til den tidligre omhu(selv om det er uklart om hen har fått muligheten til å teste denne enda). Hen forventet at en kan trykke på kalenderen for å legge til en ny aktivitet.
Deltager var i redigerings-verktøyet for aktiviteter, og prøvde å lagre, men fikk feilmelding om at ikke alle obligatoriske felter var fylt inn. Tittel-feltet manglet.	"Jeg har gjort det jo"	Brukeren la ikke merke til at tittel feltet var der.

Tabell B.7: Subjekt 1 - Oppgave 4 - Kommentarer

Oppgave 5

Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren oppretter en ny aktivitet.	Nei	Deltager gikk inn på kalender-siden igjen.
Brukeren trykker på last inn fra mal".	Nei	Trengte å bli fortalt hvordan og hvorfor denne menyen skulle åpnes.
Brukeren velger malen som heter "middag".	Ja	Første forsøk åpnet hen aldri menyen, men hen valgte den riktige malen når menyen først ble tatt frem.
Brukeren laster inn malen i editoren.	Ja	
Brukeren legger til dato på aktiviteten.	Ja	
Brukeren legger til ansatt på aktiviteten.	Ja	
Brukeren lagrer aktiviteten.	Ja	

Tabell B.8: Subjekt 1 - Oppgave 5 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
Deltager hadde laget en aktivitet med Trond inkludert som ansatt, men han var ikke ledig på tidspunktet deltageren hadde satt opp. Da hen prøvde å lagre aktiviteten, kom det opp en advarsel om dette, som hen ignorerte.	Siden advarselen ikke forklarte hvorfor det var negativt at den ansatte ikke var tilgjengelig, trykket bare brukeren på OK. Det var først da hen ble forklart hvorfor de ansatte måtte være tilgjengelige at de skjønte dette konseptet.	N/A

Tabell B.9: Subjekt 1 - Oppgave 5 - Feiltrinn

Hoppet over oppgave 6 og 7

Oppgave 8

Du har lyst til å pusse opp leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren navigerer til "min dagside.	Nei	Det var ikke intuitivt at en måtte navigere til denne siden for å fullføre denne spesifikke oppgaven.
Bruker velger de ansatte de ønsker å ha med sammenligningsfunksjonen.	Nei	Deltager fikk hint: “Det er en måte sammenligne når de ansatte er ledig.”, men dette hjalp ikke.
Brukeren går fremover i tid og ser på ulike dager.	Nei	Deltager fikk hint“Nei, hint: kanskje hvis du ser på litt andre datoer.”
Brukeren finner et tidspunkt der to ansatte er ledige samtidig.	Nei	Deltager forsto trolig ikke målet med oppgaven.

Tabell B.10: Subjekt 1 - Oppgave 8 - Kriterie for suksess

Kontekst av feiltrinn	Årsak til feiltrinn	Tid for å gjenopprette
På kalender siden, i begynnelsen av oppgaven forsøkte bruker å lage en ny aktiviteten.	Brukeren gjorde antageligvis dette fordi hen søkte gjenkjennbare omgivelser på nettsiden.	Lang

Tabell B.11: Subjekt 1 - Oppgave 8 - Feiltrinn

Kontekst av kommentar	**Kommentar**	**Utdypelse**
På dashboard i begynnelsen av oppgaven.	"Hvor skal jeg gå henn da?"	Bruker visste ikke hvor hen skulle starte med å løse oppgaven.
Deltager hadde kommet såpass langt i oppgaven at det var selektert en sammenligning mellom to ansatte, der det var både røde og grønne linjer.	"Må jeg trykke på den grønne da?"	Brukeren satt fast, og forsto ikke konseptet av strekene. Det var naturlig å trykke på det grønne, da dette betyr en "bekreftende" handling ellers på nettsiden.

Tabell B.12: Subjekt 1 - Oppgave 8 - Kommentarer

Post-test spørreskjema

Spørsmål	**Kvalitativt svar**	**Begrunnelse**
Det er enkelt å forstå hvor man skal trykke for å bytte mellom siden for dashbord og siden for "min dag".	4̃-5	Deltager syntes at“Vis” knappene var enkle å forstå.
Skriften på nettsiden var passe stor.	5	
Det er enkelt å gå tilbake til den forrige siden man var på.	5	
Dashbordet var oversiktlig.	4	
Det er enkelt å forstå hva de forskjellige knappene gjør før man trykker på de.	N/A	Deltager ser at knappene er blå.
Det er enkelt å forstå hvor man kan skrive inn tekst.	5	
Det er enkelt å forstå om det jeg har skrevet har blitt lagret.	N/A	Bruker slet med å besvare spørsmålet.
Det er tydelig når en ansatt er ledig, og når de er opptatt på kalendersiden.	N/A	Spørsmål ikke relevant.
Det er tydelig om en ansatt er ledig eller ikke når man oppretter en aktivitet.	5	Bruker forsto at grønt=ledig og rødt=ikke ledig.
Det er tilfredstillende å bruke nettsiden.	4̃-5	Ja

Tabell B.13: Subjekt 1 - Post test spørreskjema

B.8.2 Subjekt 2

Aldersgruppe: 21-30
Mobil-Kompetanse: Moderat (Mente selv høy, men det var senere funnet ut at bruker ikke var i stand til å sette opp ansikts-gjenkjenning på egen hånd.

Det var dermed besluttet å sette brukerens kompetanse på "moderat", selv om dette også trolig er for høyt.
Hyppighet av mobilbruk: 3+ ganger om dagen
Merknad: Deltageren har allerede erfaring med den eksisterende utgaven av Omhu, som hen bruker på PC.

Oppgave 1

Med å bruke nettsiden, fortell meg hva klokka er.

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren oppgir korrekt klokkeslett.	Ja	Deltager sa først at hen ikke ønsket å svare på spørsmålet. Trolig pga lese-skrivevansker. Brukeren oppga deretter korrekt klokkeslett. Når spurt hvor hen så klokkeslettet, sa hen at hen hadde det i hodet.

Tabell B.14: Subjekt 2 - Oppgave 1 - Kriterie for suksess

Oppgave 2

Når på dagen skal du på kino neste uke?

Kriterie for suksess	Grad av fullføring	Begrunnelse
Brukeren identifiserer den riktige aktiviteten på dashboard.	Ja	
Brukeren inspiserer den riktige aktiviteten.	Ja	
Bruker oppgir klokkeslettet til den riktige aktiviteten.	Ja	

Tabell B.15: Subjekt 2 - Oppgave 2 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
Kollapset kategori-boks på dashboard	Raskt, noen få sekunder.	Deltageren kom borti pilen for å kollapse boksen.
Trykker på aktivitet i stedet for "Vis" knapp	Ingen	Vant til å trykke på aktivitet fra vanlig omhu.

Tabell B.16: Subjekt 2 - Oppgave 2 - Feiltrinn

Oppgave 3

Du har lyst til å ha pølser til middag i morgen. Legg til denne endringen for din middag i morgen.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren finner aktiviteten på dashboard.	Ja	
Brukeren inspiserer aktiviteten.	Ja	
Bruker går inn på redigerings-siden for aktiviteten.	Nei	Deltager forstår ikke ordet "redigering". Også noe tvilsom om konseptet av å redigere en aktivitet var forstått. Deltager trengte hjelp for å komme seg videre herfra. Bruker redigerer beskrivelsen for å skrive inn endringen i fritekst.
Brukeren lagrer den redigerte aktiviteten.	Ja	

Tabell B.17: Subjekt 2 - Oppgave 3 - Kriterie for suksess

Oppgave 4

Du har lyst til å gå på tur med Trond, en av dine faste assistenter. Bruk nettsiden til å arrangere dette. Velg tidspunktet selv.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren kommer inn på siden for å opprette en ny aktivitet.	Nei, trengte hjelp.	
Brukeren legger til alle obligatoriske felter med informasjon.	Nei, deltageren fylte inn alt informasjon utenom tittel.	Så ikke tittel-felt eller tenkte ikke over at det måtte være med.
Brukeren legger til Trond som ansatt.	Ja	
Hvis Trond ikke er ledig, trykker brukeren på ss-ammenlign timeplan".	-	
Hvis sammenligner timeplan: brukeren blar frem og tilbake til de finner en dag som passer.	-	
Hvis sammenligner timeplan: brukeren trykker tilbake til redi-geringetterpå.	Ja	Se under feiltrinn for be-grunnelse.
Brukeren lagrer aktivite-ten.	Ja	

Tabell B.18: Subjekt 2 - Oppgave 4 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
Bruker var på dashboard, og prøvde å finne ut hvordan hen skulle legge til en ny aktivitet.	Brukeren valgte å redigere en eksisternede aktivitet, i stedet for å trykke på "ny aktivitet". Trolig da hen hadde lært redigering i en tidligre oppgave.	Lang, trengte hjelp.
Bruker var i editoren, og holdt på å opprette aktiviteten. Bruker lagret så aktiviteten uten at en ansatt var lagt til.	En advarsel kom opp, men brukeren klarte ikke å lese den raskt nok til å registrere problemet.	Lang, trengte hjelp.
Bruker var i editoren, og holdt på å opprette aktiviteten. Brukeren trykket inn på "sammenlign ansatt" uten noe klart mål med denne handlingen.	Raskt, brukeren fant "tilbake" knappen, og trykket på denne.	

Tabell B.19: Subjekt 2 - Oppgave 4 - Feiltrinn

Oppgave 5

Du får vanligvis hjelp til å lage middag hver dag. Siden dette er en rutine-aktivtet, vet du at det er forhånds-lagde maler for å opprette slike aktiviteter. Bruk en mal for å legge til en ny hendelse på planen din for middag i overimorgen.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren opretter en ny aktivitet.	Nei, trengte hjelp.	
Brukeren trykker på last inn fra mal".	Nei	Forstår ikke konseptet av en “mal”, selv etter grundig forklaring. Påstår at hen hadde brukt en mal, selv om dette ikke stemte.
Brukeren velger malen som heter "middag".	Nei	Se ovenfor. Bruker trykket seg inn på denne menyen, men valgte ikke noen mal. Usikkert hva som var formålet.
Brukeren laster inn malen i editoren.	Nei	
Brukeren legger til dato på aktiviteten.	Ja	Dette kunne brukeren fra en tidligere oppgave.
Brukeren legger til ansatt på aktiviteten.	Ja	Samme årsak som ovenfor.
Brukeren lagrer aktiviteten.	Ja	

Tabell B.20: Subjekt 2 - Oppgave 5 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
På dashboard, i begynnelsen av testen går brukeren inn og redigerer en eksisterende middag i stedet for å opprette en ny.	Lang, trengte hjelp.	Brukeren hadde glemt hvordan hen lagde nye aktiviteter, og trykket dermed der det sto “middag”.

Tabell B.21: Subjekt 2 - Oppgave 5 - Feiltrinn

Hoppet over oppgave 6 og 7

Oppgave 8

Du har lyst til å pusse opp leiligheten din. Dette er en stor jobb, og vil ha hjelp av to personer. Finn et tidspunkt der to ansatte er tilgjengelige samtidig.

Kriterie for suksess	**Grad av fullføring**	**Begrunnelse**
Brukeren navigerer til "min dagside.	-	Testen ble påbegynt på denne siden.
Bruker velger de ansatte de ønsker å ha med sammenligningsfunksjonen.	Nei,	Så ikke knappen, eller forsto ikke betydningen av den pga store lese/-skrivevansker. Følgende hint ble gitt: “Kanskje en mulighet for å sammenligne de ansatte hadde vært mulig?”. Hintet hjalp ikke.
Brukeren går fremover i tid og ser på ulike dager.	Nei	Brukeren prøvde ikke å gå frem og se på andre dager. Hint ble gitt: “Det trenger ikke å være i dag”. Dette hjalp ikke.
Brukeren finner et tidspunkt der to ansatte er ledige samtidig.	Nei	

Tabell B.22: Subjekt 2 - Oppgave 8 - Kriterie for suksess

Kontekst av feiltrinn	**Årsak til feiltrinn**	**Tid for å gjenopprette**
Bruker var på kalenderside, men trykket på knappen for å opprette en ny aktivitet.	Brukeren prøvde å finne ut hvordan hen la til ansatte.	Lang, begynte å lage en ny aktivitet.

Tabell B.23: Subjekt 2 - Oppgave 8 - Feiltrinn

Kontekst av kommentar	**Kommentar**	**Utdypelse**
Flere ansatte var selektert til sammenligning, og det var både grønn og røde timer på skjermen. Moderator stilte spørsmål: "Hva tror det det grønne og røde på skjermen betyr?"	"Grønn er ledig og rød er opptatt."	

Tabell B.24: Subjekt 2 - Oppgave 8 - Kommentarer

Post-test spørreskjema

Spørsmål	**Kvalitativt svar**	**Begrunnelse**
Det er enkelt å forstå hvor man skal trykke for å bytte mellom siden for dashbord og siden for "min dag".	N/A	Hoppet over spørsmål
Skriften på nettsiden var passe stor.	4	Skriften i menyen for selektering av ansatte er litt for liten, men ellers bra.
Det er enkelt å gå tilbake til den forrige siden man var på.	5	
Hjemsiden var oversiktlig.	3	Liker den gamle(aktivitets-siden) på den originale Omhu bedre.
Det er enkelt å forstå hva de forskjellige knappene gjør før man trykker på de.	5	
Det er enkelt å forstå hvor man kan skrive inn tekst.	5	
Det er enkelt å forstå om det jeg har skrevet har blitt lagret.	N/A	Deltageren hadde ikke et svar på dette spørsmålet.
Det er tydelig når en ansatt er ledig, og når de er opptatt på kalendersiden.	N/A	Ikke relevant.
Det er tydelig om en ansatt er ledig eller ikke når man oppretter en aktivitet.	4	Deltager forstår at grønt er ledig og rødt er ikke ledig.
Det er tilfredstillende å bruke nettsiden.	5	Deltager syntes nettsiden var behagelig og enkel å bruke.

Tabell B.25: Subjekt 2 - Post test spørreskjema

B.8.3 Identifiserte problemer

Gjennom brukertesten ble det identifisert flere problemer av varierende alvorlighetsgrad.

1. Nettsiden bruker hovedsaklig tekst for å kommunisere til brukeren. Dette ble et problem da begge deltagerene hadde en nedsatt lese og skrive evne.
2. Nettsiden bruker til tider avansert språk, f.eks “Redigere”.
3. Nettsiden har funksjonalitet som er for komplekst til at sluttbrukerene klarer å benytte seg effektivt av disse. Hovedsaklig funksjonaliteten rundt malsystemet var vanskelig å bruke.
4. Det var noen egenskaper med nettsiden som begge brukerene forventet å finne. F.eks å kunne trykke på kalenderen for å legge til en aktivitet der.

Vedlegg C

Brukertest, registrering og autentisering, Halden

C.1 Testmål

1. Identifisere mulige problem med å bruke fingeravtrykk eller ansiktsgjenkjenning som autentiseringsfaktor for mennesker i målgruppa
2. Identifisere mulige problem med å bruke sikkerhetsnøkkel som autentiseringsfaktor for mennesker i målgruppa
3. Identifisere mulige problem med å bruke fingeravtrykk eller ansiktsgjenkjenning, sammen med sikkerhetsnøkkel, som autentiseringsmetode for mennesker i målgruppa

C.2 Testoversikt

1. Introduksjon
2. Summativ test, registreringsdel
3. Summativ test, autentiseringsdel
4. Post-test spørreskjema

C.3 Spørsmål vi ønsker svar på

1. Klarer brukerene å fullføre registreringen uten hjelp fra andre?
2. klarer brukerene å logge inn etter registrering, uten hjelp fra andre?
3. Er det noen problemer med bruk av fingeravtrykk eller ansiktsgjenkjenning,

som hindrer brukerene i å autentisere seg på egen hånd?
4. Er det noen problemer med bruk av sikkerhetsnøkkel, som hindrer brukerene i å autentisere seg på egen hånd?

C.4 Testdeltakere

Testdeltakerene i denne testen er spesifikt valgt for å gjøre brukertesten så realistisk som mulig. Derfor er det kun personer i målgruppa, altså mennesker med lettere psykisk utviklingshemming, som skal utføre brukertesten.

C.5 Metodologi

De valgte metodene som er utnyttet til testen er basert på metodene funnet i boken "Handbook of usability testing" skrevet av Jeffrey Rubin og Dana Chisnell. Da denne boken er skrevet i kontekst av brukertesting innad i en større bedrift, brukes kun elementer av boken som anses som relevant til brukertesting på en mindre skala.

C.5.1 Summativ test

Del 1 og del 2 av brukertesten er en summativ test. En summativ test tar utgangspunkt i at produktet i utgangspunktet er ferdig, og testen blir gjort for å hente inn kvantitative verdier. Disse verdiene er: fullføringsrate, og om brukeren klarte oppgaven inne rimelig tid. I første del innen 5 minutt, og i andre del innen 3 minutt. Brukerene skal bli oppfordret til å si høyt det de tenker under og etter oppgavene. Brukerene skal sekvensielt følge oppgaver for å først registrere seg på en autentiserings-demo, for så å autentisere seg på den samme demoen. Testen er laget for å vurdere hvor lett brukerene synes biometri og sikkerhetsnøkkel er å bruke som autentiseringsfaktorer.

Metoden tar utgangspunkt i *within-subjects design*, som går ut på at alle personene i testgruppen skal gjøre alle oppgavene. Det motsatte ville vært å ta utgangspunkt i **independent groups design**, der ulike grupper tester forskjellige elementer ved produktet. Det vil med andre ord ikke være variasjon i hvilke oppgaver som brukerene skal testes i. Oppgavene som brukerene skal gjennomføres sekvensielt, og det er ikke meningen at brukerene skal gjøre oppgavene i tilfeldig rekkefølge.

C.5.2 Post-test spørreskjema

Etter gjennomføringen av oppgavene i del 1 og del 2, vil brukerene bli bedt om å fylle ut et muntlig spørreskjema sammen med moderator. Hensikten med dette spørreskjemaet er å samle preferansedata, det vil si deltakernes meninger og tilbakemeldinger om produktet. Dette er ett kvalitativt intervju. Her vil det også bli stilt spørsmål som ikke er direkte relevant til produktet, men er relevant for å få et overblikksbilde over brukerenes digitale vaner.

C.6 Testoppsett

Testen er utformet på en enkel måte for rask implementering på ulike steder. Deltakeren er plassert ved et bord med mobiltelefonen foran seg. Moderator sitter ved siden av for å observere skjermen. En eventuell sekretær sitter på den motsatte siden av bordet, overfor moderatoren.

C.7 Konfigurasjon av utstyr

Brukeren blir spurt om hen vil bruke sin egen mobil til testen. Det er ønskelig at brukeren bruker sin egen mobil, ettersom vi ikke kan teste biometri-delen dersom de låner en mobil fra en av testmoderatorene. Dette er fordi vi ikke kan registrere biometri på en "låne-mobil". Dersom brukeren ikke ønsker å bruke sin egen mobil, blir biometri-delen av testen hoppet over.

C.8 Oppgaver

C.8.1 Summativ test

Del 1: Registrering

Se instruksjonsheftet, vedlegg. Brukerene skal sekvensielt følge alle oppgavene her.

Del 2: Autentisering

Se instruksjonsheftet, vedlegg. Brukerene skal sekvensielt følge alle oppgavene her.

C.8.2 Post-test spørreskjema

1. *Hvordan låser du opp din egen mobil?*
2. *Bruker du sosiale medier? Hvilke da?*
3. *Hvordan logger du inn på sosiale medier?*
4. *Hva synes du om å bruke biometri til autentisering?*
5. *Hva synes du om å bruke sikkerhetsnøkkel til autentisering?*
6. *Hva tenker du om at du må ha en fysisk gjenstand for å logge inn appen? Mister du lett ting?*
7. *Kunne du heller tenkt deg å bruke passord?*
8. *Synes du det enkelt å huske passord? Må du skrive det ned?*
9. *Har det noen gang skjedd at du har mistet mobilen, eller har du vanligvis kontroll på den?*
10. *Bruker du Bankid-appen? Hvordan synes du det er å bruke den? Knotete eller enkelt?*

C.9 Test-materiale

Følg manus så nøyaktig som mulig.

C.9.1 Manus, introduksjon

1. Vi er en gruppe studenter, som studerer IT(pc-sikkerhet) i Gjøvik. Vi er Sara, Raphael og Jørgen. Vi gjør nå bachelor-oppgava vår, som er et prosjekt for en bedrift som heter Weisstch, som lager en app for helsesektoren, som heter Omhu. Har du hørt om Omhu? Denne appen blir nå kun brukt av folk som jobber i helsesektoren, og de ønsker nå å forbedre appen, slik at også folk som er brukere i helsesektoren kan bruke den. Dette gjelder folk som har BPA i hverdagen.
2. Det som skal skje i dag, er tredelt. Først skal du prøve å registrere en brukerkonto på en "liksom"-nettside som vi har laget. Dette er for at vi skal se om løsningen som vi har laget for å logge inn på appen/nettsiden, er enkel å bruke. Etter det, skal Raphael vise frem hvordan appen/nettsiden kanskje

kommer til å se ut. Han skal deretter gi deg instruksjoner som du skal gjennomføre på nettsiden. Dette er for at vi skal se om nettsiden vi har laget, er enkel nok å bruke. Husk at alt vi kommer til å vise frem i dag har vi laget selv, og når vi lager ting selv, så blir vi ofte "blinde" for feil og mangler med det vi lager. Det er derfor vi er her for å brukerteste deg, slik at vi kan sjekke hva som er bra, og hva som er dårlig. Vi forventer at noen deler kommer til å være vanskelig eller ikke mulig å gjøre. Det er produktet som vi tester, og ikke deg. Til slutt, etter at Raphael er ferdig med sin del, vil vi stille deg noen korte spørsmål. Dette er fordi vi ønsker å vite litt om din kunnskap og forhold til IT fra før. Med IT så mener jeg sosiale medier, hvor mye bruker du mobilen, hva bruker du mobilen til.

3. Imellom de ulike delene jeg nettopp nevnte, tar vi oss pauser dersom dette er nødvendig. Om du blir sliten midt i en del, så si ifra, så kan vi enten korte ned litt, eller ta en pause der og da. Alt som skjer i dag kommer ikke til å ta så lang tid som jeg skrev i eposten. Jeg la inn ekstra tid, i tilfelle en mobil sluttet å fungere elns. Spørsmål? Klar til å begynne?

C.9.2 Manus, summativ test

Målet er att den som bruker Omhu-appen, skal kunne logge seg på sin egen mobil, på en mest mulig enkel og sikker måte. Det finnes mange måter å logge seg inn på en app på mobilen på. Som en del av prosjektet vårt, skal vi prøve å finne ut av hvilken innloggingsmåte er den best mulige. Vi har da laget en "liksom"-nettside, der du kan logge inn slik som du hadde gjort dersom dette hadde vært den ekte appen. Det vi først skal gjøre, er at du får instruksjoner utdelt på ark, og skal først prøve å registrere en brukerkonto, slik du hadde gjort dersom appen var ekte. Målet er at vi har utviklet appen og instruksjonene såpass bra, at du klarer å registrere brukerkontoen, og så logge inn, uten hjelp fra oss. Om du sitter fast, kan du si ifra, så vil vi vise deg hvordan du skal løse det. Ikke stress med å gjøre det så kjapt som mulig, vi er bare interessert i om det vi har laget er enkelt å bruke eller ikke. For at våres resultat skal bli så realistisk som mulig, kan vi ikke svare på spørsmål eller si hvordan du skal gjøre ting når denne testen er startet. Men vi hadde satt pris på hvis du snakker høyt hva du tenker når du utfører instruksjonene. Det er veldig verdifull data for oss å vite hva du tenker når du gjør testen.

C.9.3 Instruksjoner, del 1

Instruksjoner til del 1 av den summative testen. Dette er registreringsdelen i demoen. Testmoderator følger disse instruksjonene.

1. Har brukeren med sin egen mobil? Hvis ikke, lag til min mobil
2. Vis brukeren sikkerhetsnøkkelen. Forklar hvordan denne fungerer. Den skal brukes nå i den summative testen.
3. Gi brukeren heftet med registreringsdelen. Forklar at brukeren nå skal følge instruksjonene så godt det lar seg gjøre. Jeg kommer ikke til å svare på noen spørsmål med mindre brukeren sitter totalt fast. Be brukeren tenke høyt.
4. Gi brukeren brukernavnet sitt og engangskoden. Forklar at hen trenger dette til denne delen.
5. Legg frem penn og papir.
6. Følg med på tiden. Dersom brukeren ikke klarer å løse oppgaven på 5 min, avbryt og vis.

C.9.4 Instruksjoner, del 2

Instruksjoner til del 2 av den summative testen. Dette er autentiseringsdelen i demoen. Testmoderator følger disse instruksjonene.

1. Gi brukeren heftet med autentiseringsdelen. Forklar at brukeren nå skal følge instruksjonene så godt det lar seg gjøre. Jeg kommer ikke til å svare på noen spørsmål med mindre brukeren sitter totalt fast. Be brukeren tenke høyt.
2. Følg med på tiden. Dersom brukeren ikke klarer å løse oppgaven på 3 min, avbryt og vis.

C.10 Resultater

C.10.1 Bruker 1

Summativ test, registrering

Merknad: *Nummer 0.0 er ikke en oppgave, men en illustrasjon på hvordan tabellen skal fylles ut.*

Nummer	**Uten hjelp?**	**Innen 5 min?**	**Vansker / Tilbakemelding**
0.0	ja/nei	ja/nei	klarte alt uten hjelp/ måtte bli guidet på hvordan plassere sikkerhetsnøkkelen
1.1	ja	ja	Ingen problemer, men ble guidet av assistent
1.2	ja	ja	Ingen problemer, men ble guidet av assistent
1.3	ja	ja	Ingen problemer, men ble guidet av assistent
1.4	ja	ja	Ingen problemer, men ble guidet av assistent
1.5	ja	ja	Ingen problemer, men ble guidet av assistent
2.1	ja	ja	Oppgaven sa at hun skulle bruke Google Chrome som nettleser, men hun oppdaget ikke dette og valgte Chrome i stedet for Safari med en tilfeldighet.
2.2	ja	ja	Ingen problemer, men ble guidet av assistent
2.3	ja	ja	Ingen problemer, men ble guidet av assistent
2.4	N/A	N/A	Biometri fungerte ikke på hennes mobil, en iphone. Det er tydelig at det var tekniske problemer fra demoen sin side. Hun fikk utdelt en lånemobil som hun fortsatte med, og vi fikk dermed ikke testet biometri.
2.5	nei	nei	Brukeren fikk ikke til sikkerhetsnøkkelen med en gang. Testmoderator måtte vise hvordan hun skulle gjøre det 3 ganger, før hun fikk det til selv. Den første gangen skjønte hun ikke hvor på mobilen sikkerhetsnøkkelen skulle plasseres. De andre gangene slet hun med "teknikken", og fikk det ikke til før på fjerde forsøk. Brukte lang tid.

Tabell C.1: Bruker 1: Demo, registrere ny bruker

Summativ test, autentisering

Merknad: *Nummer 0.0 er ikke en oppgave, men en illustrasjon på hvordan tabellen skal fylles ut.*

Nummer	**Uten hjelp?**	**Innen 3 min?**	**Vansker / Tilbakemelding**
0.0	ja/nei	ja/nei	klarte alt uten hjelp/ måtte bli guidet på hvordan plassere sikkerhetsnøkkelen
1.1	ja	ja	Ingen problemer
1.2	N/A	N/A	Brukte lånemobil pga. teknisk feil i demoen. Fikk derfor ikke teste dette.
1.3	nei	ja	Prøvde å autentisere seg med sikkerhetsnøkkelen, FØR ho trykte på knappen "klikk her for å bruke sikkerhetsnøkkelen". Ingen problem på andre forsøk når testmoderator påpekte dette.
1.4	ja	ja	Ingen problemer

Tabell C.2: Bruker 1: Demo, logg inn

Post-test spørreskjema

1. *Hvordan låser du opp din egen mobil?* Bruker ansiktsgjenkjenning når hun logger inn på nettbanken. Bruker Nordea, men har ikke BankID og kan logge inn med ansiktsgjenkjenning for å se saldo. Bruker ingenting for å låse opp mobilen, og mobilen er dermed alltid ulåst.
2. *Bruker du sosiale medier? Hvilke da?* Bruker messenger, facebook, snapchat, instagram.
3. *Hvordan logger du inn på sosiale medier?* Logger "aldri" inn på sosiale medier, fordi hun aldri er logget ut på mobilen, og får hjelp av andre dersom hun får ny mobil og må logge inn på nytt da.
4. *Hva synes du om å bruke biometri til autentisering?* Mye bedre enn passord.
5. *Hva synes du om å bruke sikkerhetsnøkkel til autentisering?* Hun ville helst brukt ansiktsgjenkjenning fremfor noe annet. Fingeravtrykk på andreplass. Hun synes sikkerhetsnøkkel er mye bedre enn passord, men ikke bedre enn ansiktsgjenkjenning eller fingeravtrykk.
6. *Hva tenker du om at du må ha en fysisk gjenstand for å logge inn appen? Mister du lett ting?* Pleier ikke å miste ting, men er alltid en ansatt der som kan passe på lommeboka når hun er på butikken.
7. *Kunne du heller tenkt deg å bruke passord?* Nei.
8. *Synes du det enkelt å huske passord? Må du skrive det ned? Isåfall hvor legger du lappen?* Hun synes ikke det er lett å huske passord, har en bok som hun alltid skriver det ned i.
9. *Har det noen gang skjedd at du har mistet mobilen, eller har du vanligvis kontroll på den?* Mister den vanligvis ikke.
10. *Bruker du Bankid-appen? Hvordan synes du det er å bruke den? Knotete eller enkelt?* Synes den er enkel å bruke. Merk: I appen har hun kun tilgang til å se saldoen sin, og ikke noe mer.

C.10.2 Bruker 2

Summativ test, registrering

Merknad: *Nummer 0.0 er ikke en oppgave, men en illustrasjon på hvordan tabellen skal fylles ut.*

Nummer	**Uten hjelp?**	**Innen 5 min?**	**Vansker / Tilbakemelding**
0.0	ja/nei	ja/nei	klarte alt uten hjelp/ måtte bli guidet på hvordan plassere sikkerhetsnøkkelen
1.1	ja	ja	Ingen problemer.
1.2	ja	ja	Ingen problemer.
1.3	nei	nei	Brukte lang tid så ble stoppet av testmoderator. Brukeren ble sannsynligvis forvirret over at bildet i instruksjonsheftet ser annerledes ut enn valgmulighetene på hans mobil.
1.4	nei	nei	Brukeren ble usikker på hva han skulle gjøre, ettersom alternativet allerede var huket av. Brukerne skjønte ikke at han da bare skulle gå videre til neste oppgave.
1.5	nei	nei	Vart også her usikker siden alternativet allerede var huket av. Han skjønte ikke at han bare skulle gå videre.
2.1	nei	nei	Brukeren skrev ikke inn riktig url, han skrev alle ordene i urlen, men ikke tegnene : og //, så han havnet på google og trykte på det første treffet på google.
2.2	nei	nei	Når brukeren kom til denne oppgaven, hadde han glemt at han fikk utdelt brukernavn og passord på begynnelesen av testen, og skjønte dermed ikke hva han skulle skrive som brukernavn.
2.3	nei	nei	Brukte svært mange forsøk på å skrive engangspassordet rett, men dette kan være fordi engangspassordet ble delt ut håndskrevet, og at brukeren så feil bokstav. Dette kunne vært unngått dersom engangspassordet var printa.
2.4	ja	ja	Brukeren brukte ansiktsgjenkjenning på sin egen mobil, og dette fungerte vellykket.
2.5	ja	ja	Her var det tekniske problemer. Sannsynligvis hadde sikkerhetsnøkkelen oppnådd maks antall passord som kan være lagret på den, nemlig 250 stk. Så når brukeren skulle prøve å registrere sikkerhetsnøkkelen, gikk ikke dette, fordi sikkerhetsnøkkelen var “full”. Når sikkerhetsnøkkelen ble restartet og brukeren fikk prøve på nytt, klarte han det fint.

Tabell C.3: Bruker 2: Demo, registrere ny bruker

Summativ test, autentisering

Merknad: *Nummer 0.0 er ikke en oppgave, men en illustrasjon på hvordan tabellen skal fylles ut.*

Steg	**Uten hjelp?**	**Innen 3 min?**	**Vansker / Tilbakemelding**
0.0	ja/nei	ja/nei	klarte alt uten hjelp/ måtte bli guidet på hvordan plassere sikkerhetsnøkkelen
1.1	ja	ha	Ingen problemer.
1.2	ja	ja	Ingen problemer.
1.3	ja	ja	Ingen problemer.
1.4	ja	ja	Ingen problemer.

Tabell C.4: Bruker 2: Demo, logg inn

Post-test spørreskjema

1. *Hvordan låser du opp din egen mobil?* Ansiktsgjenkjenning.
2. *Bruker du sosiale medier? Hvilke da?* Ja, bruker mange forskjellige sosiale medier.
3. *Hvordan logger du inn på sosiale medier?* Logger ikke inn, fordi han logger aldri ut av sosiale medier på mobilen.
4. *Hva synes du om å bruke biometri til autentisering?* Liker ikke fingeravtrykk, fordi han jobber som gartner ute, og når han da skal logge inn på mobilen, så går ikke dette dersom hendene er skitne. Liker ansiktsgjenkjenning.
5. *Hva synes du om å bruke sikkerhetsnøkkel til autentisering?* Liker sikkerhetsnøkkelen veldig godt, han kunne tenkt seg å bruke dette i stedet for ansiktsgjenkjenning, sier han selv. Dette er fordi at når han jobber ute, kan han få problemer med ansiktsgjenkjenning(trolig pga. dårlige lysforhold, briller, maske eller lignende, ren spekulasjon).
6. *Hva tenker du om at du må ha en fysisk gjenstand for å logge inn appen? Mister du lett ting?* Hadde ikke vært et problem, sier han.
7. *Kunne du heller tenkt deg å bruke passord?* Nei, han liker ikke passord. Fordi plutselig skriver han feil passord, og da vet han ikke om han har rett passord, men har skrevet feil, eller om han har feil passord som han har skrevet rett.
8. *Synes du det enkelt å huske passord? Må du skrive det ned?* Har en bok som han skriver det ned i.
9. *Har det noen gang skjedd at du har mistet mobilen, eller har du vanligvis kontroll på den?* Har aldri mista mobilen.
10. *Bruker du Bankid-appen? Hvordan synes du det er å bruke den? Knotete eller enkelt?* Enkelt, men synes det er irriterende å gå ut og inn(når han skal au-

tentisere seg med push-meldinger). Merk: I motsetning til mange personer prosjektets målgruppe, så har han tilgang til BankID, også slik at han kan kontrollere økonomien selv.

Vedlegg D

Brukertest av autentiseringsformer

D.1 Introduksjon

1. Vi er en gruppe studenter med NTNUs linje for cybersikkerhet, jeg heter <navn>. Vi er i slutten av vårt tredje år. For vår bacheloroppgave har vi fått i oppdrag å kartlegge forskjellige metoder for å logge inn på en nettside. Firmaet vi jobber for har en nettside som fungerer som en slags timeplan og planleggingsverktøy for personer som er under helse- og omsorgssektoren. Denne nettsida krever at du logger inn, og vi skal derfor kartlegge forskjellige måter å logge inn på, og vi må derfor finne ut av hvilken metode som er enklest for dette formålet.
2. Når du logger deg inn på en nettside, så må du som oftest autentisere deg. Å autentisere betyr å bevise at du er du, slik at rett person kan logge seg inn på rett brukerkonto på nettsiden. Den vanligste typen digital autentisering er passord. Andre gjenstander, som f.eks en husnøkkel, er også en form for autentisering i den fysiske verden.
3. Husk at det som skal testes av deg nå er noen mer avanserte former for autentisering, og kan oppleves som litt knotete og vanskelig å få til. Men prøv ditt beste, og ta den tiden du trenger. Om du sitter helt fast, så sier du i fra. Vi vil da avslutte testen, vise hvordan det gjøres, og så kan du prøve på nytt om du ønsker. Uansett om du gjør det perfekt på første forsøk, eller det tar lang tid og bruker flere forsøk, så er dette verdifull data for oss. Vår oppgave er jo tross alt å finne den metoden som folk synes er enklest å bruke.
4. Vi kommer til å ta tiden på de ulike testene, men det er kun for vår egen del, så vi har noe vi kan skrive i rapporten. Du må ikke stresse med å gjøre

ting så fort som mulig, fordi poenget er at vi skal sammenligne forskjellen i tid mellom de ulike metodene. Det er med andre ord ingen hastverk i denne testen. Ta den tiden du trenger.

D.2 Del 1 - autentisering

1. Vi skal gjøre to tester på forskjellige typer autentisering. For begge testene har vi allerede satt opp slik at det eneste du trenger å gjøre er å faktisk autentisere deg. I den første testen skal du bruke en sikkerhetsnøkkel, og i den andre testen skal du bruke en autentiseringsapp.
2. Etter at du har gjennomført disse testene, skal vi ha et kort intervju før vi går videre med del 2 av brukerundersøkelsen.

D.2.1 Sikkerhetsnøkkel - autentisering

Hva er en sikkerhetsnøkkel

1. En sikkerhetsnøkkel er denne brikken her. Den brukes til å oppbevare en kode inni seg, som lar deg bevise at du er den du utgir deg for å være til en digital tjeneste, som f.eks en nettside. Det er litt som en husnøkkel, men for digitale tjenester. Du kan bruke den til å låse opp døren til nettsiden, da ingen andre enn deg har en nøkkel som fungerer.
2. For å bruke en slik nøkkel, må du holde nøkkelen inntil toppen av mobilen, samtidig som du har en finger på den gullfargede sirkelen på sikkerhetsnøkkelen.

Autentiser ved hjelp av sikkerhetsnøkkel

1. Først skal du prøve å autentisere deg med sikkerhetsnøkkelen på denne nettsida. Dette skal forestille at du logger deg inn på et sted, som f. eks. Facebook. Vi trykker på “log in” knappen for deg, så det eneste du skal gjøre nå er å bruke sikkerhetsnøkkelen til å autentisere deg, og dermed “logge inn”. Dersom du er nødt til å skrive inn en pin-kode for sikkerhetsnøkkelen, så er denne koden 8888. Dersom du glemmer koden, kan vi minne deg på det, men ellers kan vi ikke gi noen instruksjoner gjennom testen. Si ifra om du sitter fast, så viser vi hvordan du skal gjøre det, så kan du prøve på nytt.
2. Om innloggingesforsøket er mislykked, kan du fortsette å prøve så lenge selv ønsker, frem til du får til innloggingen, eller til du ikke vil mer.
3. Begynn test:

   a. Trykk på "authenticateknappen i demo. Begynn å ta tiden.
   b. Gi mobilen og yubikey til brukeren. Pin-koden til yubikeyen er 8888. Observer.
   c. Vent til brukeren har fullført autentisering, eller gir opp.
   d. Observer punkter av frustrasjon og hesitering i trinn.

4. Intervju etter brukertest:

   a. Var det noe du syntes var vanskelig med dette? I så fall hvorfor?
   b. Er dette en måte du kunne tenkt deg å bruke som autentiseringsfaktor?
   c. Hva tenker du om å ha en fysisk gjenstand som du må ha kontroll på?

D.2.2 Passord og autentiseringsapp - autentisering

Hva er en autentiseringsapp?

1. En autentiseringsapp er en app en har på mobilen som lager engangskoder som du bruker til å logge inn på nettsteder, f. eks. Facebook. Når du bruker en autentiseringsapp som har en kode som kun finnes på din mobil, beviser du da at du er du, ettersom kun du har tilgang til mobilen din.
2. For å sette opp en slik app, vil du få et langt passord bestående av tilfeldige bokstaver, som må legges til i autentiseringsappen. Når dette er gjort, vil appen bruke koden du la inn til å produsere en kode som endrer seg hvert 30'iende sekund. Det er denne koden som du bruker til å logge inn, vanligvis sammen med et vanlig passord.
3. For å logge inn med engangskodene, må du lese de av i autentiseringsappen, for så og bytte vindu tilbake til nettstedet du prøver å logge inn på, og skrive inn denne koden på nettstedet, før koden endrer seg.
4. På iPhone kan man gå ut til dashbordet med å trykke på den runde knappen i midten av mobilen. Nettleseren "safari" har nettsiden du logger inn på. Det røde ikonet er autentiserings-appen.

Passord og autentiseringsapp - lag ny bruker

1. Først så skal du lage en ny bruker med et valgfritt navn(f. eks. ditt eget), og deretter lage et passord. Passordet skal ha 12 bokstaver, men ellers er det ingen flere krav. Det er viktig å huske passordet til etterpå. Du bestemmer selv om du vil skrive det ned eller huske det i hodet.
2. Nettsiden vil gi tilbakemelding på hva som er galt med passordet om det ikke oppfyller kravene.
3. Når brukeren har laget en ny bruker med brukernavn og passord, skal hen stoppe, og vi går videre med autentiserings-delen.

4. Gå inn på nettsiden for brukeren. Gi de mobilen. Begynn klokka.
5. Observer og noter reaksjoner og vanskeligheter.
6. Husk å stopp brukeren når hen har laget en ny bruker.
7. Intervju etter brukertest:
    a. Var det noe du syntes var vanskelig med dette? I så fall hvorfor?

Passord og autentiseringsapp - autentisering

Gå inn på totp nettsiden.

1. Nå skal du prøve å autentisere deg på den nylagede brukeren. Vi har allerede satt opp autentiseringsappen. Du skal nå navigere mellom vinduet der du nettopp laget en ny bruker, og autentiseringsappen. Du navigerer på iphone slik: trykk på hjem knappen, det røde ikonet er autentiseringsappen, og dette blåhvite ikonet er internett. Koden i autentiseringsappen du skal bruke, har navnet "brukertest".
2. Gå til "log inn". Skjermen vil lyse grønt om innloggingen var velykket, og rødt om den var mislykket. Det vil stå en begrunnelse for hvorfor innloggingen var mislykket.
3. Om innloggingesforsøket er mislykket, kan du fortsette å prøve så lenge selv ønsker, frem til du får til innloggingen, eller til du ikke vil mer.
    a. Gi brukeren mobilen. Start klokka og observer.
    b. Dersom brukeren er usikker på hvilken av kodene i autentiseringsappen som er rett(det er en annen kode der for Sara), så kan de få hjelp med dette. Ellers får de ingen hjelp med mindre de sier at de sitter fast.
4. Intervju etter brukertest:
    a. Var det noe du syntes var vanskelig med dette? I så fall hvorfor?

D.2.3 Del 1 - intervju

1. Hvilken autentiseringsmetode benytter du til å logge deg inn på din egen mobil?
    a. Fingeravtrykk / Ansiktsgjenkjenning
    b. PIN, passord eller mønster
    c. Ingen
2. Hvis brukeren benytter seg av biometri for å logge seg inn, be dem logge seg inn på sin egen mobil. Merk at dette er valgfritt. Dette er for at vi kan ta tiden for å måle tidsbruken.

   a. Ta tiden.
   b. Observer
   c. Var det noe du syntes var vanskelig med dette?

3. Har du erfaring med å logge inn med BankID eller MinID? Dersom BankID, bruker du kodebrikke eller app? Hva synes du om det? Dersom MinID, bruker du SMS eller app? Hva synes du om det?
4. Du skal nå få noen lapper som du skal bruke på å rangere de ulike autentiseringsmetodene du nå har testet, sammen med andre metoder du kanskje har brukt før. Lappene kan rangeres på siden av hverandre, som betyr at de er like enkle/vanskelige å bruke. Ellers setter du de enkleste måtene øverst.
5. Gi de lappene. Observer. Spør hvorfor de rangerer de slik.

D.3 Del 2 - registrering

1. Da begynner vi på del 2 av brukertestingen. Nå skal du prøve å registrere, altså sette opp, de ulike metodene du testet i stad.

D.3.1 Sikkerhetsnøkkel - registrering

1. Først skal du prøve å registrere nøkkelen på en nettside. Dette er noe en kun gjør en gang første gang en skal bruke nettsiden. Litt som å installere en lås på døren inn til nettsiden, som kun kan åpnes med den nøkkelen.
2. Følg instruksjonene, og forsøk å registrere nøkkelen. Du vil bli spurt om en pinkode. Pinkoden til nøkkelen er forhåndslaget, og er 8888. Om du glemmer den kan vi minne deg på det.
3. Som i stad, så kan vi ikke hjelpe deg etter du har startet, men si ifra viss du sitter fast, så viser vi deg og du kan starte på nytt.
   a. Trykk på “register ny autentiseringsmetode“ for brukeren.
   b. Begynn å ta tiden.
   c. Gi brukeren mobilen og nøkkelen, og observer.
   d. Vent til brukeren har fullført autentisering, eller gir opp.
   e. Observer punkter av frustrasjon og hestitering i trinn.
4. Intervju etter brukertest:
   a. Var det noe du syntes var vanskelig med dette? I så fall hvorfor?

D.3.2 Autentiseringsapp - registrering

1. Nå skal du lage en ny bruker med et nytt passord igjen. Du kan godt gi brukeren det samme navnet og det samme passordet som du hadde i stad.

Når du har skrevet inn brukernavn og passord, kan du trykke ny bruker". Du vil da få opp en lang kode bestående av bokstaver.

2. Når du har kommet til dette punktet, skal du gå inn i autentiseringsappen og legge til en ny konto.
3. Sørg for at den gamle autentiseringskoden er slettet. Vis brukeren en gang til hvordan hen går inn og ut av apper på iphone. Brukeren er fri til å bruke penn og papir, eller hen kan huske det i hodet.
4. Du skal prøve å legge til en ny konto på autentiseringsappen. Siden du har fått en bokstavkode og ikke en qr-kode, må du legge kontoen til manuelt i appen. Dersom du får mulighet til å gi kontoen et navn, kan du kalle den "test".
5. Som vanlig kan du be om å stoppe dersom du ikke får det til, så kan vi vise deg, og du kan starte på nytt om du vil.

    a. Gi brukeren mobilen. Observer. Ta tiden.

6. Intervju etter brukertest:

    a. Var det noe du syntes var vanskelig med dette? I så fall hvorfor?

D.3.3 Del 2 - intervju

- Dersom du bruker BankID eller MinID, fikk du hjelp når du først skulle "sette" det opp på mobilen/pc-en din? Var det noe du syntes var vanskelig med det?
- Dersom du bruker biometri eller pin for å logge på mobilen. Fikk du hjelp til å "sette" det opp på mobilen? Var det noe med det som var vanskelig?
- Bruker rangerer vanskelighetsgraden på registreringer.

    1. Gi brukeren papirbiter med forskjellige typer autentisering skrevet på.

    2. Nå skal du rangere metodene for registreringene du har prøvd til nå, sammen med andre metoder du kanskje har brukt før. Lappene kan rangeres på siden av hverandre, dette betyr at de er like enkle/vanskelige å bruke. Ellers kan lappene settes over hverandre, der den som er høyest oppe er enklest å bruke.
    3. Gi brukeren lapp for

        - Sikkerhetsnøkkel
        - Autentiseringsapp
        - Passord og brukernavn
        - **Hvis kjent:** Fingeravtrykk
        - **Hvis kjent:** Ansiktsgjenkjenning
        - **Hvis kjent:** Pin kode

    4. La brukeren rangere lappene til de er fornøyd. Svar bare på spørsmål om de er relevante til oppgaven.

D.4 Resultater

D.4.1 Bruker nr1

Test	Tid	Forsøk	Antall forsøk	Vansker / Tilbakemelding
Sikkerhetsnøkkel aut	1.37 20	1 2	2 forsøk	Hun skjønte ikke med en gang hvor hun skulle plassere sikkerhetsnøkkelen på/i mobilen. Skjønte ikke med en gang at den skulle plasserest trådløst inntil mobilen.
Passord og brukernavn reg	20	1	1 forsøk	Hun påpekte at passordet hun lagde nå er enkel å huske, men ikke spesielt sikkert. Det var enkelt pga. at hun lagde et enkelt passord.
Passord og brukernavn med autentiseringsapp aut	45	1	1 forsøk	Var ingenting vanskelig med å logge inn på denne måten her.
Bimoetri(pin og fingeravtrykk) aut	1s	1	1 forsøk	Ingenting vanskelig med dette.
Sikkerhetsnøkkel reg	59 26	1 2	2 forsøk	Ikke direkte vanskelig, men ikke intuitivt. Visste ikke helt hva hun skulle gjøre. Ganske logisk når du allerede vet hvordan du skal registrere nøkkelen.
Passord og brukernavn med autentiseringsapp reg	2.46 1.25	1 2	2 forsøk	Klarte å lage brukeren, kopierte koden, men fikk ikke til å lage ny konto i autentiseringsappen. Etter andre forsøk: Var ingenting vanskelig egentlig, når hun skulle lage ny konto i appen første gang, trykte ho på ferdig i staden for arkiver. Derfor kom ikke koden opp på autetiseringsappen.
Biometri (fingeravtrykk) reg	N/A	N/A	N/A	Var veldig enkelt å sette opp fingeravtrykk på mobil.
BankID reg	N/A	N/A	N/A	Satt opp BankID selv, med et familiemedlem som backup

Tabell D.1: Brukertest 1 - Bruker 1, kvantitative verdier

Intervju etter autentiseringsdel

1. Hun tror hun kunne brukt sikkerhetsnøkkel som en autentiseringsmetode. Er egentlig mer glad i passord, er ikke så glad i duppeditter. Hun er veldig glad kodebrikka til BankID er borte. Hun tror derimot at for personer som sliter med å huske passord, så er sikkerhetsnøkkel en god ide.
2. BankID: Hun bruker BankID med app. Synes det er greit å ha alt på ett sted.

Kan være litt knotete dersom man begynner påloggingsprosessen på appen man skal logge på først, for deretter å gå inn på BankID og ut igjen. Da må man ofte starte prosessen på nytt etter at man har gått inn på BankID og ut igjen. Sett bort ifra dette er hun fornøyd med BankID.

Rangering 1 - autentisering

1. Fingeravtrykk/sikkerhetsnøkkel/pinkode - det er jo det aller letteste, kan raskt logge seg inn. Ho syns sikkerhetsnøkkelen er lettest uansett, men det innebærer at ho må ha den med seg.
2. BankID/autentiseringsapp - du finner alt på autentiseringsappen/BankID-appen og trenger ikke passord.
3. Brukernavn og passord - mer å huske på enn de andre alternativene.

Intervju etter registreringsdel

1. Satt opp BankID selv, med et familiemedlem som backup
2. Var veldig enkelt å sette opp fingeravtrykk på mobil.

Rangering 2 - registrering(første forsøk)

1. Fingeravtrykk, autentiseringsapp, pinkode
2. Sikkerhetsnøkkel - Var ikke så intuitiv som hun først trodde, menyen på mobilen var vanskelig å skjønne. Hun sier at sikkerhetsnøkkel sikkert er enkelt når man har lært seg det, men hun har

D.4.2 Bruker nr2

Test	Tid	Forsøk	Antall forsøk	Vansker / Tilbakemelding
Sikkerhetsnøkkel aut	1.10 16	1 2	2 forsøk	Hun trodde først at det kom til å bli vanskelig, men når hun fikk mobilen så hun at alt som hun skulle gjøre stod på mobilen. Vi glemte å si pinkoden først, så hun ble forvirret på det punktet. På andre forsøk når hun visste pinkoden, gikk det ganske greitt.
Passord og brukernavn reg	55	1	1 forsøk	Syntes det var utfordrende å først finne et passord, og deretter telle hvor mange tegn det var i passordet. Kravet var 12 tegn.
Passord og brukernavn med autentiseringsapp aut	1m 30s	1 2	2 forsøk	Synes det er en utfordring å huske koden fra autentiseringsappen, og huske på den helt til hun navigerer tilbake til nettleseren for å skrive den inn. Hun synes det hadde vært enklere dersom det var slik som på norsk tipping appen. Da får du 4-sifret kode på sms, og denne koden blir automatisk limt inn i appen.
Passord og brukernavn med autentiseringsapp aut (ekstra der hun visste om klipp og lim)	45 8	1 2	2 forsøk	Etter at vi hviste henne at det går an å klippe og lime fra appen.
Bimoetri (ansiktsgjenkjenning) aut	2s	N/A	N/A	Ingen vanskeligheter.
Sikkerhetsnøkkel reg	1.17 34	1 2	2 forsøk	Var ganske enkelt, men så ikke at å legge inn sikkerhetsnøkkel som autentiseringsmetode var et alternativ. Endte dermed opp på å trykke på legg til qr-kode".
Passord og brukernavn med autentiseringsapp reg	1.35 2.20	1 2	2 forsøk	Hun tror ikke hun hadde fått det til uten hjelp. Så ikke det pluss-tegnet i autentiseringsappen, der man kan legge til nye kontoer. Hadde også problem med å logge inn på totp nettside. Var for mange ledd. Hadde vært enklere visst hun f. eks. kunne brukt faceid i staden for.
Biometri reg	N/A	N/A	N/A	Fikk hjelp av et familiemedlem
BankID reg	N/A	N/A	N/A	Fikk hjelp med bakid på mobil, men bankid på app fikset hun selv.

Tabell D.2: Brukertest 2 - Bruker 2, kvantitative verdier

Intervju etter autentiseringsdel

1. Hun kunne tenkt seg å ha sikkerhetsnøkkel som autentiseringsmetode. Fordi det er færre ledd enn mange andre metoder. Brikka er trådløs, noe hun synes er bra. I try-webauthn burde setningen "legg brikka på toppen av mobilen" vært uthevet. Hun synes det er en utfordring med alle passord som skal huskest på, og synes derfor det er bra med en passordløs metode. Hun tenker at det ikke er et problem at sikkerhetsnøkkelen ikke trenger å være sammen med mobilen, fordi man kan ha den på nøkkelknippe eller lommebok.
2. BankID: Bruker BankID med app. Synes ikke den er vanskelig å bruke. Var litt vanskelig første gang, men ikke når hun ble vant til det.

Rangering 1 - autentisering(før hun visste at hun kunne klippe og lime i autentiseringsapp)

1. Ansiktsgjenkjenning - trenger ikke å gjøre noe.
2. Sikkerhetsnøkkel - hun trengte kun å følge instruksjonene på mobilen.
3. BankID - er vant med BankID, og den scorer dermed høyrere enn autentiseringsapp.
4. Autentiseringsapp - har gløymt engangskoden før hun klarer å navigere til nettleseren. Må skrive ned tall for at det skal gå enkelt.
5. Brukernavn og passord - krever mer tenking enn de andre alternativene.

Rangering 1 - autentisering(etter hun visste at hun kunne klippe og lime i autentiseringsapp)

1. Ansiktsgjenkjenning - trenger ikke å gjøre noe.
2. Autentiseringsapp - slipper å tenke på hvor du har nøkkelen. Vart brått mye enklere når hun kunne klippe og lime.
3. Sikkerhetsnøkkel - er en fysisk gjenstand
4. Bankid
5. Brukernavn og passord

Intervju etter registreringsdel

1. Hun fikk hjelp med oppsett av Bankid på mobil. Når hun gikk over fra BankID på mobil til BaniID appen, så ordna hun det selv.
2. FaceID klarte hun å sette opp selv, men fikk bekreftelse på at hun gjorde rett for hvert ledd.

Rangering 2 - registrering:

1. Ansiktsgjenkjenning - fikk hjelp, men hadde sannsynligvis klart det uten hjelp.
2. Sikkerhetsnøkkel - klarte å registrere den selv ved å følge instruksjonene. Hadde litt problemer med å finne alternativet for å legge til sikkerhetsnøkkelen på try-webathn grensesnittet.
3. BankID - her fikk hun hjelp til å sette opp
4. Brukernavn og passord - Slipper å navigere mellom apper/faner
5. Autentiseringsapp - mange ledd. Hun mener man må ha en viss kunnskap om mobil for å kunne klare å registrere dette. Det å klippe og lime og navigere mellom apper kan være svært krevende for folk som ikke er vant til det.

D.4.3 Bruker nr3

Test	Tid	Forsøk	Antall forsøk	Vansker / Tilbakemelding
Sikkerhetsnøkkel aut	1.57	1	1 forsøk	Synes ikke det var spesielt vanskelig. Det er bare det å få det til første gang man bruker det som kan være litt utfordrende.
Passord og brukernavn reg	23s	1	1 forsøk	Ingenting vanskelig med dette.
Passord og brukernavn med autentiseringsapp aut	2.52 1.17 55	1 2 3	3 forsøk	Var flere mislykkede forsøk der testpersonen gjorde "alt rett", men fikk likevel opp meldingen om at engangskoden var feil. Dette skyltest at personen var treg, og rakk ikke å skrive inn engangskoden og trykke logg innfør tiden gikk ut, og engangskoden ble generert på nytt. Når tidsbegrensningen ble påpekt av testmoderator, så klarte hun det på tredje forsøk. Tidsbegrensningen ble også forklart på forhånd, men ikke registrert av testpersonen. Hun mente at det var mye rot med av autentiseringsapp, og at dette er ikke noe hun hadde klart å ordne opp i selv.
Bimoetri (fingeravtrykk) aut	2s	1	1 forsøk	Ingen vanskeligheter.
Sikkerhetsnøkkel reg	2.22	1	1 forsøk	Ingen vanskeligheter
Passord og brukernavn med autentiseringsapp reg	1.18 37 17	1 2 3	3 forsøk	Første forsøk fant hun ikke ut hvor hun skulle legge til ny konto i autentiseringsappen. Ander forsøk lagde hun en ny konto, men trykte på ferdig"i stedet for "arkiver". Siste forsøk når hun fikk vite at hun skylle trykke "arkiver", så klarte hun det fint uten problemer. Hun synes ikke det hadde vært vanskelig dersom hun hadde fått opplæring. Det er ikke konseptet i seg selv som er vanskelig, men det er vanskelig å vite hvor man skal trykke osv. uten opplæring. Dersom hun hadde vist dette på forhånd, tror hun at hun skulle klart det selv.
Biometri reg	N/A	N/A	N/A	Første gang hun satt opp fingeravtrykk på mobilen, fikk hun hjelp. Hun måte derimot endre fingeravtrykket og registrere på nytt ved en senere anledning, da klarte hun det selv uten problemer.
BankID reg	N/A	N/A	N/A	Fikk hjelp til å sette opp både BankID på mobil, og BankID app. Dette hadde hun nok ikke klart å sette opp selv.

Tabell D.3: Brukertest 3 - Bruker 3, kvantitative verdier

Intervju etter autentiseringsdel

1. Hun kunne tenkt seg å brukt sikkerhetsnøkkel som autentiseringsalternativ. Passord husker hun aldri, og synes det er utfordrende med en stadig økende mengde med digitale kontoer som krever unike og helst lange og gode passord. Hun har ingen problemer med å måtte ha med seg en fysisk gjenstand rundt. Hun mister "aldrismå gjenstander som nøkler og lommebok.
2. Hun bruker BankID appen, og synes det er veldig enkelt å bruke. Det gikk fort å lære, og veldig enkelt når man først har lært det mener hun.

Rangering 1 - autentisering

Merk: Testpersonen mener at nummer 1, 2 og tre er på samme nivå med hverandre i vanskelighetsgrad. Det som skiller alternativene, er bruken av tid og kompleksiteten i autentiseringen. Det samme gjelder nummer 4, 5 og 6. Disse er like vanskelige i forhold til hverandre, men noen er mindre tidkrevende og/eller mindre komplekse enn andre.

1. Fingeravtrykk/sikkerhetsnøkkel - Man trenger ikke å “bruke hodet”.
2. Pinkode - I utgangspunktet enkelt, men er noe man må huske.
3. Brukernavn og passort - Bruker lengre tid enn overnevnte alternativ. Dessuten noe man må huske, noe som kan bli krevende når hun blir eldre, mener hun.
4. Autentiseringsapp - Tar tid og er krevende å navigere mellom apper. Er ikke vanskeligere enn BankID eller brukernavn og passord.
5. BankID - Hun synes egentlig ikke at BankID er vanskelig, men det tar lengre tid og er mer komplekst enn de andre alternativene. Dessuten må man uansett skrive BankID passordet også, i tillegg til det andre stedet man prøver å logge inn.

Intervju etter registreringsdel

1. BankID: Fikk hjelp til å sette det opp. Hadde ikke klart det selv.
2. Fingeravtrykk: Fikk hjelp første gang hun satt det opp, men klarte det selv ved en senere anledning.

Rangering 2 - registrering

Merk: Testpersonen mener at Bankid og autentiseringsapp er på samme nivå i kompleksitet(mye navigering mellom faner, fungerer likt sett fra brukerens perspektiv), men at hun ikke er vant til å bruke autentiseringsapp, og derfor er den rangert lavere enn BankID. Hun mener også at nummer 1 og 2 er like enkle, men nummer 2 tar lengre tid enn nummer 1.

1. Fingeravtrykk/pinkode
2. Brukernavn og passord/BankID
3. Sikkerhetsnøkkel - både sikkerhetsnøkkel og autentiseringsapp hadde vært enkle hvis hun hadde gjort det før, noe hun ikke har.
4. Autentiseringsapp

D.4.4 Bruker nr4

Test	Tid	Forsøk	Antall forsøk	Vansker / Tilbakemelding
Sikkerhetsnøkkel aut	25s	1	1 forsøk	Trodde først at han skulle plugge nøkkelen inn i ladeporten på mobilen, noe som han ikke fikk til. Han visste ikke på forhånd at det var en nfc nøkkel, så han visste ikke at det var mulig å bruke den trådløs.
Passord og brukernavn reg	15s	1	1 forsøk	Misfornøgd med brukergrensesnittet. Han syntes det var rart at han måtte trykke "ny bruker" etter at han hadde skreve inn brukernavn og passord. Testen i seg selv var han ikke misfornøyd med.
Passord og brukernavn med autentiseringsapp aut	30s	1	1 forsøk	Ingenting vanskelig med dette.
Bimoetri (fingeravtrykk) aut	1s	1	1 forsøk	Ingen vanskeligheter. Han nevner at det kan være problematisk å bruke fingeravtrykksautentisering i situasjoner der han f. eks. bruker hansker, eller er grisete på fingrene.
Sikkerhetsnøkkel reg	2.05	1	1 forsøk	Brukergrensesnittet var vanskelig, ettersom brukeren må "bla ned" for å finne alternativet for å registrere en sikkerhetsnøkkel. Ellers var det ingenting vanskelig med dette.
Passord og brukernavn med autentiseringsapp reg	2.04	1	1 forsøk	Var litt utfordrende i å finne ut av hvor du skulle trykke inne på autentiseringsappen, men ellers ingenting vanskelig.
Biometri reg	N/A	N/A	N/A	Ingenting vanskelig med dette
BankID reg	N/A	N/A	N/A	Satt opp BankID selv. Hadde ikke noe problem med dette, men tok litt tid å ordne.

Tabell D.4: Brukertest 4 - Bruker 4, kvantitative verdier

Intervju etter autentiseringsdel

1. Sikkerhetsnøkkel: Han kunne ikke tenkt seg å bruke sikkerhetsnøkkel som en autentiseringsfaktor. Han mener det er upraktisk å ha med seg en fysisk nøkkel overalt. Han hadde sannsynligvis mista den med en gang. Blir enda en ting å holde styr på, i tillegg til bilnøkler og lommebok.
2. BankID: Synes BankID app som autentiseringsmetode fungerer greitt, men nevner også at han synes det er irriterende å måtte navigere inn på den, trykke "ja det er meg", for så å navigere tilbake på nettsiden du i utgangspunktet skal logge inn på. I tillegg til at en gjerne må skrive et passord på

nettsiden man skal logge inn på, må man uansett skrive inn BankID passordet på appen. Han mener det er unødvendig mange "ledd" å måtte gå gjennom. Synes ikke at BankID appen er noe mer brukervennlig enn BankID på mobil, som ham brukte før.

Rangering 1 - autentisering

1. Fingeravtrykk
2. Pinkode - enklere å huske enn et passord
3. Sikkerhetsnøkkel - var enkel å bruke, men det faktum at en må ha med seg en fysisk gjenstand trekker den ned
4. Autentiseringsapp - kjedelig å navigere mellom faner
5. BankID - Må uansett skrive passordet til BankID appen, det er mye frem og tilbake mellom faner.
6. Brukernavn og passord - Kjedelig å måtte huske på alle brukernavn og passord til enhver konto man har laget.

Intervju etter registreringsdel

1. BankID. Han registrerte seg selv. Var ingen problemer som han kan huske, men han husker det var litt "knotete" å få til. Det kan hende at registreringen fungerer annerledes i dag.

Rangering 2 - registrering

1. Pinkode
2. Fingeravtrykk
3. Brukernavn og passord
4. BankID - hadde veldig gode instruksjoner på hva man skulle gjøre
5. Autentiseringsapp - Skjønte ikke helt hvordan han skulle legge inn en ny konto med en gang.
6. Sikkerhetsnøkkel - Skjønte ikke helt hvordan man skulle registrere sikkerhetsnøkkelen med en gang, han har aldri gjort det før.

D.4.5 Bruker nr5

Test	Tid	Forsøk	Antall forsøk	Vansker / Tilbakemelding
Sikkerhetsnøkkel aut	1m 36s	1	1 forsøk	Skjønte ikke hvor man skulle legge på sikkerhetnøkkelen
Passord og brukernavn reg	39s	1	1 forsøk	Ble for mye med 12 tegn å huske, men følte han fikk det til greit.
Passord og brukernavn med autentiseringsapp aut	1.28 28s	1 2	Fikk ikke til noen av forsøkene	Viste ikke hva man skulle gjøre når han kom til autentiseringsappen. Vanskelig å bytte mellom apper på IOS når han bruker Android til vanlig.
Bimoetri aut	N/A	N/A	N/A	N/A
Sikkerhetsnøkkel reg	56s N/A	1 2	Fikk ikke til på forsøk 1 eller 2	Ble for mange prosesser
Passord og brukernavn med autentiseringsapp reg	54s	1	Fikk det ikke til på forsøk 1 ønsket ikke ett nytt forsøk	Det ble for mange steg følte han, må ha mere tid for å øve det inn.
Biometri reg	N/A	N/A	N/A	N/A
BankID reg	N/A	N/A	N/A	Fikk ikke til å sette opp bankID selv måtte ha hjelp i banken.

Tabell D.5: Brukertest 5 - Bruker 5, kvantitative verdier

Intervju etter autentiseringsdel

1. c) Bruker ingen ting for å logge på telefonen
2. BankID: Bruker bankID med app. Han synes det fungerer bra og enkelt og logge seg inn.
3. Det var ikke noe han følte var vanskelig med det, det var kanskje vanskelig med autentiseringsappen og navigere fremm og tilbake noe han ikke fikk til.
4. Han foretrekker bruk av brukernavn og passord
5. Det har ikke vært noen problem og ha hatt en fysisk gjenstand siden han har brukt kodebrikke for bankID før.

Rangering 1 - autentisering

1. Sikkerhetsnøkkel, passord og brukernavn, BankID
2. Autentiseringsapp

Han rangerte de slik for han ikke fikk til autentiseringsapp

Intervju etter registreringsdel

1. Bruker ikke biometri eller pinkode
2. BankID: Fikk hjelp for å sette opp bankID

Rangering 2 - registrering:

1. Sikkerhetsnøkkel
2. BankID
3. Autentiseringsapp

Han rangerte de slik fordi sikkerhetsnøkkel var nok så enkelt, BankID fikk han hjelp, men han følte han kunne ha greid det selv og autentiseringsapp ble for vanskelig.

D.4.6 Bruker nr6

Test	Tid	Forsøk	Antall forsøk	Vansker / Tilbakemelding
Sikkerhetsnøkkel aut	1.18 21	1 2		Første gang plasserte hun ikke nøkkelen nærme nok mobilen, hun holdt den en halv cm ifra. Det var lite forklaring på mobilen hva hun skulle gjøre, det burde stått blant annet at nøkkelen må helt inntil for at det skal fungere. Var heller ikke lett å skjønne at man må holde på logoen på sikkerhetsnøkkelen når den blinker grønt, det stod det ingenting om.
Passord og brukernavn reg	1.28	1		Hun har aldri skjønt forskjellen på passord og brukernavn. Hvorfor må passordet og brukernavnet være forskjellig? Det gir mening at passord skal være hemmelig, men hvorfor trenger hun brukernavn? Sett bort fra dette var det ingenting vanskelig med dette. Hun påpeker at totp-demoen ikke gir noe tilbakemelding dersom hun skriver passordet feil. Dette er dumt, fordi hun da aldri får vite om passordet er riktig skrevet inn eller ikke.
Passord og brukernavn med autentiseringsapp aut	2.14	1	I løpet av denne tiden prøvde hun flere ganger å skrive inn koden fra aut. appen, men ingen av forsøkene fungerte.	Hun fikk det ikke til, sannsynligvis fordi hun hadde mellomrom mellom sifrene, eller at tiden gikk ut for hvert forsøk. Koden blir fornyet hvert 30. sek. Hun mener at 30 sek. er veldig lite. Hun skrev ned engangskoden på papir, og hun mener at eldre mennesker aldri hadde fått til dette på 30s.
Bimoetri (fingeravtrykk) aut	1	1		Kan være problematisk med våte eller grisete fingre. Bortsett fra dette er dette den kjappeste måten å autentisere seg mener hun.
Sikkerhetsnøkkel reg	1.28 1.12 24s	1 2 3		Første gang fant hun ikke alternativet for sikkerhetsnøkkel, hun trykte på "registrer med qr-kode" i stedet for. Andre forsøk gjorde hun alt rett, men sikkerhetsnøkkelen responderte ikke. Teknologien fungerte ikke. Tredje forsøk fungerte alt fint. Hun påpeker at tekstblokkene som dukker opp på mobilskjermen når du skal registrere nøkkelen, kan være tunge å lese når man er sliten i hodet, og det hadde vært bedre med en punktliste. Hun hadde nok spurt andre om hjelp dersom hun hadde gjort dette alene.

Tabell D.6: Brukertest 6.1 - Bruker 6, kvantitative verdier

Test	Tid	Forsøk	Fullføringsrate	Vansker / Tilbakemelding
Passord og brukernavn med autentiseringsapp reg	2.09 0.47 2.14	1 2 3		Første forsøk misforstod hun oppgaven, hun begynte å logge inn slik som i autentiseringsoppgava. Altså hun registrerte ikke. Andre forsøk kom hun til "add manually" delen i autentiseringsappen, der hun skal manuelt legge til en "nettside/konto". Hun stoppet opp fordi hun ikke skjønte hvordan hun skulle få alle bokstavene i totp-generatoren inn i autentiseringsappen. Hun trodde hun skulle gjøre noe spesielt som hun ikke forstod. Tredje forsøk skreiv ho ned bokstavkoden for hånd, hun vet det går an å klippe å lime, men vet ikke hvordan. Hun sier at det tok litt tid før hun skjønte hva vi ville hun skulle gjøre. Det å lage brukernavn og passord er enkelt, men registreringsdelen var skikkelig avansert, hadde ikke klart det alene. Hadde vært enklere med god veiledning. Hun skjønte først ikke at hun skulle bruke den lange bokstavkoden, og gjekk rett til logg inn. Det stod ingenting om bruk denne kodennoe sted.
Biometri reg	N/A	N/A	N/A	Hun registrerte fingeravtrykk på mobilen sin selv. Det var ganske selvsagt og "idiotsikkert". Veldig visuelt med punktsteg, hun skjønte alt hun skulle gjøre.
BankID reg	N/A	N/A	N/A	Fikk hjelp til å sette opp Bankid på mobilen. Husker ikke så mye av det, var sikkert mannen som gjorde det, sier hun.

Tabell D.7: Brukertest 6.2 - Bruker 6, kvantitative verdier

Intervju etter autentiseringsdel

1. Feedback sikkerhetsnøkkel: Hun kunne tenkt seg å bruke nøkkel i stedet for passord, fordi da slipper hun å huske på passordet. Hun mener hun hadde hatt sikkerhetsnøkkelen på nøkkelknippe. Hun påpeker at man likevel bør ha passord eller noe annet som backup i tilfelle du mister nøkkelen. Instruksjoner er nødvendig, i tekstblokkene på mobilen leste hun ikke siste setningen fordi hun var sliten i hodet før hun kom dit. Det hadde vært bedre med instruksjoner som en punktliste.
2. Hun bruker TouchId(fingeravtrykk) som autentiseringsmetode på mobilen. Hun synes dette er den beste måten å autentisere seg på. Kan være proble-

matisk med f. eks. klissete fingre, men ellers ikke noe problem med dette sier hun.
3. Hun bruker BankID appen på mobil. Hun har ingen problemer med dette og synes det er greitt å bruke. Mye bedre enn å logge på nettbanken med kodebrikke. Så synes hun at det er fint at all informasjon over kontoene osv. ligger på appen.

Rangering 1 - autentisering

1. Fingeravtrykk - Krever ingen tenking
2. Pinkode - Ligger i "ryggmargen", har brukt det i mange tiår, hun bruker samme pinkode på vipps og mobil.
3. Brukernavn og passord, autentiseringsapp, BankID - Må tenke litt og huske tall. Er egentlig ikke vanskelig, men det krever jo litt mer av deg. Hun synes BankID og autentiseringsapp ligner mye. Det står ikke så mye på autentiseringsappen, og dermed er autentsieringsapp kanskje litt enklere enn bankid.
4. Sikkerhetsnøkkel - Er noe nytt som hun ikke har prøvd før. Du må huske å ha den med deg, men samtidig tenker hun at det er en vanesak, og at det egentlig sikkert ikke er vanskelig. Men som sagt så er hun ikke vant til det.

Intervju etter registreringsdel

1. Fikk hjelp til å sette opp BankID appen. Husker ikke så mye av det, men var sikkert mannen hennes som gjorde det.
2. Å registrere fingeravtrykk på mobil ordna hun selv. Var ganske selvsagt og idiotsikkert. Veldig visuelt, alt ble forklart med bilder og tegn. Dette synes hun er bra.

Rangering 2 - registrering

1. Fingeravtrykk, brukernavn og passord - Fingeravtrykk var som sagt veldig visuelt. Brukernavn og passord gjør hun hele tiden og har gjort mange ganger, så det har "satt seg", og er dermed veldig gjenkjennbart. Alt som man gjør ofte er enkelt sier hun.
2. Sikkerhetsnøkkel - Var egentlig enkelt, men på andre forsøk når hun skulle registrere den, så fungerte ikke teknologien. Hun ble dermed usikker på om hun i det hele tatt gjorde det rett, selv om hun gjorde alt riktig. Hvis ikke det var for dette, så hadde sikkerhetsnøkkel vært på nummer 1 også.
3. Autentiseringsapp - Var vanskelig å forstå, mye å sette opp og ikke så intuitivt.

BankID har hun ingen formening om, ettersom hun ikke registrerte seg der selv, hun fikk noen andre til å gjøre det.

Vedlegg E

Instruksjonshefte, brukertest registreringsdel

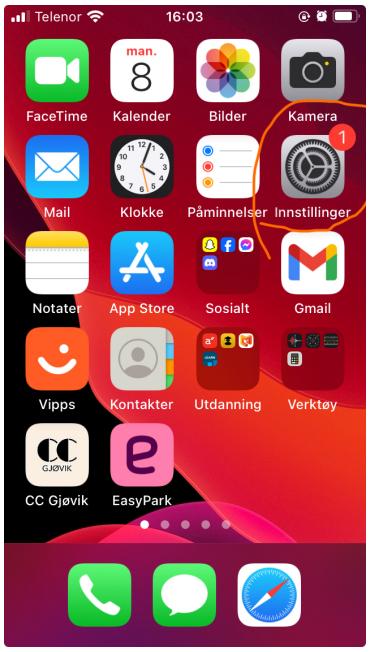
Dette er instruksjonsheftet som ble brukt under brukertestingen i Halden. Dette instruksjonsheftet inneholder oppgavene for registrering av konto med sikkerhetsnøkkel og biometri som autentiseringsmetoder, på autentiseringsdemoen.

1 For iPhone-brukere

Dersom du har iPhone, må du gjøre dette på forhånd, FØR du starter registreringen. Dersom du ikke har iPhone, kan du hoppe over kapittel 1, og gå rett til kapittel 2.

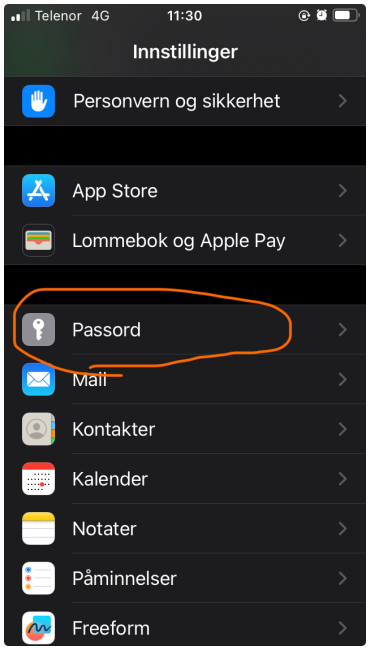
1.1 Gå inn på innstillinger på mobilen:

Gå til til innstillingene på mobilen. Logoen til innstillingene er sirklet rundt med oransje oppe til høyre i bildet:



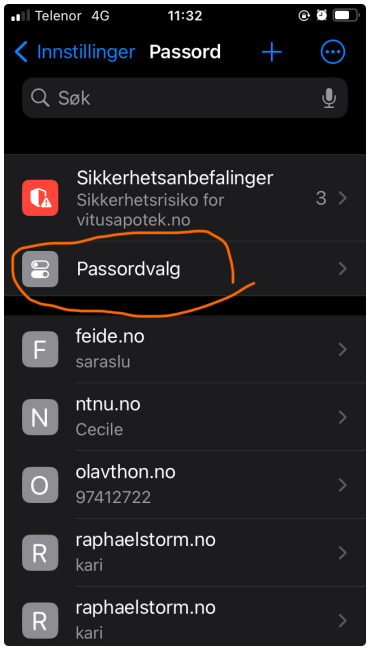
1.2 Finn innstillingene for passord:

Bla nedover i innstillingene. Finn alternativet for "passord". Trykk på denne:



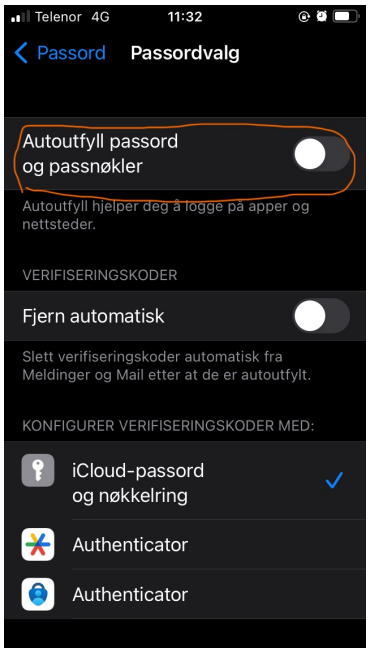
1.3 Passordvalg:

Trykk på alternativet "Passordvalg":



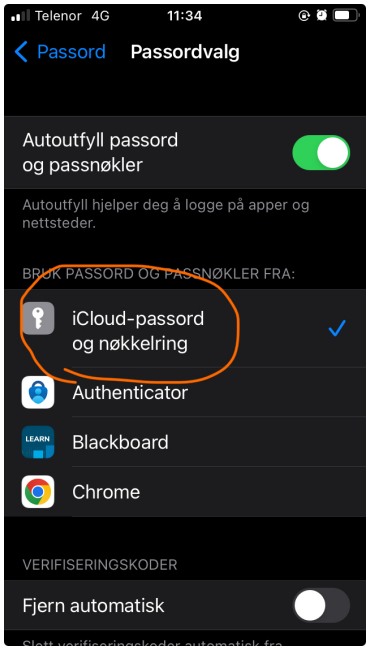
1.4 Autofyll passord og passnøkler:

Dersom dette alternativet IKKE er huket av(altså alternativet har ikke fargen grønn), huk av boksen "Autofyll passord og passnøkler". Dersom alternativet allerede er huket av, trenger du ikke trykke på noe. Gå videre til neste instruks:



1.5 iCloud-passord og nøkkelring:

Under "BRUK PASSORD OG PASSNØKLER FRA:", skal du trykke på alternativet "iCloud-passord og nøkkelring". Når dette er gjort, kan du gå ut av innstillingene.



2 Registrer ny brukerkonto:

Her starter kapittel 2. Begynn direkte her om du ikke har iPhone.

2.1 Gå inn på nettsiden:

Gå inn på **https://omhu.raphaelstorm.no/** i nettleseren på mobilen. Du vil da komme til denne nettsiden:
OBS: *Det kan hende du må bruke Google Chrome som nettleser, det er ikke alltid det er mulig å gå inn på nettsiden på Safari.*

2.2 Start registrering:

I boksen “Brukernavn”, skriver du inn brukernavnet som du har fått. Du må skrive inn store og små bokstaver slik som du har fått oppgitt. F. eks. Sara med stor S, er ikke det samme som sara med liten s. Trykk “Begynn registrering” når brukernavnet er skrevet inn. Dersom du skriver inn brukernavnet feil, kommer denne meldingen opp:

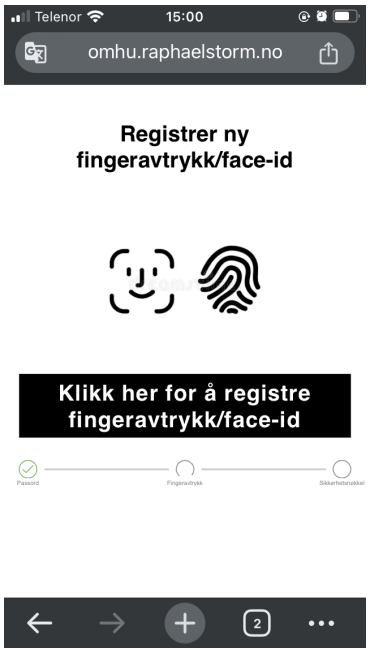
2.3 Skriv inn engangspassord:

Du har sammen med brukernavnet, fått oppgitt et engangspassord. Dette passordet skal du skrive inn i boksen “Èngangspassord”. Husk å skriv inn store og små bokstaver nøyaktig slik det har blitt oppgitt. Trykk “Bekreft” når passordet er skrevet inn.

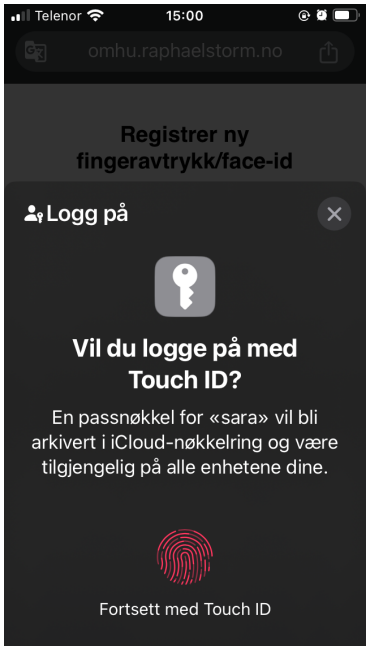
Dersom du skriver inn feil engangspassord, kommer denne meldingen opp:

2.4 Registrer fingeravtrykk/ ansiktsgjenkjenning/ kode

Når engangspassordet er skrevet inn og du har trykt på "Bekreft", kommer du til denne siden. Her skal du registrere enten fingeravtrykk, ansiktsgjenkjenning eller kode. Det er innloggingsmetoden du bruker for å låse opp mobilen som blir brukt her. Dersom du har lagret ansiktsgjenkjenning på mobilen, vil nettsiden be om ansiktsgjenkjenning, dersom du bruker fingeravtrykk til å låse opp mobilen, vil nettsiden be om fingeravtrykket ditt. Trykk på "Klikk her for å registrere fingeravtrykk/face-id" for å komme i gang.

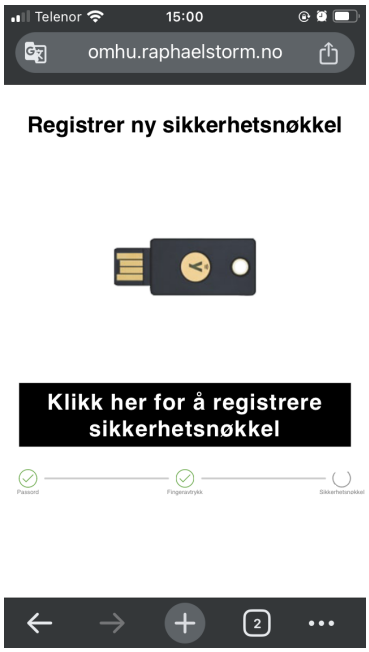


Dersom du har iphone og bruker fingeravtrykk for å låse opp mobilen, vil dette alternativet komme opp. Hvordan instruksjonene ser ut vil variere fra mobil til mobil.

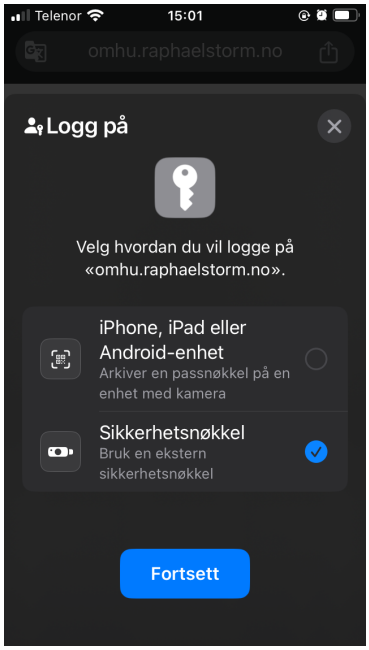


2.5 Registrer sikkerhetsnøkkel

Her skal du registrere sikkerhetsnøkkelen du har fått utdelt. Trykk på "Klikk her for å registrere sikkerhetsnøkkel" for å komme i gang.



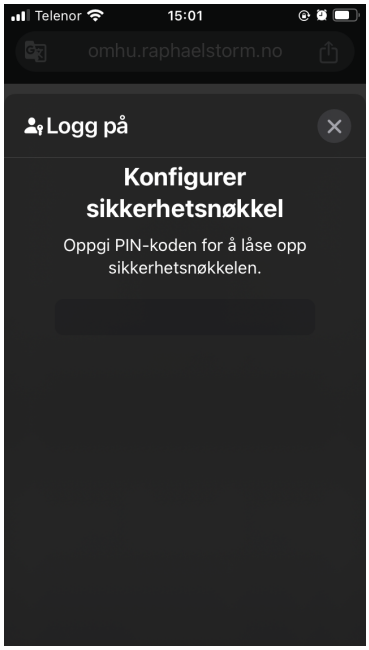
Hvordan instruksjonene ser ut når du starter registreringen av sikkerhetsnøkkelen, varierer fra mobil til mobil. Du kommer sannsynligvis til å få opp ulike alternativer som kan registreres. Her må du trykke på alternativet for sikkerhetsnøkkel. Dersom du har iphone, kommer det til å se slik ut. Trykk fortsett når sikkerhetsnøkkel er huket av:



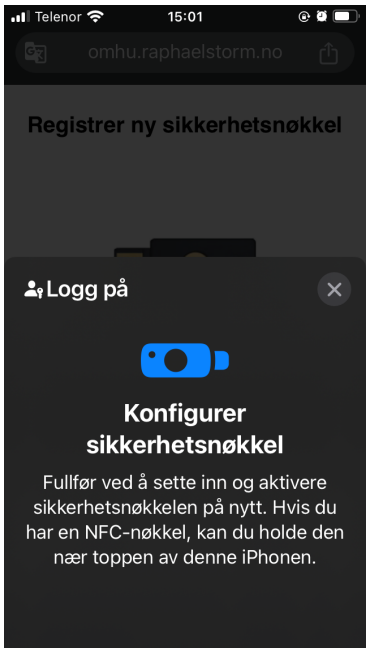
Mobilen vil gi deg instruksjoner på hvordan du skal "koble" sikkerhetsnøkkelen til mobilen. Sikkerhetsnøkkelen du har fått utdelt, er en NFC-nøkkel. Det betyr at den trådløst kan koble seg til mobiler som har denne muligheten. For å koble til trådløst med NFC, følg instruksjonene på mobilen. Dersom mobilen ikke har mulighet for å koble seg til med NFC, kan den fysisk plugges inn i en USB-C port. Dersom du har iPhone, så har ikke mobilen UCB-C. Du er da nødt til å bruke NFC. Følg instruksjonene på mobilen.

Dersom du registrere sikkehetsnøkkelen med USB-C, berør logoen i midten av nøkkelen når den "blinker" grønt:

Dersom du må oppgi koden for sikkerhetsnøkkelen, er dette en forhåndsbestemt kode som du må skrive inn. **Koden er 8888**.



På noen mobiler må du "koble" til sikkerhetsnøkkelen en gang til, etter at du har skrevet inn overnevnte kode. Følg instruksjonene på mobilskjermen, har du iphone, kan det hende det ser slik ut:



2.6 Kontoregistrering vellykket

Dersom registreringen av sikkerhetsnøkkelen er vellykket, kommer du til å få opp denne siden. Du har nå vellykket registrert en brukerkonto.

Vedlegg F

Instruksjonshefte, brukertest autentiseringsdel

Dette er instruksjonsheftet som ble brukt under brukertestingen i Halden. Denne instruksjonsheftet inneholder oppgavene for autentisering på autentiseringsdemoen.

1 Logge inn etter registrering:

Dette skal gjørest ETTER at brukerkontoen er registrert, og må gjøres hver gang du skal logge inn på nettsiden:

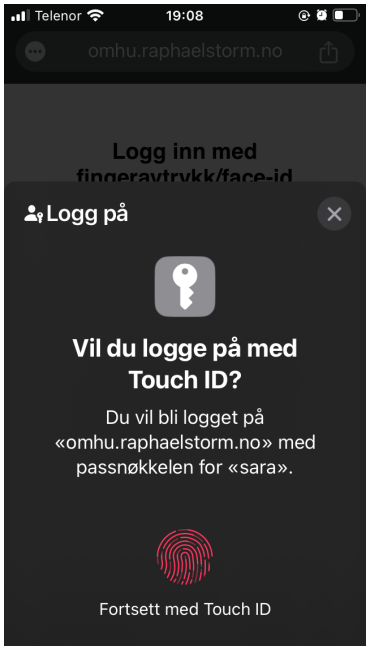
1.1 Start innlogging:

Når du er ferdig med registreringen, har du kommet til denne siden. Trykk på "Trykk her for å logge inn".

1.2 Fingeravtrykk / ansiktsgj.

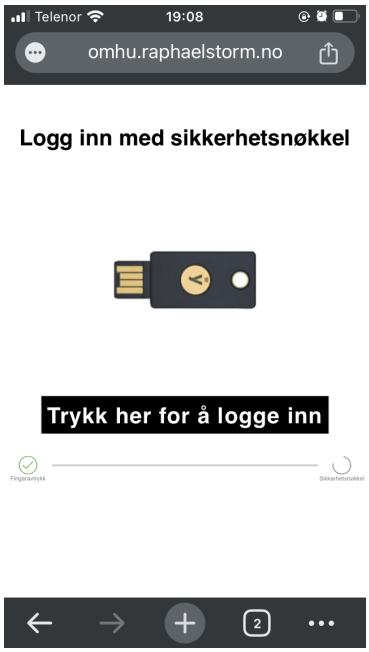
Her skal du logge inn med enten fingeravtrykk, ansiktsgjenkjenning eller kode, avhengig av hva du registrerte tidligere. Trykk på "Trykk her for å logge inn". Følg instruksjonene på mobilen.

Dersom du har iphone og registrerte fingeravtrykk som innloggingsmetode, kommer skjermen til å se slik ut:

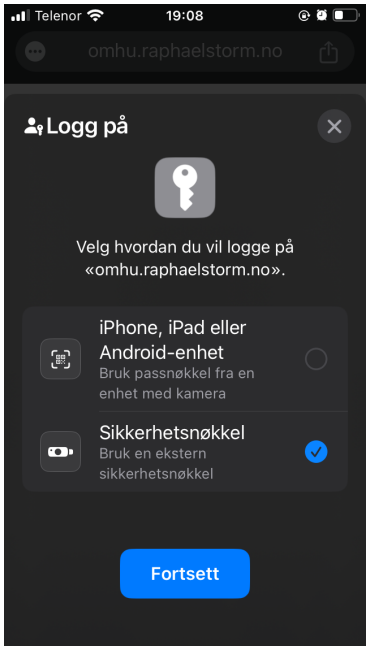


1.3 Sikkerhetsnøkkel

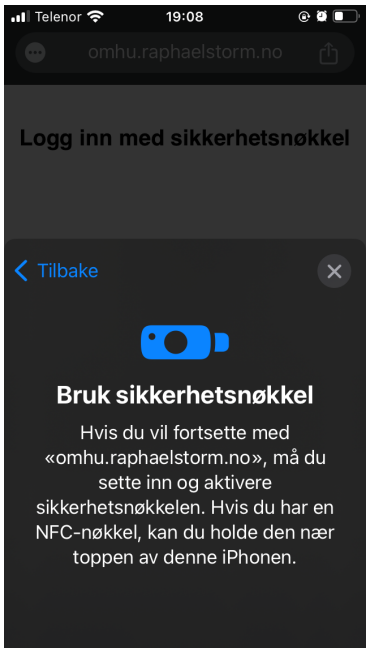
For å logge inn med sikkerhetsnøkkel, gjør det samme som ved registreringen. Trykk på "Trykk her for å logge inn". Hvordan instruksjonene ser ut etter at du har trykt her, varierer fra mobil til mobil.



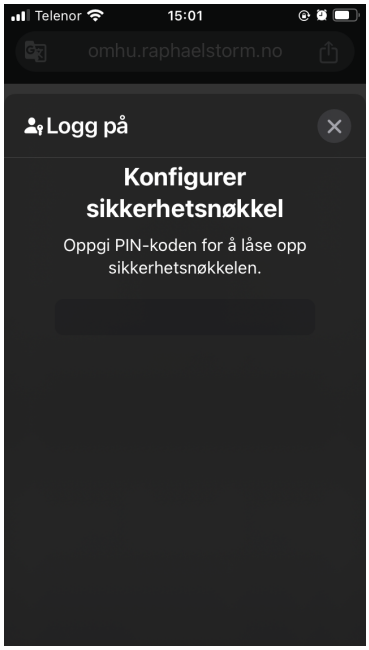
Dersom du har iphone, vil instruksjonene se slik ut. Velg ekstern sikkerhetsnøkkel, og trykk "Fortsett".



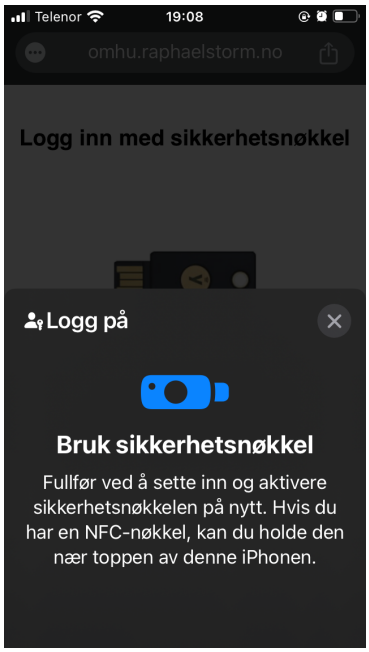
"Koble" til sikkerhetsnøkkelen slik som du gjorde i registreringsdelen. Enten ved å bruke NFC, altså trådløst, eller ved å plugge den fysisk inn i en USB-C port.



Dersom du blir bedt om å oppgi kode til sikkerhetsnøkkelen, så er koden **8888**.



Fullfør ved å "koble" til sikkerhetsnøkkelen en gang til.



1.4 Innlogging vellykket

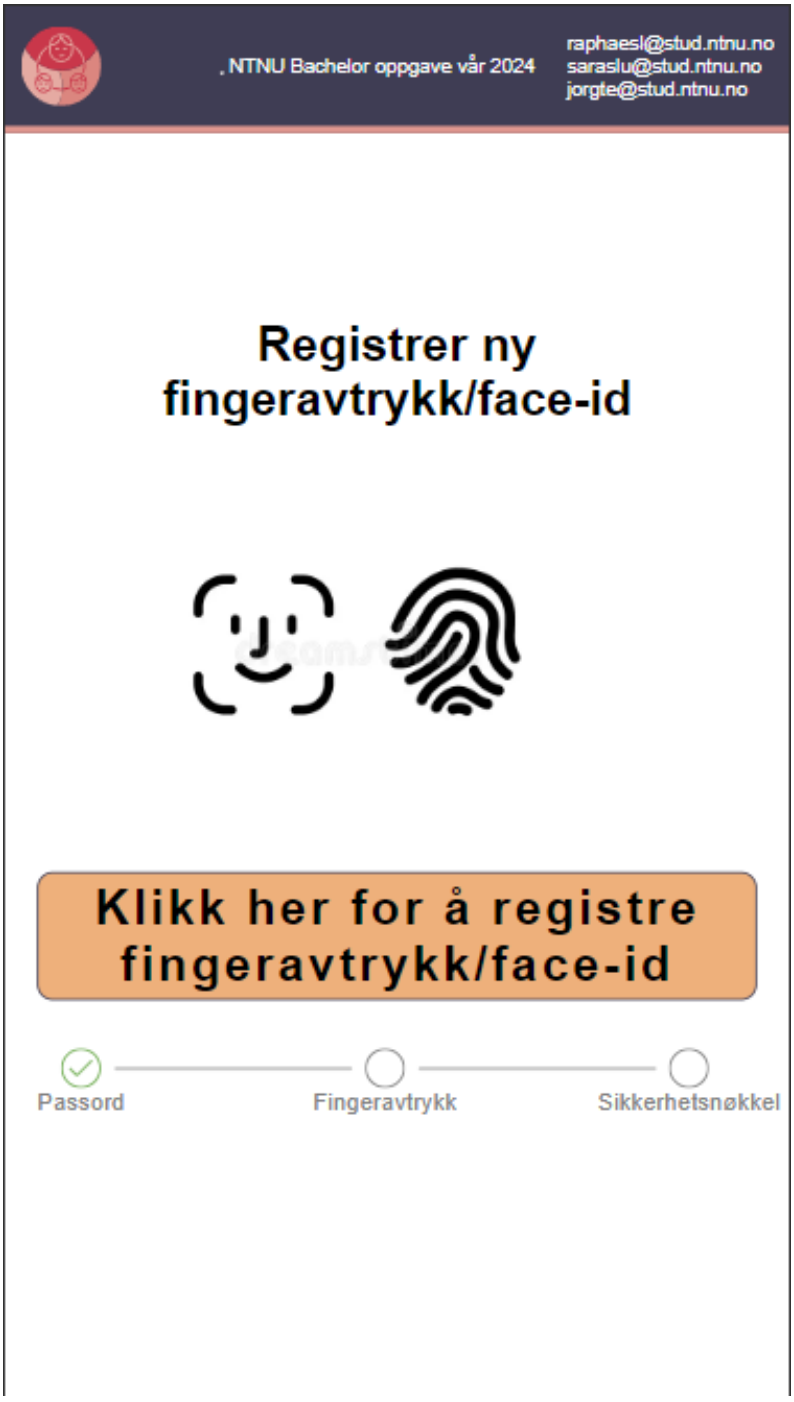
Du har nå vellykket logget inn på nettsiden.

Vedlegg G

Gjennomgang av webauthn demo

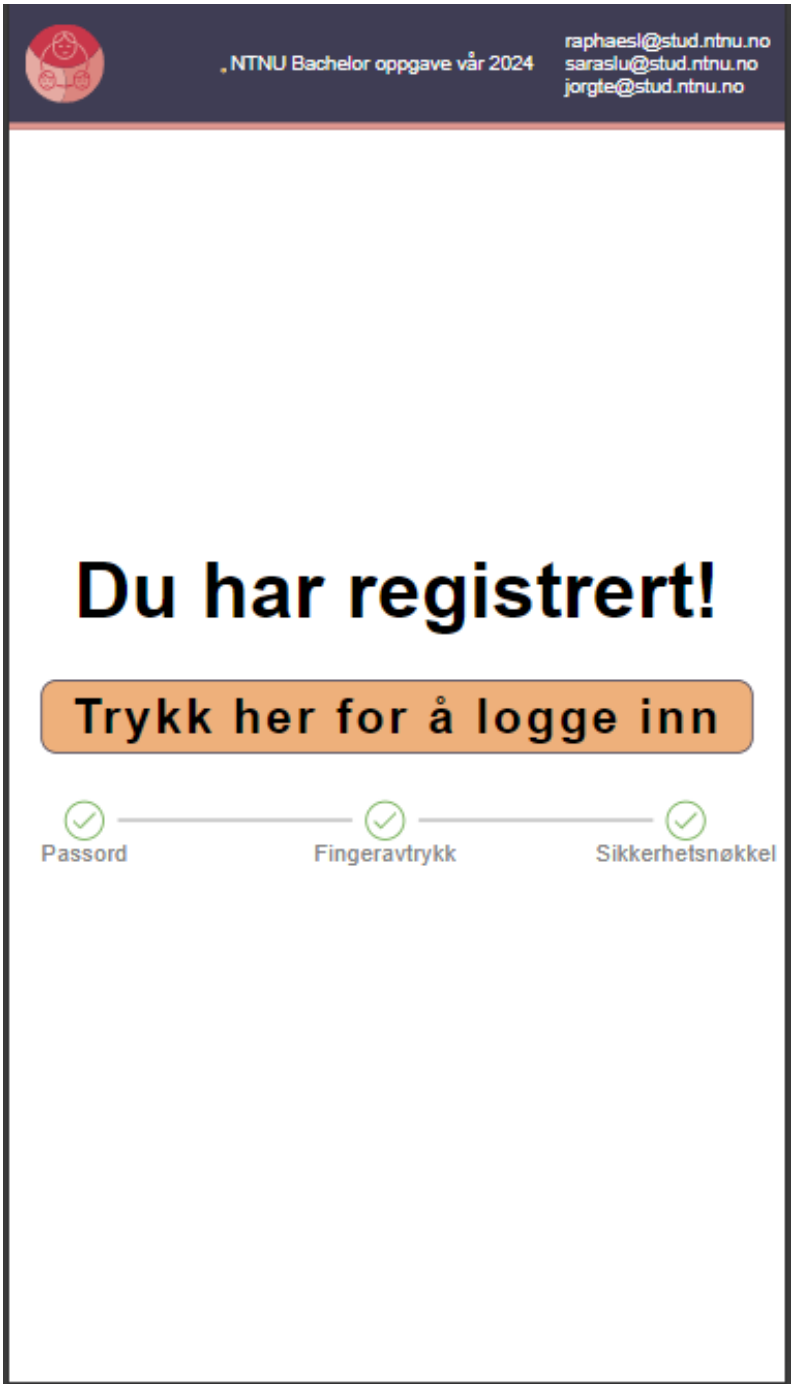
Figur G.1: Registrerings og login brukernavn

Figur G.2: Registrering engangspassord



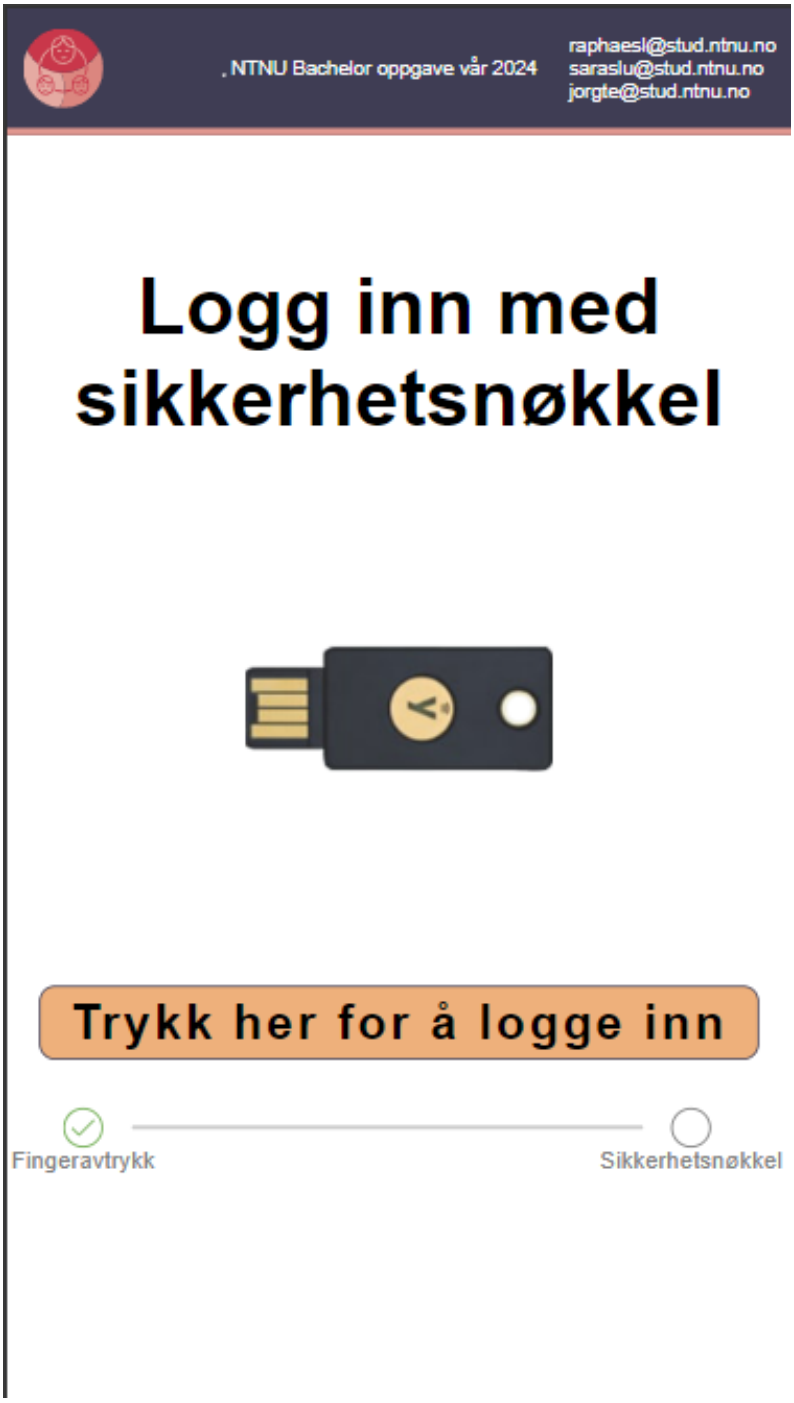
Figur G.3: Registrering finger/face-id

Figur G.4: Registrering sikkerhetsnøkkel



Figur G.5: Regestrering fullført

Figur G.6: Login face/finger-id



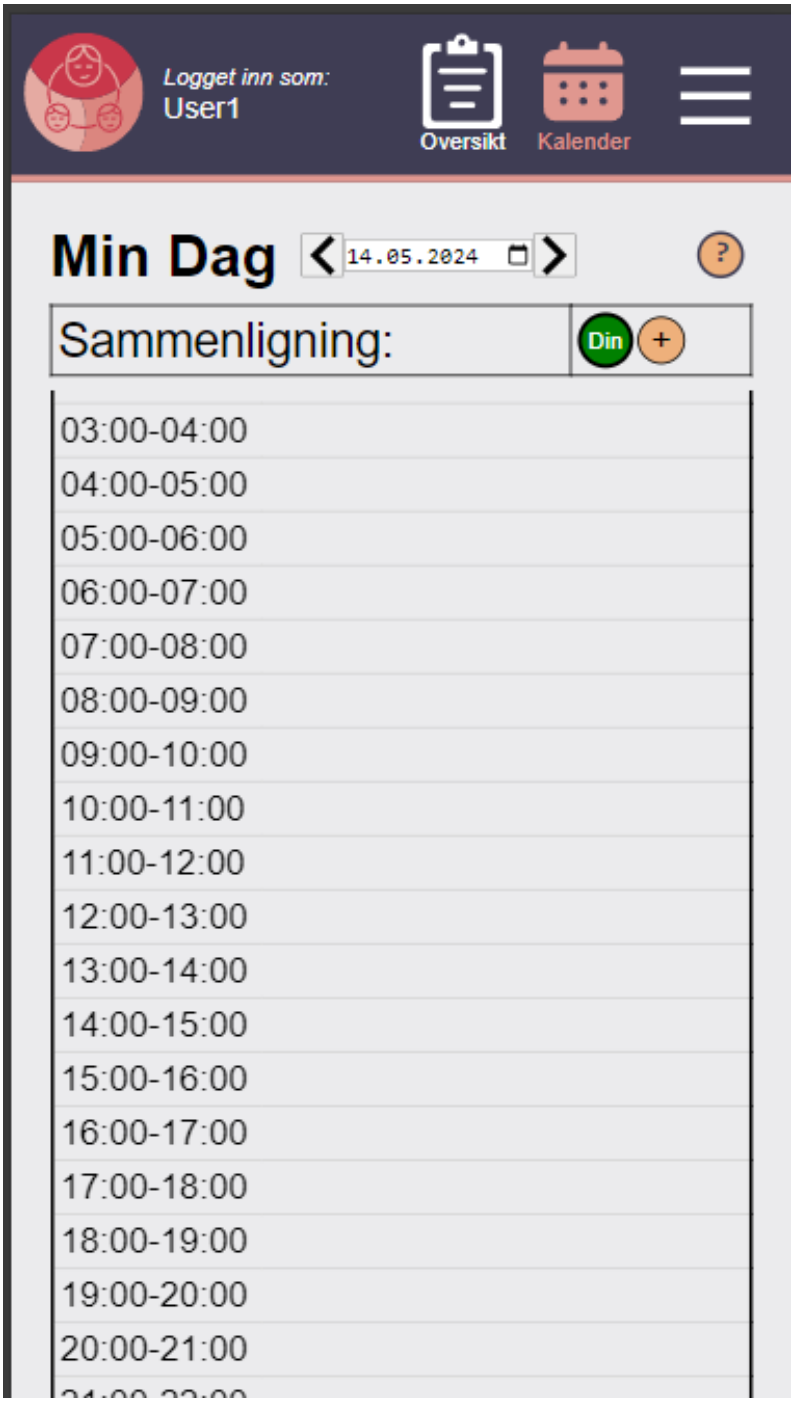
Figur G.7: Login sikkerhetsnøkkel

Figur G.8: Login fullført

Vedlegg H

Gjennomgang av pasientmodul

Figur H.1: Oversikt side over aktiviteter



Figur H.2: Kalender for aktiviteter

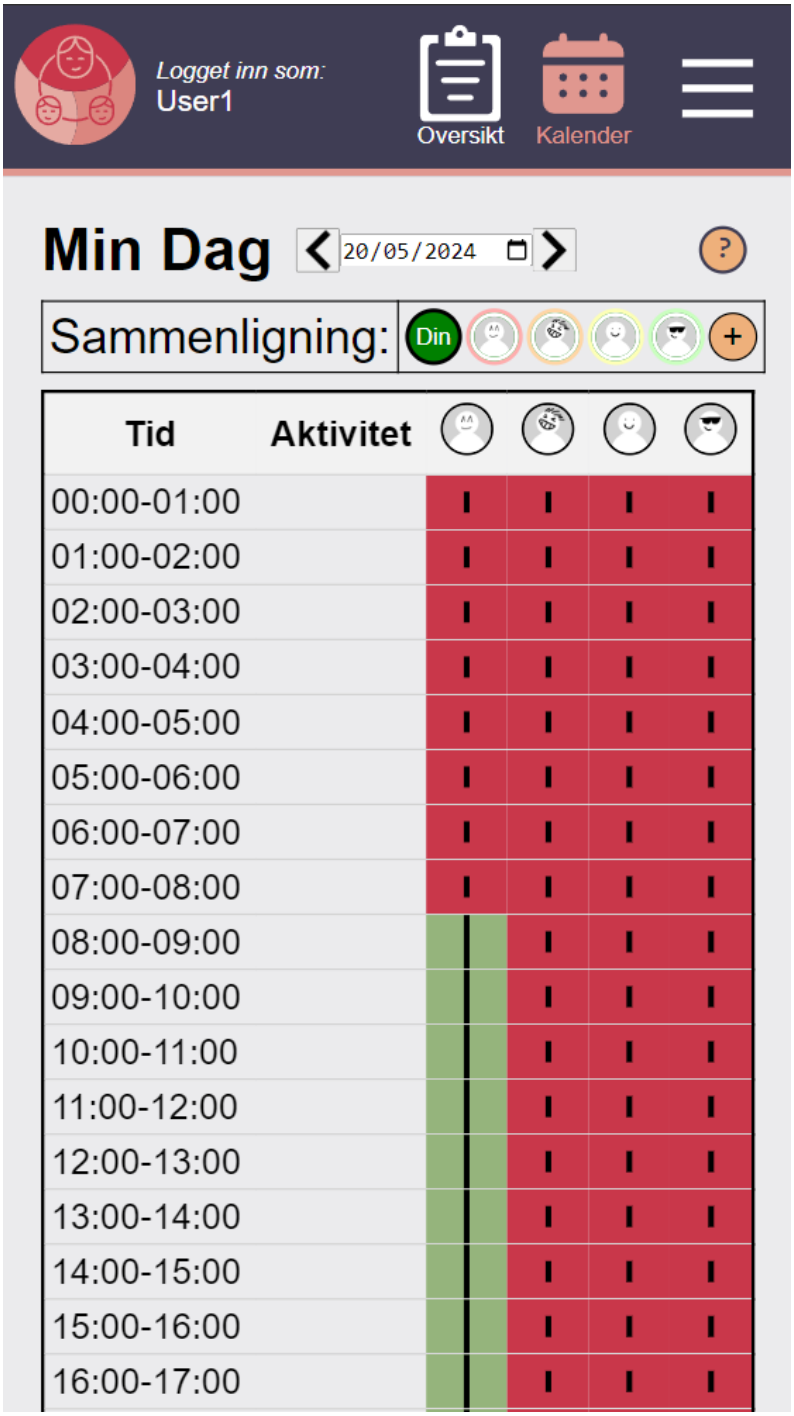
Figur H.3: Lage ny aktivitet

Figur H.4: Velg fra mal

Figur H.5: Se eksisterende maler

Figur H.6: Se eksisterende maler

Figur H.7: Pop-up for å legge til/fjerne ansatte



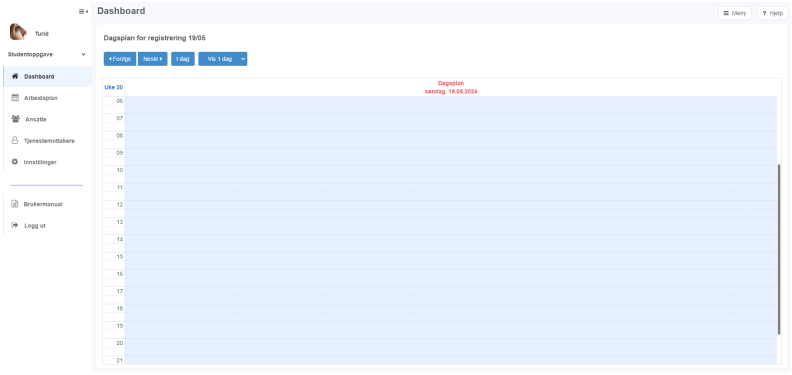
Figur H.8: Sammenligning av timeplan med flere selekterte ansatte

Vedlegg I

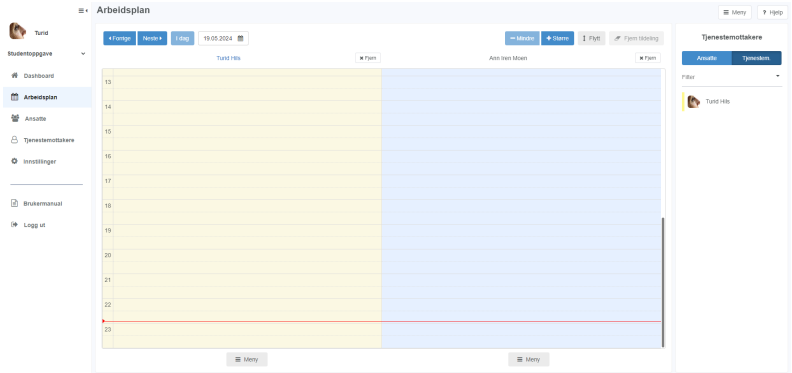
Nåverende Omhu, web-applikasjon for ansatte

Vedlegg J

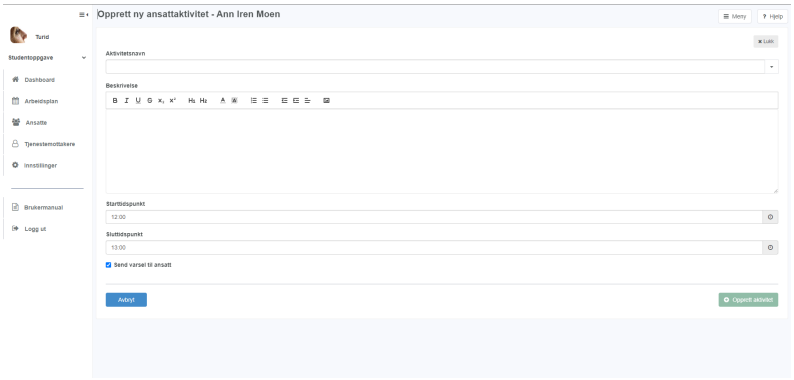
Gjennomgang av nåværende omhuside



Figur J.1: Dashbord omhuside



Figur J.2: Arbeidsplan omhuside



Figur J.3: Lage ny aktivitet omhuside

Vedlegg K

Intervju med eksperter og fagpersoner

Vedlegg L

Ekspertintervjuer

L.1 Eksterne

L.1.1 Bian Yang

Detaljer

Dato:
Tid: kl 13:30 - 14:45
Lokasjon: Gjøvik Campus, Topas T540
Oppmøte: Sara, Raphael, Jørgen, Bian Yang
Loggfører: Sara

Møteplan

- Forklare han oppgava og vise han hvordan vi har gitt de ulike kvantitative verdiene til de ulike løsningene
- Finne ut om det er noe vitenskapelig litteratur vi kan forankre oppgaven i. For eks. finne en vitenskapelig studie som poenggir de ulike attributtene vi har funnet, på en vitenskapelig måte

Resultater

- Den første timen fikk ut på at Yang fortalde oss om interessante historer fra virkeligheten, og fortalde oss om nyttig teknologi, og gav oss også innsikt

i hvordan enkelte autentiseringsløsninger faktisk fungerer. Her i Norge har blant anna BankID kontroll på alle individers digitale nøkler. Kvifor har dei det? Jo, fordi me stolar på dei. Er det lurt? Tjaaa... BankID i Sverige(den norske BankID har ein liten kundebase i Sverige) gir kundene sine hver sin sikkerhetsnøkkel, som YubiKey. Så den digitale nøkkelen er ikke lagret på en server på kontoret til BankID, men på en egen sikkerhetsnøkkel som brukerene har kontroll på selv.

- biofy.no
- Hvorfor kan vi ikke kryptere biometrisk data(som ansiktet), og sende det over Internett og dekryptere det på server-siden? Fordi når du tar eit bilde av ansiktet, så vil det bildet aldri bli helt likt som bildet på serveren...(merk: med bildet", så menes det egentlig den krypterte stringen som beskriver bildet, og ikke en JPEG-fil). Så i praksis vil en person aldri bli autentisert dersom ansiktet blir kryptert og sendt på denne måten, fordi stringen vil aldri bli lik som på server-siden. Derfor bruker man heller: distance keeping hash = hash som har en tolereringsevne for usikkerheter, gjør at en kan sammenligne ciphertext. Med andre ord: hash verdien som blir sendt til serveren, trenger ikke å være helt lik den hash verdien som er lagret på serveren.
- Omhu ligner veldig på Jodacare
- eIDAS: han gikk gjennom viktigheten av dette
- Secure Enclave: så lenge chipen aldri forlater mobilen, kan den bli brukt som en possession fakort(noe man har).
- W3C passkey
- Yang tok opp både FIDO1 og FIDO2: - FIDO1: er laga for å erstatte passordet med noe man har", altså en possession faktor. Vart utvikla for å forminske den enorme bruken av passord i vår tid. - FIDO2: De fant ut at med en fysisk autentiseringsnøkkel, så er det et problem dersom man mister den. Så nå har vi plutselig en floating key", som kan lastes opp i skyen", for eksempel iClouds Keychain. Dette kan for eksempel være biometri. Det ironiske er: Når man mister mobilen sin, og må kjøpe ny mobil og få tilgang til sine passkeys, som er i skyen, da må man logge inn på iCloud. Hvordan gjør man det? Med passord... Så da er ikke denne løsningen helt passordløs likevel.
- Yang mente vi burde fokusere enten på det menneskelige levelet av autentiseringen, eller det tekniske levelet. På den menneskelige delen av autentisering, bør vi gjøre brukerundersøkelser. Gjerne gjøre en kvalitativ undersøkelse med intervju og spørsmål. Gjerne få brukerene til å prøve autentiseringsløsninger selv. Vi bør bestemme oss på forhånd om vi skal stille spørsmål til hvordan det går med autentiseringen fortløpende, eller om vi skal ikke forstyrre brukeren, og stille spørsmål til slutt.
- Kvalitativ research: - kvifor gjorde du det? (dersom ein brukar gjere noko uforventa når dei logger inn i brukerundersøkelsen)
- Yang snakket mye om problemer rundt dette med at folk har en tendens til å stole på andre, spesielt venner og familie, fordi det er praktisk. F. eks.

sykepleierene på Innlandet sykehus har en tendens til å dele pin-kode og lignende med hverandre, fordi det er praktis. Mange personer i parforhold har en tendens til å legge inn biometrien til partneren sin på sin egen mobil, slik at partneren kan logge inn på den andres mobil med enten ansikt eller fingeravtrykk. Er dette så lurt, egentlig?

L.1.2 Møte med Andrine Løberg, fagansvarlig vernepleier, assistermeg.no

Detaljer

- **Dato:**
- **Tid:** kl10:00-10:30
- **Lokasjon:** Digitalt
- **Oppmøte:** Andrine Løberg, Sara, Raphael, Jørgen
- **Loggfører:** Sara

Møteplan

- Få overblikk over målgruppas mobilbruk, og om pc/ipad er vanlig eller ei.
- Få overblikk over hvordan en sikkerhetsnøkkel/fysisk gjenstand ville fungert. Har de kontroll på gjenstander, eller mister de lett ting?
- Få innblikk i målgruppas evne til å stå imot vanlige cybertrusler, som scam og phishing.
- Brukergruppas generelle autonomi og selvstendighet. Er det vanlig at de kan bestemme aktiviteter selv?
- Få overblikk over målgruppas generelle "ITerfaring. Bruker de Facebook og sosiale medier?
- Problem rundt dette med BankID som innloggingsmetode.
- Få innblikk i målgruppas evne til å huske og ha kontroll på passord. Er dette et reelt alternativ?
- Passord vs fysisk gjenstand/sikkerhetsnøkkel.
- Få et generelt overblikk over hvordan BPA fungerer, hvordan de ansatte jobber, relasjonen mellom brukerene og de ansatte(har brukerene faste ansatte, rullerer det?). Kommer de ansatte noen timer av dagen, eller er de der en hel dag? Osv.

Resultater

- Mobilbruk: Unge personer i målgruppa har ofte smartmobil, mens de i alderen 40 pluss har som oftest gamle ikke-smart mobiler. Ekstremt få personer i målgruppa har pc. Noen som har behov for å ha en app eller tilgang til internett, har gjerne en ipad. Hun påpekte at en sikkerhetsnøkkel ikke ville fungert på personer i alderen 40 pluss, fordi disse har ikke smartmobil, og som vi vet er en sikkerhetsnøkkel avhengig av NFC eller en inngang med USB, Lightning eller lignende. Vi tenker at dette ikke er et problem for vår oppgave, ettersom de personene som ikke har smartmobil, kan heller ikke

bruke mobilen til å logge på Omhu uansett.

- Kontroll på gjenstander: Verken de unge eller de gamle i målgruppa har særlig kontroll på gjenstandene sine. Ofte er det de ansatte som har kontroll på hvor ting befinner seg i leiligheten. Dette gjelder alle aldre. Når de er på butikken, er det ofte de ansatte som passer på lommeboka mens de går rundt og handler, og gir lommeboka tilbake til brukeren når hen skal betale. Unntaket er mobilen. De fleste har god kontroll på mobilen. Løberg har aldri opplevd at noen har mistet eller glemt hvor de har lagt mobilen.
- Scam/phishing: Løberg sine erfaringer er at brukerene pleier å spørre om det er noe de er usikre på. Løberg har aldri opplevd at noen hun har jobbet med har fått f. eks. phishing SMS og lignende, men hun sier at brukerene pleier å spørre i slike tilfeller, noe de sannsynligvis hadde gjort i dette tilfellet også.
- Angående brukerens mulighet til å bestemme aktiviteter selv(legg til aktivitet funksjon i MVP): Slik som Løberg har jobbet, så har hun jobbet rundt på institusjonslignende steder. Der har brukerene hatt en tavle på veggen, en dagsplan, der de kan selv legge inn aktivitetene de vil gjøre den dagen. Dette ligner veldig på løsningen vi har vurdert i del 2 MVP, hvor brukerene selv kan legge inn aktiviteter på timeplanen. Det er kjempeviktig at brukerene er aktive og kan bestemme sin egen hverdag. Av og til må de ansatte gripe inn, slik at det ikke bare blir dataspill hele tiden.
- Generell "ITerfaring: De fleste av de hun har jobbet med, har veldig lite erfaring med sosiale medier. Ingen har hatt epost, og kun de mest oppegående har hatt facebook.
- BankID: Løberg har vært vitne til veldig mange problem angående det at brukerene ikke har hatt BankID.
- Passord vs sikkerhetsnøkkel: Hun sier at brukerene sannsynligvis ville latt de ansatte passet på sikkerhetsnøkkelen, ettersom de ikke er så flinke til å passe på dette selv. Hun er likevel positiv til at sikkerhetsnøkkel sannsynligvis vil være en bedre løsning enn passord. De gangene hun har vært vitne til at personer har hatt Facebook eller lignende, har de lagret passordet på enheten, slik at brukeren aldri trenger å skrive inn passordet, men kommer rett inn.
- **Interessante opplysninger som ikke er direkte relevant for oppgava:**
- Hvordan fungerer assistermeg BPA: Foreldrene har ansvarsfordelingen. Foreldrene setter opp aktiviteter, og BPA'ene er foreldrenes "ansatte". Her er det ingen rullering på ansatte. De ansatte er ansatt for den spesifikke brukeren. Assistermeg hjelper brukere(altså foreldrene til brukeren), med å legge ut en annonse og finne BPA'er. Dersom brukeren er oppegående nok, kan hen bestemme hvilken person som skal ansettes. Hvis ikke er det foreldrene som bestemmer.
- Hvordan fungerer BPA i praksis: Veldig variert. Noen brukere har behov for hjelp 24/7. Da er det en skiftordning, der det alltid er ansatte på jobb. Andre brukere har BPA f. eks. 4 timer i uka, der noen kommer innom og brukeren

får hjelp til å gå på butikken, eller blir tatt med ut på f. eks. kino. Disse klarer seg ellers selv i hverdagen.

- Som nevnt over, så har Løberg jobbet på mer institusjonslignende steder. Assistermeg skiller seg fra disse stedene mtp. brukerenes bosituasjon. Brukerene til assistermeg bor for seg selv, og har BPA'er som kommer innom der de bor.
- Vi viste demoen til Løberg. Hun var positiv og mente dette var enkelt, og noe som de fleste brukere kom til å få til.

L.1.3 Møte med Halden kommune

Detaljer

Dato:
Tid: kl12:00-12:30
Lokasjon: Digitalt
Oppmøte: Sara, Raphael, Jørgen, Philip, Ingvild, Halden
Loggfører: Sara

Møteplan

- Gjennomgå rammer og praktisk informasjon rundt brukertestingen med Halden kommune. Planlegge en dato.

Resultater

- Satt opp at vi skal være i Halden den 9. april, møterom i Halden er booka fra halv 1 og utover. Uke 15.
- En av de er ferdig på jobb i to-tida, og den andre har fri hver onsdag.
- Bruker 1 blir fort sliten og kan konsentrere seg maks en halvtime. Bruker 2 kan holde ut en time før pause. Bruker 1 sliter med dialekt.
- Halden kommune mente passord ikke er en god løsning, og virka veldig positive til en sikkerhetsnøkkel.
- 1. person har bankID og er god med IT
- 2. person har bankid på mobil, men er ikke så vant til å bruke det
- kari.anne.bertelsen@halden.kommune.no Kari Anne Torp Bertelsen

L.1.4 Uformell fagsamtale etter brukertesting i Halden

Detaljer

Dato:
Lokasjon:
Oppmøte: Sara, Raphael, Jørgen, Kari Anne Torp Bertelsen(fagrådgiver i enhet Bo og miljøarbeidertjeneste, Halden kommune), Espen Søyland(vernepleier og avdelingsleder Grønliveien og Bergheimveien, Halden kommune)
Loggfører: Sara

Resultater

- Søyland har vært tilskuer på begge brukertestene vi har gjort i Halden. Han har flere tilbakemeldinger:
    a. Søyland mener vi bør heller bruke bilder og piktogram i stedet for tekst i produktene som vi utvikler, hovedsakelig pasientmodulen. Dette er fordi mange i målgruppa sliter med å lese, og kan ha problemer med å skjønne enkelte ord.
    b. Søyland liker veldig godt ideen vår med å ha en funksjon i pasientmodulen som gjør det mulig for brukeren å sammenligne når konkrete ansatte er på jobb og tilgjengelig eller ikke. Han påpeker at dette sannsynligvis er vanskelig å få til, ettersom de ansatte har et turnusprogram som blir levert av en annen bedrift(gatsoft turnusprogram). For at en slik funksjon skulle vært mulig å implementere, må denne bedriften og WeissTech samarbeide, noe som grunnet ressurser er krevende å få til.
    c. Søyland savner en funksjon, som kan gjøre det mulig for brukerene å gi tilbakemelding på tjenestene de får. Har assistenten som kom i dag, gjort jobben sin skikkelig? Kom assistenten for sent? Har brukeren opplevd at assistenten har vært uprofesjonell eller ikke gjort jobben sin på en forventet måte? Bare en funksjon som gjør det mulig for brukerene å "huke av" at jobben er gjort, hadde vært et must.
- Vi er interessert i å vite litt om hvordan vaktordningene til de ansatte fungerer, ettersom dette er relevant i forhold til hvordan "sammenlign med tilgjengelige ansatte"-funksjonen i pasientmodulen skal fungere. Søyland har følgende å fortelle om turnusprogrammet deres:
    a. Det er i utgangspunktet satt opp ansatte på hele vakter. Altså, de ansatte er hos den samme brukeren gjennom hele vakta.
    b. Det skjer av og til at en ansatt kan være f. eks. en halv vakt hos en bruker, og være hos en annen bruker resten av vakte.

   c. Halden kommune tilbyr ikke *brukerstyrt personlig assistanse(BPA)*, men "kun" *personlig assistanse*. Med dette menes at tjenestene som brukerene får, ikke er brukerstyrte, men de får tjenestene de har krav på fra kommunen. Med andre ord, så er tjenestene personuavhengige, det er ikke slik at brukerene selv nødvendigvis kan bestemme hva de vil ha hjelp til.

- Både Søyland og Bertelsen påpeker at journalløsningene som eksisterer i helse- og omsorgssektoren rundt omkring er "helt umulige" å ha med å gjøre. Flere av de digitale løsningene de har erfaring med:

   a. Er vanskelige å bruke, selv for de som har brukt det mange ganger.
   b. Er såpass "knotete" at man bruker ekstremt lang tid på å gjøre de enkleste oppgaver i systemet.
   c. De kan ikke skrive ut grafer, tabeller og lignende, noe som hadde vært ganske nyttig. Er med andre ord vanskelig å eksportere data mellom journalløsningen og filsystemer.
   d. Tilgangsstyringen i forhold til hva leger kan se, og hva de ansatte vernepleierene som jobber med brukerene kan se, er utrolig '"knotete" laget, og gir lite mening. Dette gjør kommunikasjonen og samhandlingen mellom de ulike instansene(i dette tilfellet mellom fastlegen og kommunehelsetjenesten) utrolig ineffektiv.
   e. Det er mange forskjellige innlogginger som kreves både "her og der", det kreves flere innlogginger for de enkleste ting. Rett og slett en ineffektiv og lite gjennomtenkt tilgangsstyring.

  De nevner blant annet Gerica, som er et pasientjournalsystem for kommunehelsetjenesten. I tillegg har de et annet fagprogram tilsvarende Omhu. Ingen av disse er enkle å bruke.

Vedlegg M

Møtereferat med oppdragsgiver, veiledere og gruppemøter

Vedlegg N

Møterapporter

N.1 Scrumrapporter

Sprint 1

Detaljer

Startdato:
Sluttdato:
Ukenummer: 3
Scrum Master: Sara
Team: Raphael, Jørgen

Sprintmål:

- Første møte med oppdragsgiver
- Ferdigstille prosjektplan
- Jobbe ca. 30 timer per person

Resultat

- Fikk gjennomgå det vi lurte på med oppdragsgiver. Var et godt og informativt møte.
- Prosjektplan ble ferdigstilt og sendt inn på sprintslutt.

- Få arbeidsoppgaver, gikk tom for oppgaver å gjøre underveis.

Konklusjon

- Det var alt for få arbeidsoppgaver per person denne sprinten. Dette pga at vi er i startfasen av prosjektet, og har dermed ikke så mange konkrete arbeidsoppgaver ennå. Dessuten en smule skjevfordeling i arbeidstimer. Dette vil forbedres etterhvert når flere konkrete arbeidsoppgaver dukker opp.

Sprint 2

Detaljer

Startdato:
Sluttdato:
Ukenummer: 4
Scrum Master: Jørgen
Team: Sara, Raphael

Sprintmål:

- Få oversikt over 10 autentiseringsmetoder
- Ferdigstilling av standardavtalen
- Jobbe ca. 30 timer per person

Resultat

- Fant ulike autentiseringsmetoder, som vi kan skrive om i rapporten.
- Strukturert og startet med sluttrapporten

Konklusjon

- Vi greide nesten alle målene vi sett for sprinten, og til og med begynte med noen av de fra neste ukes sprint. Standard avtalen må bli ferdigstillt neste uke.

Sprint 3

Detaljer

Startdato:
Sluttdato:
Ukenummer: 5
Scrum Master: Raphael
Team: Sara, Raphael

Sprintmål:

- Bli ferdig med todo-lista i løpet av uken
- Skrive de fleste/alle autentiseringsmetodene
- Bestille Yubikey
- Undersøke mulighet for spørreundersøkelse og evt sende det ut

Resultat

- Vi stemmer over valg av autentiseringsmetode til bruk i demo. Vi velger Yubikey til fysisk faktor, og fingeravtrykk til biometrisk.
- Vi sender utkast av spørreundersøkelse til Omhu.

Konklusjon

- Omtrent alle de opprinnelige oppgavene lagt ut i denne sprinten ble fullført. Likevel følte gruppen at arbeidet kunne ha vært bedre den første delen av uken. Derfor ble ukens oppgaver utvidet betraktelig på torsdag. Gruppen jobbet effektivt resten av uken, inkludert Lørdag. Av disse oppgavene ble likevel bare noen fullført.
- Gruppen vil forsøke å jobbe mer effektivt den neste sprinten for å fullføre oppgavene. Gruppen legger også fokus på å ha flere oppgaver fra starten av uken, så ikke gruppemedlemmene skal få en falsk opplevelse av god tid.
- Gruppen har oppnådd administrative mål denne uken. Yubikey er bestillt og mail er sendt til oppdragsgiver.

Sprint 4

Detaljer

Startdato:
Sluttdato:
Ukenummer: 6
Scrum Master: Sara
Team: Raphael, Jørgen

Sprintmål:

- Bli ferdig med todo lista
- Bli ferdig med minst tre ROS-analyser over identifiserte løsninger
- Begynne på utvikling av demo, lage gode fundamenter, researche, brainstorme ideer, planlegge
- Rydde i rapporten, forbedre rapportstruktur

Resultat

- Vart ikke ferdig med todo-lista. Hovedårsaken til dette var møtet med Bian Yang, som endra fokuset vårt og skapte forvirring rundt prioritetene våre.
- Ingen ROS-analyser ble gjennomført.
- Raphael har lest seg opp på implementasjon av demo, sekvensdiagram er også laget. Domenemodell er ikke laget ennå.

Konklusjon

- Forrige uke endra planene våre, og vi gjorde dermed ikke alt på todo-lista. Vi har fått godkjenning til å utvikle en demo ved hjelp av security key og biometri.

Sprint 5

Detaljer

Startdato:
Sluttdato:
Ukenummer: 7
Scrum Master: Raphael
Team: Sara, Jørgen

Sprintmål:

- Til onsdag:
  - Undersøke normer for brukerundersøkelse.
  - Kontakte eldrehjem for å sette av time på torsdag eller fredag.
  - Lage brukerundersøkelse.
- Gjennomføre en brukerundersøkelse eller ha alle brukerundersøkelser planlagt og klargjort til neste uke.
- Lese seg opp på relevant litteratur. Artikler fra IEEE og ACM tar prioritet.
- Fullføre backlog fra forrige uke, hovedsaklig peer review.
- Begynne på demo og ha mesteparten av støttende dokumentasjon ferdig.

Resultat

- Mål ble ikke oppnådd, da sprinten har vært noe ueffektiv samt at målene var litt vel ambisiøse.
- Brukerundersøkelser har blitt påbegynt, og det har allerede blitt arrangert noen undersøkelser som skal gjennomføres i løpet av uke 9.
- Demoen for omhu er godt underveis, men den støttende dokumentasjonen (domene modell, sekvensdiagram og dataflytdiagram) ligger etter.
- Backloggen fra forrige uke har i all hovedsak blitt wrappet opp, men det har blitt fylt opp nye issues i “pending review” som må fullføres til neste sprint.
- Litt relevant litteratur har blitt funnet.

Konklusjon

- Har havnet bak skjema, så del 1 av prosjektet har fått en uke ekstra i første omgang.

Sprint 6

Detaljer

Startdato:
Sluttdato:
Ukenummer: 8
Scrum Master:Jørgen
Team: Raphael, Sara

Sprintmål:

- Planlegg brukertest
- Fortest av bruketesten
- Finne og lese på litteratur til rapporten
- Bli ferdig med demo av loggin side

Resultat

- Ble ikke helt ferdig med loggin side/demo
- Fikk plan lagt og testet brukertest
- Ikke noe mer litteratur funnet

Konklusjon

- Ble ikke helt ferdig med loggin side.
- Ellers gikk planlegging og sette opp brukertester relativt greit.
- Ikke funnet noe mer litteratur for og støtte opp rapporten.

Sprint 7

Detaljer

Startdato:
Sluttdato:
Ukenummer: 9
Scrum Master: Sara
Team: Jørgen, Raphael

Sprintmål:

- Bli hundre prosent ferdig med demo innen tirsdag 27.02 klokka 23:59.
- Gjennomføre planlagte brukerundersøkelser på onsdag.
- Planlegge møte med fagfolk, assistermeg.no
- Starte å se på del 2, få til en enkel wireframe

Resultat

- Demoen er hundre prosent ferdig
- Har gjennomført 4 brukerundersøkelser.
- Har ikke fått kontakt med assistermeg.no
- Fikk ikke tid til å se noe på del 2

Konklusjon

- Ligger ennå en uke bak skjema. Demoen er ferdig, og det som gjenstår på del 1 av oppgaven er hovedsakelig analysering av data og rapportskriving.

Sprint 8

Detaljer

- **Startdato:**
- **Sluttdato:**
- **Ukenummer: 10**
- **Scrum Master: Raphael**
- **Team: Jørgen, Sara**

Sprintmål:

- Bli ferdig med en skikkelig wireframe.
- Alle gruppemedlemmene skal lage en enkel wireframe hver til onsdag kl 18.
- Skrive ferdig del om argumentering for valg rundt demoen.
- Få kontakt med assistermeg.no

Resultat

- Wireframe er for det meste fullført, revisjon må fortsatt gjøres.
- Wireframen er delvis lagt til i rapporten, men har fortsatt en del igjen.
- Et møte er booka med en kontakt fra assistermeg.no.

Konklusjon

- Har gjort alt for lite denne sprinten(også). Den gjennomsnittlige motivasjonen og initiativet i gruppa er lav. Derfor skal grupperollene bli omfordelt: Fra neste sprint har vi blitt enige om at Sara er møteansvarlig, og Raphael er gruppeleder. Grunnen er at disse rollene passer bedre til korresponderende gruppemedlemmer. Tidligere gruppeleder har ikke fordelt arbeidsoppgaver godt, og heller ikke passet på at arbeidsoppgaver blir gjort godt nok. Dette har ført til urettferdig foreling av arbeidsoppgaver, og kvaliteten på arbeidet har heller ikke blitt verifisert skikkelig.

Sprint 9

Detaljer

- **Startdato:**
- **Sluttdato:**
- **Ukenummer: 11**
- **Scrum Master: Raphael**
- **Team: Jørgen, Sara**

Sprintmål:

- Skrive begrunnelse for valg av design for del 1 og del 2 i rapport.
- Fullføre wireframe med modifikasjoner før onsdag.
- Begynne å lage interaktiv demo av nettside.

Resultat

- Begrunnelse av valg for del 1 er ca 80% ferdig, del 2 er så vidt påbegynt.
- Wireframen har ikke blitt mer modifisert.
- Interaktiv demo for nettside er godt underveis. Det gjenstår å lage “min dag” siden, samt legge til andre ekstra features som chat og favorisert ansatt seksjon.

Sprint 10

Detaljer

- **Startdato:**
- **Sluttdato:**
- **Ukenummer:** 12
- **Scrum Master: Raphael**
- **Team: Jørgen, Sara**

Sprintmål:

- Innspurt før påska for å ta igjen arbeid. Viktig at alle gruppemedlemmer har **minst 30 timer** arbeid denne uka.
- Jørgen & Raphael: Fullføre interaktiv demo for del 2 før onsdag.
    - Jørgen: Lag ferdig "Min dag" side.
- Få oversikt og lage backlog over hva som må gjøres for del 1 rapport før Onsdag.
- Få del 1 seksjon av rapporten så klar som mulig innen lørdag.
- Nytt evaluerings-møte på onsdag.

Resultat

- Laget ny iterasjon av gantt-chart. Iterasjon 4.

Sprint 11

Detaljer

- **Startdato:**
- **Sluttdato:**
- **Ukenummer:** 14-15
- **Scrum Master:** Raphael
- **Team:** Jørgen, Sara

Sprintmål:

- Gjøre en til brukertest for nettsiden.
- Implementere de enkleste forbedrings-potensialene fra brukertesten.
- Pynte på DEL 1 demo.
- Designe oppsummerende brukertest for del 1.
- Sende melding til Halden med hva som kommer til å være i brukertesten.
- Forberede oss til å dra til Halden 9. april for å brukerteste to personer i målgruppa.

Resultat

- Fikk gjort en brukertest til av nettsiden, før Halden.
- Enkle forbedringspunkter i nettsiden er implementert.
- Designet oppsummerende(summativ) brukertest for del 1 før Halden.
- Fikk gjennomført alt som planlagt med brukertestene i Halden den 9. april.

Sprint 12

Detaljer

- **Startdato:**
- **Sluttdato:**
- **Ukenummer:** 15-16
- **Scrum Master:** Raphael
- **Team:** Jørgen, Sara

Sprintmål:

- "Pynte" på og bearbeide data for brukertestene vi gjennomførte i Halden.
- Finne kilder for UX design for brukere med nedsatt funksjonsevne.
- Bruke funn til å skrive en god liste med forbedringsområder for versjon tre av pasient-modul.
- Sende mail til Halden og be om bekreftelse av at brukerene vi testet på var representative for den generelle brukerbasen.
- Være klare til å begynne med implementering av endringer neste sprint.

Resultat

- Data fra brukertestene i Halden er bearbeidet.
- Funnet noen relevante UX-design kilder for mennesker med psykisk funksjonshemming.
- Laget liste for forbedringspotensialer til pasientmodulen.
- Er klare til å begynne å implementere endringer neste sprint.

Sprint 13

Detaljer

- **Startdato:**
- **Sluttdato:**
- **Ukenummer:** 17
- **Scrum Master:** Raphael
- **Team:** Jørgen, Sara

Sprintmål:

- Sara skal skrive kapittel 1 i rapport førsteutkast ferdig før onsdag.
- Sara begynner å skrive kapittel 2 i rapport førsteutkast onsdag til fredag.
- Raphael skriver kapittel 3 i rapport førsteutkast ferdig i løpet av uka.
- Jørgen skal fikse en bug og ferdiggjøre oppgaver på DEMO før onsdag.
- Jørgen begynner på koderevidering og unit-testing fra onsdag.

Resultat

- Målene for sprinten er bortimot oppnådd. Kapittel 3 testing ble ikke påbegynt.
- Unit-testing av kode har god fremgang.

Sprint 14

Detaljer

Startdato:
Sluttdato:
Ukenummer: 18
Scrum Master: Raphael
Team: Sara, Jørgen

Sprintmål:

- Ferdigstille førsteutkast av rapport, slik at veileder kan lese gjennom å gi tilbakemelding.
- Fullføre unit testing av demo backend.

Resultat

- Kapittel 1 introduksjon, 2 teori og 3 metode ble ferdig til innlevering.
- Unit testing ble ferdig.

Sprint 15

Detaljer

Startdato:
Sluttdato:
Ukenummer: 19
Scrum Master: Sara
Team: Raphael, Jørgen

Sprintmål:

- Bli ferdig med uviktlings kapittelet.
- Bli ferdig med resultat kapittelet.
- Lag vedlegg med screenshots av autentiserings-demo.

- Oppdater og gjør styling på autentiserings-demo mer i stil med pasient-modulen.

Resultat

- Midt-sprint evaluerting:
    - Redesign av autentiserings-demo frontend er nesten ferdig. Skal bli lagt til email, overskrift og noen visuelle bugs skal fikses.
    - Domenemodell er ferdig, og har blitt evaluert av gruppen.
    - Utviklings-kapittel er ferdig i løpet av uken.
    - Begynner å skrive på resultat i dag(onsdag).

Sprint 16

Detaljer

Startdato:
Sluttdato:
Ukenummer: 20
Scrum Master: Raphael
Team: Sara, Jørgen

Sprintmål:

- Kapittel 5, resultat skal fullføres innen onsdag.
- Vedlegg for møtereferat, ekspertmøte, skjermbilder av webauthn demo samt pasientmodul.
- Nytt møte holdes torsdag kl10.

N.2 Gruppemøter

N.2.1 Gruppemøte 1 - Introduksjonsmøte

Detaljer

Dato:
Tid: kl10:15-14:00
Lokasjon: Gjøvik Campus, Smaragd S409
Oppmøte: Alle
Loggfører: Raphael

Møteplan

- Begynne på arbeidskontrakt med grupperegler.
- Avtale møte med veileder.
- Sette opp system for loggbok, timetelling og generell dokumenthåndtering.

Resultater

- Sendte mail til Eirik og Ernst for å planlegge møte. Når som helst utenom onsdag.
- Opprettet overleaf dokument for rapport, timetelling og grupperegler.
- Opprettet github repository. https://github.com/raphaelstorm/bachelor
- Skrev utfyllende grupperegler. Dokumentet kan bli funnet i overleaf under grupperegler.tex".

Arbeidsøkt

Detaljer

Dato:
Tid: kl10:15-13:00
Lokasjon: Gjøvik Campus, Topas T115
Oppmøte: Alle
Loggfører: Raphael

Møteplan

- Fullføre planlegging av møte med oppdragsgiver.
- Lage noen spørsmål for Erik og Ernst for møtet til i morgen.
- Begynne å legge opp struktur for prosjektplan.

Resultater

- Møte med oppdragsgiver er satt Torsdag kl 14:00.
- Skrev spørsmål til veileder. Disse kan bli funnet i discord.
- Noterte idemyldring på MFA oppgave.
- Sorterte mappestruktur i overlfeaf.
- Begynte på GANT-chart over fremdriftsplan.
- Begynte sammensetning av prosjektplan.

Mål til neste møte

- Skrive ferdig og kvalitetsikre prosjektmål.

N.2.2 Gruppemøte 2 - Møte etter seminar

Detaljer

Dato:
Tid: kl14:00-16:00
Lokasjon: Gjøvik Campus, Gneis G215
Loggfører: Raphael
Oppmøte: Alle

Møteplan

- Revisjon av reglemanget utifra innehold av seminar.
- Skrive avgrensing av oppgaven basert på innehold av seminar.

Resultater

- Forbedret gruppereglene i rapporten.
- Skrev bakgrunn, oppgavebeskrivelse, og problemområde i rapport.

Mål til neste møte

- Forberede presentasjon av valg av prosessrammeverk.
- Alle må lese en rapport av en tidligre bachelor oppgave.
- Lage et bedre system for timetelling i excel.

N.2.3 Gruppemøte 3 - Etter veileder møte

Detaljer

Dato:
Tid: kl10:30-14:00
Lokasjon: Gjøvik Campus, Topaz T115
Oppmøte: Jørgen, Sara, Raphael
Loggfører: Raphael

Møteplan

- Jørgen går gjennom research på ulike typer prosesstrukturer.
- Gjennomgang av standardavtale.

Resultater

- Agile, Waterfall, Scrum, Kanban, Devops er alternativer for rammeverk.
  - Waterfall er oversiktlig, men rigid og ineffektivt.
  - Agile er tilpassningsdytig men har lite krav om dokumentasjon.
  - Scrum er enkelt og bruke, med sprint. Ligner på det vi allerede har. Inkluderer sprint rapport.
  - Kanban, basert på git issue boards. Kortere type dokumentasjon.
- Vi gjør beslutning på type struktur. Vi stemmer, og velger å bruke hovedsakelig Scrum med elementer fra Kanban. Kanban er fokusert på kontinuerlig utvikling, mens Scrum er bygget rundt fiksa sprinter. Siden vi allerede har lagt opp til sprinter med mandagsmøtene, var dette naturlig. Vi skal velge scrum-master på begynnelsen av uken. Denne personen skal skrive en rapport etter sprinten. Vi bruker gitlab issue board til å spore oppgavene, der hver sprint blir designert som en egen milestone. Raphael skal opprette milestone på begynnelsen av hver uke.
- Vi går gjennom standardavtale, og beslutter å ikke gi oppgavegiver eiendomsrett, men fortsatt bruksrett for oppgaven.
- Vi gjør risikoanalyse og skriver det inn i forprosjektet.

N.2.4 Gruppemøte 4 - Start på sprint 3

Detaljer

Dato:
Tid: kl10:15-12:00
Lokasjon: Gjøvik Campus, Topaz T116
Oppmøte: Jørgen, Raphael, Sara
Loggfører: Raphael

Møteplan

- Fullføre sprint 2
- Velge SCRUM master for sprint 3
- Designere eksisterende gruppeoppgaver
- Drøfte alternative oppgaver
- Forberede spørsmål til oppgavegiver
- Andre forberedelser til møte med oppgavegiver

Resultater

- Gjennomgang av ny backup løsning med github og overleaf synkronisering.
- Sara er ukens utvalgte scrum master.
- Gruppen gjorde en revisjon av leste over grupperegler før printing og signering. Alle gruppemedlemmer er fornøyd med nåværende reglemang.
- Gjennomgang av rapporten for å identifisere og opprette nye issues til sprint 3.
- Utdeling av issues som skal fullføres innen sprinten.

N.2.5 Gruppemøte 5 - Start på sprint 4

Detaljer

Dato:
Tid: kl10:15-14:00
Lokasjon: Gjøvik Campus, Topaz T207
Oppmøte: Jørgen, Sara, Raphael
Loggfører: Raphael

Møteplan

- Scrum sprint 3 rapport

Resultater

- Sprint 3 rapport
  - Fullført alle mål: møte med oppdragsgiver, ferdigstille prosjektplan, jobbe ca 30 timer per pers
  - Ikke så mye og gjøre, selvstudium var ikke helt nok.
  - Dette forbedres etter hvert når det kommer flere konkrete arbeidsoppgaver, ikke et problem
- Starter Sprint 4:
  - Jørgen er SCRUM master for denne uken.
  - Hovedmål: få oversikt over muligheter for autentisering, lage dokumenter og litt struktur på del 1 rapport, se på appen for gøy.
- Vi "claimer" produkter i discord, så vi ikke jobber over hverandre.
- Et digitalt møte er planlagt til onsdag morgen, der vi skal deligere vidre lesing på funn av metoder.
- Vi har fått invitasjon til test omhu platform, kredentsialer deles i discord.
- Vi drøftet rundt gantt chartet, det er mulig vi kan forskyve prosjektplan frem 2 uker om vi blir ferdig med tidlig research fase denne sprinten.
- Vi diskuterte innkjøp av eventuelle fysiske produkter. Dette burde gjøres ganske snart da levering kan ta en del tid. Offesiell start på demo-utvikling er 12. februar, men kan skje mye tidligre hvis vi fremskynder planen.
- Yubikey, som virker som det mest lovende for øyeblikket, produserer og sender fra både USA og EU. Hvis vi går ut i fra 2 uker transport, må vi bestille produkt innen 29. februar.
- Aspekter med produkter en bør være oppmerksom på:

- Tilgjengelighet
- Pris
- Brukervennlighet
- Sikkerhet
- Vanskelighetsgrad av implementasjon

N.2.6 Gruppemøte 6: Midt-sprint reevaluering

Detaljer

Dato:
Tid: Kl. 10:00-12:00
Lokasjon: Digitalt, Discord
Oppmøte: Jørgen, Sara, Raphael
Loggfører: Raphael

Møteplan

- Ved sprintens start identifiserte alle gruppemedlemmer fire autentiseringsmetoder som de skulle utforske grundigere. I dette møtet presenterer hvert gruppemedlem funnene sine angående autentiseringsmetoder for resten av gruppen.
- Treffe beslutning om hvilke metoder som skal inkluderes i kartleggingen.
- Diskutere andre beslutninger vedrørende arbeidsstrukturen.

Resultater

- Valg av autentiseringsmetode:
  - MS Azure Face API: Temmelig sikkert, men krevende å implementere.
  - Authenticator: Moderat enkel å implementere. God, testet, men litt tungvint å bruke.
  - Google login: Moderat sikkerhet, mulighet for tofaktorautentisering. Enkel å implementere.
  - Fingeravtrykk: Relativt sikkert, enkelt å bruke og implementere.
  - Certificate: Svært trygt, men vanskelig å implementere.
  - Geolokasjon: Usikkert, men kanskje egnet som tredje faktor.
  - QR: Relativt sikkert, rimelig og enkelt å implementere.
  - Yubikey: 290 kr, USB-C og NFC. Enkel å bruke. Tilgjengelig for mobiler under 10 år.
  - Iris Scanner: Krever dyrt kamera, spesifikk mobil, ubehagelig å registrere og operere. Sikkert.
  - Stemmegjenkjenning: Diskutert, men besluttet at denne autentiseringsmetoden ikke var passende for produktet.
- Påbegynner implementering av autentiseringsmetodene i hovedrapporten.
- Besluttet å fremskynde prosjektet med en uke. Uke 5 fra gantt-diagrammet komprimeres til uke 4.

- Skal sende ut spørreskjema så tidlig som mulig. Diskuterer med Phillip på mandag.
- Vurderer å bruke DIRI for risikoanalyser.
- Vurderer Yubikey og QR-basert system for å lage en demo. Vi vil presentere dette for oppdragsgiveren på det neste oppdragsgivermøtet.

N.3 Oppdragsgivermøter

N.3.1 Oppdragsgivermøte 1

Detaljer

Dato:
Tid: kl10:00-12:00
Lokasjon: Digitalt, teams
Oppmøte: Jørgen, Raphael, Sara, Erik Hjelmås, Phillip Weisser, Jan Egil Jægersborg
Loggfører: Raphael

Møteplan

- Gjennomgang og evt. signering av standardavtale.
- Gjennomgang/demo av Omhu og forklaring av problemstilling rundt brukergrensesnitt og autentisering.
- Oppgavegivers forventninger til prosjektet.
- Brukerundersøkelser og kunde-feedback.
- Rammer og begrensinger for oppgaven.
- Avtale for bruk av ressurser.
- Planlegging av fremtidige regelmessige møter.

Resultater

- Møtet startet med en gjennomgang av standardavtalen, der alt var i orden. Oppdragsgiver informerte om at mindre kostnader for prototyper og transport vil bli dekket av Weisstech AS.
- Oppdragsgiver gikk gjennom Omhu og funksjonaliteten dens. Funksjonaliteten som vi skal fokusere på er timeplanen, der sluttbrukeren kan se hva som er på agendaen, hvilke ansatt som er ansvarlig for den aktiviteten, og hva som ble rapportert under den aktiviteten. Den andre funksjonaliteten er for brukeren og selv legge til aktiviteter, som for øyeblikket er litt knotete med tanke på at en ansatt må registreres til alle aktiviteter laget av pasienter.
- Oppdragsgiver gikk gjennom oppgaven og forventninger for resultatet.
    - Oppgaven er i all hovedsak teoretisk. Weisstech ønsker en kartlegging av mulige potensielle løsninger for inlogging som ikke krever bankID eller bypass, og som er enkelt nok til at sluttbrukerene kan få det til.

    - Det er ønsket at vi ser på en stor bredde av løsninger, for så og utelukke det som ikke er aktuelt, og informere om det som kanskje er aktuelt. Drøftingen er kjernen av oppgaven, men det hadde vært en god bonus om vi kunne ha laget en demo av den mest lovelige innloggingsløsningen.
    - Det samme gjelder MVP av brukergrensesnittet, der vi som minimum bare skal lage skisser og designe. Om det er ressurser og spare, kan vi utvikle en "kopi" av nettsiden der vi implementerer forslaget til designet vårt.
    - Vi får tilgang til Omhu systemet på en QA server, men vi skal ikke implementere noe direkte på deres systemer. De skal gå over til Svelte som javascript bibliotek, så det kan vi bruke om vi ønsker. Men dette er ikke et krav da de ikke skal bruke koden vår, bare konsepter vi presenterer. De bruker også .net til backend systemer, men dette er heller ikke særlig relevant da vi fikser vår egen backend løsning om det skal være nødvendig.
    - Sluttbrukerene vi skal fokusere og tilrettelegge for har hovedsakelig lettere kognetive nedsettelser som f.eks asperger, downs syndrom og lignende. Oppdragsgiver spesifiserer at dette er burkerene vi skal spesialisere oss på, og at det er mange flere som bruker omhu. Rammene på prosjektet er altså denne målgruppen.
    - Oppdragsgiver oppmuntrer til å prate med sluttbrukere, og har til og med flere forslag til bedrifer vi kan besøke. Den mest lovende av disse var for Halden kommune, og det var oppmuntret til at gruppen reiser hit med kostnader dekket av Weisstech.
    - De fleste brukerene benytter mobil tjenesten. Vi utvikler MVP og demo med mobile-first approach.
    - MVP av omhu burde fokusere på dashbord og arbeidsplan funksjonaliteten.
- Vi ble enige om å ha et møte med arbeidsgiver annen hver mandag fra kl10:30 til 11:00.

N.3.2 Møte med oppdragsgiver 2

Detaljer

Dato:
Tid: kl10:30-11:00
Lokasjon: Digitalt, Teams
Oppmøte: Jørgen, Raphael, Sara, Phillip Weisser, Jan Egil Jægersborg
Loggfører: Raphael

Møteagenda

- Kort presentasjon av utvalgte autentiseringsmetoder og spørsmål til oppdragsgiver om foretrukken metode for utvikling av demo.
- Gjennomgang av brukerundersøkelsen og planlegging av distribusjon for denne.
- Planlegging av brukertester med fokus på hvorfor Halden kommune er spesielt relevant for dette prosjektet.
    - Runde 1 - Wireframe: Uke 10
    - Runde 2 - Demo: Uke 12
    - Runde 3 - Sluttprodukt: Uke 15
- Klarhet rundt graden av sammenknytning mellom del 1 og 2 av oppgaven.
- Diskusjon angående valget mellom Confides og Bypass SaaS som løsning.
- Drøfting av oppdragsgivers prioriteringer når det gjelder sikkerhet, brukervennlighet og kostnader. Nåværende prioritering fra høy til lav: Brukervennlighet -> Dekning av målgruppe-> Sikkerhet -> Kostnad for kunde -> Kostnad av implementering.

Resultater

- Oppdragsgiver ønsker å endre prioritertingsrekkefølgen til: *Sikkerhet -> Brukervennlighet -> Kostnad for kunde -> Kostnad av implementering*
- Oppdragsgiver klargjorde for at vår målgruppe ikke skal ha tilgang på helseopplysninger, og i utgangspunktet bare er en nivå 3 sikkerhetskategori. Med tanke på dette vil sikkerhetskravet gå ned.
- Oppdragsgiver mente at fysisk sikkerhet kanskje kan være vanskelig, men det kan også passord.
- Oppdragsgiver var positiv til biometriske løsninger som ansiktsgjenkjenning og fingeravtrykk.
- Oppdragsgiver var også positiv til en kombinasjon av biometri og fysisk nøk-

kel var tilstrekkelig for en passord-løs innloggingsløsning.

- Oppdragsgiver informerte om at Halden kommune var mest "moden" med tanke på målgruppen, og at det er to eller tre sluttbrukere som snart skal ta i bruk Omhu appen.
- Oppdragsgiver informerte om andre kunder i lillehammer omerådet, og mente at det var realistisk å ta de første to rundene med undersøkelser der, og den siste i Halden kommune.

N.3.3 Møte med oppdragsgiver 3

Detaljer

Dato:
Tid: kl10:30-11:00
Lokasjon: Digitalt, Teams
Oppmøte: Jørgen, Raphael, Sara, Phillip Weisser, Jan Egil Jægersborg, Ingvild Melbye
Loggfører: Raphael

Agenda for møtet

- Anmode om bekreftelse på gjennomføring av testing med YubiKey.
- Be om statistikk angående nåværende antall brukere innen målgruppen og estimert vekst i fremtiden, inkludert antall daglige innloggingsforsøk.
- Utforske muligheten for å gjennomføre kvalitative undersøkelser med eldre, ettersom dette kan være enklere å gjennomføre.
- Drøfte oppdragsgivers preferanse mellom en menneskeorientert og en teknisk orientert tilnærming.
- Ta opp muligheten for å prioritere del 1 over del 2 av oppgaven.

Resultater

- Oppdragsgiver opplyste om omtrent 250 brukere per dags dato, med forventet vekst til 10 000 brukere innen de neste fire årene.
- Det ble estimert at det er omtrent 2 autentiseringsforsøk per dag.
- Oppdragsgiver foretrekker bruk av grafer og tall, og er positiv til kvantifisering av egenskaper.
- Det ble gitt tillatelse til å starte kvalitative intervjuer med eldre, da oppdragsgiver er enig i at eldre representerer et sammenlignbart segment av målgruppen. Fokus bør ligge på å gjøre appen tilgjengelig og intuitiv for brukerne.
- Målgruppen har generelt en grunnleggende teknologisk kompetanse på linje med resten av befolkningen, spesielt blant de yngre brukerne som ofte har mer erfaring enn hjemmehjelpene.
- Møtet i morgen med Halden kommune vil fokusere på rammebetingelser og lignende, og vil vare fra kl. 12:00 til 13:30. Møtet vil holdes via Google Meet.

N.3.4 Møte med oppdragsgiver 4

Detaljer

Dato:
Tid: kl10:30-11:00
Lokasjon: Digitalt via Teams
Oppmøte: Sara, Raphael, Jørgen, Philip Weisser
Loggfører: Sara

Møteplan

- Gjennomgang av demo og hvordan vi har løst ulike problemer knyttet til denne.
- Planlegge brukertester i nærområdet angående wireframe.
- Få kontaktinformasjon til en ekstern bedrift som har erfaring i å hjelpe målgruppa med å sette opp digitale tjenester.

Resultater

- Oppdragsgiver var fornøgd med demoen.
- Brukertester i nærområdet skal finne sted i løpet av uke 12.
- Fikk kontaktinformasjon til fagfolk som det er aktuelt å ha et intervju med angående del 1, autentiseringsfaktorer.
- Weisser nevnte også muligheten for at en journalist ønsker å ha et intervju i nær fremtid. Dette pga Halden kommune's store utvikling de siste åra mtp. BPA, og en journalist fra naku.no ønsker å skrive en sak om Halden. Kan derfor hende vi blir kontaktet for et intervju angående dette.

N.3.5 Møte med oppdragsgiver 5

Detaljer

Dato:
Tid: kl10:30-11:00
Lokasjon: Digitalt via Teams
Oppmøte: Sara, Raphael, Jørgen, Philip Weisser
Loggfører: Sara

Møteplan

- Har startet på del 2 av prosjektet, MVP pasientmodul
- Gå gjennom første utkast, del 2 wireframe
- Få oppklaring i timeplanen skal utformes: hvordan jobber de ansatte?
- Få oppklaring i hvorvidt de ansatte rullerer på brukerene, eller om det er faste ansatte på faste brukere.
- Skal brukerene ha tilgang til å legge inn aktiviteter?
- Er aktivitetene felles for flere brukere?

Resultater

- Ansatte kan være hos brukere i noen timer av gangen, men de kan også komme og være hos en bruker en hel dag. Dette vil variere.
- Når en bedrift ansetter en person, vil hen hovedsakelig få opplæring i en eller noen få brukere. Det vil gradvis rullere, slik at en ansatt ikke er fast på en bruker.
- Det er ønskelig at brukerene skal kunne legge inn aktiviteter selv. Problemet er at kunder i offentlig sektor ikke er "modne" for dette ennå. Derfor bør kundene/kommunene/tjenestegiverene ha mulighet til å kunne ha kontroll på tilgangsstyringen selv, og dermed begrense handlingsrommet til brukeren. Visjonen til BPA'er er at brukerene skal kunne legge til aktiviteter selv, men det er vanskelig å implementere dette på nåværende tidspunkt.
- Mange tjenestegivere/kommuner kan arrangere aktiviteter som er felles for flere brukere. Ideen vår med å legge til en "offentlig aktivitet" funksjon kan dermed være aktuell, men her er personvern viktig. Brukere skal IKKE kunne se hvilke andre brukere som får tjenester osv.
- Det er verdt å merke seg at personvern gjør at å implementere en funksjon for at brukeren kan se timeplanen til ansatte, kan være problematisk. Brukere skal blant annet ikke kunne se hva den ansatte gjør og hvor hen er når hen ikke er hos aktuelle bruker.

- Oppdragsgiver var positiv til chat-funksjon mellom brukere og ansatte, men dette er også noe som offentlig sektor sannsynligvis ikke er modne til ennå.

N.3.6 Møte med oppdragsgiver 6

Detaljer

Dato:
Tid: kl12:30-13:00
Lokasjon: Digitalt via Teams
Oppmøte: Sara, Raphael, Jørgen, Ingvild, Jan Egil
Loggfører: Sara

Møteplan

- Førsteutkast av grensesnittet er ferdig.
- Demo for autentisering er ferdig.
- Vi holder på å forbedre brukergrensesnittet før besøket til Halden neste uke.
- Vi har hatt en brukertest, og fått en del negative tilbakemeldinger. Skal ha en eller noen få tester til før Halden.

Resultater

- Gikk gjennom fremdriften for Weisstech, gikk gjennom resultater fra brukertest del 2, og forbedringen av nettsiden(MVP'en) deretter.
- Aktivitetsmaler i MVP kan være veldig variert fra person til person. Maler vi kan legge inn som er ganske generelle er f. eks. måltidssituasjoner, fysisk aktivitet, somatisk tilrettelegging.

N.3.7 Møte med oppdragsgiver 7

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Digitalt via Teams
Oppmøte: Sara, Raphael, Jørgen, Ingvild, Jan Egil
Loggfører: Sara

Møteplan

- Prate om turen til halden kommune
    a. Vi testet både inloggingsløsningen og pasient-modulen
    b. Det kom frem en del problemer som vi ikke hadde forutsett, mye nyttig data.
    c. <fjernet> og <fjernet> var kjempeflinke, det var veldig gøy og møte de.
- Spørsmål om features:
    a. Konseptet av maler var vanskelig for de å forstå. Diskuter om det er noe som skal fjernes.
    b. Lese og skrivevansker var langt større en vi trodde. Er det en statistikk på hvor mange av sluttbrukerene som sliter med dette? Eventuelt er det rimelig å si at en signifikant del av brukergruppen har problemer med dette?
    c. Det virker litt tvilsomt at de vil kunne klare å bruke appen uten grundig opplæring eller tilgjengelighet for hjelp.
    d. Sikkerhetsnøkkelen virker lovende.
- Veien videre nå:
    a. Nå er vi i utgangspunktet ferdig med utvikling og datainnsamling, så nå er det rapportskriving.

Resultater

- Vi kan ta som utgangspunkt, i at det er like vanlig som uvanlig å ha lese- og skrivevansker i målgruppa.
- Omhu har ikke lov til å samle inn brukerstatistikk, så er vanskelig for de å svare på hvor stor andel som har kognitive vansker. Pga. korleis data blir lagra på servere, så har dei ikke lov til å drive med tracking av brukerene

sine. Altså se på hvilke funkjsoner de bruker mest osv.
- Funfact: Omhu har 800 brukere per dags dato.
- Maler trenger ikke å være en del av pasientmodulen, men kan være en del av modulen til de ansatte.

N.4 Veiledermøter

N.4.1 Veiledermøte 1

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Sara, Ernst, Eirik
Loggfører: Raphael

Møteplan

- Spørre om en demo er forventet for del 1 av oppgaven.
- Spørre om prosjekt er bedre gjennomført parallelt eller sekvensielt.
- Diskutere standardavtale.
- Spørre om forslag til tidligre oppgaver å lese.

Resultater

- Ernst og Eirik informerte om at de gjerne ønsket å delta på det første møter med oppdragsgiver. Vi sender mail til oppdragsgiver for å informere om dette.
- Vi fikk svar på diverse spørsmål:
    - Når det gjelder arbeidsflyt, bør vi ikke låse oss til en streng sekvensiell rekkefølge, men heller flytte noen ressurser over på neste oppgave når en oppgave kommer i gang. Det viktigste er og ha oversikt og slingringsrom.
    - Arbeidsavtalen består kun av standardavtalen, ingen ting ekstra er krevet.
    - Digitale underskrifter vil være tilstrekkelig for standardavtalen.
    - Vi burde unngå og søke om ressurser fra NTNU(utenom SkyHigh) da det medfører store mengder papirarbeid. Heller høre med oppgavegiver om vi trenger noe.
    - Den tidligre bachelorgraden “Sikkerhet i mobilinfrastruktur/autentisering” er anbefalt å lese gjennom da den har mange av de samme temaene som vår egen oppgave.

N.4.2 Veiledermøte 2

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, T432
Oppmøte: Sara, Raphael, Jørgen, Ernst
Loggfører: Sara

Møteplan

- Repetisjon av møte med oppdragsgiver
- Vising av gruppemål
- Spørsmål om skrivemetode på rapporter
- Spørsmål om kontakt med andre personer av interesse for prosjektet
- Spørsmål om Gantt skjemaet, hvor detaljert skal det være? Usikre datoer.

Resultater

- Vi repeterte det viktigeste fra møtet med oppdragsgiver til veileder.
- Veileder er fornøgd med prosjektplanen så langt. Han leste ikke gjennom planen, men fikk se innholdsfortegnelsen og grovt over hele, han så ikke noe tydelig mangelfult i prosjektplanen.
- Å kontakte andre personer av faglig interesse til prosjektet er absolutt innafor.
- Gant skjemaet trenger ikke være kjempenøyaktig, alt vi gjør i prosjektplanen(inkludert Gant) er egentlig for våres egen del. Gant skjemaet er derfor hovedsakelig for at vi skal ha en viss kontroll selv på forhånd.

N.4.3 Veiledermøte 3

Detaljer

Dato:
Tid: kl. 10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Sara, Raphael, Jørgen, Ernst, Erik
Loggfører: Raphael

Møteplan

- Gjennomgang av det vi har gjort frem til nå. Presentasjon av våre identifiserte løsninger.
- Få veileder til å se over strukturen av prosjektet og Gantt-diagram.
- Spørre om det er lov til å referere til kommersielle produkter.
- Tilbakemelding på prosjektplan.
- Spørsmål om spørreskjema i henhold til persondata og lovverk.

Resultater

- Erik spesifiserte at vi bør bruke nummererte lister for våre prosjektmål slik at sensurer kan referere til spesifikke mål. Et prosjekt dømmes ofte ut fra hvor tydelige mål som er satt i begynnelsen, og hvor godt prosjektet oppfyller disse målene.
- Når det gjelder QR-autentiseringen vi har i konseptfasen, har gruppen fått anbefalt å kontakte "Bian Yamg", en professor ved NTNU som er spesialist innenfor autentisering og leder av forskergruppen innen e-helse. Det vil være relevant å spørre om hvor realistisk QR-kortkonseptet ville vært å innføre.
- Veileder anbefaler å kontakte "Frode Volden" for anbefalinger om brukerundersøkelser med tanke på personvern.
- Veileder tipset også om at QR-koder brukes i autentisering for Sveriges ekvivalent til BankID; dette kan være verdt å undersøke.

N.4.4 Veiledermøte 4

Detaljer

Dato:
Tid: kl. 10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Sara, Raphael, Jørgen, Ernst
Loggfører: Raphael

Møteplan

- Gjennomgang av møte med oppdragsgiver.
- Spør om input på problemstilling med todelt oppgave.
- Dele planer for uken og arbeidsfremgang fra forrige uke.

Resultater

- Vi tok en gjennomgang av møte med oppdragsgiver, der vi blandt annet informerte om oppdragsgivers likegyldighet til å ha en rød tråd mellom del 1 og 2 av oppgaven. Vi diskuterte med Ernst, og kom frem til at en sammenslåing av demo'ene for del 1 og 2, samt litt skriving om brukervennlig design i demo til del 1 vil være tilstrekkelig rød tråd for oppgaven. Ernst syntes også det var oppklarende å vite at målgruppen ikke enda hadde mottatt produktet, og at bacheloroppgaven er et forstadie til en utvidelse av Omhus brukerbase.
- Gruppen informerte om at vi var klare til å begynne med utvikling av DEMO, og at vi hadde bestemt oss for autentiseringsmetoder. Veileder ga utrykk for at vi hadde bestemt tidlig, og at vi muligens kunne kjøre ekstra analyser og sammenligninger i rapporten før vi bestete oss helt. Erst fortalte at vi burde drøfte og diskutere rundt spørsmål relevant til valg av autentisering, slik at vi og oppdragsgiver kunne gjøre et informert valg om autentiseringsmetode til demo og Omhu. Dette inkluderer også "risikomatriser", der en kan se en oversikt over hvilken form for autentisering som gjør hva best.
- Vi pratet med veilder om kilder, der vi ble informert om at mengden kilder vi har til nå, som gruppemedlemmene opplevde som mye, var omtrentlig den tettheten med kilder som er forventet.

N.4.5 Veiledermøte 5

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Sara, Raphael, Jørgen, Ernst, Eirik
Loggfører: Raphael

Møteplan

- Spørre om kvantifisering av egenskaper

Resultater

- Veileder mente at vår løsninger for kvantifisering av egenskaper var et gyldig konsept, men at det var utrolig viktig at vi vurderte egenskapene ut i fra andres for-eksisterende vurdering. Bruk av kilder er ekstremt viktig her. De mente at dette systemet kunne bli veldig bra hvis kildene var tilstrekkelige, men at det for øyeblikket virket litt "omtrentlig"og uvitenskapelig. Kildene trenger ikke nødvendigvis å være en helt 1/1 sammenligning, men må være grunnlagt i fakta fra trovedrige kilder. F.eks android sine tall på sikkerhet var bra.
- Skalaen vi bruker til vurdering sier implisitt noe om nøyaktighetsnivået på vurdringen vi gir. Om en har 1/100 betyr det at vi kan vurdere dette med høy sikkerhet. En 1/3 sier at det vanskelig å få en vurdering med større nøyaktighet.

N.4.6 Ekstramøte med Erik

Detaljer

Dato:
Tid: kl10:30-10:50
Lokasjon: Gjøvik Campus, Topaz, Erik sitt kontor
Oppmøte: Sara, Raphael, Erik
Loggfører: Sara

Møteplan

- Få avklart forvirring rundt oppgaven grunnet møte med Bian Yang dagen før.

Resultater

- Erik mente at Yang hadde et poeng, men at det vi har gjort frem til nå på ingen måte er dårlig arbeid eller feil å gjøre
- Erik mente at det kan være mulig å gjøre brukertester, eller å kun planlegge brukertester og ikke gjennomføre dem. Oppdragsgiver vil få god bruk for en godt planlagt brukertest, som de kan gjennomføre selv i en senere anledning.
- Det er også mulig å droppe del 2 av oppgaven, og kun fokusere på del 1, dersom vi ser at del 1 er alt for krevende å gjøre som kun halve oppgaven.
- Erik mente vi nå må fokusere på å finne relevant litteratur som støtter opp under det vi allerede har gjort med kvantitative verdier.
- Dersom vi finner ut at vi må gjennomføre brukertester for del 1 av oppgava, og bestemmer oss for at det er lettere å bruke f. eks. eldre mennesker i stedet for folk fra målgruppa, så må dette godkjennes fra oppdragsgiver, ettersom oppdragsgiver har større kompetanse på om dette går an å sammenligne. Vi må uansett lese oss opp på kvalitative brukertester, dersom vi ønsker å gjennomfører dette. Se logg fra første møte med Bian Yang for mer info.
- Erik hjalp oss å finne litteratur, f. eks. denne: Security and Usability of a Personalized User Authentication Paradigm: Insights from a Longitudinal Study with Three Healthcare Organizations. Link: https://dl.acm.org/doi/10.1145/3564610
- Han anbefalte publikasjoner fra ACM og IEEE. Se etter ACM tranactions, som betyr at artikkelen i det minste har blitt delvis peer reviewed. Små publikasjoner i disse organisasjonene som ikke har blitt transactioned", er ikke alltid til å stole på.

N.4.7 Veiledermøte 6

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Sara, Ernst, Eirik
Loggfører: Raphael

Møteplan

- Gå gjennom brukerundersøkelse, få tilbakemelding

Resultater

- Vi fikk tilbakemelding på brukerundersøkelsen:
  a. Legge til ikoner til lapper som gjør det enklere å rangere de
  b. Ha powerpoint som viser planen for brukerundersøkelsen
  c. Unngå bruk av ord gi opp", senk terskelen
  d. Kort ned introduksjon
  e. Ikke bruk fagutrykk, datanøkkel"i stedet for yubikey
  f. Vurder om vi skal la brukeren fortsette dersom hen gjør feil, eller avbryte.

N.4.8 Veiledermøte 7

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Sara, Ernst, Eirik
Loggfører: Sara

Møteplan

- Vise frem ferdig demo
- Diskutere rundt starten på del 2, MVP.

Resultater

- Veilederne mente demoen var bra gjennomført.
- Teorien rundt del 1, demo og teori rundt autentiseringsmetoder, kommer til å bli den viktigste teoretiske delen i rapporten. Det er dermed essensielt at vi drøfter godt rundt dette med valg vi har gjort i brukerundersøkelser og utvikling av demo. For eks. valg av design av brukegrensesnitt, kodespråk, og teori rundt brukerundersøkelser. Viktigste å skrive om backend vil være hvordan vi har konfigurert webauthn.

N.4.9 Veiledermøte 8

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Sara, Ernst, Eirik
Loggfører: Sara

Møteplan

- Laget demo for del 2, prosessert en del av data for brukertester.
- Diskutere innlevering av del 1, måten vi har satt opp rapporten på. Skal vi fylle inn delkappitteler som er relevante til den 1? Fortsatt en del brukertesting vi ikke har gjort.
- Hvordan gjør vi det med kodedelen som vi har gjort? Hvor passer det inn i rapporten?

Resultater

- Kan bruke "vi" i kontekst av dialog med leseren
- Husk tilbakekall til andre deler av rapporten
- Ha utviklings kapittel seperat fra metode kapittel. Gjerne ett eget kapittel for hver demo. Disse kapitlene kan gjerne komme mellom "metode" og "diskusjon".
- Metode-kapittel skal si hvordan problemet skal løses

N.4.10 Veiledermøte 9

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Ernst, Eirik
Loggfører: Sara

Møteplan

- Snakk om forberedelser til å brukerteste personer i målgruppa i Halden
- Hvordan skal vi begrunne endringer vi gjør i prototypen etter brukertester?
- Vi har dårlig tid til å bli ferdig med pasientmodulen, del 2. Hva tenker Ernst og Erik om dette?

Resultater

- For å begrunne endringer i prototypene i rapporten, skriv; dette har vi klart å påvise i brukertesten at er for vanskelig, og vi finner det i litteraturen at det er for vanskelig, så derfor forandra vi det.
- Skriv i rapporten dersom vi ser det er noen feil vi gjorde i brukertestingen, som er fort gjort for andre å gjøre feil senere.
- Erik mener vi ikke skal lage et komplett prototype opplegg til del 2, men heller peke"i rikitg retning.
- Ernst sier at design kan være mye forskjellig, og det trenger ikke bety at vi skal lage en skikkelig nettside. Design i databaser f. eks. har ingen utseende.
- Erik seier vi skal snakke med oppdragsgiver og si at vi har dårlig tid til å få del 2 til å bli perfekt". Spør hva oppdragsgiver prioriterer å få svar på.

N.4.11 Veiledermøte 10

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Ernst, Eirik
Loggfører: Jørgen

Møteplan

- Gå igjennom Halden brukertest
- Hva vi skal gjøre videre

Resultater

- Begrunne resultat og data i rapporten.
- Ntnu open dysleksi og teknologi.
- Spørre om fordeling av hvem har skrivevansker, downsyndrom og andre.

N.4.12 Veiledermøte 11

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Sara, Ernst, Eirik
Loggfører: Sara

Møteplan

- Snakke om ferdigstille Omhu pasientmodul, ut i fra resultatene fra brukertesten

Resultater

- Alt er bra med pasientmodul, nå må vi fokusere på rapport.

N.4.13 Veiledermøte 12

Detaljer

Dato:
Tid: kl10:00-10:30
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Sara, Ernst, Eirik
Loggfører: Sara

Møteplan

- Fullt fokus på rapportskriving

Resultater

- Vi skal levere et rapportutkast til Ernst og Erik lørdag kveld, 4. mai.
- Dropper veiledermøte på torsdag, og tar det mandag 6. mai i staden for, kl. 11:30.
- I førsteutkastet skal kapittel 1 og 2 være polert.
- Konklusjonen kan være ferdig før innmaten, tenk smidig utvikling, rapporten trenger ikke å bli skrevet i fossefallsmetoden. Erik meiner at begynnelsen og slutten på rapporten er det viktigeste.
- Enkelte deler fra forplanen kan vi kopiere rett inn i hovedrapporten.

N.4.14 Veiledermøte 13

Detaljer

Dato:
Tid: kl11:30-12:00
Lokasjon: Gjøvik Campus, Topaz T540
Oppmøte: Jørgen, Raphael, Sara, Ernst, Eirik
Loggfører: Sara

Møteplan

- Sendte det vi har skrevet i rapporten frem til nå, på lørdag 4. mai, til Ernst og Erik. Kun kapittel 1, 2 og 3 var noenlunde ferdigstilt, og det er derfor kun dette som vi fikk tilbakemelding på nå. Gikk gjennom tilbakemeldingene i løpet av møtet.

Resultater

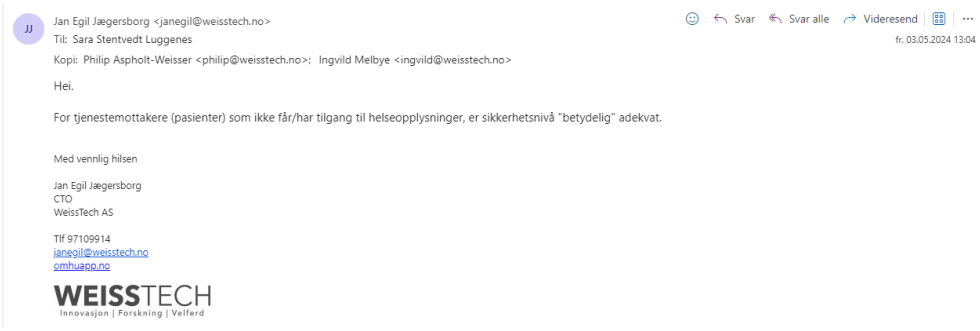
- Bildene vi har limt inn i rapporten fra andre kilder, kan vi lage selv med vector grafikk og skrive "inspirert av den og den kilden". Dette vil gjøre rapporten finere.
- Gjennom metode og nedover i rapporten er sikkerhetsnøkkel ofte nevnt. Det blir likevel aldri forklart hva det er, og det kunne absolutt bli nevnt ganske langt oppe i teorien. Nevn det som "noe man har".
- Kilder kan skrivest så tidlig som mulig i avsnittet, selv om setninger som kommer etter kilden, også er fra den samme kilden.
- Noe rart latex greier har skjedd i bibliografien, fiks.
- Mellom en kapittel-overskrift og en delkapittel-overskrift, skriv innledningstekster som ikke er selvforklarende mtp. kapittelnavnet.
- Description liste i latex bør vurderes.
- Omrokker målene, prosessmål er mindre viktig enn resultatmål.
- Hva betyr IDporten? Og biometri?
- I metodekapittelet kan man skrive i nåtid, mens i resultat og konklusjon kan man skrive i fortid.
- Ellers er det en del setninger som med fordel kan omformulerest osv.

Vedlegg O

Epost-kommunikasjon

Vedlegg P

Epost fra oppdragsgiver



JJ

Jan Egil Jægersborg <janegil@weisstech.no>

Til: Sara Stentvedt Luggenes

Kopi: Philip Aspholt-Weisser <philip@weisstech.no>; Ingvild Melbye <ingvild@weisstech.no>

Svar | Svar alle | Videresend

fr. 03.05.2024 13:04

Hei.

For tjenestemottakere (pasienter) som ikke får/har tilgang til helseopplysninger, er sikkerhetsnivå "betydelig" adekvat.

Med vennlig hilsen

Jan Egil Jægersborg
CTO
WeissTech AS

Tlf 97109914
janegil@weisstech.no
omhuapp.no

WEISSTECH
Innovasjon | Forskning | Velferd

Vedlegg Q

Standardavtale

NTNU

Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett
Er den rett som den som skaper et åndsverk har til å fremstille eksemplar av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater
Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater
Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn
Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring
Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt for informasjonssikkerhet og kommunikasjonsteknologi
Veileder ved NTNU: Ernst Gunnar Gran e-post og tlf. ernst.g.gran@ntnu.no 99644916
Veileder ved NTNU: Erik Hjelmås e-post og tlf. erik.hjelmas@ntnu.no 93034446
Ekstern virksomhet: WeissTech AS Ekstern virksomhet sin kontaktperson, e-post og tlf.: Philip Andreas Aspholt-Weisser, philip@weisstech.no 41484552
Student: Jørgen Teigen Fødselsdato: 260402
Student: Sara Stentvedt Luggenes Fødselsdato: 150499
Student: Raphael Storm Larsen Fødselsdato: 110602

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 08.01.24
Sluttdato: 21.05.24

Oppgavens arbeidstittel: Tilpasning av modul for klinisk egenrapportering innen tilrettelagte tjenester og psykiatri

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:

- Kan få støtte til å kjøpe inn og teste eventuelle innloggings-alternativer
- Ved reising for å møte sluttbrukere eller reising av andre grunner, skal oppdragsgiver støtte kostnader til transport og eventuelt hotell.
- Ved behov for større innkjøp, skal det diskuteres med oppdragsgiver på forhånd.

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven[1]. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

[1] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

Alternativ a) (sett kryss) Hovedregel

X	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i

denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss		Sett dato
	ett år	
	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:
Veileder ved NTNU: Dato: 30.01.2024
Ekstern virksomhet: WeissTech AS Dato: 26.01.24 Philip Andreas Aspholt-Weisser
Student: Jørgen Teigen Dato: 29.01.24
Student: Sara S. Huggunes Dato: 29.01.24
Student: RAPHAEL STORM LARSEN Dato: 29.01.24

Vedlegg R

Oppgavebeskrivelse av bacheloroppgaven

Oppgave 40 BPROG, BIDATA, DIGSEC 2-4 stk

Oppgavetittel: Tilpasning av modul for klinisk egenrapportering innen tilrettelagte tjenester og psykiatri

Bedrift:	WeissTech AS
Kontaktperson:	Philip Andreas Aspholt-Weisser
E-post:	philip@weisstech.no
Telefon:	41484552
Lokasjon:	Valdres

Beskrivelse av oppgaven

WeissTech AS er et innovativt teknologiselskap fra Valdres. Vi spesialiserer oss på forenkling av komplekse helse- og omsorgstjenester og har på få år knyttet til oss mange spennende kunder og samarbeidspartnere i dette oppdraget.

Vi leverer Omhu, et fag og journalsystem som leveres som en Web-applikasjon. Kundene logger inn gjennom nettleser på telefon, pc eller tablett. All data lagres kryptert i skyen(Azure), og innlogging skjer via ID-porten. Hver kundene har sin egen database med egen admin-side hvor kundens egne superbrukere kan tilpasse Omhu etter virksomhets behov.

I Omhu behandler vi svært personsensitiv informasjon.

I systemet har vi lagt opp til en egen side hvor tjenestemottakerne/pasientene kan logge inn selv for å få oversikt over planlagte tjenester, samt være deltakende i egen behandling via selvmonitorering og egenrapportering.

Mange av pasientene har ikke BankID. Dette hindrer de i å komme inn på sin egen side. Andre sliter med å lære seg å manøvrere i systemet.

Dette ønsker vi å gjøre noe med. Og tenker det kan være en spennende oppgave for bachelorstudentene på NTNU

Oppgave:

Del 1.

Kartlegge og skissere alternative innloggingsløsninger som i større grad tilgjengeliggjør Omhu for pasientene samtidig som vi ivaretar personvernet på en tilfredsstillende måte. Samt begrunne løsningsforslag på innlogging.

Del 2.

Kartlegge og designe en MVP av en pasientmodul som er lett og venne seg til, intuitiv og enkel å benytte for pasienter med forskjellige forutsetninger for å nytte seg av teknologien vi tilbyr.

Oppgave 40 BPROG, BIDATA, DIGSEC 2-4 stk

Vi ser for oss at dette kan være et samarbeidsprosjekt på tvers av linjene. der man kan bake inn momenter fra både spilldesign, datasikkerhet og interaksjonsdesign i prosjektet.

WeissTech AS har med seg mange innovative kunder hvorav flere er åpne for å bidra i prosjektet.

Studentene som eventuelt kan tenke seg å ha dette som bacheloroppgave vil få et unikt innblikk i komplekse helse og omsorgstjenester. Og får gjennom dette anledning til å bidra til bedre tjenester for de som kanskje trenger det mest.

Vi kommer og presenterer oppgaveforslaget 02.11.23 dersom forslaget blir vurdert relevant for studentene.

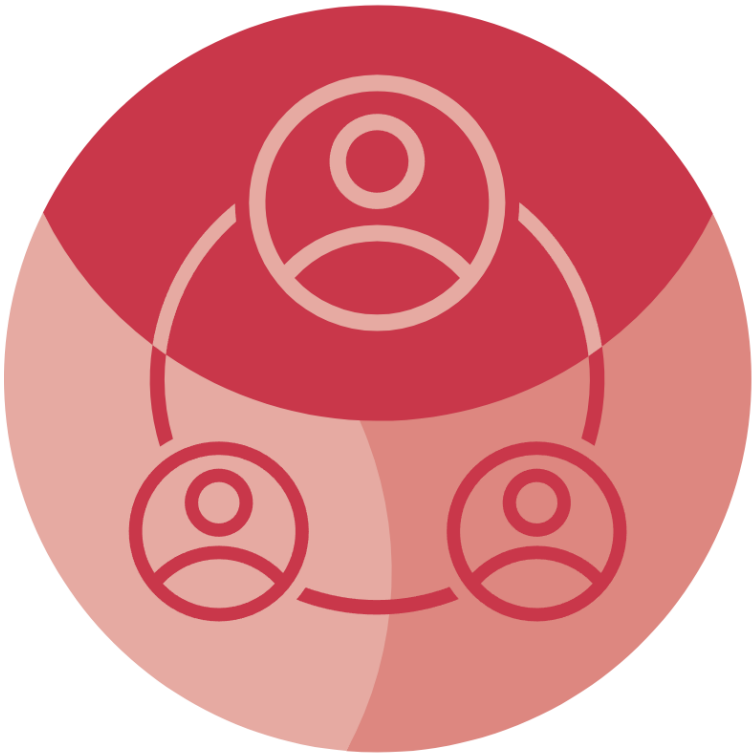
Vedlegg S

Prosjektplan

Prosjektplan

Bachelor-oppgave BDIGSEC V2024

Tilpasning av modul for klinisk egenrapportering



Gruppe 120

Jørgen Teigen	561475
Raphael Storm Larsen	561419
Sara Stentvedt Luggenes	522471

NTNU i sammarbeid med WEISSTECH Innovasjon | Forskning | Velferd

Innhold

1 Prosjektmål og rammer

1.1 Bakgrunn

Omhu er et digitalt fag- og journalsystem innenfor helse- og omsorgsektoren, levert av WeissTech AS, et teknologifirma lokalisert i Valdres-regionen. Tjenesten har blitt lansert hos flere kunder i helsesektoren, og er i kontinuerlig vekst.

Omhu blir brukt av forskjellige målgrupper med ulike forutsetninger og behov. Tjenesten har som mål å gjøre det enklere for klienter å holde seg oppdatert og involvert i statuser og beslutninger for sin egen behandling, og dermed gir klientene en autonomi som tidligere ikke har vært mulig.

For å logge inn på Omhu's klientside, kreves det per dags dato BankID. Ettersom mange brukere ikke har egen BankID, får de heller ikke tilgang til å logge inn og bruke funksjonene som tjenesten tilbyr. Mange brukere synes dessuten det er vanskelig å manøvrere i systemet.

Vår jobb er todelt å kartlegge og skissere alternative innloggingsløsninger til BankID, slik at personer uten BankID også kan ta i bruk Omhu. Vi skal også designe en MVP, "Minimum Viable Product", av en klientmodul som er lett å venne seg til, intuitiv og enkel å benytte for klienter med forskjellige forutsetninger for å benytte teknologien som WeissTech tilbyr.

1.2 Prosjektmål

Prosessmål

1. Holde en effektiv og god arbeidsflyt innad i gruppen gjennom hele prosjektet
2. Ha en løpende og tett kommunikasjon med oppdragsgiver og veiledere
3. Jobbe etter Scrum metodikken
4. Dokumentere og loggføre fremgangen av arbeid

Effektmål

1. Mer fornøyde sluttbrukere av Omhu
2. Det blir enklere for sluttbrukerene å følge med på og gi tilbakemelding på deres behandling og aktiviteter
3. En mer oversiktlig hverdag for sluttbrukere av Omhu

Resultatmål

1. Kartlegge og skissere flere alternative innloggingsløsninger
2. Utvikle en demo som et konseptbevis for et potensielt autentiseringsalternativ til Omhu
3. Utvikle en interaktiv demo for nytt brukergrensesnitt til Omhu
4. Oppnå en målbar forbedring av brukervennligheten til Omhu's grafiske brukergrensesnitt for målgruppen

Læringsmål

1. Lære mer om brukervennlig design
2. Dokumentere og formidle resultatene av brukertester for å forbedre sluttproduktet
3. Gjøre oss kjent med prosessene rundt det å utvikle et produkt for en kunde
4. Bli kjent med alternative, sikre innloggingsmuligheter som ikke basserer seg på tilgang til BankID
5. Lære mer om standarder relatert til autentisering og brukersentrert design

1.3 Rammer

Rammene for prosjektet er som følger:

- Gruppen skal kartlegge metoder for sikker autentisering som alternativ til IDportalen.
- Gruppen skal designe et nytt brukergrensesnitt for Omhus dashbord og arbeidsplan-fane.

Som det fremgår av rammene, er oppdraget fra Weisstech et svært åpent prosjekt, der kravene for minste akseptable løsning er relativt beskjedne. Det er derfor store muligheter for å utvide oppgaven i den retningen vi selv ønsker. I kapittel 2.2 gjennomgås gruppens ønsker for hvordan prosjektet skal fullføres, og i kapittel 2.3 defineres interne avgrensninger satt av gruppen. Risikoen for å falle under minstekravene til prosjektet er identifisert som en kategori 3-risiko (se side 7). Selv om risikoen for scope-creep er mer alvorlig, er det fortsatt viktig å være oppmerksom på at oppgaven ikke bør legges for lavt, selv om det skulle bli knapt med ressurser.

2 Tema og oppgave

2.1 Oppgavebeskrivelse

Oppgaven fra Weisstech AS er som følgende:

> **Del 1.** Kartlegge og skissere alternative innloggingsløsninger som i større grad tilgjengeliggjør Omhu for pasientene samtidig som vi ivaretar personvernet på en tilfredsstillende måte. Samt begrunne løsningsforslag på innlogging[1].
>
> **Del 2.** Kartlegge og designe en MVP av en pasientmodul som er lett og venne seg til, intuitiv og enkel å benytte for pasienter med forskjellige forutsetninger for å nytte seg av teknologien vi tilbyr[1].

2.2 Problemområde

Oppgaven gitt av Weisstech AS går ut på å kartlegge og drøfte mulige løsninger for problemstillinger knyttet til brukerinteraksjon og sikkerhet med Omhu. WeissTech ønsker å forbedre brukervennligheten i både innloggingsautentisering og webgrensesnittet til applikasjonen. Disse to prosjekt-delene er forskjellige, men det går en "rød tråd" gjennom begge med utgangspunkt i brukervennlighet. Dette vil være hovedfokuset vårt, i tillegg til sikkerhet.

2.2.1 Del 1

Omhu er en web-applikasjon som lagrer diverse typer helseinformasjon for sluttbrukere, noe som gjør konsekvensene av dårlig sikkerhet svært kritiske. Sikkerhet og personvern har derfor høy prioritet i utviklingen av applikasjonen. Av sikkerhetshensyn benytter Omhu IDporten for innlogging. Denne løsningen er sikker, men det oppstår utfordringer ettersom deler av brukerbasen til Omhu ikke har tilgang til BankID, Commfides eller BuypassID, de faktorene som IDporten bruker for å identifisere og autentisere brukere. Mange sluttbrukere av Omhu har en lettere kognitiv nedsettelse, noe som ofte betyr at de ikke har myndighet til å ha BankID. Utfordringen i del 1 av oppgaven ligger derfor i å finne et alternativ til BankID som fortsatt tilfredsstiller sikkerhetsbehovene for en applikasjon som lagrer sensitive helseopplysninger om sine brukere.

Med dette som utgangspunkt skal vi undersøke og drøfte alternative innloggingsløsninger og presentere disse for oppdragsgiveren med en demo. Kjernen i denne delen av oppgaven er å identifisere et godt utvalg potensielle løsninger og vurdere fordeler, ulemper, praktikalitet og kostnader ved hver av dem. ROS-analyse skal gjennomføres. Dette er for å gi oppdragsgiveren en oversikt over eksisterende løsninger, slik at de kan ta informerte beslutninger videre i applikasjonens utvikling. Deretter vil gruppen gå i dybden på de løsningene som virker lovende for formålet og utforske disse i større detalj. I den siste fasen av oppgaven, hvis det er tilstrekkelige ressurser, vil gruppen anskaffe det mest lovende produktet eller programvaren, som deretter implementeres i en demo som kan presenteres for oppdragsgiver som et "proof of concept".

2.2.2 Del 2

Den andre delen av oppgaven handler om å utvikle en forbedret versjon av Omhus frontend som utviklerne kan bruke som inspirasjon for videreutvikling av Omhu. Grensesnittet som brukes i dag, har alle funksjoner implementert, men kan oppleves som vanskelig å navigere i for sluttbrukere. Hovedfokuset for denne delen av oppgaven er å utvikle en MVP med forbedret brukervennlighet i forhold til det eksisterende grensesnittet.

Det grunnleggende designet kan utføres med skisser og wireframes som et "proof of concept", men utover prosjektet er det ønskelig at gruppen produserer en fungerende interaktiv demo av løsningen som en web-applikasjon, separat fra Omhus faktiske applikasjon. Koden i denne demoen vil ikke være direkte relevant for oppgaven, da den kun skal brukes som inspirasjon for Weisstech, og ikke knyttes direkte til Omhu på noen måte. Denne demoen kan også integreres i samme plattform som demo for autentisering.

2.2.3 Annet

Vi skal gjennomføre brukerundersøkelser i del 2. Her vil vi møte brukere fra målgruppen, og gjennomføre klassisk brukertesting for å undersøke egenskaper ved nettsiden som kan forbedres. I del 1 er det også ønskelig å sende ut spørreskjema, for å undersøke hvilken autentiseringsløsninger som kan være aktuelt. Dette er usikkert om det lar seg gjøre, ettersom spørreskjema stiller krav til personvern og anonymitet. Det er likevel noe som er ønskelig å gjennomføre tidlig i prosjektet.

2.3 Avgrensing

Oppdraget for denne bacheloroppgaven har klart definerte mål, men gir gruppen betydelig frihet når det gjelder hvordan og i hvilken grad av kompleksitet vi ønsker å utføre prosjektet. Gruppen har identifisert "scope-creep" som en kategori 4-risiko (se side 6), noe som betyr at det kan være svært skadelig for prosjektet hvis det oppstår. Det er derfor viktig å etablere tydelige avgrensninger for oppgaven for å hindre at rammene på prosjektet utvides utover vår evne til å fullføre det.

Prosjektet vil primært levere en kartlegging og en skissering for både del 1 og del 2, og ikke et ferdig produkt. Ulike løsninger for autentisering vil bli kartlagt og undersøkt, og en MVP for et brukervennlig grensesnitt vil bli utviklet. En enkel demo av den mest lovende autentiseringsløsningen vil også bli utviklet. Gruppen vil derimot ikke utvikle ferdige løsninger, kun presentere forslag til oppdragsgiver, som kan videreutvikle ideene kartlagt og skissert i prosjektet.

I del 1 vil vi først undersøke et bredt spekter av autentiseringsløsninger. Et eksakt antall med kartlagte alternativ er ennå ikke bestemt, men et omfang på mellom fem og ti ulike alternativ virker oppnåelig.

Av de kartlagte alternativene, vil to eller tre av disse bli grundigere undersøkt og skissert. ROS-analyse skal gjennomførest på alle alternativene. En enkel demo for et av alternativene vil bli utviklet. Denne autentiseringsdemoen vil ikke bli koblet til IDportalen eller Omhu. I stedet vil det bli laget som en isolert løsning, med formål å demonstrere hvordan autentiseringen kommer til å fungere i praksis. Demoen vil bestå av en enkel innloggingsside der autentiseringsmetoden brukes for å logge inn på en bruker. Demoen trenger ikke å støtte avanserte funksjoner som endring av passord, registrering av bruker, integrasjon med Google-bruker eller IDportalen, og den trenger ikke å støtte registrering, lagring eller behandling av data.

Den andre delen av oppgaven gir like mye frihet som den første, og det er mulig å utforske oppgaven i mange retninger. Primært er dette en utforskning av et nytt brukergrensesnitt for målgruppen, uten hensyn til behovene til andre brukergrupper som også bruker Omhu, for eksempel ansatte. Demoen vi ønsker å utvikle, vil være en enkel nettside. Nettsiden kommer til å bli kodet i JavaScript, CSS og HTML i frontend. Dette er språkene som Omhu allerede bruker, og dessuten de eneste frontend-språkene som gruppa har erfaring med. Backenden vil bestå av en enkel webserver og API. Disse vil sannsynligvis bli kodet i Golang, ettersom det er det språket gruppa har mest erfaring med.

For distribusjon vil vi dra nytte av NTNU's tilbud om skykapasitet i Skyhigh OpenStack. Dette er bare en demo og trenger derfor ikke å ha full funksjonalitet. Gruppen vil utvikle dashbordet og arbeidsplanen, men andre faner og funksjoner til stede i den faktiske Omhu-webappen vil ikke gjenskapes. Vi vil heller ikke utvikle en database i backend for å lagre brukerdata mellom økter. Demoens funksjonalitet vil derfor oppleves som ufullstendig, med mange knapper som ikke har noen funksjon, og data som mest sannsynlig ikke blir bevart hvis brukeren lukker nettleseren eller logger inn på en annen enhet.

2.4 Ressursbehov

Oppdragsgiver vil dekke alle eventuelle kostnader knyttet til reising for å gjøre brukertester og lignende. Vi har også fått innvilget forespørsel til å få dekket kostnader knyttet til innkjøp av utstyr for å teste mulige innloggingsalternativer. For eksempel en security key kan være aktuelt. OpenStack vil bli brukt for å programmere en demo, noe som blir dekket av NTNU sin skyløsning, SkyHigh.

3 Organisering av kvalitetssikring

3.1 Rammeverk

Som utviklingsmodell er det ønskelig med en smidig metodikk som tåler endringer underveis i prosjektet. Med tanke på dette har vi valgt å bruke Scrum som et utgangspunkt for vårt rammeverk. Siden oppgaven ikke er direkte programmeringsrelatert, er ikke utviklingsmodeller som Extreme Programming og Open-source software development aktuelt for oss. Andre metoder som vannfallsmetoden og den vitenskapelige metode er heller ikke aktuelle. Vannfallsmetoden er basert på å fullføre spesifikke deler av prosjektet før man går videre til den neste delen. Dette gjør at det er vanskelig å gå tilbake og endre på ting etter at en del er markert som fullført. Noe som er veldig upraktisk i et prosjekt der vi skal ha jevnlige møter med oppdragsgiver, og møte sluttbrukere som skal teste løsningene våre og gi forslag til forbedringer. Vannfallsmetoden fokuserer dessuten ikke på jevnlige brukertester i løpet av utviklingen, noe vi ønsker å gjøre.

Valget falt derfor på Scrum, men blandet med elementer fra Kanban. Scrum har ikke et så stort fokus på dokumentasjon som vi ønsker å ha. Gjennom prosjektet ønsker gruppen å prioritere dokumentasjon, da spesielt valg og beslutninger som tas underveis. Dette for å sikre så god kvalitet på sluttrapporten som mulig.

Gruppen har valgt å ha sprintlengde på en uke, der sprinten starter på det ukentlige mandagsmøtet, og varer til den nestkommende fredagen. Dette møtet blir sprint planning"møtet hver uke, da vi diskuterer hva som må bli gjort i løpet av sprinten. Slingringsrommet mellom fredag og mandag kan brukes til å fullføre oppgaver som det ikke var tid til i løpet av sprinten. Fredag kveld er det scrum master sin jobb å skrive en rapport på hvilke oppgaver som ble gjort, og hvilke som står igjen etter sprinten. På mandag før vi starter en ny sprint, skal scrum master gå gjennom forrige ukes rapport. Ettersom vi bare er tre på gruppa, virker det unødvendig å ha et 15 minutters sprint møte før hver arbeidsdag. Vi fokuserer i stedet på å ha et slikt møte de dagene vi uansett møtest fysisk, som er mandager, tirsdager og torsdager.

Product owner: Philip Weisser(oppdragsgiver)
Scrum master: Skal gå på rundgang mellom gruppemedlemene
Team: Skal gå på rundgang mellom gruppemedlemmene

For opprettholde kontroll på arbeidsoppgavene bruker vi issueboard funksjonen i GitHub Projects, dette fungerer som prosjektets Kanban board. Her legger vi inn arbeidsoppgaver på mandagsmøtet, og deler oppgavene mellom gruppemedlemmene. På fredag vil Scrum Master rapportere hvilke oppgaver som er fullført til planlagt tid, og hvilke som må gjørest enten i helga, eller i løpet av neste sprint.

3.2 Dokumentasjon

I hovedsak bruker vi Overleaf for lagring av dokumenter og annen dokumentasjon, inkludert forprosjekter, sluttrapporter og andre tekstbaserte dokumenter. For logging av arbeidstimer blir det benyttet et Excel-dokument. Møteinnkallelser blir ikke lagt til på Overleaf, men publiseres på Discord.

For å sikre dokumentasjonen tar vi daglig sikkerhetskopi av alt på Overleaf ved å laste opp endringene til GitHub minst én gang om dagen. Dette sørger for at gruppen ikke mister viktig dokumentasjon og forenkler gjenopprettingsprosessen ved behov.

Når vi skriver kode, inkluderer vi kommentarer i koden og bruker et system for push-meldinger til Git. Her beskriver vi hva vi har gjort med koden og legger til en kort kommentar på norsk. For ytterligere informasjon, se gruppereglene.

3.3 Verktøy

Navn	**Bruksområde**
Overleaf	For skriving og oppbevaring av dokumenter.
GitHub	Versjonskontroll av kode, lagring av dokument, backup av overleaf.
GitHub Actions	CI/CD for uvikling av demo.
Github Projects	Oppgavefordeling og administrasjon av Scrum/Kanban
Visual Studio Code	IDE for programmering av demo og integrasjon med GitHub.
draw.io	Grafer, wireframes, mapping, diagrammer og andre grafiske visninger.
Discord	Gruppens hovedkanal for kommunikasjon og interne digitale møter.
Teams	Kommunikasjonskanal med arbeidsgiver og veileder for digitale møter.
OpenStack	For hosting av demo web-applikasjon.
Excel	Timeregistrering og Gant-skjema.

Tabell 1: Verktøy

3.4 Kvalitetssikring

Som angitt i gruppereglene, benytter vi "GitHub issue" for å overvåke fremgangen og fordele arbeidsoppgaver. Innenfor dette systemet inkluderes også kvalitetssikring. Når en ny arbeidsoppgave blir tilgjengelig, opprettes det en issue som beskriver oppgaven. Et gruppemedlem kan deretter velge å ta på seg oppgaven ved å flytte den til "in progress" kolonnen av GitHub-dashboardet. Når oppgaven er fullført, flyttes den videre til "pending review". Her skal alle gruppemedlemmene gjennomgå arbeidet før oppgaven blir plassert i "done" kolonnen. For å sikre at alle gruppemedlemmene gjennomgår oppgaven før den blir plassert i "done", merker vi den med en spesifikk etikett som indikerer at dette gruppemedlemmet har vurdert oppgaven.

For å opprettholde ryddighet i git commits, har vi utarbeidet en plan for commit-meldinger som alle gruppemedlemmer må følge. Ytterligere informasjon finnes i gruppereglene.

Testing av koden utføres ved hjelp av GitHub Actions CI/CD workflows. Spesifikt for eventuell backend-kode skrevet i Golang, benytter vi språkets integrerte rammeverk for testing.

3.5 Brukertesting

I løpet av prosjektperioden vil det bli gjennomført brukertesing av MVP i del 2, om nødvendig vil det også bli gjennomført for et innloggingsalternativ i del 1. Brukertestingen vil bli gjennomført på personer fra målgruppen, oppdragsgiver vil være behjelpelig med å skaffe sluttbrukere.

3.6 Risikovurdering

I dette kapittelet er mulige hendelser som kan påvirke prosjektet identifisert og vurdert. For vurdering av risiko, er det benyttet en risikomatrise med tre verdier for sannsynlighet, og tre verdier for konsekvens. Verdiene er målt i prosent. Risikoene har blitt rangert ved at alle gruppemedlemmene anonymt har gitt hver sin prosentverdi for sannsynlighet og konsekvens. Verdiene for sannsynlighet og konsekvens funnet i tabellen for identifiserte risikoer, er et gjennomsnitt av disse. Risikorangeringen blir dermed funnet ved hjelp av risikomatrisen under. Forebyggende og begrensende tiltak for hver identifiserte risiko er beskrevet i den tredje tabellen i dette kapittelet.

	Ikke alvorlig(0-30)	Alvorlig(31-60)	Veldig alvorlig(61-100)
Veldig sannsynlig(61-100)	3 - Moderat	4 - Høy	5 - Kritisk
Sannsynlig(31-60)	2 - Lav	3 - Moderat	4 - Høy
Ikke sannsynlig(0-30)	1 - Marginal	2 - Lav	3 - Moderat

Tabell 2: Rangering av risiko

Nr	Hendelse	Sannsynlighet	Konsekvens	Risiko
1	Mild sykdom	45%	25% - Mister 1/3 av arbeidskraft i opp til en uke.	2 Lav
2	Alvorlig sykdom	10%	70% - Mister et gruppemedlem permanent.	3 Moderat
3	Intern konflikt	53%	23% - Tid sløses på konfliktløsning og møter	2 Lav
4	GitHub nedetid	13%	22% - Vi taper litt tid da vi ikke kan pushe til repoet.	1 Marginal
5	Dokumenttap	18%	96% - Utallige timer arbeid går tapt, mulig at prosjektet er ødelagt.	3 Moderat
6	Ujevn arbeidsfordeling	80%	41% - Kvaliteten av prosjektet og sluttrapporten kan bli betraktelig dårligere, gruppemedlem slites ut og gruppemiljøet blir dårlig. Helhetsintrykket av prosjektet blir dårligere	4 Høy
7	"Scope-Creep"	43%	90% - Svært ødeleggende for prosjektet som en helhet. Kvalitet synker jevnt over hvis en pådrar seg for mye arbeid.	4 Høy
8	Forskjell i individuelle ferdigheter	58%	26% - Kan føre til enkelte gruppemedlemmer "horder" oppgaver, noe som også kan føre til ujevn arbeidsfordeling.	2 Lav
9	Dårlig planlegging	53%	70% - En går tom for tid og rekker ikke fullføre prosjektet. Kan føre til dårlige løsninger	4 Høy
10	Uforutsette hendelser	5%	75% - Å miste et gruppemedlem vil gjøre videre fremgang vanskeligere.	3 Moderat
11	Eksterne personer avbryter planer	48%	33% - Sløst bort tid	3 Moderat
12	Oppgaven oppfyller ikke minstekrav fra oppdragsgiver	10%	100% - Oppgaven er "feilet", og gir ikke tilstrekkelig nytte for oppdragsgiver.	3 Moderat

Tabell 3: Vurdering av identifiserte risikoer

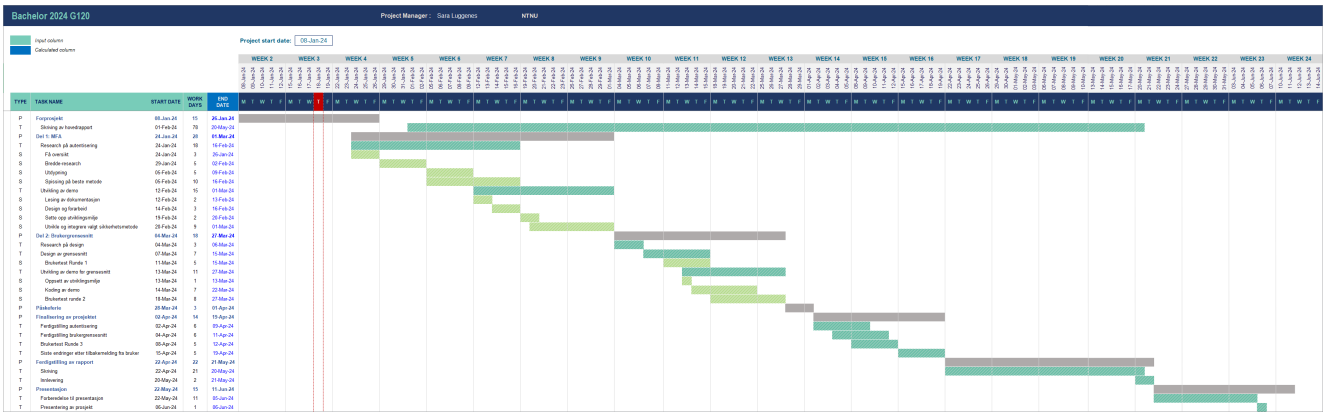
Nr	Forebyggende tiltak	Begrensede tiltak
1	Ingen forhåndsregler påkrevd.	Det aktuelle gruppemedlemmet skal gjøre så mye hen klarer av arbeidsoppgavene sine. Resten av gruppemedlemmene må jobbe litt ekstra denne perioden.
2	Ingen forhåndsregler påkrevd.	Dersom et gruppemedlem opplever alvorlig sykdom og må "droppe ut" av prosjektet, må de to andre gruppemedlemmene gjøre så godt de kan resten av prosjektet.
3	For å forhindre intern konflikt, oppfordrer vi til en åpen kommunikasjon. Problem, uenigheter og manglende trivsel innad i gruppa, bør identifiserest på forhånd og bli tatt tak i av gruppeleder.	Dersom det har oppstått en konflikt, bør prosedyren i henhold til gruppereglene følges.
4	Følge med på planlagte oppdateringer og nedetid på GitHub, og sette arbeidsøktene til utenfor denne tidsperioden.	Dersom GitHub går ned uten forvarsel, bør gruppemedlemmene finne en annen arbeidsoppgave som ikke krever tilgang til GitHub mens hen venter.

5	Vi har implementert synkronisering mellom Overleaf og GitHub, slik at vi enkelt kan "pushe" endringer i dokumentene i Overleaf til GitHub. Dette gjørest hver dag. Slik blir alle filene i Overleaf sikkerhetskopiert til GitHub jevnlig.	Dersom vi likevel mister viktige dokumenter, må alle gruppemedlemmene sette seg ned og prioritere å få gjort dokumentene på nytt. Da blir det jobbing 12 timer om dagen helt til vi er "a jour".
6	Gruppeleder har hovedansvar over at arbeidsfordelingen blir rettferdig fordelt. Alle gruppemedlemmene har et eget ansvar ved å ta på seg ekstra arbeidsoppgaver dersom hen ser at allerede gitte oppgaver er mindre tidkrevende enn forventet. God planlegging, bruk av issueboard, og bruk av scrum metodikken er forebyggende tiltak.	Årsaken må identifiserest og bli tatt hånd om. Dersom problemet er dårlig planlegging, må gruppeleder ta ansvar og delegere arbeidsoppgavene på nytt. Ved sykdom og lignende er ujevn arbeidsfordeling noe som må tolererest over en liten periode. Dersom et gruppemedlem ikke jobber tilstrekkelig, følg prosedyre i henhold til grupperegelene.
7	En godt beskrevet avgrensning, realistiske rammer og god planlegging, alt i forhold til prosjektbeskrivelsen, for forebygge at vi tar oss "vann over hodet". Være klar ovenfor oppdragsgiver hva vi har kunnskap og kapasitet nok til å gjøre, og hva vi ikke kan bruke ressurser på.	Dersom vi ser at vi har alt for mange arbeidsoppgaver å gjøre som ikke er en del av oppgavebeskrivelsen, må problemet bli tatt tak i med en gang. Omfanget må revurderest så fort som mulig sammen med oppdragsgiver. Veiledere må kanskje kontaktes for rådgivning.
8	Sørge for at gruppemedlemmer får oppgaver som hen klarer å gjøre enten med eller uten selvstudie. Selvstudie til et akseptabelt nivå er forventet. Gruppemedlemmer som er ekstra flinke på et fagområde, bør være behjelpelige og gi tips og veiledning til de andre på gruppa angående aktuelle arbeidsoppgaver.	Dersom et gruppemedlem, tross selvstudie, har store problemer med å fullføre arbeidsoppgaver innenfor et område, bør de andre på gruppa prioritere å ta ansvar for gjeldende oppgaver. Det aktuelle gruppemedlemmet får da ansvar for andre oppgaver som hen klarer å fullføre.
9	Sette klare avgrensninger og rammer tidlig i prosjektperioden. Være åpne med hverandre og med arbeidsgiver over kunnskapnivå og evner i gruppa. Ha realistiske visjoner og mål over hva vi skal oppnå med prosjektet.	Dersom vi oppdager at vi ikke kommer til å rekke å bli ferdig med prosjektet i henhold til fremdriftsplanen, må vi revurdere hvilke områder vi må prioritere med en gang. Dette bør gjørest i samråd med oppdragsgiver. Andre deler må kanskje sløyfest.
10	Uspesifiserte, uforutsette hendelser kan være blant annet at et gruppemedlem dropper ut eller lignende. Ingen forhåndsregler påkrevd.	De to gjenværende gruppemedlemmene må restrukturere prosjektmålet til et realistisk nivå mtp. antall arbeidstimer som skal brukes.
11	Alle gruppemedlemmene bør være "på" når det gjelder oppdragsgiver og andre eksterne personer. Vi bør møte godt forberedt til møter, ta initiativ og være lett å samarbeide med. Dette minsker sannsynligheten for avbrytelser og dårlig kontakt fra den andre parten sin side.	Dersom vi får problemer med kontakt og avlysninger fra oppdragsgiver eller lignende, må vi prøve å jobbe godt med oppgaver som ikke krever direkte kontakt med aktuelle person. Dersom problemet vedvarer, må vi prioritere å gjenopprette kontakten så fort som mulig.
12	God kommunikasjon med oppdragsgiver vil minimere sannsynligheten for at prosjektet faller under minstekravet. Gitt at planleggingen vår er tilstrekkelig, vil oppdragsgiver antageligvis se om vi har lagt målene til prosjektet for lavt, og kan informere om dette i tide til å rette opp på prosjektet.	Da denne risikoen først går i effekt med slutten av prosjektet, er det ingen mulige tiltak for å minimere konsekvensen av dette.

Tabell 4: Forebyggende og begrensede tiltak

4 Fremdriftsplan

For å planlegge en omtrentlig fremdriftsplan benytter gruppen seg av et Gantt-skjema. Her er alle viktige aktiviteter og milepæler vi skal gjennom i løpet av prosjektet kartlagt. Blå linjer representerer "faser" av prosjektet, hvor slutten av hver fase kan betraktes som en milepæl. Lysegrønne aktiviteter er sub-oppgaver til den mørkegrønne aktiviteten over. Mørkegrønne aktiviteter er ordinære oppgaver. Excel-dokumentet med det interaktive Gantt-diagrammet kan finnes under "/docs/gantt.xlsx".



Referanser

[1] Philip Andreas Aspholt-Weisser. *Tilpasning av modul for klinisk egenrapportering*. PDF. 2023.

[2] NTNU. *NTNU*. URL: `https://logogenerator.ntnu.no/index.php?type=hovedlogo`.

[3] WeissTech. *Omhu*. URL: `https://omhuapp.no/wp-content/uploads/2020/09/logo-std.svg`.

[4] WeissTech. *WeissTech*. URL: `https://www.valdres-nhage.no/om-oss/valdres-naeringshage`.

Grupperegler

Gruppe 120, Oppgave 40

15. januar 2024

Introduksjon

Dette dokumentet går gjennom regler og retningslinjer for prosjektarbeidet innad i gruppen. Dokumentet skal være til hjelp for et effektivt samarbeid, god kommunikasjon, og ellers medvirke til en god gjennomføring av bachelorprosjektet.

Gruppemedlemmer

- Raphael Storm Larsen
- Jørgen Teigen
- Sara Stentvedt Luggenes

Kommunikasjon

- **Kommunikasjonskanal:** For vanlig kommunikasjon og møteinnkallelser innad i gruppa, bruker vi Discord. Kontakt med arbeidsgiver og veiledere vil hovedsakelig være via epost.
- **Responstid:** Gruppemedlemmene skal være tilgjengelig fra 09:00 til 18:00 i ukedager. Dette innebærer å svare på meldinger innen 1 time er gått, med mindre noe annet er avtalt. Gruppemedlemmene skal også være tilgjengelig i helger, med mindre man har klargjort på forhånd at man da ikke er tilgjengelig, med en responstid på 12 timer. Alle bør likevel følge med jevnlig i gruppechatten på Discord, for å unngå at "hasteoppgaver" blir oversett.

Roller og ansvar

- **Gruppeleder:** Skal ha et godt overblikk over alle oppgavene, skal ha hovedansvaret for å delegere arbeidsoppgaver mellom gruppemedlemmene, skal sørge for at arbeidsmengden blir rettferdig fordelt. Har et ekstra ansvar ved konflikter og uenigheter, ved at hen vurderer alle synspunkt, og ved behov kontakter veileder for megling.
  Ansvarlig gruppemedlem: Sara
- **Kommunikasjonsansvarlig:** Har ansvar for kontakt med oppdragsgiver og veiledere. Dette innebærer å avtale møter og sørge for at oppdragsgiver og eventuelt veiledere får nødvendige dokument tilsendt.
  Ansvarlig gruppemedlem: Sara
- **Møteansvarlig:** Har ansvar for å skrive møtereferat av møter, sende ut møteinnkallelse og booke rom til gruppemøter.
  Ansvarlig gruppemedlem: Raphael
- **Dokumentansvarlig:** Har hovedansvar for å opprette og vedlikeholde dokumenter i Overleaf og GitHub. Printe ut nødvendige dokument, håndtering av underskrift og lignende.
  Ansvarlig gruppemedlem: Jørgen

Arbeidsflyt

- **Regelmessige møter innad i gruppa:** Regelmessige gruppemøter hver mandag fra kl 10:15 til 12:00 der vi går gjennom oppgavene gjort siden sist møte, går gjennom eventuelle endringer, og planlegger hva som skal gjørest av hvem til neste møte. Minimum skal det holdes et møte i uka, enten digitalt eller fysisk.
- **Regelmessige møter med veiledere:** Møte med veiledere har fast tid fra kl 10:00 til 10:30 hver torsdag.
- **Regelmessige felles arbeidsøkter:** På tirsdager og torsdager skal alle gruppemedlemmene sitte sammen på campus og jobbe med prosjektet.
- **Deadlines:** Hver mandag lager vi deadlines til fredag kl 23:59 som følger prosjektplanen. Dersom vi ikke klarer å fullføre alle deadlines innen fristen, skal alle gruppemedlemmene være klare for å jobbe litt i helga for å fullføre oppgavene.
- **Arbeidsinnsats:** Hvert gruppemedlem har gitt samtykke om å investere rundt 620 timer +-50 timer arbeid inn i oppgaven. Dette tilsvarer ca. 30 timer i uka, regnet fra uke 2(mandag 8. januar) til uke 23(søndag 9. juni). Hvert gruppemedlem bør prøve å bruke minst 30 timer hver uke for å nå timemålet. Antall arbeidstimer og hva timene har blitt brukt til skal skrivest inn i loggboka fortløpende. Hvert gruppemedlem har selv ansvar for å legge inn arbeidstimer i loggboka, og sørge for at tilstrekkelig antall timer i uka blir gjort. Gyldige unntak for regelen om ca. 30 arbeidstimer i uka er sykdom og uventede eksterne hendelser som f. eks. dødsfall i nær familie osv.
- **Verktøy og plattform:** Vi forholder oss til plattformen Discord for kommunikasjon, Overleaf for rapportskriving og dokumentasjon, Github for kodereleaterte oppgaver samt resterende dokumenter.
- **Tilstedeværelse:** Når vi har gruppemøter og på andre måter jobber sammen, skal alle ha fullt fokus på arbeidsoppgaven. Unødvendig mobilbruk og å konsentrere seg om andre ting skal ikke skje. Dette gjelder ikke dersom gruppemedlemmet har pause.
- **Innkalling til møte og møtereferat:** Før vi har et møte med veilederne eller oppdragsgiver, skal en kort møteinnkallelse bli sendt til de som skal være med i møtet. Denne skal oppsummere agendaen for møtet. Videre etter møtet skal et enkelt møtereferat skrives, dette blir lagt inn i loggboka.
- **Språk:** Oppgaven skrives på norsk bokmål. Tekniske utrykk skrives på norsk eller engelsk dersom dette passer bedre. Commit meldinger skal være på norsk, mens kommentarer i kode skal skrives på engelsk.
- **Issue tracking:** Gruppemedlemmene går aktivt inn for å bruke github issues for å spore fremgang og fagfellevurdering av arbeidsoppgaver i prosjektet. Alle arbeidsoppgaver må gå gjennom en fagfellevurdering før den er regnet som ferdig. Vi sikter til å legge inn nye issues på mandager, og forsøker å bli ferdig med alle i løpet av ukens deadline, som hovedsakelig vil være på fredager.
- **Atomiske commits:** Github commits burde være atomiske, og om mulig være knyttet direkte opp til en issue.
- **Commit-meldinger:** Vi følger en felles konvensjon for commit-meldinger.
  - **feat:** En ny funksjon eller forbedring lagt til i kodebasen.
  - **fix:** En feilretting eller korreksjon for å løse et problem.
  - **docs:** Endringer eller oppdateringer i dokumentasjonen.
  - **style:** Endringer relatert til kodeformatering, innrykk eller mellomrom.
  - **refactor:** Kodeomstrukturering uten å legge til nye funksjoner eller fikse feil.
  - **test:** Legg til eller endre tester.
  - **chore:** Andre endringer som ikke direkte påvirker koden (for eksempel scripts og avhengigheter).

Konflikthåndtering

- **Uenigheter:** Dersom det oppstår uenigheter, skal det først og fremst prøves å løse uenigheten ved hjelp av at begge/alle partene inngår et kompromiss. Selv om det er to mot en, skal alle være åpne for å inngå et kompromiss med den uenige tredjeparten.
- **Konflikt:** Dersom det oppstår en konflikt innad i gruppa som ikke kan løses ved hjelp av et kompromiss, skal veileder kontaktes og hjelpe med å løse konflikten. Veileder skal gi råd om hvordan vi bør løse konflikten, og alle gruppemedlemmene skal ta hensyn til det veilederene råder oss til.
- **Muntlig og skriftlig advarsel:** Dersom et gruppemedlem...
  - ikke gjør tildelte oppgaver på et vedvarende nivå
  - ikke bruker et tilstrekkelig antall arbeidstimer i uka på prosjektet på et vedvarende nivå
  - har en tendens til å legge minimal innsats inn i arbeidsoppgavene sine(f. eks. bryr seg ikke om kvalitet, mye skrivefeil, åpenbart har en tendens til å ta letteste løsning)
  - ikke møter opp til avtalte møter
  - ikke utfyller tildelte grupperolle
  - bryter gruppereglene på et gjentagende nivå
  - er betraktelig initiativløs i gruppemøter og ved tildeling av oppgaver på et vedvarende nivå
  - skaper andre store problemer innen orden, trivsel eller arbeidseffektivitet

  ...skal det først gis en muntlig advarsel fra de to andre medlemmene. Om problemet vedvarer, skal det gis en formell skriftlig advarsel. Denne advarselen skal ta opp hva som er problemet og hvilken regler som er brutt, og skal beskrive konsekvensene dersom aktuelt gruppemedlem ikke forbedrer seg til et akseptabelt nivå. Om dette ikke virker, kontaktes veileder og deretter vil det diskuteres en utkastelse av gruppemedlemmet.

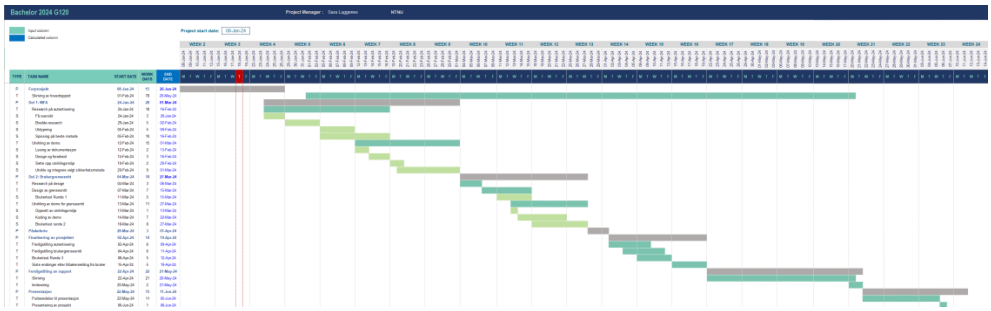
Signatur

Ved å signere nedenfor, erkjenner jeg at jeg har lest og godtar å følge gruppereglene som er skissert i dette dokumentet.

Jørgen Teigen	Raphael Storm Larsen	Sara Stentvedt Luggenes

Vedlegg T

Gantt skjema



Figur T.1: Gantt skjema

Vedlegg U

Timeliste

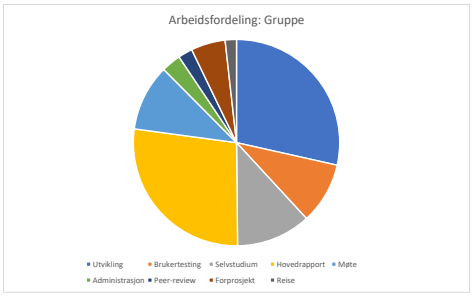
Gruppemedlem	Totale Arbeidstimer	Andel av gruppens timer	Timer denne uken	Timer i dag
Raphael	432,15	36,24 %	7	0
Sara	365	30,61 %	0	0
Jørgen	395,25	33,15 %	12	6

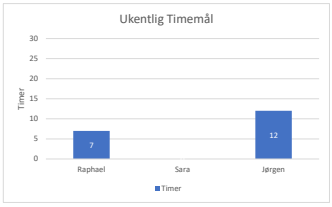
Aktivitet	Timer
Utvikling	338,25
Brukertesting	114,25
Selvstudium	138,75
Hovedrapport	323,9
Møte	123,5
Administrasjon	36,25
Peer-review	26,75
Forprosjekt	63,75
Reise	21

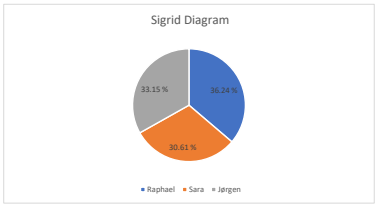
	Faktisk	Ønsket
SUM TIMER	1192,4	1773
MÅL TIMER	1800	1800
Fremgang	66 %	99 %

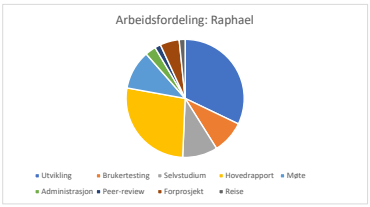
Start Date	08.01.2024
End Date	22.05.2024
Current Date	20.05.2024
Fremgang	99 %

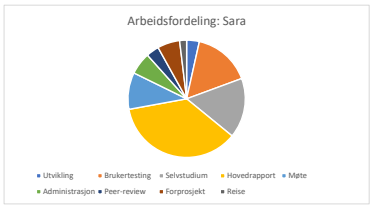
Hvor mange timer må vi jobber hver dag inkludert helg for å oppnå timemålet?
101,27 timer

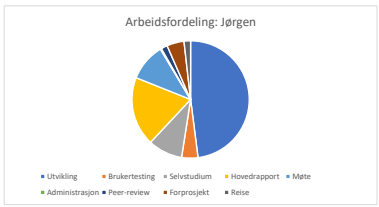






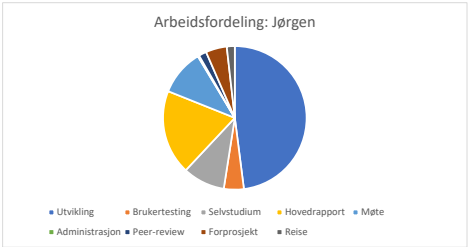






Dato	Kommentar	Timer	Aktivitet
08.01.2024	Intromøte	4	Møte
09.01.2024	Arbeid med prosjektplan	3	Forprosjekt
10.01.2024	Arbeid med prosjektplan	2	Forprosjekt
10.01.2024	Seminar om bachelor oppgave	2	Selvstudium
11.01.2024	Møte med veileder og arbeidsøkt	4,5	Forprosjekt
12.01.2024	Se og lest på bacheloroppgaver	1	Selvstudium
15.01.2024	Gruppe møte	2	Møte
15.01.2024	Arbeid med doukumentasjon del og verktøy	3	Forprosjekt
15.01.2024	Peer review	0,5	Peer-review
15.01.2024	Tabel of content	0,5	Administrasjon
15.01.2024	Lese over for prosjekt og bachelor oppgaver	1	Selvstudium
16.01.2024	Forberedring for møte	0,5	Administrasjon
16.01.2024	Møte med arbeidsgiver	1	Møte
16.01.2024	Arbeidsøkt	3	Forprosjekt
16.01.2024	Peer review	0,5	Peer-review
17.01.2024	Peer review	1	Peer-review
17.01.2024	Skrive og fikse mål	1	Forprosjekt
17.01.2024	Finne standarer for autentiserings	3	Selvstudium
18.01.2024	Møte med veileder og arbeidsøkt	0,5	Møte
18.01.2024	Leste på autentisering FIDO og noen andre	2	Selvstudium
18.01.2024	Arbeid med forprosjekt	1	Forprosjekt
19.01.2024	Lesing av rapport	1	Selvstudium
19.01.2024	Reppitisjon av html, css og javascript	2	Selvstudium
19.01.2024	Ferdig stilling og levering av rapport	0,25	Administrasjon
22.01.2024	Gruppe møte	1,5	Møte
22.01.2024	Micresoft azure face api og mer	4,5	Selvstudium
23.01.2024	Selvstudium MFA	4,5	Selvstudium
24.01.2024	Møte og gjennomgan av MFA	1,75	Møte
24.01.2024	Skriving om mobil autentisering	3,5	Hovedrapport
25.01.2024	Møte med veileder og arbeidsøkt	0,5	Møte
25.01.2024	Peer review	0,75	Peer-review
25.01.2024	Se/leste kjap over Bian Yang sine tekster	0,25	Selvstudium
25.01.2024	Skrive tekst både på mobil autentisering og google loggin	3	Hovedrapport
25.01.2024	forbedring og se over forprosjektet	1	Forprosjekt
26.01.2024	Skrive og fikse på mobil autetnisering og google	3	Hovedrapport
26.01.2024	Lese på Bian Yang sine tekster	1	Selvstudium
26.01.2024	Oppfriske ferdigheter av html,css og Javasript og se litt på swelte framwork	2	Selvstudium
29.01.2024	Møteprepp	0,5	Møte
29.01.2024	Møte med arbeidsgiver	2,25	Møte
29.01.2024	Skrive om MinID og fikse underskrift på stndardavtale	2	Hovedrapport
30.01.2024	Skriving på MinID og face autentisering	4	Hovedrapport
30.01.2024	Peer review	0,5	Peer-review
31.01.2024	Skriving	2	Hovedrapport
31.01.2024	Peer review	0,25	Peer-review
01.02.2024	Møte med veilder	0,5	Møte
01.02.2024	Arbeidsøkt med gruppa	4,5	Hovedrapport
01.02.2024	Skrive om buypass	1,5	Hovedrapport
01.02.2024	Peer review	0,5	Peer-review
02.02.2024	Forberede til arbeidøkt me gruppe	0,75	Selvstudium
02.02.2024	Arbeidsøkt med gruppa	2,5	Hovedrapport
02.02.2024	Skrive og revider og legge til scoring fingeravtrykk og ansiktsautentisering	2,5	Hovedrapport
02.02.2024	peer review	0,5	Peer-review
02.02.2024	Skrive og revider mobil autentisering	1	Hovedrapport

Aktivitet	Timer
Utvikling	186,75
Brukertesting	17,5
Selvstudium	37
Hovedrapport	74,25
Møte	40,25
Administrasjo	1,25
Peer-review	6,75
Forprosjekt	18,5
Reise	7

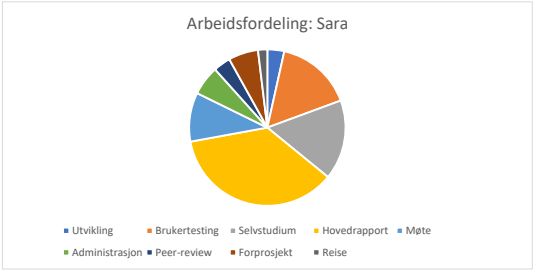


03.02.2024	Arbeidsøkt med gruppa	2	Hovedrapport	
05.02.2024	Prøvde og fikse tabel struktur	1	Hovedrapport	
05.02.2024	Leste på og om prising på de ulike en faktor løsningene og gikk ove rapporten for skrive feil p	1	Hovedrapport	
05.02.2024	Møte	1,75	Møte	
05.02.2024	Fikse tabell og skriving i rapport	2	Hovedrapport	
05.02.2024	Oppfriskning på ROS-analyse	1	Selvstudium	
07.02.2024	Rapportskriving	4,75	Hovedrapport	
08.02.2024	Møte	2,5	Møte	
08.02.2024	Arbeidsøkt med gruppa	2,5	Hovedrapport	
12.02.2024	Møte	0,5	Møte	
12.02.2024	Peer review	0,75	Peer-review	
13.02.2024	Lese om kvalitative bruker tester	2	Selvstudium	
13.02.2024	Lette etter kilder for rapporten	2	Selvstudium	
14.02.2024	Digitalt møte med gruppa	0,5	Møte	
14.02.2024	Kode loggin side	2,5	Utvikling	
15.02.2024	Møte med veileder og arbeidsøkt	0,5	Møte	
15.02.2024	Arbeidøkt med gruppa	3,5	Brukertesting	
16.02.2024	Kode loggin side	4	Utvikling	
19.02.2024	Møte med gruppa	1,75	Møte	
19.02.2024	Kode loggin side	0,75	Utvikling	
20.02.2024	Forsette og kode loggin side	4	Utvikling	
21.02.2024	Kode loggin side	4	Utvikling	
21.02.2024	Se gjennom relevant litteratur	1	Selvstudium	
21.02.2024	Peer review	1	Peer-review	
22.02.2024	Møte	2	Møte	
22.02.2024	Gjennomgang av bruertest	1	Brukertesting	
23.02.2024	Koding	3,5	Utvikling	
25.02.2024	Koding	4	Utvikling	
26.02.2024	Møte prep	0,5	Møte	
26.02.2024	Møte	2	Møte	
26.02.2024	Koding front end	1	Utvikling	
27.02.2024	Koding av front end	5	Utvikling	
28.02.2024	Brukertest	2,5	Brukertesting	
29.02.2024	Møte med veileder og gruppa	2	Møte	
01.03.2024	Front-end styling	2	Utvikling	
29.02.2024	Sjekke hva omhu sin web-app på mobil mangler	1	Selvstudium	Selvstudium
01.03.2024	Kodin messageHandler	4	Utvikling	
04.03.2024	Møte med gruppa	1	Møte	
05.03.2024	Wireframe	4	Selvstudium	
06.03.2024	Wireframe	2	Selvstudiu	
07.03.2024	Møte med veileder	0,25	Møte	
07.02.2024	Felles arbeidsøkt	3	Brukertesting	
08.03.2024	Forberede brukertest	0,5	Brukertesting	
09.03.2024	Brukertest	0,5	Brukertesting	
11.03.2024	Møte med gruppa	2	Møte	
11.03.2024	Koding av containere og header	1,5	Utvikling	
12.03.2024	Møte	0,5	Møte	
12.03.2024	Utvikling header og mer	4	Utvikling	
13.03.2024	Utvikling av Min side og header	8	Utvikling	
14.03.2024	Utvikling	6	Utvikling	
12.03.2024	Peer review	0,5	Peer-review	
15.03.2024	Utvikling av Min side	2	Utvikling	
18.03.2024	Utvikling av Min side	6	Utvikling	
19.03.2024	Utvikling av Min side	10	Utvikling	

20.03.2024	Utvikling	2	Utvikling
20.03.2024	Møte med gruppa	1	Møte
21.03.2024	Utvikling	6,5	Utvikling
22.03.2024	Utvikling av Min side	10	Utvikling
02.04.2024	Fikset git branche	1	Administrativt
03.04.2024	Møte med oppdraggiver	1	Møte
04.04.2024	Fikse bugs	2	Utvikling
04.04.2024	Gruppemøte	0,5	Møte
05.04.2024	Fikset noen bugs	0,5	Utvikling
06.04.2024	Fikse bugs	4	Utvikling
07.04.2024	Fikse bugs	5	Utvikling
08.04.2024	Møte med gruppa	1	Møte
08.04.2024	Utvikling	3,5	Utvikling
09.04.2024	Kjøring	7	Reise
09.04.2024	Brukertesting	6,5	Brukertesting
11.04.2024	Møte med veileder og sprintmøte	1,5	Møte
12.04.2024	Finne litteratur til rapporten	1	Hovedrapport
15.04.2024	Gruppemøte	0,75	Møte
15.04.2024	Finne ting som kunne forbedre demoen	1	Selvstudium
17.04.2024	Jobbe med V3 av demoen	6	Utvikling
18.04.2024	Jobbe med V3 av demoen	3	Uvikling
19.04.2024	Jobbe med V3 av demoen	5	Utvikling
22.04.2024	Møte med oppdraggiver og scrummøte	1	Møte
22.04.2024	Videre forbedring av demoen	2	Utvikling
23.04.2024	Videre forbedring av demoen	5	Utvikling
24.04.2024	Videre forbedring av demoen	4	Utvikling
25.04.2024	Videre forbedring av demoen	1	Utvikling
17.04.2024	Scrum møte	1,25	Møte
26.04.2024	Utvikling	6	Utvikling
28.04.2024	Utvikling	1,5	Utvikling
29.04.2024	Utvikling	5	Utvikling
30.04.2024	Utvikling of finn pussing av demoer	4	Utvikling
01.05.2024	Utvikling	5	Utvikling
02.05.2024	Utvikling	5,5	Utvikling
03.05.2024	Utvikling	3	Utvikling
06.05.2024	Fin pussing av demo	4,5	Utvikling
07.05.2024	Fin pussing av demo	5	Utvikling
08.05.2024	Fin pussing av demo	6	Utvikling
09.05.2024	Skrive tester	3	Utvikling
10.05.2024	Skrive tester	4,5	Utvikling
12.05.2024	Skrive tester	5	Utvikling
13.05.2024	Legge til vedleg i rapport	3	Hovedrapport
14.05.2024	Skrive rapport	2	Hovedrapport
15.05.2024	Legge til vedleg i rapport	3	Hovedrapport
16.05.2024	Fikse kilder i rapporten	3,5	Hovedrapport
17.05.2024	Fin pussing av rapport	2	Hovedrapport
18.05.2024	Fin pussing av rapport	5	Hovedrapport
19.05.2024	Fin pussing av rapport	6	Hovedrapport
20.05.2024	Fin pussing av rapport	6	Hovedrapport

Dato	Kommentar	Timer	Aktivitet	Uke Nr
08.01.2024	Introduksjonsmøte	4	Møte	2
09.01.2024	Liten arbeidsøkt	3	Forprosjekt	2
09.01.2024	Kvalitetssikring og gitlab issue board revisjon	1	Peer-review	2
10.01.2024	Lynkurs i prosjektstyring	2	Selvstudium	2
10.01.2024	Revisjon grupperegler, rollefordeling	2	Forprosjekt	2
10.01.2024	Research bacheloroppgave	2	Selvstudium	2
11.01.2024	Møte med veiledere	0,5	Møte	2
11.01.2024	Risikoanalyse forprosjekt	4	Forprosjekt	2
15.01.2024	Gruppemøte	1,5	Møte	3
15.01.2024	Risikoanalyse tiltak	1,5	Forprosjekt	3
15.01.2024	Forberedt møte med oppdragsgiver	0,75	Selvstudium	3
15.01.2024	Omskrevet bakgrunn	0,5	Forprosjekt	3
15.01.2024	Peer review	0,5	Peer-review	3
15.01.2024	Overleaf referanseliste	0,5	Selvstudium	3
15.01.2024	Rammeverk opplesing og skriving	2	Forprosjekt	3
16.01.2024	Møteprep.	0,5	Administrasjon	3
16.01.2024	Møte med oppdragsgiver	1	Møte	3
16.01.2024	Felles arbeidsøkt	3	Forprosjekt	3
16.01.2024	Peer review	0,5	Peer-review	3
16.01.2024	Opplesing på ROS, brukertesting	1	Forprosjekt	3
16.01.2024	Opplesing WCAG standard	0,5	Selvstudium	3
17.01.2024	Peer review	0,25	Peer-review	3
17.01.2024	Opplesing på ISO/WCAG osv	3,5	Selvstudium	3
17.01.2024	Bacheloroppgave lesing	2	Selvstudium	3
18.01.2024	Møte med veiledere	0,5	Møte	3
18.01.2024	Ferdigstilling gantt, felles arbeidsøkt	2,5	Forprosjekt	3
18.01.2024	Lesing, repetisjon HTML, CSS	1,5	Selvstudium	3
19.01.2024	OpenStack fiksing, troubleshooting	3	Utvikling	3
22.01.2024	Gruppemøte	1,5	Møte	4
22.01.2024	Selvstudie MFA	5	Selvstudium	4
22.01.2024	Sett på Omhu for gøy	0,5	Selvstudium	4
23.01.2024	Selvstudie MFA	4	Selvstudium	4
23.01.2024	Laget spørreskjema, sluttrapport	2	Administrasjon	4
24.01.2024	Gruppemøte	1,75	Møte	4
24.01.2024	Rapport, yubikey, standarder	5,25	Hovedrapport	4
25.01.2024	Møte med veiledere	0,5	Møte	4
25.01.2024	Forbedring av prosjektplan i gruppe	3	Forprosjekt	4
25.01.2024	Kodebrikke, RSA SecurID, Sverige	3,25	Hovedrapport	4
25.01.2024	Peer review	0,5	Peer-review	4
25.01.2024	Iris-recognition, epost og sånt	1	Administrasjon	4
29.01.2024	Møte-prep	0,5	Administrasjon	5
29.01.2024	Møte med oppdragsgiver	0,5	Møte	5
29.01.2024	Gruppemøte, arbeidsøkt	3	Hovedrapport	5
29.01.2024	Peer review	0,75	Peer-review	5
29.01.2024	Hovedrapport	0,75	Hovedrapport	5
30.01.2024	Arbeidsøkt med gruppa	3,5	Hovedrapport	5
30.01.2024	Peer review	0,75	Peer-review	5
31.01.2024	Skriving	1,5	Hovedrapport	5

Aktivitet	Timer
Utvikling	12,75
Brukertesting	58
Selvstudium	60,25
Hovedrapport	132,25
Møte	37
Administrasjon	22,25
Peer-review	13
Forprosjekt	22,5
Reise	7

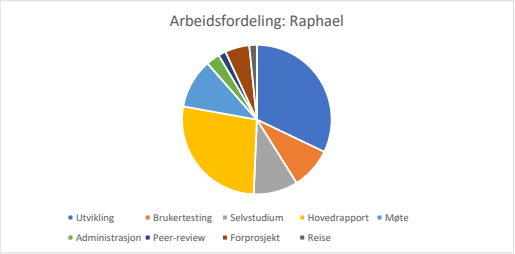


	31.01.2024	Peer review	0,5	Peer-review	5
	31.01.2024	Diri	1	Selvstudium	5
	01.02.2024	Møte med veiledere	0,5	Møte	5
	01.02.2024	Arbeidsøkt med gruppa	4,5	Hovedrapport	5
	01.02.2024	Peer review	1,25	Peer-review	5
	01.02.2024	Skrive om passord	1,5	Hovedrapport	5
	01.02.2024	Bestille yubikey	0,25	Administrasjon	5
	02.02.2024	Felles digital arbeidsøkt	2,75	Hovedrapport	5
	02.02.2024	Skriving, lesing, peer review	4	Hovedrapport	5
	03.02.2024	Felles arbeidsøkt	2	Hovedrapport	5
	05.02.2024	Møte, scrum	1,75	Møte	6
	05.02.2024	Buypass, lesing, skriving	2	Selvstudium	6
	05.02.2024	Troubleshoot, referanse til tabell	0,75	Administrasjon	6
	05.02.2024	Peer review	1,5	Peer-review	6
	05.02.2024	FaceID, azure api, skriving, lesing	2	Hovedrapport	6
	07.02.2024	Peer review	2,5	Peer-review	6
	07.02.2024	Skriving face api, 2 faktor løsninger	0,75	Hovedrapport	6
	08.02.2024	Møte med veiledere	0,5	Møte	6
	08.02.2024	Felles arbeidsøkt	2,5	Hovedrapport	6
	08.02.2024	Møte med Bian Yang	1,25	Møte	6
	08.02.2024	Møtereferat	0,25	Administrasjon	6
	08.02.2024	Lesing på bachelor, research	2	Selvstudium	6
	09.02.2024	Ekstramøte med Erik	0,5	Møte	6
	09.02.2024	Research usability testing	2	Selvstudium	6
	12.02.2024	Research usability testing	4	Selvstudium	7
	12.02.2024	Møte med oppdragsgiver	0,5	Møte	7
	13.02.2024	Møte med Halden kommune	0,5	Møte	7
	13.02.2024	Research usability testing	1	Selvstudium	7
	13.02.2024	Openstack administrasjon	3	Administrasjon	7
	14.02.2024	Peer review	2	Peer-review	7
	14.02.2024	Digitalt møte med gruppa	0,5	Møte	7
	15.02.2024	Møte med veiledere	0,5	Møte	7
	15.02.2024	Felles arbeidsøkt, brukertesting	2,5	Brukertesting	7
	15.02.2024	Forberedelse brukertesting	2	Brukertesting	7
	19.02.2024	Møte med gruppa	1,5	Møte	8
	19.02.2024	Openstack, dual ip, troubleshoot	2	Administrasjon	8
	19.02.2024	Peer review	1	Peer-review	8
	20.02.2024	Openstack, global ip	4,5	Administrasjon	8
	21.02.2024	Brukertesing prep	4	Brukertesting	8
	22.02.2024	Møte med veiledere	0,5	Møte	8
	22.02.2024	Gruppemøte	1,5	Møte	8
	22.02.2024	Brukertesing skriving	2	Brukertesting	8
	25.02.2024	Frontend checkliste	5	Utvikling	9
	26.02.2024	Møte med oppdragsgiver	0,5	Møte	9
	26.02.2024	Gruppemøte	1,5	Møte	9
	26.02.2024	Frontend checkliste	4,75	Utvikling	9
	27.02.2024	Brukertest prep	4	Brukertesting	9
	28.02.2024	Brukertesting	2,5	Brukertesting	9
	28.02.2024	Brukertesting, etterarbeid	2	Brukertesting	9

	28.02.2024	Epost-skriving	0,5	Administrasjon	9
	29.02.2024	Møte med veiledere	0,5	Møte	9
	29.02.2024	Felles arbeidsøkt, brukertesting	1,5	Brukertesting	9
	01.03.2024	Brukertesting, Jorunn og Simen	3	Brukertesting	9
	03.03.2024	Brukertesting, etterarbeid	1	Brukertesting	10
	04.03.2024	Gruppemøte	1	Møte	10
	05.03.2024	Rapportskriving	2	Hovedrapport	10
	06.03.2024	Laget wireframe, første utkast del 2	5	Selvstudium	10
	07.03.2024	Møte med veiledere	0,25	Møte	10
	07.03.2024	Felles arbeidsøkt	3	Møte	10
	08.03.2024	Forberedelse intervju, epost	2	Administrasjon	10
	11.03.2024	Møte med oppdragsgiver	0,5	Møte	11
	11.03.2024	Gruppemøte	1,5	Møte	11
	11.03.2024	Lest kvantifisering av brukervennlighet	3	Selvstudium	11
	12.03.2024	Lest kvantifisering av brukervennlighet	2	Selvstudium	11
	13.03.2023	Rapport, valg rundt metode	2	Hovedrapport	11
	14.03.2024	Rapport, brukervennlighet	1	Hovedrapport	11
	17.03.2024	Rapportkurs, lest tidlig. oppgaver, struktur	6	Selvstudium	12
	18.03.2024	Møte med gruppa	2	Møte	12
	21.03.2024	Møte med veiledere	0,5	Møte	12
	21.03.2024	Lest meg opp på brukervennlighet	4	Selvstudium	12
	27.03.2024	Brukertest	1	Brukertesting	13
	03.04.2024	Lage brukertest for del 1, Halden	4	Selvstudium	14
	04.04.2024	Møte med veiledere	0,5	Møte	14
	05.04.2024	Planlegge brukertest i Halden, administrasjon	4	Administrasjon	14
	06.04.2024	Lage instruksjonstekst, del 1, Halden	2	Brukertesting	14
	07.04.2024	Lage instruksjonstekst, del 1, Halden	3	Brukertesting	15
	04.04.2024	Brukertest	2	Brukertesting	14
	08.04.2024	Forberedelse Halden, brukertest	8	Brukertesting	15
	08.04.2024	Forberedelse, reise, fylle bensin	1	Administrasjon	15
	09.04.2024	Reising, Halden	7	Reise	15
	09.04.2024	Brukertesting i Halden	6,5	Brukertesting	15
	10.04.2024	Sett på resultater fra brukertest	5	Brukertesting	15
	11.04.2024	Møte med veiledere	0,5	Møte	15
	11.04.2024	Gruppemøte	1	Møte	15
	15.04.2024	Gruppemøte	0,75	Møte	16
	15.04.2024	Bearbeide brukertest reslutater, finne kilder	6	Brukertesting	16
	16.04.2024	Lese og skrivevansker finne kilder	2	Selvstudium	16
	17.04.2024	Mid-srum møte	1,25	Møte	16
	18.04.2024	Sammenlagt arbeid siste måned	90	Hovedrapport	16
					0

Dato	Kommentar	Timer	Aktivitet	Uke Nr
08.01.2024	Introduksjonsmøte	4	Møte	2
09.01.2024	Liten arbeidsøkt.	3	Forprosjekt	2
09.01.2024	Kvalitetssikring og gitlab issue board revisjon	1	Peer-review	2
10.01.2024	Seminar: lynkurs i prosjektskriving	2	Selvstudium	2
10.01.2024	Arbeidsøkt etter seminar	2	Forprosjekt	2
10.01.2024	Skriving av excel dokument.	2	Administrasjon	2
11.01.2024	Ettermøte	4	Forprosjekt	2
11.01.2024	Veildermøte	0,5	Møte	2
15.01.2024	Jobbet på risikovurdering og forberedelser til møte	0,5	Forprosjekt	3
15.01.2024	Ukentlig gruppemøte	1,5	Møte	3
15.01.2024	Leser gjennom prosjektplan	0,5	Selvstudium	3
15.01.2024	Misc peer review	0,25	Peer-review	3
15.01.2024	Skrev avgrensing	1	Forprosjekt	3
15.01.2024	Fikse excel	1	Administrasjon	3
16.01.2024	Oppsett før møte	0,5	Administrasjon	3
16.01.2024	Møte med oppdragsgiver	1	Møte	3
16.01.2024	Arbeid etter møte	3	Forprosjekt	3
16.01.2024	Peer review på slutten av økt + senere på kvelden	0,75	Peer-review	3
16.01.2024	Skrev avgrensing(igjen), fikset forside, skrev oppgaverammer	1,25	Forprosjekt	3
16.01.2024	Fikset excel	0,5	Administrasjon	3
17.01.2024	8:45-9:15 Risiko + forside	2	Forprosjekt	3
17.01.2024	9:15-13:00 + 14:25 - 16:30 Leser gjennom tidligre bachelor oppgave	5,75	Selvstudium	3
17.01.2024	Peer review	0,25	Peer-review	3
17.01.2024	Fant nytt gant chart	0,75	Forprosjekt	3
18.01.2024	8:45-10:00 + 10:30-12:00 + 14:55-15:20 + 15:40-16:30 Gantt chart	4	Forprosjekt	3
18.01.2024	10:00-10:30 Møte med veilder	0,5	Møte	3
18.01.2024	Gjennomgang av dokument, fikling med formatering på tables	1,25	Forprosjekt	3
18.01.2024	Peer review	0.25	Peer-review	3
19.01.2024	Selvstudium på https server 9:45-11:05	1,25	Selvstudium	3
19.01.2024	openstack	0,25	Utvikling	3
22.01.2024	Gruppemøte 10:15-12	1,75	Møte	4
22.01.2024	15:00 - 16:22 + 17:55-19:30 researcher autentisering	2,75	Selvstudium	4
23.01.2024	6:30-8:45 9:30-11:00 reseacher autentisering	3,75	Selvstudium	4
23.01.2024	11:00-11:30 12:45-13:45 Lager tidlig struktur på hovedrapport	1,5	Hovedrapport	4
23.01.2024	13:45-15:00 Leser opp på beste kort-printer	1,25	Selvstudium	4
24.01.2024	10:00-11:30 gruppemøte	1,5	Møte	4
24.01.2024	11:30-12:30 møtereferat og github issues	1	Administrasjon	4
24.01.2024	12:30-13:00 13:45-16:45 18:30-19:15 begynner å skrive	4,25	Hovedrapport	4
24.01.2024	19:15-19:30 Skrev møteagenda	0,25	Administrasjon	4
25.01.2024	møteprepp	0,25	Administrasjon	4
25.01.2024	veiledermøte	0,5	Møte	4
25.01.2024	gruppearbeid 10:30-12:30 møtereferat og møteagenda	2	Administrasjon	4
25.01.2024	12:30-13:30 research på kodebrikke	1	Selvstudium	4
25.01.2024	16:15-16:45 fikser excel skjema	0,5	Administrasjon	4
25.01.2024	16:45 - 18:45 peer reviewer greier	2	Peer-review	4
26.01.2024	11:15-13:45 lager qr kort bilde	2,5	Utvikling	4
29.01.2024	10:00-10:30 møteprepp	0,5	Administrasjon	5
29.01.2024	10:30-12:45 møte	2,25	Møte	5
29.01.2024	17:30-20 skriving	2	Hovedrapport	5

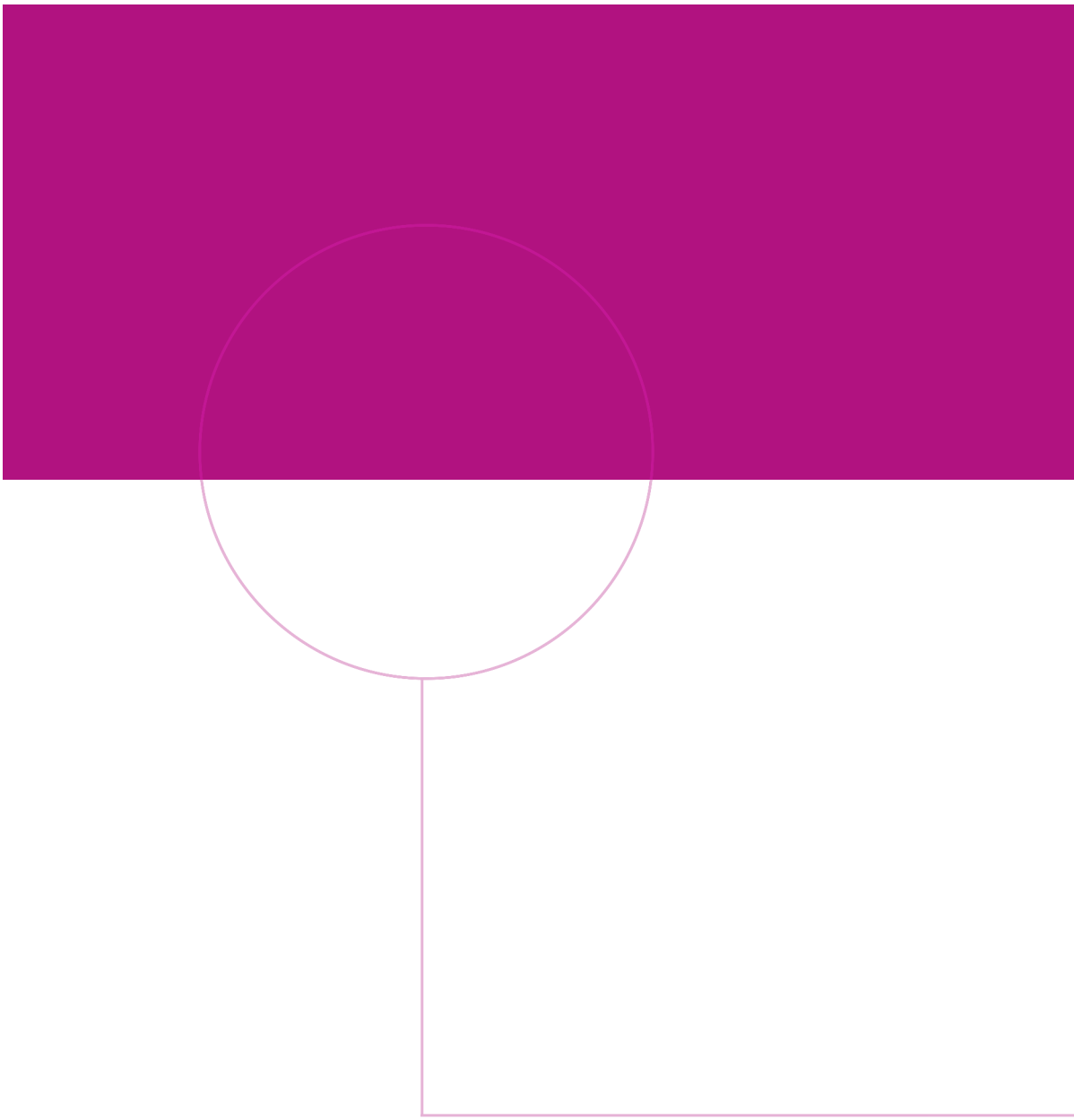
Aktivitet	Timer
Utvikling	138,75
Brukertesting	38,75
Selvstudium	41,5
Hovedrapport	117,4
Møte	46,25
Administrasjon	12,75
Peer-review	7
Forprosjekt	22,75
Reise	7



29.01.2024 17:30-20 peerreview	0,5	Peer-review	5
30.01.2024 11:15-13:15 definering av utrykk og endringer av format	2	Hovedrapport	5
30.01.2024 10:15-12:15 research FIDO standarder	1	Selvstudium	5
30.01.2024 13:25-13:50 | 14:10-14:45 peer review	1	Peer-review	5
30.01.2024 18:41-20:41 skriving	2	Hovedrapport	5
31.01.2024 10:00-12:30 14:00 - 16:30 skriving	5	Hovedrapport	5
31.01.2024 19:45-20:45 peer review	1	Peer-review	5
01.02.2024 møte med veileder + gruppemøte 10:00-10:30	0,5	Møte	5
01.02.2024 10:30-15:00 arbeidsøkt	4,5	Hovedrapport	5
01.02.2024 17:00 - 17:30 møtereferat	0,5	Administrasjon	5
01.02.2024 18:30-20:30 lagde excel mal for sammenligninger	2	Hovedrapport	5
02.02.2024 9:45-13:45	4	Hovedrapport	5
03.02.2024 10:00-12:00 prioritering av faktorer	2	Hovedrapport	5
05.02.2024 Issues, rom-booking etc	0,25	Administrasjon	6
05.02.2024 mandagsmøte	1,75	Møte	6
05.02.2024 16:30-18:30 | 19:30-21:15	3,75	Hovedrapport	6
06.02.2024 11:00 - 12:00 | 12:00 -15:00 | 21:00-21:30	4,5	Hovedrapport	6
07.02.2024 12:00 - 16:00 | 18:00 - 19:00 leser gjennom FIDO2 standarden	5	Selvstudium	6
07.02.2024 19:00-20:45 sekvensdiagram av førstegangsregistrering	1,75	Utvikling	6
07.02.2024 20:45-21:00 peer review	0,25	Peer-review	6
08.02.2024 10:00-10:30 | 13:30 - 15:30 møte med veileder og bian yang	2,5	Møte	6
08.02.2024 etterarbeid etter møte 10:30-13:00 | etterarbeid	2,5	Administrasjon	6
08.02.2024 research på kvantifiserbare data for brukervennlighet. 18:00 - 21:00	3	Selvstudium	6
09.02.2024 Møte med erik	0,5	Møte	6
09.02.2024 planla fremmtid for prosjekt etter møte	0,5	Administrasjon	6
09.02.2024 lagde møteagenda for møte med oppdragsgiver	0,25	Administrasjon	6
12.02.2024 Møte med oppdragsgiver og scrum møte	2	Møte	7
12.02.2024 Begynner koding av demo	1	Utvikling	7
13.02.2024 Møte med Halden kommune	0,5	Møte	7
13.02.2024 Leser meg opp på implementasjon av FIDO2 i golang	2,75	Selvstudium	7
13.02.2024 17:00-17:30| Leser meg opp på implementasjon av FIDO2 i golang	0,5	Selvstudium	7
13.02.2024 17:30 - 20:30 | Koder registrering for demo	3,5	Utvikling	7
13.02.2024 Fiksing av issues	0,25	Administrasjon	7
14.02.2024 9:45 - 11:45 | 12:15- 14:45| 16:00 - 20:30 | -en halvtime et sted inni der | Utvikling av registrering	8,5	Utvikling	7
14.02.2024 Dgitalt møte med gruppa	0,5	Møte	7
15.02.2024 Møte med veileder	0,5	Møte	7
15.02.2024 brainstorming av brukertester |10:30 - 12:45	2,25	Brukertesting	7
15.02.2024 fikset totp demo for brukertester	3	Utvikling	7
16.02.2024 bugfixer demo for omhu | 12:35-13:35	1	Utvikling	7
18.02.2024 bugfixer demo for omhu	0,5	Utvikling	8
19.02.2024 sprint møte med gruppe	2	Møte	8
19.02.2024 bugfixer demo og installerer SSL sertefikat 17:30-22:00 -30	4	Utvikling	8
20.02.2024 prøver for harde livet å sette opp SSL AAAAAAAAAAAAAAAAAAAAAAA 10:15-13:15| 15:00-18:00	6,5	Utvikling	8
21.02.2024 fortsetter å lage demo | 10:30-11:00 | 12:00-14:00 |	2,5	Utvikling	8
21.02.2024 Hjelper til med brukertester | 18:15 - 20:30 | 21:15 - 22:00	3	Brukertesting	8
21.02.2024 Integrerer ny frontend med webserver	0,75	Utvikling	8
22.02.2024 møte med veileder og gruppemøte	2	Møte	8
22.02.2024 gjennom gang av brukertester	1	Brukertesting	8
24.02.2024 demo koding på backend	3	Utvikling	8
25.02.2024 fiksing av frontend i demo	5	Utvikling	9
26.02.2024 fiksing av frontend i demo	3,5	Utvikling	9
26.02.2024 møte med oppdragsgiver	2	Møte	9
27.02.2024 Fullfører autentiserings-demoen	6	Utvikling	9

28.02.2024	brukerundersøkelser	2,5	Brukertesting	9
29.02.2024	møte med veileder	2	Brukertesting	9
02.03.2024	Lagde sekvensdiagram	1	Utvikling	9
04.03.2024	gruppemøte scrum møte	0,75	Møte	10
05.03.2024	ser på forelesning	1	Selvstudium	10
04.03.2024	ser på wireframe	1	Selvstudium	10
05.03.2024	Identifiserer problemer med omhu og lager wireframe	3	Selvstudium	10
06.03.2024	13:00-15 lager ferdig wireframe	2	Utvikling	10
07.03.2024	Arbeidsøkt på skolen og møte	3	Møte	10
08.03.2024	Fullførte wireframe	2	Utvikling	10
09.03.2024	Skriver om wireframe i rapport 20:00	1	Hovedrapport	10
10.03.2024	Skriver om wireframe i rapport	1,5	Hovedrapport	11
11.03.2024	16:50-17:50 demo del 2	1	Utvikling	11
11.03.2024	Møte med oppdragsgiver og sprint møte	2	Møte	11
12.03.2024	Intervju med assistermeg	1	Brukertesting	11
12.03.2024	Jobbing på del 2 demo	4	Utvikling	11
13.03.2024	Frontend jobbing 8:30-10:00 | 11:30-15:00 | 17:15 - 18:45	6,5	Utvikling	11
14.03.2024	8:30-10:30 | 11:30-15:00 | 17-21:30	9	Utvikling	11
17.03.2024	Jobbing på ansatt-seksjon demo	2	Utvikling	12
18.03.2024	Scrum møte på mandag	2	Møte	12
18.03.2024	Jobbing på demo	2	Utvikling	12
19.03.2024	Jobbing på demo 8:45-13:30 | 17:00-22:00	9,50	Utvikling	12
20.03.2024	Gjør ferdig demo 10:00-13 | 17:00-22:15	8,25	Utvikling	12
21.03.2024	Møteprepp og møte 9:45-11:00	1,25	Møte	12
21.03.2024	Leser meg opp på brukertester |11:00 -12:45 | 19:00 -19:45	2,5	Selvstudium	12
22.03.2024	Leser på brukertester	1	Selvstudium	12
22.03.2024	Begynner å skrive brukertest	3,25	Brukertesting	12
24.03.2024	Leser på tog	1	Selvstudium	13
27.03.2024	Brukertest	1	Brukertesting	13
28.03.2024	Forbereder brukertester for del 2 16:00-20:00	4	Brukertesting	13
30.03.2024	Lagde test plan	4,5	Brukertesting	13
31.03.2024	Testforberedelser og brukertest	2	Brukertesting	14
03.04.2024	Oppdragsgiver-møte	1	Møte	14
03.04.2024	Bug fixing	1	Utvikling	14
04.04.2024	Brukertest	2	Brukertesting	14
04.04.2024	Implementerer mal-editor	5	Utvikling	14
05.04.2024	Fikset noen bugs	0,5	Utvikling	14
06.04.2024	Koding 12:00-14:00 + 18:00-21:30	5,5	Utvikling	14
07.04.2024	Koding 15:00-16:00 18-21	4	Utvikling	15
08.04.2024	Møte med gruppa 10-11	1	Møte	15
08.04.2024	Fikser bugs og polerer nettside 16:45-21:45	5	Utvikling	15
09.04.2024	Kjører frem og tilbake til Halden	7	Reise	15
09.04.2024	Brukertester i halden	6,5	Brukertesting	15
11.04.2024	Møte med veileder og sprint møte	1,5	Møte	15
15.04.2024	Gruppemøte	0,75	Møte	16
15.04.2024	Skriver inn resultater fra undersøkelser 17:15-18:30	1,25	Brukertesting	16
16.04.2024	Bearbeider data fra brukertester 10:30-13:00	2,5	Brukertesting	16
16.04.2024	Leser opp på UX for analfabete	1,5	Selvstudium	16
17.04.2024	Mid-scrum møte	1,25	Møte	16
17.04.2024	Jobber på V3 av pasient-modul 11:15-16:00 18:30-20:30	6,75	Utvikling	16
18.04.2024	Jobber videre på V3 av pasient modul 11:30-14:30 18-20:15	5	Utvikling	16
19.04.2024	Bug fixer og rydder opp i kodebase 10:30-13:00	2,5	Utvikling	16
21.04.2024	Fikser bugs og styling	3	Utvikling	17

22.04.2024	Møte med oppdragsgiver og scrum møte etterpå	1	Møte	17
22.04.2024	Skriver på metode	3	Hovedrapport	17
23.04.2024	Skriver på metoder	4	Hovedrapport	17
24.04.2024	Starter endelig å skrive etter masse prokrastinering	4	Hovedrapport	17
25.04.2024	Møte med oppdragsgiver	0,5	Møte	17
25.04.2024	Skriver på hovedrapport	1	Hovedrapport	17
01.05.2024	Skriver utviklings-kapittel 9:45-11:45	2	Hovedrapport	18
04.05.2024	Jobbing på rapport 13:15-15:30 | 19:30-21:30	4,25	Hovedrapport	18
06.05.2024	Møte på morgenen	1	Møte	19
07.05.2024	Domenemodell	3	Hovedrapport	19
08.05.2024	lite møte på morgenen	0,5	Møte	19
08.05.2024	Skriving på hovedrapport	4,5	Hovedrapport	19
10.05.2024	Skriving på utviklings-kapittel	4	Hovedrapport	19
09.05.2024	skriving på utviklings-kapittel	1	Hovedrapport	19
11.05.2024	skriving	4	Hovedrapport	19
12.05.2024	12:30-15:00 17:00-19:45	5,25	Hovedrapport	20
14.05.2024	12:00-14:45 17:45-21:00	6	Hovedrapport	20
15.05.2024	15:00-15:45 18:00-22:15	5	Hovedrapport	20
16.05.2024	10:00-10:15	0,5	Møte	20
16.05.2024	14:00-15:45 17:45-23:15	7,25	Hovedrapport	20
17.05.2024	Nasjonaldags-grind 13:00-14:00 17:00-21:15	5,15	Hovedrapport	20
18.05.2024	13:00- 15:00 15:30-15:45 18:00-22:45	7	Hovedrapport	20
19.05.2024	11:30-14:30 18:00-22:00	7	Hovedrapport	21
20.05.2024	11:15 - 13 14-15:30 finpussing av oppgave	2,75	Hovedrapport	21
				0
				0
				0
				0



NTNU

Kunnskap for en bedre verden