UNIVERSITETET I OSLO
Institutt for informatikk

Universell utforming

Inkluderende og tilgjengelige autentiseringsløsninger

Masteroppgave

Ola Njå Bertelsen

31. oktober 2012

Sammendrag

Innlogging har vist seg å være en stor barriere for brukere av informasjonssystemer. Dette er spesielt et problem for personer med nedsatt sensorisk, motorisk eller kognitiv funksjon. I verste fall kan disse personene oppleve å bli stengt ute fra det digitale samfunnet og sentrale digitale tjenester som bank, handel, offentlige tjenester og sosial kontakt.

Diskriminerings- og tilgjengelighetsloven setter krav til at IKT-tjenester skal ha en universell utforming og være tilgjengelig for flest mulig, uten ekstra tilpasning. Foreløpig mangler de offentlige tilsynsmyndighetene en forskrift til loven som kan fortelle hvilke krav loven setter til disse tjenestene. Det finnes lite forskning på universell utforming av autentiseringsløsninger, og i eksisterende retningslinjer for universell utforming finnes det ingen ingen direkte krav til autentiseringsløsninger.

I denne oppgaven undersøkes rammevilkårene for å utvikle tilgjengelige autentiseringsløsninger. Det undersøkes og foreslås retningslinjer til slike løsninger, og til slutt vurderes det hvordan nærfeltskommunikasjon kan brukes for å skape en universelt utformet autentiseringsløsning.

Noen sentrale funn er at man må se på hele brukerens belastning og ikke bare vurdere enkeltsituasjoner. I dag ligger kostnaden ved autentiseringsløsningene på brukerne. Gjennom krav til å håndtere passord, brukernavn og kontoer utnytter tjenesteleverandørene brukerens hukommelse som om det var en uregulert allmenning. Passord og brukernavn står ikke foran en snarlig død. Derfor må systemet håndtere og være kompatibelt med eksisterende løsninger. Tilgjengelige løsninger må være stabile og ikke kreve at brukeren stadig lærer seg nye metaforer, designkonvensjoner og terminologi. Kompleksiteten med å innføre *stedet du er* som en autentiseringsfaktor og håndtering av mange ulike kontoer på en enhet kan føre til at systemet blir for usikkert og umulig for brukeren å konfigurere på en sikker måte.

Forord

Det har vært spennende å utforske temaet i denne oppgaven. Etter hvert har jeg skjønt at det ikke bare er et akademisk interessant tema, men et viktig tema som kan gjøre hverdagen til mange mennesker bedre. Det er utrolig at jeg knapt visste forskjell på en- og to-faktor autentisering når jeg begynte på oppgaven for et knapt år siden. Hadde jeg bare visst det jeg vet nå. Men sånn er det vel alltid, uansett hva vi foretar oss.

Jeg hadde løyet om jeg hadde sagt noe annet enn at jeg er lettet når jeg skriver dette. For selv om veien hit og ikke minst alle omveiene har vært interessante og temaet fremdeles engasjerer sterkt er jeg glad for å nærme meg slutten på denne oppgaven. Jeg er glad for at perioden hvor det er litteraturen, mitt hode og meg som utgjør brorparten av en arbeidsdag er over.

Jeg håper resultatet, det dokumentet du sitter med nå, kan gi deg noen gode ideer og innspill. At det kan være et bittelite skritt i en retning mot inkluderende løsninger.

En stor takk til de som stilte på intervju, workshop og til testing. Dere har for alltid gitt deres anonyme bidrag til oppgaven og kan dessverre ikke nevnes med navn.

En takk går også til alle de personene som utgjør E-me prosjektet. Det har vært uvurderlig å ta del i det arbeidet som er blitt gjort og de tankene som er delt.

Ikke alle er så heldige at de får oppleve en levende vitamininnsprøytning under veiledning. Jo Herstad skal ha en stor takk for innspill, utspill og diskusjoner i løpet av perioden. Det er alltid inspirerende å prate med deg.

De jeg har delt tak med det må også ha en takk. Jeg kan ikke forestille meg hvor mye dere gleder dere til å slippe diskusjoner om autentisering. Innspurten har også krevd tålmodighet fra dere. Takk Liv og Gina.

Silje, takk for kommentarer og innspill. Du er i en eksklusiv klubb når du har lest hele denne oppgaven.

Ola Njå Bertelsen
Stavanger
31.oktober 2012

Innhold

Figurer

Tabeller

Kapittel 1

Introduksjon

autentise´re v. gr.-lat
gå god for ektheten av

1.1 Innledning

Dette er en masteroppgave om brukerautentisering og universell utforming. For de fleste av oss er autentisering synonymt med innlogging til ulike nettjenester som nettbank og e-post. Du autentiserer også kjøp når du betaler med visakort i butikken. Og hver gang du låser opp en dør med nøkkel. Eller når du for n'te gang må slå PIN-koden på mobiltelefonen for å sjekke e-post eller ringe noen.

En ting er at vi får flere kontoer, passord og brukernavn for hver dag som går. Det er en utfordring de fleste av oss klarer å håndtere på et vis. Verre er det for alle de hvor brukerautentiseringen står i veien for å gjøre helt nødvendige ting som å betale regninger i nettbanken, opprettholde sosial kontakt med venner og familie og ikke minst levere selvangivelsen. De blir i praksis satt på siden av det digitale samfunnet. Utestengelsen kan henge sammen med senorisk, kognitiv eller motorisk funksjonsnedsetting. Det de opplever er et gap mellom evner og krav, noe som fører til en funksjonshemning. Det er antagligvis noe vi alle vil få oppleve på en eller annen måte. Nedsatte sensoriske, kognitive og motoriske evner er en naturlig del av aldringsprosessen.

Universell utforming er utforming av programmer og tjenester på en slik måte at de kan brukes av alle mennesker, i så stor utstrekning som mulig, uten behov for tilpassning og en spesiell utforming. Og denne oppgaven ser nærmere på hvordan vi kan utforme løsninger for brukerautentisering på en måte som gjør den tilgjengelig for flest mulig. På den måten kan vi gå fra ekskluderende autentiseringsløsninger til inkluderende autentiseringsløsninger.

Oppgaven har bakgrunn i fagfeltet interaksjonsdesign som henter inspirasjon fra mange ulike akademiske disipliner. Temaet for oppgaven er en del av et større forskningsprosjekt på *inkluderende identitetshåndtering* i nye sosiale medier, E-Me prosjektet.

1.2 Motivasjon

Motivasjonen for denne oppgaven ligger på tre plan. Det ene er egoistisk og kortsiktig. Det handler om å forbedre min situasjon i møte med utallige kontoer med ulike passord og brukernavn. Jeg har nøkler, dingser og enheter som må håndteres sikkert. Kodebrikke fra banken, kode til nettbanken, PIN-kode til mobilbanken en annen PIN-kode til visakortet og en siste PIN-kode til kredittkortet. De seks bare for å håndtere betalinger. En stadig økende mengde med kontoer på web som oprettes hist og her av mer eller mindre uklare grunner. Resultatet er en brukernavn/passord/konto/dingsekabal som står ustøtt som et korthus i lett bris. Det er allerede krise og helt åpenbart ikke en bærekraftig utvikling.

Det andre planet er i større grad altruistisk. Det handler om at kommunikasjons- og informasjonsteknologi bør være et gode alle får ta del i. Jeg skriver denne oppgaven med menneske-maskin-interaksjon og interaksjonsdesign som teoretisk bakgrunn. Vi designer interaksjoner. Eller skaper interaksjoner. I dette ligger en makt og en plikt til å lage systemer som inkluderer, ikke ekskluderer mennesker. Utover denne etiske plikten ser vi også at universell utforming er på full fart fremover. Det er et kjent begrep innen arkitektur. Nå ser vi at krav om universell utforming også kommer til informasjonssystemer. Det ligger tydelige politiske mål om dette, noe som har materalisert seg i Diskriminerings- og tilgjengelighetsloven (DTL) som setter krav til universelt utformede løsninger. Samfunnet forøvrig forventer også dette. Brukerne forventer det.

På det tredje planet og det som gjør dette spesielt spennende er at det tilsynelatende finnes få retningslinjer for hvordan vi kan utforme brukerautentisering slik at det er tilgjengelig for alle. Problemet blir ikke mindre. Det går heller i motsatt retning. Vi får flere og flere kontoer på web. Vi får flere og flere enheter som skal kobles opp mot hverandre og internett. Det blir vanskeligere og vanskeligere å ikke ha tilgang til digitale tjenester. Forhåpentligvis kan denne oppgaven være med på å bidra til økt kunnskap om hvordan vi kan kombinere informasjonssikkerhet, brukeropplevelse og universell utforming i løsninger som inkluderer flest mulig. I løsninger som er sikre, tilgjengelige og som tilbyr gode brukeropplevelser.

1.3 Problemstilling

Spørsmålene jeg vil belyse i denne oppgaven er

1. Hvilke rammefaktorer står en overfor i utvikling av universelt utformede autentiseringsløsninger?

2. Hva kreves av en universelt utformet autentiseringsløsning?

3. Hvordan kan nærhetsteknologi brukes for å skape en universelt utformet autentiseringsløsning?

1.3.1 Hvilke rammefaktorer står en overfor i utvikling av universelt utformede autentiseringsløsninger

Jeg ønsker å finne ut av hvilke rammefaktorer som har eller kan ha stor betydning for utviklingen av universelt utformede autentiseringsløsninger. Det vil være naturlig å se nærmere på retningslinjer for universell utforming. Aktuelt lovverk vil være interessant å se på. Kunnskapsnivået rundt dette temaet vil være en viktig rammefaktor. Eventuelt andre incentiver eller faktorer som legger til rette for, eller står i veien for, utvikling av tilgjengelige løsninger vil også kunne bli identifisert og beskrevet.

1.3.2 Hva kreves av en universelt utformet autentiseringsløsning?

Hva ligger i begrepet universell utforming? Hva krever en løsning med tanke på brukeropplevelse og tilgjengelighet? For å kunne svare på det må jeg finne ut av hvilke krav folk har både til funksjonalitet og til bruk. Det vil også være essensielt å vite hvordan brukeren vurderer risikoen og sikkerhetsbehovet til ulike enheter og tjenester.

1.3.3 Hvordan kan nærhetsteknologi brukes for å skape en universelt utformet autentiseringsløsning?

Teknologi basert på kort og mellomkort kommunikasjon er i vinden. Hva er nærhetsbasert autentisering? Kan det brukes? Og i tilfelle hvordan kan det brukes for å skape universelt utformede løsninger for brukerautentisering? Her vil det være spesielt interessant å se på tidligere forskning og forsøk rundt temaet.

1.4 Bakgrunn

Dette er en oppgave om brukerautentisering. Norsk senter for informasjonssikring (NorSIS) sier følgende om identifisering og autentisering:

> **Identifisere**
>
> Å gi seg til kjenne. Når man logger seg på datamaskinen identifiserer man seg først ved å angi brukernavn, så autentiserer man seg med å angi passord.
>
> **Autentisering**
>
> Å bevise at man er den man utgir seg for å være. Autentisering skal bekrefte en påstått identitet. Dette kan skje gjennom noe du vet (passord), noe du er (fingeravtrykk/ biometri) eller noe du har (nøkkelkort). Kombinasjoner av disse er også mye brukt. Den som autentiseres kan være en person som bruker en datamaskin, kun en datamaskin eller et program. [22]

Identifisering, autentisering, adgangskontroll, «identity management». Et system skal vite at du er den du oppgir deg for å være når du prøver

å få adgang til et system. Implisitt ligger det i dette at systemet vet hva en identitet er autorisert[1] til. Dermed kan vi si at så snart det er mulig å fastsette identitet vil resultatet være autorisasjon.

O'Gorman [71] skriver hvordan autentisering var enklere før i tiden.

> «In times gone by, authentication was not a complex task. One person, call her Alice, would meet another person, Bob, and either recognize him by visual appearance or not. If Alice did not recognize Bob, he could explain that he was a friend of a friend, or a business envoy, etc. and Alice could decide whether to believe him. Of course, if Alice and Bob were spies, they would use more formal methods for mutual authentication-from piecing together two halves of a ripped page to exchanging prearranged nonsense statements. But spies were the exception.
>
> Enter the computer era, and authentication has changed. Now we cannot see the entity on the remote end of a computer network, and indeed the entity could be a friend, a machine, or an attacker. We exchange personal information, such as financial and health data, that we wish to remain as private and as confidential as correspondence between spies.» [71, Side 1]

Bare siden Gorman skrev dette i 2003 har de fleste av oss fått enda flere enheter å håndtere, enda flere kontoer. Hver eneste dag bruker vi enheter med prosessorer i. Bell and Dourish [33] mente i 2007 at vi allerede var kommet til Weisers fremtid [87] med allestedsnærværende prosessering, med den forskjellen at bruken ikke var slik Weiser forutså. Parallelt med utbredelsen av prosessorer og enheter som kjører software har behovet for autentisering økt. Først gjennom utbredelsen av dataenheter, deretter har vi vært, og er i, en periode med stor vekst i antall webapplikasjoner som krever innlogging. Kanskje er vi i startgropen på tredje bølge av autentiseringskrav, drevet av fysiske enheter gjennom utbredelsen av tingenes internet? De ulike utviklingstrekkene peker i en og samme retning, mot mer og flere krav til menneske-maskin autentisering. En tidsalder hvor vi er blitt vant til allestedsnærværende datamaskiner og blir tvunget til å tåle det jeg vil kalle et *allestedsnærværende autentiseringsbehov i en maskinlesbar verden*.

På tross av at vi har mellom 20 og 30 år bak oss med forskjellige forsøk på autentisering gjennom andre former enn brukernavn/passord metaforen (B/P)[53, 35] har vi per i dag ikke noen alternativer med særlig utbredelse. Dog har vi flere tillegg til B/P metaforen for eksempel BankID og Smartkort. Disse blir lagt til som et ekstra sikkerhetselement for å skape fler-faktor autentisering. Det er gjort forsøk på å lage nærhetsbaserte og kontekstbevisste løsninger som skal gjøre det lettere å få adgang [se for eksempel 32, 31, 54, 72]. Flere av disse forsøkene virker lovende med tanke på å kunne tilby tilgjengelige systemer med gode brukeropplevelser.

[1] Autorisering er prosessen med å beslutte å gi en person, en datamaskin eller et program tillatelse til å bruke bestemte IT-ressurser. Eksempler på en IT-ressurs kan være filer, nettverksstasjoner og prosesser.[22]

Som nevnt under motivasjon kommer det krav fra ulike hold til at informasjonsløsninger skal være universelt utformede. DTL er et eksempel [24] Vi ser en politisk agenda for å fremme tilgjengelige løsninger i utredninger og stortingsmeldinger [28, 25, 27]. Behovet for tilgjengelige løsninger er dokumentert i ulike forskningsrapporter[46, 45].

Inspirert av Pullin [74] ønsker jeg å snu det som oppleves som en negativ egenskap (manglende syn, bevegelse, hukommelse ol.) i forbindelse med autentisering til en styrke. Det vi opplever i dag med allestedsnærværende autentisering er at vi blir blinde (tingene mangler skjerm), vi blir døve (ingen høytaler), vi mangler evnen til å taste inn B/P (ikke noe tastatur). Vi har problemer med å huske lange nok, og mange nok, passord og PIN-koder(hukommelse). I det hele tatt har vi alle i større og mindre grad latt teknologien gjøre oss funksjonshemmede. Løsningen på inkluderende autentisering kan være løsningen på allestedsnærværende autentisering og motsatt.

1.4.1 E-me prosjektet

Oppgaven er en del av E-me prosjektet hvor vi jobber for å skape det som kalles «inkluderende identitetshåndtering». Først og fremst med tanke på at «autentiseringsløsninger ikke skal stå i veien for deltagelse i sosiale medier og det digitale samfunnet»[1]. Vårt utgangspunkt er at «[En] Funksjonshemning oppstår når det foreligger et gap mellom individets forutsetninger og omgivelsenes utforming eller krav til funksjon.»[26] Funksjonshemning er med andre ord ikke en individuell egenskap, men et forhold eller en situasjon som kan oppstå i et individs møte med samfunnet. Derfor er vår oppgave å lage løsninger som forhindrer at det oppstår en funksjonshemmning i utgangspunktet.

Prosjektet er finansiert gjennom VERDIKT-programmet i Norges forskningsråd. Det eies av Norsk Regnesentral (NR) og Karde AS leder prosjektet. E-me prosjektet startet opp i mai 2010, og varer ut 2013.[1] Det empiriske forskningsarbeidet blir gjort ut i fra organisasjoner som gir konkrete kasuser å jobbe med. De organisasjonene som er en del av E-me forskningen er: Brønnøysundregistrene, Storebrand ASA, Encap AS, Dysleksi Norge, Norges Blindeforbund og Seniornett Norge [1].Det er allerede publisert resultater fra forskningen og mer vil bli publisert i løpet av det kommende avsluttende året for E-me prosjektet. Et sentralt funn som er gjort tidlig i prosjektet er Fuglerud et al. [46], Fritsch et al. [45] som begge finner at det er gjort en del arbeid når det gjelder sikkerhet og brukervennlighet, men lite når det gjelder universell utforming og brukerautentisering: «*Det ser altså ut til at det er gjort svært lite arbeid når det gjelder universell utforming av sikkerhetsløsninger*»[46, Side 14].

1.5 Kapitteloversikt

Strukturen i denne oppgaven er som følger: Kapittel to går igjennom relevant litteratur. Her går jeg inn på konsepter og begreper som blir

brukt gjennom oppgaven. Først ser jeg nærmere på hva interaksjonsdesign er, hvordan man kan skape gode brukeropplevelser og sammenhengen mellom informasjonssikkerhet og brukeropplevelse. Deretter ser jeg på hva universell utforming er, hvordan vi forstår funksjonshemning og hva inkluderende identitetsforvaltning er. Jeg går igjennom begreper og konsepter rundt informasjonssikkerhet, før jeg ser på tidligere forskning på nærhetsbasert autentisering.

I kapittel tre redegjør jeg for metodene som er brukt i oppgaven. Hvorfor jeg har valgt et kasusstudie og bakgrunnen for å bruke intervju og workshop som viktige kilder til informasjon.

I kapittel fire redegjør jeg for kasuset. Jeg forklarer sammenhengen mellom denne oppgaven og E-me prosjektet. Beskriver fokusområdet for dette kasuset før jeg beskriver de ulike teknologiene som er brukt for å demonstrere systemer for intervjuobjektene og deltakerne i workshopen.

I kapittel fem legger jeg frem funnene som er gjort. Dette er funn under rammevilkår for universell utforming, funn fra intervjuene, workshopen og testen av LastPass.

I kapittel seks diskuterer jeg først rammefaktorer for universelt utformede autentiseringsløsninger. Deretter temaet universell utforming og autentisering, hvor jeg kommer med forslag til retningslinjer for en tilgjengelig autentiseringsløsning. Til slutt diskuterer jeg hvordan nærhetsteknologi kan brukes for å skape en universelt utformet autentiseringsløsning.

I kapittel syv presenterer jeg konklusjonene fra diskusjonskapittelet.

Kapittel 2

Teori

> «The continiued domination of passwords over all other methods of end-user authentication is a major embarrassment to security researchers»
> Bonneau et al. [35]

2.1 Brukeropplevelse

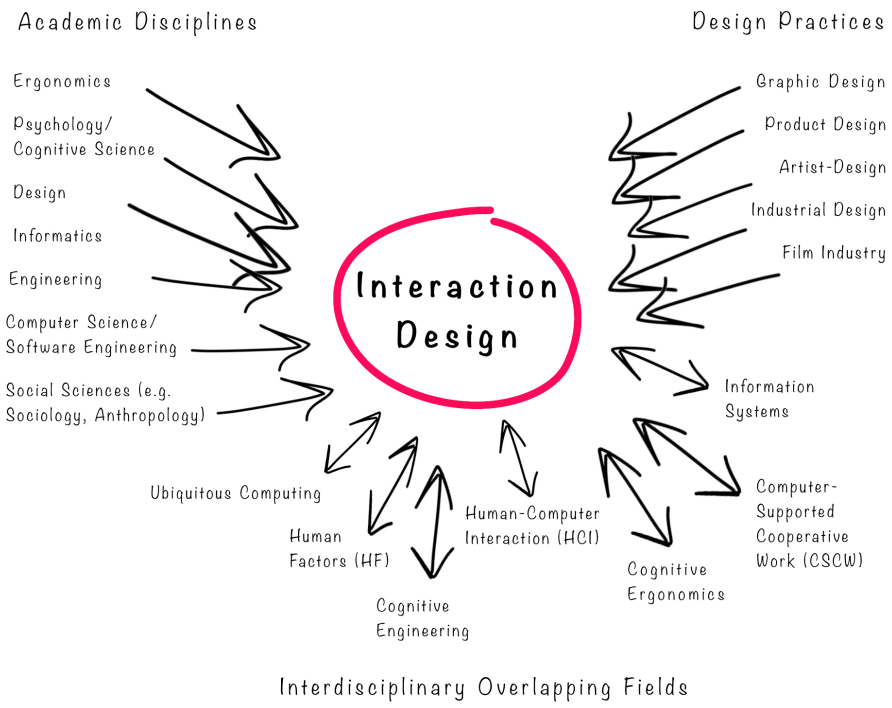
2.1.1 Hva er interaksjonsdesign?

Sharp et al. [78] definerer interaksjonsdesign på følgende måte:

> **designing interactive products to support the way people communicate and interact in their everyday and working lives.**[78, side 9]

De sier videre at en rekke begreper brukes for å dekke forskjellige aspekter ved det som blir designet. Dette inkluderer *user interface design*, *software design*, *user-centered design*, *product design*, *web design*, *experience design* og *interactive system design*. Interaksjonsdesign blir her brukt som en fellesbetegnelse på disse begrepene. Fokuset innenfor interaksjonsdesign ligger på praksis, med andre ord: «hvordan designe brukeropplevelser»[78]. En er ikke knyttet spesielt til én måte å gjøre ting på. I stede fremmes en rekke metoder, teknikker og rammeverk. [78] illustrasjon av denne posisjoneringen av interaksjonsdesign vises i figur 2.1 på side 8. Der illustreres interaksjonsdesign gjennom et samspill med en rekke forskjellige akademiske disipliner. [78] forklarer at det på grunn av den store tverrfagligheten ikke kan kreves at èn person mestrer alle fagfeltene det er heller grupper sammensatt av forskjellige personer med forskjellige bakgrunner som utgjør et designteam. Hvem teamet består av avhenger selvsagt av oppgaven, omfang og designfilosofien til selskapet eller gruppen [78]. De skriver følgende om oppgaver de mener gruppen må håndtere:

> Designers need to know many different things about users, technologies, and interactions between them in order to create effective user experiences. At the very least, they need to understand how people act and react to events and how they



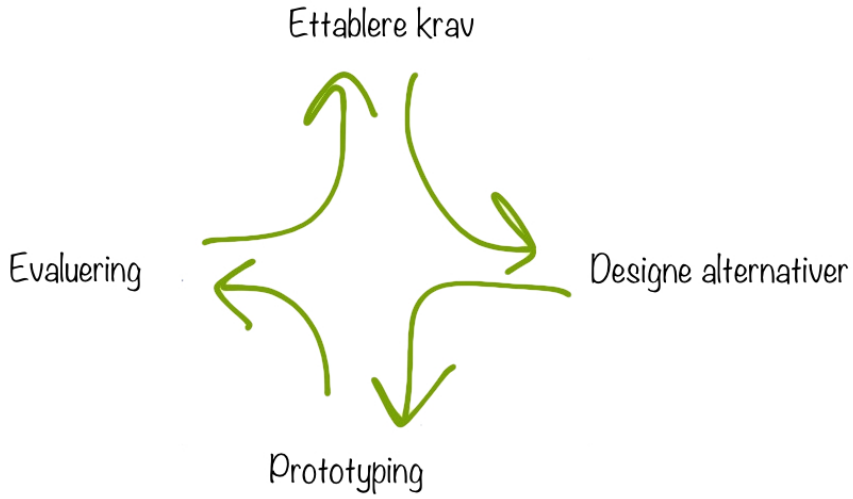
Figur 2.1: Relasjonen mellom interaksjonsdesign og andre akademiske disipliner fra [78, side10]

> communicate and interact with each other. To be able to create engaging user experiences they also need to understand how emotions work, what is meant by aestethics, desirability, and the role of narrative in human experience. Developers also need to understand the business side, the technical side, the manufacturing side, and the marketing side. [78, side 11].

Et sentralt anliggende innen interaksjonsdesign er å utvikle interaktive produkter som er brukbare. Med dette menes generelt sett at det er *enkelt* å lære, *effektivt* å bruke og at det gir en *gledelig* brukeropplevelse Sharp et al. [78, side 2]. Gjennom å identifisere spesifikke styrker og svakheter av forskjellige interaktive systemer kan vi begynne å forstå hva det betyr om noe er brukbart eller ikke. Når man designer interaktive produkter kreves det at en tar hensyn til hvem som skal bruke dem, hvordan de skal bli brukt og hvor de skal bli brukt [78, side 6].

Et nøkkelspørsmål innenfor interaksjonsdesign er: hvordan optimaliserer du for brukerens interaksjoner med et system, miljø eller produkt, slik at de støtter eller utvider brukerens aktiviteter på en effektiv, nyttig og brubkar måte [78, side 7]. I følge [78] kan en bruke intuisjonen og håpe på det beste, men de anbefaler selvsagt å begrunne designvalgene gjennom å forstå brukeren.

- Taking into account what people are good and bad at.



Figur 2.2: Interaksjonsdesign prosessen [78, side 15]

- Considering what might help people with the way they currently do things.
- Thinking through what might provide quality user experiences.
- Listening to what people want and getting them involved in the design.
- Using tried and tested user-based techniques during the design process. [78, side 8]

Sharp et al. [78] omtaler fire grunnleggende oppgaver innenfor interaksjonsdesign disse er illustrert i figur 2.2. Disse oppgavene påvirker hverandre og skal gjentas slik at produktet stadig forbedres. Evaluering av produktet eller løsningen er viktig for å få tilbakemelding fra brukerne og fra bruk av produktet. Blant annet nevnes observasjon, spørsmålsskjema og intervjuer som metoder å få tilbakemeldinger på. En like viktig del av evalueringen er å forstå hva folk gjør. Hvordan handler de? Hvilke evner, følelser, behov og begjær har de? Hva får dem til å bli irritert, frustrert, miste tålmodigheten eller kjede seg ?[78]

Nettopp det å lære seg mer om folk og hva de gjør kan være med å avsløre ukorrekte antagelser som designeren har om enkelte brukergrupper og hva de trenger. Sharp et al. [78] trekker frem antagelsen mange gjør med at eldre personer ønsker at ting skal være store på grunn av nedsatt syn og fingerferdighet som eksempel. Det viser seg at mange personer i 70- og 80-års alderen fint klarer å håndtere ting med standard størrelse, selv små grensesnitt som mobiltelefoner. Mange av disse personene ønsker heller ikke spesiallagde løsninger som kan minne

dem, og omverdenen, om at de blir eldre og at kognisjon og fingerferdighet ikke er som før. [78]

2.1.2 Brukeropplevelse

I følge Sharp et al. [78] bruker den siste internasjonale versjonen av «standard for human-centered design» (ISO 13407) *brukeropplevelse* som en samlebetegnelse som dekker nytte (usefulness), attrådverdighet (desirability), kredibilitet (credibility) og tilgjengelighet (accessibility). Det er et begrep som er bredere enn det tradisjonelle brukervennlighet (usability) og tar i større grad hensyn til at disse begrepene henger uløselig sammen [78].Sandnes [75] skriver at begrepet brukervennlighet, også omtalt som brukskvalitet, stammer fra den engelske betegnelsen usability. Standarden ISO 9241-11 definerer brukervennlighet slik (oversatt fra engelsk) «At et produkt kan brukes av bestemte brukere for å oppnå et spesifikt mål med effektivitet og tilfredshet i brukskonteksten» [75, side 16]. Norman [66] skriver om hvor viktig attrådverdigheten er og i hvor stor grad følelsene våre slår inn og har betydning for brukeropplevelsen. Gjennom boken viser han tydelig hvor viktig det er at interaksjonen også inneholder og bygger opp om det brukeren vil og en gir en god følelse til brukeren. Sharp et al. [78] lister opp seks velkjente brukervennlighetsmål:

- Effektivt å bruke. (Effectiveness)
- Virkningsfult å bruke. (Efficiency)
- Trygt å bruke.
- Ha god nytte.
- Lett å lære.
- Lett å huske hvordan det skal brukes.

[78, side 19]

Disse målene kommer i litt forskjellige versjoner. Nielsen [10] har fem punkter hvor «feil» og «tilfredsstillelse» står som to andre mål eller komponenter. Listene er relativt like i betydning når en ser på helheten, selv om begrepene som brukes er noe ulike.

Pettersen [73] skriver i sin analyse av begrepene tilgjengelighet og brukbarhet at retningslinjer for tilgjengelighet ofte egentlig dreier seg om *teknisk tilgjengelighet*. Han konkluderer med at nettsider som er tilgjengelige ikke trenger være brukbare og at det mellom begrepene tilgjengelighet og brukbarhet ligger delte utfordringer som er både tilgjenglighets- og brukbarhets utfordringer. Dette kaller han *universell brukbarhet* se figur 2.4 på side 21.

Begrepet brukeropplevelse brukes i denne oppgaven som en samlebetegnelse og med den forståelsen som er redegjort for over nemlig at begrepene tilgjengelighet, brukervennlighet, attråverdighet, nytte eller andre begreper er knyttet uløselig sammen og gjensidig avhengig. Det er dermed

ikke sagt at det ikke kan være nyttig å bruke smalere definisjoner for å være tydelig på hva en omtaler.

2.1.3 Brukergrensesnitt

> «Brukergrensesnittet er det mest synlige i et datasystem, og befolkningens port mot den digitale verden. Uansett hva som ligger under panseret, og uansett hvor avansert eller enkel den underliggende datateknologien er, så er det brukergrensesnittet som gir inntrykk av tjenesten som tilbys. På mange måter er brukergrensesnittet den viktigste kompontenten i et datasystem med tanke på å skape tillit, trygghet og tilfredshet blant brukerne. I den kommersielle verden er det ofte brukergrensesnittet som avgjør om du vinner konkurransen om kunder.» [75, side 13]

For de fleste brukere er det brukergrensesnittet som *er* systemet. Det er dette grensesnittet som definerer brukeropplevelsen. Men som vi skal se er det like viktig hvordan systemet er satt sammen for å få brukergrensesnittet til å fungere slik en ønsker. Først skal vi gå igjennom noen vanlige typer brukergrensesnitt.

Ulike typer brukergrensesnitt

Brukergrensesnitt har hele tiden vært i utvikling. Går vi langt nok tilbake hadde ikke datamaskinene en gang en skjerm eller et tastatur. Musen kom første gang på 60-tallet og andre former for brukergrensesnitt kan være vanskelig å tidfeste nøyaktig. Situasjonen i dag er at vi har en økende mengde former for grensesnitt mot datamaskiner. Først og fremst fordi vi har hatt en enorm økning i antall enheter med en datamaskin i og en endring i størrelse av enhetene. Sharp et al. [78] lister opp hele 20 forskjellige typer grensesnitt. Det inkluderer blant annet: Kommandobasert, grafisk, touch, tale, multimodal, usynlig, intelligent, adaptiv, håndgripelig[1], haptisk og flerbrukeranvendelse[2]. I følge Sharp et al. [78] vil hvilke typer brukergrensesnitt som er aktuelt for en spesifikk løsning bli tydelig i en designprosess. Dette vil være avhengig av en rekke faktorer så som pålitelighet, sosial aksept, personvern, etikk og lokasjon.

Bruce Tognazzini skriver sågar i [39]

> The ideal interface is no interface at all, and most of the complexity of a multilayered security scheme could and should be hidden from the user. Those parts that are visible should enable the user to simply and flexibly change security parameters. [39, side 45]

Dette fører oss videre til retningslinjer for design.

[1] Engelsk: Tangible

[2] Se [78, side 158] for en mer utfyllende liste

2.1.4 Designretningslinjer

Det finnes en rekke, om ikke utallige retningslinjer for design i litteraturen. Sharp et al. skriver at disse retningslinjene som regel har opphav fra en miks mellom kunnskap, teori, erfaring og sunn fornuft. Og at de som regel er ment som tips for designere slik at en husker å få med seg visse funksjoner i løsningen. Noen av de best kjente og utbredte retningslinjene er *synlighet, tilbakemelding, restriksjoner, overensstemmelse* og *ytelse*[3][78, side 26] Tognazzini er bare én av de som har beskrevet noen av disse retningslinjene mer utfyllende [13]. Normans klassiker The Design of Everyday Things gir også en god innføring i begrepene [65].

Andre retningslinjer er mer spesifikke med tanke på hvordan grensesnittet skal utformes. De er mest interessant i utvikling av et grensesnitt. Men Norman [65] anbefaler å følge designkonvensjoner så langt som mulig for å hjelpe brukeren å forstå hvilke handlinger han skal gjøre og la brukeren se hvilke handlinger som er mulige. Spesielt en ting er viktig å få med seg og det er at de metaforene vi bruker og de grensesnittene og konvensjonene vi utnytter ikke er medfødt. I følge Norman [68] finnes det ikke noe slikt som naturlige grensesnitt, heller ikke når man flytter interaksjonen fra mus og tastatur til touchflater.

Psykologisk akseptabilitet

En annen utfordring når en designer systemer er den økende graden av kompleksitet som tvinger seg frem. For stor kompleksitet kan gå ut over sikkerheten i følge Matt Bishop han skriver følgende:

> ≪ A fundamental precept of designing security mechanisms is that, as the mechanisms grow more complex, they become harder to configure, to manage, to maintain, and indeed even to implement correctly. Errors become more probable, thereby increasing the chances that mechanisms will be configured erroneously, mismanaged, maintained improperly, or implemented incorrectly. This weakens the security of the system. So the more complex a system is, the more secure it should be–yet the less secure it is likely to be, because of the complexity designed to add security!≫ [39, side 1]

Bishop skriver i denne sammenheng om prinsippet om psykologisk akseptabilitet fra Saltzer og Schroeder:

> ≪**The Principle of Psychological Acceptability** "It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of

[3](Engelsk: Visibility, Feedback, Constraints, Consistency, Affordance

> his protection needs into a radically different specification language, he will make errors."–Jerome Saltzer and Michael Schroeder» [39, side2]

Bishop trekker frem tre faktorer for å illustrere dette problemet det er passord, «patching» og konfigurasjon[39]. For passord er det spesielt den iboende motsetningen mellom at et passord må være lett å huske for brukeren og samtidig vanskelig å gjette seg frem til. For B/P metaforen skriver han at brukerens tendens til å velge for enkle passord kommer av at brukeren gjør dette for å gjøre autentisering gjennom B/P psykologisk akseptabel. Patching tar utgangspunkt i administratoren av systemer. Nye patcher for å reparere noen kjente feil kan føre til interferens og stoppe programmer som er kritiske. Derfor er hele prosessen med patching av programvare for krevende til å kunne leve opp til idealet om psykologisk aksept. Han nevner den økende graden av auomatisk patching i privat sammenheng som en positiv trend, men som vi vet for lite om konsekvensene av enda. Når det gjelder konfigurasjon sier han det aller best med egne ord:

> Building a secure system does not assure its security: the system must also be installed and operated securely. Configuration is a key component of secure installation and operation, because it constrains what users and the system processes can do in the particular environment where the system is used. [39, side9]

2.1.5 Informasjonssikkerhet og brukeropplevelse

Brukeropplevelse og informasjonssikring er ikke et nytt forskningsfelt. Adams og Sasses artikkel fra 1999[29] blir nevnt i de aller fleste studier som omfatter brukere og autentisering eller informasjonssikkerhet. Weir et al. [86] skriver:

> Although service providers should set appropriate levels of security, they must also consider the users' willingness to adopt procedures.(...) Typically, a compromise is found which balances actual security levels with user and usage perspectives. If security levels are perceived to be unwieldly, users will workaround them and compromise security or avoid use.» [86, s 154].

Adams og Sasses skriver i sin klassiske artikkel «If a password mechanism is incompatible with users' work practices, they perceive the security mechanisms as not sensible"and circumvent it» [29, side 45]. Også Bardram omtaler dette fenomenet [31]. Norman illustrerer på en fornøyelig måte hvordan vi håndterer slike fenomener, hvor sikkerhet er i veien, i hverdagen [67]. Han beskriver hvordan ulike «sikkerhetsnivåer» og tilgang til dører gjør at et møterom hvor også utenforstående har tilgang ligger utenfor sonen hvor toalettene ligger. Dette fører til at ingen utenforstående uten nøkkel kan komme fra det åpne og tilgjengelige

møterommet til toalettene uten følge fra noen med nøkkel. Dette blir løst så enkelt at døren som krever nøkkel blir holdt åpen med en dørstopper slik at behovet for nøkkel ikke lenger er der.

Sasse og Flechais [39] skiver «We view secure systems as socio-technical systems; thus, we are not just concerned with improving the usability of security mechanisms for individual users: our aim is to improve the effectiveness of security, and reduce the human and financial cost of operating it.» [39, side 14]. De skriver videre at en forutsetning for å få til dette er å innvolvere brukeren i designprosessen. Blant annet må ikke kompromissene mellom sikkerhet og brukeropplevelse bli tatt av sikkerhetseksperter. Brukeren må også læres opp og trenes i å forstå sikkerhetsproblemer og behov. Systemet må unngå å kreve «merkelig oppførsel» fra brukeren. Med andre ord må systemet ikke kreve at brukeren gjør ting som ikke er sosialt akseptable. Sasse og Flechais skriver for eksempel at brukere som er veldig opptatt av sikkerhet og følger alle sikkerhetsråd blir sett på som paranoide og pertentlige, egenskaper de fleste ikke ønsker å bli forbundet med. En kan heller ikke kreve av brukeren at han skal ha inngående kjennskap til systemene. [39]

Tognazzini [39] oppsummerer det godt i én setning:

> «The goal of security is not to build systems that are theoretically securable, but to build ones that are actually secure.»
> [39, side 31]

Han tar til orde for å gjøre begrepet sikkerhet noe mer elastisk i forhold til situasjonen brukeren befinner seg i. Blant annet trekker han frem mobile systemers evne til å være mer eller mindre stedsbevisste gjennom GPS posisjon. WiFi MAC adressen kan også fortelle maskinen at du sitter på hjemmenettverket. Han foreslår tre nivåer fra lav til høy sikkerhet alt etter hvor du befinner deg som en mer sofistikert tilnærming til sikkerhet [39]. En må også stole på brukeren og overlate noen valg til brukeren om hvordan sikkerheten skal eller bør være. For eksempel om brukeren vil at passordet skal være synlig slik at denne kan sjekke om det hun har trykket på en feil tast. Han skriver om utviklingen av Tresor 2.2, en nøkkelringapplikasjon som lot brukeren se deler av passordet slik at det var lettere å kontrollere om det var riktig skrevet [39], og beskriver opplevelsen av å bli for opptatt av «worst-case scenario»

> It had suddenly seemed to me sacrilegious to implement anything that could even remotely help an eavsdropper, regardless of what it cost the user. I was gripped with a terrible fear that someday, some document would "get out," and it would be my fault.
>
> When I pulled back, I stopped considering only the worst-case scenario, which for me was the user typing in passwords while standing in Grand Central Station with 12 people in trench coats hovering over her shoulder while another battery of 12 people trained high-tech cameras on her screen. I instead strove for a balance between user and bad guy, and then gave

> the user the power to control her own use of the product.» [39, side 37]

Gutmann and Grigg [51] skriver at sikkerhet må følge brukervennlighet, ikke den andre veien. Vi er villige til å akseptere noe høyere kompleksitet dersom verdien er høyere. Men det må være opplevd verdi, sikkerhet oppleves stort sett ikke som å ha høy nok verdi. De mener vi kanskje må leve med å legge sikkerheten til etterpå, de nevner SSL, SSH som eksempler. De viser også til en kjent kryptograf Auguste Kerckhofs som skrev om sikkerhet i kommunikasjonssystemer. Han hadde seks krav til et system[Kerckhoffs 1883, her fra 51] :

1. Systemet må være praktisk om ikke matematisk ukrypterbart.
2. Det må kunne falle i «fiendens» hender. Med andre ord det må ikke være basert på hemmelighold.
3. Nøkkelen må være kommuniserbar.
4. Det må være kompatibelt med kommunikasjonsløsningen.
5. Det må være portabelt og ikke kreve flere aktører.
6. Systemet må være enkelt å bruke. Ikke kreve mental styrke eller kunnskap om en lang serie av regler.

Gutmann and Grigg [51] påpeker at de fleste av punktene på listen ikke er sikkerhetskrav men brukeropplevelseskrav.

Marcelo Carlomagno Carlos [60] skriver om svakheten i kommunikasjonen mellom menneske og maskin har bakgrunn i:

- Lack of knowledge of computing.
- Lack of knowledge of security.
- Lack of knowledge of security threats, inaccurate mental models.

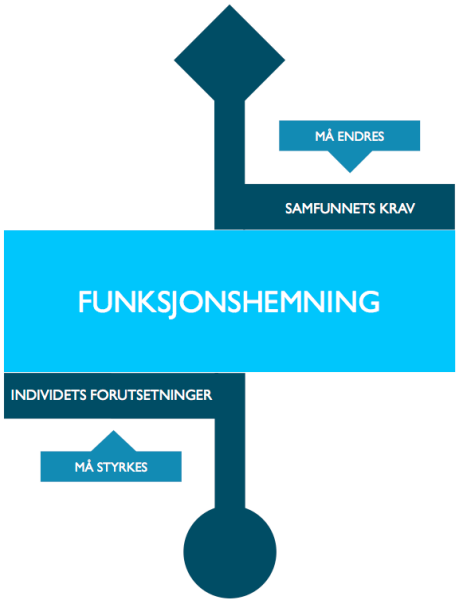
[60]

Han beskriver videre hvilke styrker og svakheter vi har når det gjelder autentisering:

- Users are good at authenticating people they know.
- Users are not good at authenticating strangers.
- Users are not good at authenticating objects.
- Users are not good at authenticating digital objects.

[60]

Han legger vekt på hvor dårlige vi er til å skille mellom objekter og ukjente ting. Han anbefaler at man, i det han kaller *menneske-protokoll interaksjon*, fjerner behovet for at brukeren skal utføre autentiseringsoppgaver (for eksempel autentisere en nettside eller en avsender basert på sertifikater)[60].



Figur 2.3: GAP-modellen. Finnes i [75, side 24], også i [26, side 9] med litt annerledes begrepsbruk

2.2 Universell utforming

> «Løsninger som er utformet med tanke på mangfoldet i befolkningen og som ivaretar hensynet til universell utforming, vil være funksjonelle og ha kvaliteter som alle vil ha nytte og glede av. Konkrete løsninger som er nødvendige for noen, er gode for alle.»[15]

For å forstå begrepet universell utforming må vi først forstå hva som forårsaker en funksjonshemning og forskjellen på en funksjonsnedsettelse og en funksjonshemning.

2.2.1 Funksjonsnedsettelse og funksjonshemning

Forståelsen av funksjonshemning har endret seg fra et fokus på individets skavanker til et relasjonelt syn der både samfunnets mangel på tilgjengelige løsninger og individets funksjonsnedsettelse er årsaken til funksjonshemning. Bare når det er et gap mellom samfunnets krav til funksjon og individets funksjonsevne for tilgang til en tjeneste, oppstår funksjonshemning. En funksjonsnedsettelse er vanligvis sensorisk, motorisk eller kognitiv. [75]

Gap-modellen setter samfunnets krav opp mot individets forutsetninger. Funksjonshemning oppstår i gapet mellom den enkeltes forutsetninger og de krav samfunnet stiller [26, 75, side 5, side 11]. Sandnes [75] illustrerer dette gapet godt i sine eksempler:

> «Hvis en butikk forventer at kunden skal bruke trappen for å komme inn i butikken, og en kunde er rullestolbruker, vil

> det oppstå et gap fordi rullestolbrukeren ikke er i stand til å bruke trappen. De fleste billettautomater med berøringsskjem fordrer at reisende er i stand til å se innholdet på skjermen. en blind reisende vil ikke være i stand til å se innholdet på en berøringsskjerm, og det oppstår dermed et gap.» [75, side 25]

Sandnes [75] skriver at Funksjonsnedsettelse forstås som tap eller skade på en kroppsdel eller kroppsfunksjon. Slike tap eller skader kan selvsagt være medfødte og trenger ikke være noe som kommer i ettertid. Det trenger heller ikke oppstå plutselig og uventet. Aldring er jo en helt naturlig prosess hvor funksjonsevnen svekkes. I følge Sandnes [75] utgjør pensjonistene den gruppen som har størst andel av personer med nedsatt funksjonsevne og i følge SSB vil andelen av eldre bare øke det kommende århundret, også kjent som eldrebølgen [75].

«Min alderdom listet seg inn på meg;
en dag var jeg falt i hans klør.
Han tok meg med til et annet land,
og der var jeg ikke som før.»
(William Shakespeare)

For å ytterligere illustrere hvor viktig samfunnets krav er for å forstå en funksjonshemning kan en se hva et barn på 6 år er i stand til. De motoriske ferdighetene er relativt lave, de sensoriske evnene fremdeles ikke fullt utviklet og de kognitive evnene er enda langt i fra det samfunnet ville forvente fra en voksen. Men ingen vil komme på å si at en seksåring som ikke klarer å skrive alfabetet fra A-Å (motorisk og kognitivt) har en funksjonshemning. Vi vil også ha problemer med å si at seksåringen har en funksjonshemning dersom denne ikke klarer å åpne en tung dør. Samfunnets stiller ikke krav om at seksåringen skal kunne skrive alfabetet. Og seksåringen har ikke tap eller skade på sensoriske, motoriske eller kognitive funksjoner. De er bare ikke ferdig utviklet enda. Allikevel vil både seksåringen og andre som møter større krav enn det forutsetningene deres kan parere oppleve et gap. Det er nok ikke riktig å kalle dette en funksjonshemning, i så tilfelle står en overfor en mulig utvanning av hele begrepet funksjonshemning. Det er en diskusjon som ikke skal tas her. Men la oss nå for enkelhetsskyld kalle det et funksjonsgap, gapet mellom kravene samfunnet setter og forutsetningene individet har i situasjoner hvor det er vanskelig å påberope seg en funksjonshemning. Og la oss anta at forutsetningene individet har er det vi gjerne kaller «normale». Fremdeles vil vi kunne finne mange eksempler på mennesker som møter funksjonsgap i hverdagen. Enten det er gjennom IKT systemer brukeren ikke forstår eller det er mer håndfaste ting vi støter på fra tid til annen. Norman [65] har mange gode eksempler på slike gap. Norman bruker ordet handlingsgap (Gulf of Execution) for å beskrive dette gapet. Da har vi plutselig tatt steget fra det tradisjonelt sett negative ordet funksjonshemning via Gap modellen og over til helt dagligdagse brukergrensesnitts utfordringer som vanligvis ikke blir forklart med at

brukerne har for lave forutsetninger men at det er noe galt med selve brukergrensesnittet og interaksjonen. Dette er noen av de utfordringene universell utforming prøver å håndtere.

2.2.2 Tilgjengelighet og universell utforming

De siste femten årene har vi gått fra et samfunn hvor servicefunksjonærer er mennesker til et samfunn hvor servicefunksjonen blir ivaretatt av en IKT løsning. Vi opplever en stadig økende grad av selvbetjening enten det er for å betale regninger i nettbanken eller du skal kjøpe billetter til offentlig transport og kulturarrangementer. Også offentlige og helt nødvendige oppgaver som kreves av privatpersoner blir i større grad overført til selvbetjening for eksempel innlevering av selvangivelsen. I mange tilfeller er det fremdeles mulig å gjøre disse tingene på en måte som ikke krever bruk av IKT utstyr, men dette blir i større og større grad avgiftsbelagt. På den måten tvinges en etter hvert over til selvbetjening gjennom IKT løsninger. Da må brukergrensesnittet være tilgjengelige. World Wide Web Consortium (W3C) har egne retningslinjer for tilgjengelighet på internett (WAI) [16] som skal sikre at også folk som opplever funksjonshemninger skal kunne bruke web. For å få til dette brukes gjerne egne tilrettelagte spesialløsninger eller en kan bruke kompenserende teknologi (Assistive technology) [75].

> «Dersom noen ikke får tilgang til en tjeneste, vil de oppleve utestegning eller diskriminering. Når samfunnet forventer at borgerne skal benytte en tjeneste, blir det også en folkerett å kunne benytte tjenesten. Målet er derfor å bevege seg fra tilgjengelighet via spesialløsninger tilpasset spesielle brukergrupper til universalløsninger utformet for alle.»[75, 27]

Dette er noe også Fritsch et al. skriver i sin beskrivelse av universell utforming. At tjenester og produkter skal være tilgjengelige for så mange som mulig.

> «Tilnærmingen til universell utforming handler ikke om å lage et spesielt design for en smal brukergruppe men om å utvide den potensielle brukergrupper av ordinære produkter og tjenester til å inkludere funksjonshemmede, eldre og personer med dårlig IKT-ferdigheter, personer med lese-og skrivevansker osv.» [45, side 6].

Erkjennelsen av at brukerne er vidt forskjellige, i kontrast til å designe for en gjennomsnittsbruker, er viktig. Derfor må en også kjenne til de ulike brukernes behov, preferanser og evner.

Universell utforming er en strategi for planlegging og utforming av produkter og omgivelser for å oppnå et inkluderende samfunn med full likestilling og deltakelse for alle[61] The Center for Universal Design, North Carolina State University[85](NCSU) blir ofte sitert i sammenheng med

universel utforming. Deres definisjon er også gjengitt i sin helhet i FN-konvesjonen om rettighetene til mennesker med nedsatt funksjonsevne. I FN-konvensjonen er det foretatt noen få presiseringer og lagt til en presisering om retten til å ta i bruk kompenserende teknologi (Presiseringene FN la til i sin konvensjon er markert med kursiv for å vise forskjellen mellom den og NC State universitys):

> «**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 tilpassning og en spesiell utforming. *Universell utforming skal ikke utelukke hjelpemidler for bestemte grupper av mennesker med nedsatt funksjonsevne når det er behov for det.*»
>
> *(Gjengitt fra Sandnes [75] som gjengir fra uoffisiell norsk oversettelse fra Barne og LikestillingsdepartementetSandnes2011.)*

Norge har fremdeles ikke ratifisert denne konvensjonen når denne oppgaven blir skrevet [5]. Derfor baserer en seg på en uoffisiell oversettelse av konvensjonen [4][75].

Begrepet stammer opprinnelig fra arkitekturen for å beskrive tilgjengeliggjøringen av utearealer, tilgang til bygninger og skilting [75]. Men som vi ser av FN-konvensjonen og i Miljøverndepartementets avklaring omfatter begrepet universell utforming mye mer enn arkitektur. I Norge er det også lovfestet at IKT løsninger skal ha en universell utforming dersom de retter seg mot allmenheten.

Kjært barn har mange navn heter det, og begrepet *universell utforming* er ikke noe unntak. Selv *i* denne oppgaven frykter jeg at det tross mange gjennomlesinger vil ordene bli brukt om hverandre. Fritsch et al. nevner uttrykkene: «universal design», «design for all», «universal usability», «accessible design», «universal access» og «sensitive inclusive design»[45]. Fuglerud and Røssvoll skriver enkelt og greit i begrepsavklaringen:

> «In the current context, refers to the design of ICT solutions suh that they can be used by as many people as possible. Also known as design for all»
> [50, side 9].

7 prinsipper for universell utforming

Det er utformet 7 prinsipper som grunnlag for å forstå universell utforming de norske oversettelsene varierer noe men har samme betydning. Jeg har valgt å gjengi Sandnes (2011) oversettelse samtidig som jeg henviser til to andre kilder for de leserne som skulle ønske å se språkforskjellene.

[4]Originalen finnes her http://www.un.org/disabilities/default.asp?id=262

Enkel og intuitiv bruk Utformingen skal være lett å forstå uten hensyn til brukerens erfaring, kunnskap, språkferdigheter eller konsentrasjonsnivå.

Forståelig informasjon Utformingen skal kommunisere nødvendig informasjon til brukeren på en effektiv måte.

Toleranse for feil Utformingen skal minimalisere farer og skader som kan gi ugunstige konsekvenser, eller minimalisere utilsiktede handlinger.

Like muligheter for alle Utformingen skal være brukbar og tilgjengelig for personer med ulike ferdigheter.

Fleksibel bruk Uansett individuelle preferanser og ferdigheter. Den synshemmede skal kunne høre, den hørselshemmede se.

Lav fysisk anstrengelse Utformingen skal kunne brukes effektivt og bekvemt med minimum av besvær.

Størrelse og plass for tilgang og bruk Hensiktsmessig størrelse og plass skal muliggjøre tilgang, rekkevidde, betjening og bruk, uavhengig av brukerens kroppsstørrelse, kroppststilling og mobilitet.

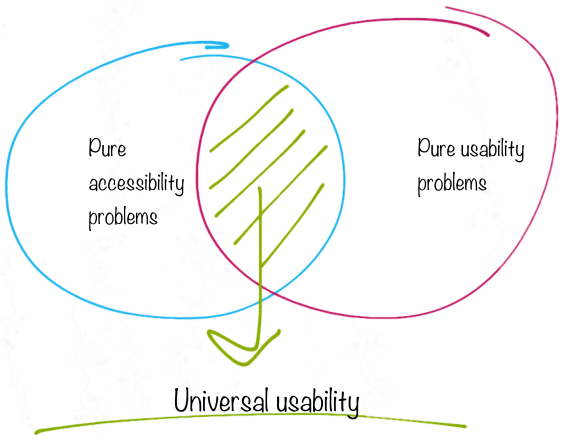
[15, 85, 75]

2.2.3 Retningslinjer for tilgjengelighet

I mange land så som USA, Australia, Japan og EU er det på plass lover som skal sikre at tjenester og produkter er tilgjengelige og kan brukes av så mange brukere som mulig, inkludert eldre personer og personer med funksjonsnedsettelser. Derfor er mange standardiserings initiativer stimulert av EU-kommisjonen og andre nasjonale organer. I tillegg finnes det interessenter og frivillige organisasjoner som bidrar til å utvikle retningslinjer og standarder innenfor dette feltet [45]. Det er fremdeles relativt få formelle standarder innenfor dette området og mange lover viser til mindre formelle retningslinjer hvor et av de best kjente eksemplene er retningslinjene fra *Web Accessibility Initiative* fra World Wide Web Consortium (W3C) også kjent som WAI retningslinjene[16]. Dette inkluderer WCAG (Web Content Accessibility Guidelines) og ARIA (Accessible Rich Internet Applications). Disse retningslinjene er så og si universelt akseptert som referansepunkt når det gjelder web tilgjengelighet [45].

Men det finnes så langt jeg har klart å bringe å det rene ingen retningsnlinjer for tilgjengelige sikkerhetsløsninger. Det eneste kjente er det Fritsch et al. [45] har funnet av retningslinjer fra W3Cs *Web Security Context workin group*[17]. Denne gruppen var klar over tilgjengelighetsutfordringer men har begrensede forslag til hvordan de kan løses [45].

Fritsch et al. [45] skriver også at selv om gjeldende standarder og retningslinjer blir fulgt vil det være flere problemer knyttet til tilgjengelighet og brukbarhet av sikkerhetsløsninger som ikke blir adressert. For det første



Figur 2.4: Relasjonen mellom brukervennlighet- og tilgjengelighetsproblemer Petrie and Kheir, 2007 her fra Pettersen [73, side 88]

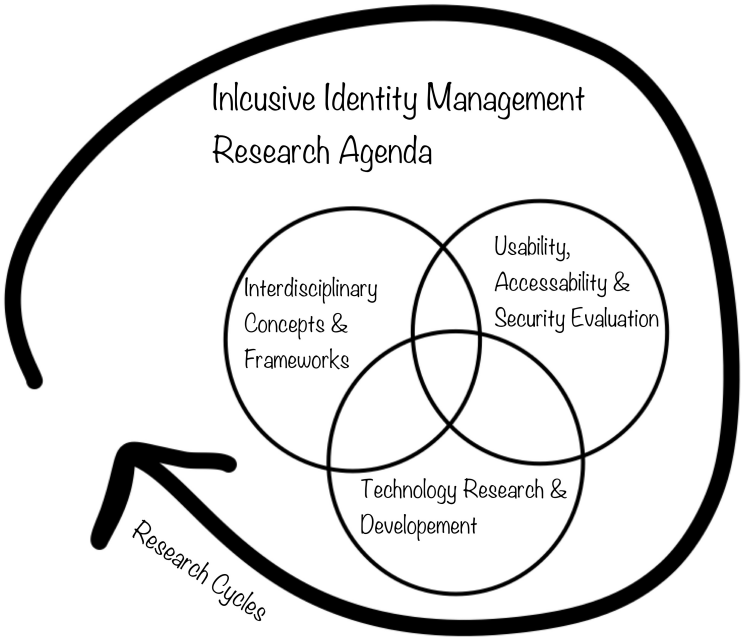
trenger ikke systemene være brukbare selv når de følger standardene, for det andre finnes det mange uløste problemer med tanke på tilgjengeligheten til forskjellige sikkerhetsmekanismer. Pettersen [73] skriver i sin analyse av tilgjengelighet versus brukbarhet at retningslinjer for tilgjengelighet ofte egentlig dreier seg om *teknisk tilgjengelighet*. Han konkluderer med at nettsider som er tilgjengelige ikke trenger være brukbare og at mellom begrepene tilgjengelighet og brukbarhet ligger det delte utfordringer som er både tilgjenglighets- og brukbarhets utfordringer. Dette kaller han *universell brukbarhet* se figur 2.4 på side 21

2.2.4 Inkluderente identitetsforvaltning

Hva er inkluderende identitetsforvaltning?

Fritsch et al. tar til orde for det de kaller inkluderende identitetsforvaltning (Engelsk: Inclusive identity management, IIDM) og et skifte innen forskning på identitetsforvaltning til å lage inkluderende løsninger. Løsningene må være tilgjengelige for en bred rekke brukere, ideelt sett skal alle typer brukere kunne bruke løsningen. Uavhengig av brukerens alder, dyktighet, ulike evner og uavhengig av kultur. [45]. Forskning på IIDM bør være tverrfaglig og spesielt trekke erfaring fra informasjonssikkerhet, universell design og personverns forskning. Forskning på IIDM må også vise veien for nye muligheter innenfor identitetsforvaltning. Universell design fokuserer på fleksible og multimodale systemer tilpasset forskjellige brukere, dette står i kontrast til den tradisjonelle vinklingen innenfor informasjonssikkerhet som ser på en enkelt sikkerhetsmetode på riktig sikkerhetsnivå. Den tverrfaglige tilnærmingen til forskning på IIDM illustreres som en forskningssirkel bestående av:

- Usability, accessibility and security evaluation. Testing of concepts



Figur 2.5: Forskningssirkel IIDM research agenda for e-inclusive identity management Fritsch et al. [45, side 3]

and solutions must be based upon approaches that integrate the usability and accessibility needs as well as security and privacy concerns in common, integrated evaluation and testing frameworks.

- Technology R&D. New concepts must be implemented, preferably as prototypes that can be tested out and eventually provide sustainable solutions.

- Concepts and frameworks drawn from a range of disciplines, such as human computer interaction (HCI) and information security design, should be combined.

[45]

Se figur 2.5 for en illustrasjon av denne forskningssirkelen.

Fritsch et al. [45] deler IDM opp i tre kategorier hvor kategori 1 er den mest aktuelle i denne oppgaven «Type 1 IMS [Identity management systems] for account management, implementing authentication, authorization, and accounting.» Med denne inndelingen ser vi at inkluderende autentisering bare er en liten del av forskningen innenfor IIDM.

Bakgrunn for inkluderende identitetsforvaltning

Det er flere grunner til at vi trenger inkluderende identitetsforvaltning. Hele Europa, og andre steder i verden, står en overfor et demografisk skifte mot en aldrende befolkning. I Norge populært kalt «eldrebølgen». Utbredelsen av nedsatte funksjonsevner øker med alderen. Dette vil bare

øke behovet for tilgjengelig teknologi som kan kompensere for fysiske og psykiske hindringer og funksjonshemninger [45]. Undersøkelser fra USA viser at hele 60% av befolkningen i arbeidsfør alder sannsynligvis vil dra nytte av universelt utformet teknologi. Også 19,4% av befolkningen har en funksjonsnedsettelse som forstyrrer hverdagsaktiviteter [45].

Et økende politisk press for at løsninger skal være inkluderende er en viktig rammefaktor for utvikling av IIDM. I EU har en blant annet skrevet under på FN-konvensjonen om rettighetene til mennesker med nedsatt funksjonsevne [45]. Men siden denne avtalen ikke er ratifisert av Norge [5] er det bedre å se til Norsk lovgivning på området.

Diskriminering- og tilgjengelighetsloven (DTL)

I diskriminerings- og tilgjengelighetsloven av 2008 står det følgende:

> «§ 9. Plikt til generell tilrettelegging (universell utforming)
>
> Offentlig virksomhet skal arbeide aktivt og målrettet for å fremme universell utforming innenfor virksomheten. Tilsvarende gjelder for privat virksomhet rettet mot allmennheten.
>
> Med universell utforming menes utforming eller tilrettelegging av hovedløsningen i de fysiske forholdene, herunder informasjons- og kommunikasjonsteknologi (IKT), slik at virksomhetens alminnelige funksjon kan benyttes av flest mulig.
>
> Offentlig og privat virksomhet rettet mot allmennheten har plikt til å sikre universell utforming av virksomhetens alminnelige funksjon så langt det ikke medfører en uforholdsmessig byrde for virksomheten. Ved vurderingen av om utformingen eller tilretteleggingen medfører en uforholdsmessig byrde skal det særlig legges vekt tilretteleggingens effekt for å nedbygge funksjonshemmende barrierer, hvorvidt virksomhetens alminnelige funksjon er av offentlig art, de nødvendige kostnadene ved tilretteleggingen, virksomhetens ressurser, sikkerhetsmessige hensyn og vernehensyn.»[24]

Loven trådde i kraft fra 1. januar 2009 i følge DTL §18. Og videre fra §11 annet ledd:

> «Nye IKT-løsninger som underbygger virksomhetens alminnelige funksjoner, og som er hovedløsninger rettet mot eller stillet til rådighet for allmennheten, skal være universelt utformet fra og med 1. juli 2011, men likevel tidligst tolv måneder etter at det foreligger standarder eller retningslinjer for innholdet i plikten. For eksisterende IKT-løsninger gjelder plikten fra 1. januar 2021. Plikten omfatter ikke IKT-løsninger der utformingen reguleres av annen lovgivning.» [24, §11].

Barne- og likestillingsdepartementet har ansvar for loven. Og Fornyings-, administrasjon- og kirkedepartementet (FAD) har ansvar for utforming av

forskrift til loven. Denne ligger per dags dato til behandling i departementet og er ikke sendt på høring enda. Det er Direktoratet for forvaltning og IKT (DIFI) som skal ha tilsynsansvar med forskriften til loven. Likestillings- og diskrimineringsombudet (LDO) skal håndheve Diskriminering- og tilgjengelighetsloven.

DIFI er underlagt FAD og har også blant mange andre oppgaver ansvar for ID porten og herunder MinID.

LDO er faglig uavhengig av, men administrativt underlagt Barne-, ungdoms- og familiedirektoratet (Bufdir).

> «Likestillings- og diskrimineringsombudet skal fremme likestilling og bekjempe diskriminering uavhengig av blant annet kjønn, etnisitet, religion, funksjonsevne, seksuell orientering og alder. Ombudet håndhever diskrimineringsforbudene i lovverket, gir veiledning og er en pådriver for likestilling og mangfold. (...) Alle som meiner seg diskriminerte, skal kunne leggje fram saka si for ombodet, som vil be om opplysningar frå begge partar, vurdere saka objektivt og seie om dei meiner at det har skjedd diskriminering.» [6]

De lovene LDO skal håndheve er: Likestillingslova, diskrimineringslova, diskriminerings- og tilgjengelova, arbeidsmiljølova – kapittel 13 om likebehandling, bustadlovene – føresegnene om ikkje-diskriminering, husleigelova, burettslagslova, bustadbyggjelagslova, eigarseksjonslova. [6]

Bufdir har også ansvar for forsknings og utviklingsmidler på vegne av BLD. Statens råd for likestilling ligger under Bufdir.

Det gjør også Deltasenteret, Statens kompetansesenter for deltakelse og tilgjengelighet.

> «Hovedmålet til Deltasenteret er å bidra til at personer med nedsatt funksjonsevne kan ta del i samfunnet på linje med andre. Visjonen er deltakelse og tilgjengelighet for alle. Deltasenteret skal gjennom sitt arbeid bidra til regjeringens målsettinger om økt tilgjengelighet og universell utforming.»[4]

Forskriften er forsinket. I BLDs handlingsplan «Norge universelt utformet 2025» som er regjerningens handlingsplan for universell utforming og økt tilgjengelighet for 2009-2013, kan vi lese at de opprettholder målsettingen fra DTL om at forskriften skal være klar 1.januar 2010. [70]. Siden den gang er det satt flere nye frister og nå venter blant annet DIFI å få denne til høring i løpet av høsten 2012.

Denne forsinkelsen er noe alle etatene jeg har vært i kontakt med har påpekt.

Eksisterende forskning på inkluderende identitetsforvaltning

Fuglerud et al. skriver om forskningsprosjektet DIADEM (EU prosjekt som gikk fra 2006-2009) at selv om prosjektet har avgrenset seg fra autentisering og fokuserer på utforming av skjemaer er det «*Ut i fra de foreløpige*

brukertestene og erfaringer i prosjekter er det imidlertid på det rene at universell utforming av pålogging og autentisering er en viktig problemstilling.» [46, side 13]. I prosjektet UNIMOD (Støttet av VERDIKT programmet og gikk fra 07-09) fant de at pålogging var en betydelig barriere i bruken av altinn.no og så mye som en tredjedel av henvendelse til brukerstøtte gjaldt innloggingsproblematikk. Heller ikke søk i EU's prosjektdatabase har gitt resultater i søk etter lignende prosjekter [46]. Heller ikke Fritsch et al. [45] kommer frem til noe annet enn at det finnes lite forskning på området, men at innlogging kan stå for en vesentlig del av henvendelsene til helpdesk [45]. Lav brukbarhet er kjent å være en kilde til feil, risikoer og barrierer for å sikre IT systemer.

Fuglerud et al. [46], Fritsch et al. [45] finner at det er gjort en del arbeid når det gjelder sikkerhet og brukervennlighet. Fuglerud et al. konkluderer med at «Det ser altså ut til at det er gjort svært lite arbeid når det gjelder universell utforming av sikkerhetsløsninger»[46, side 14].

> «Det er behov for å se dagens løsninger i en videre kontekst enn det som har vært vanlig til nå. Man må se universell utforming, brukervennlighet, tilgjengelighet, fleksibilitet og sikkerhet i sammenheng. For å lage bedre løsninger er det helt nødvendig å ta utgangspunkt i brukerens muligheter og funksjonsevne, brukssituasjon og behov, og man må se på hvordan brukere løser problemer med nåværende og framtiige sikkerhetsmekanismer i praksis. Det er derfor også nødvendig å involvere brukere med svært ulike behov og nedsatt funksjonsevne i denne forskningen.»[46, side 14]

Fuglerud et al. [46] lister opp alternative autentiseringsmekanismer det er følgende: Taleteknologi, enten opplesning av OTP koder og captchas eller indirekte ved OTP på SMS hvor telefonen har taleteknologi. Dessute minibanker som kan gi instruksjon. Bilder og symboler fremfor tall og bokstaver. Å erstatte tall og bokstaver med bilder og symboler kan være en fordel for folk med skrive- og lesevansker, det blir også trukket frem som et alternativ til de med kognitive nedsettinger. Near field communication kan være et alternativ som gjør mange oppgaver enklere for brukeren. For eksempel adgang og identifisering ved hjelp av mobiltelefonen. Biometri, her nevnes flere typer biometriske løsninger. Men også utfordringer ved bruk av biometri. Spesielt dette med at kjennetegnet kan bli svakere ved alderdom og at det kan forsvinne helt eller endre seg.

En sentral utfordring innenfor inkluderende identitetshåndtering er personvern. Det er mange brukere med funksjonsnedsettelser som ikke ønsker at en tjenesteleverandør skal få informasjon om deres funksjonsnedsettelse. [46, 50]

Fuglerud et al. skriver også at informantene deres ikke ønsker mindre sikre løsninger. Men at «Det bør være opp til banken/tjenesteleverandøren å vurdere sikkerheten. Tjenesteleverandøren bør kun tilby så sikre løsninger at de selv er villige til å bære eventuelle tap.» [46, 45].

Om muligheten til å lage en universelt utformet sikkerhetsløsning skriver Fuglerud et al. videre at:

> «Det synes som mange sikkerhetsmiljøer tar det for gitt at det er mulig å velge en enkelt optimal sikkerhetsløsning for hver tjeneste. En konklusjon vi mener å kunne trekke fra arbeidet i dette forprosjektet er at det i overskuelig framtid ikke er mulig å finne en enkelt autentiseringsmetode som er tilgjengelig for alle og som oppfyller det ønskede sikkerhetsnivå. Dette får konsekvenser for hvordan man tenker rundt det med sikkerhet. Er det mulig å tilby brukeren alternative sikkerhetsmekanismer, alt etter hva som passer brukeren best?» [46, side 45].

Det foreslås å finne portefølje av egnede sikkerhetsmetoder og deretter klassifisere disse etter sikkerhetsegenskapene de har. Det trekkes frem noen eksempler på parametre som må tas hensyn til i en slik klassifisering disse er:

- Identity theft - volatility and mobility of the identifiers used.
- Replacement upon loss
- Resistance against brute.force attacks
- Need to upgrade mechanisms
- Robustness of implementation
- Predefines requirements and assumptions
- Gathering or processing of personal information
- Secrecy requirements
- Cost of management, distribution and initialization of mechanism
- Exchangeability with another mechanism without security compromise

Fritsch et al. [45] diskuterer autentiseringsløsninger opp i mot ulike brukergrupper med ulike funksonsnedsettinger, for en nærmere diskusjon om de enkelte funksjonene se [45]. Den kondenserte versjonen av hvilke mekanismer som egner seg for hvilke grupper kan du se i tabell 2.6 på side 27.

2.3 Informasjonssikkerhet

«There's an old joke that computers are actually easy machines to secure: just turn them off, lock them in a metal-lined room, and throw away the key. What you end up with is a machine that is very secure, just not very usable.»
[39, side 5]

> «The goal of security is not to build systems that are theoretical securable, but to build ones that are actually secure.»
> [39, side 31]

Method	Feature	Visually imaired	Hearing impaired	Physically impaired	Cognitively impaired	Dyslexia
Passwords	Tekst token	OK	OK	NO	NO	NO
Text captchas	Disturbed text	NO	OK	NO	NO	NO
Smartcards	Small card with chip; card reader	NO	OK	NO	NO	NO
Numer tokens	Challenge - response	NO	OK	NO	NO	NO
Fingerprint scanning	Small scanner	NO	OK	NO	OK	OK
Voice recognition	Microphone on computer system	OK	NO	OK	OK	OK

Figur 2.6: Tilgjengelighetsutfordringer og autentiseringsmekanismer fra Fritsch et al. [45, side 15]

2.3.1 Et kort historisk tilbakeblikk

En gang på 1960-tallet ble det nødvendig å kontrollere tilgangen til et datasystem for første gang. Passord er ikke noe nytt, vi kjenner til bruk som går tilbake til romertiden. Og mye tyder på at det er eldre en dette også. Forskjellige former for beviser på hvem man er eller hvem man representerer er også kjent tilbake til den tiden. Hele pengesystemet vårt er basert på denne formen for bevis. I begynnelsen var mynter ikke noe mer enn en standardisert vekt på sølv eller gull. Verdien lå altså ikke i selve mynten men sølvets verdi i vekt. Dette ble etter hvert en tungvindt måte å representere store summer på og verdipapirer eller penger i form av papir ble vanligere. For at et slikt pengesystem skal fungere må man ha et fysisk bevis på summen, dette må kunne autentiseres av mottakeren. Beviset er helt avhengig av at begge parter stoler på det og har tillit til betalingsformen. Uten denne tilliten vil ikke seddelen ha noen verdi.

På tross av at vi ikke har mer enn 50 års erfaring med sikring av tilgang til datasystemer har vi altså gjennom historien vært borti mange av disse problemene tidligere. Tilgang, enten det er til informasjon eller for eksempel rom har vi lang erfaring med, låser og nøkler er jo ingen ung oppfinnelse. Samtidig som informasjonssikkerhet i en digital kontekst har mange av de samme utfordringer som i en analog kontekst ser utfordringene gjerne helt annerledes ut i en digital hverden. Vi kan begyne med å se på hvilke oppgaver informasjonssikkerhet skal håndtere.

Informasjonssikkerhetsoppgaver

I Handbook of Human Factors and Ergonomics [77] finner vi en taksonomi over informasjonssikkerhetsoppgaver. Ut i fra denne ser vi tydelig hvor mange oppgaver som er en del av det å sørge for god informasjonssikkerhet. Denne oppgaven fokuserer på det første punktet identifisering og autentisering.

1. Identifisering og autentisering
2. Dataintegritet

3. Datakonfidensialitet
4. Datatilgjengelighet
5. Systemintegritet
6. Inntrengelsesoppdagelse

[77, side 1264]

2.3.2 Identifisering & autentisering

Så hva ligger i uttrykkene identifisering og autentisering? I følge *Handbook of Human factors and Ergonomics* er de to uttrykkene ganske like når det kommer til hva en mener med det. «*Identification* means proving one's identity. *Authentication*, very similar in meaning to identification, means proving one's identity for the purpose of accessing a system or network.»[77, side 1264].

Vi ser også at Norsk senter for informasjonssikring (NorSIS) skriver:

> **Identifisere**
>
> Å gi seg til kjenne. Når man logger seg på datamaskinen identifiserer man seg først ved å angi brukernavn, så autentiserer man seg med å angi passord.
>
> **Autentisering**
>
> Å bevise at man er den man utgir seg for å være. Autentisering skal bekrefte en påstått identitet. Dette kan skje gjennom noe du vet (passord), noe du er (fingeravtrykk/ biometri) eller noe du har (nøkkelkort). Kombinasjoner av disse er også mye brukt. Den som autentiseres kan være en person som bruker en datamaskin, kun en datamaskin eller et program. [22]

Autentisering er ordet som er brukt gjennom denne oppgaven om den handlingen de fleste av oss vil kjenne igjen som «innlogging» og som mer presist er en brukerautentisering[71].

Når du identifiserer et annet menneske gjør du det ved hjelp av hvordan personen ser ut. Når vi møter venner eller personer vi kjenner identifiserer vi dem umiddelbart på utseende. I følge Carlos og Price er vi veldig gode til å autentisere folk vi kjenner men ikke fullt så gode på å autentisere folk vi ikke kjenner, heller ikke objekter eller digitale objekter er vi spesielt gode på [60].

Fuglerud [48] Skriver om en firestegs prosess som innebærer:

Enrollement/Registration matching the user with a secret (the authentication key). They can be issued by the system or provided by the user, with the latter being more common.

Authentication the user is challenged by the system to provide the key. The provided key is compared to the stored key. If they match the user is granted access.

Replacement thus occurs if the user forgets the key and needs to have a new one issued.

De-registration the user should have the right to close his or her account together with all details removed from the system.

[Renaud et. al 2009, her fra 48]

Bonneau and Preibusch [34] deler i sin studie opp nettsider som bruker passord i tre kategorier. Den første er *identitetssider*, hvor de største eksemplene er webmail, sosiale tjenester og blogger. De tar også med forum, og samarbeidstjenester som Wikipedia med i denne kategorien. Den neste kategorien er *netthandel*. Nettsider hvor hovedmålet er å selge varer til brukeren. Mange sider tilbyr brukeren å opprette konto (noen krever dette) som gir mulighet for å spore kjøp, se kjøpshistorikk med mer. *Innholdssider* er den siste kategorien. Sider som bruker innlogging for å tillate brukeren å tilpasse sidene og innholdet eller for eksempel sette opp spesielle søk som kan videreformidles til e-post.

Dette er ikke ment å være en eksluderende kategorisering, men det gir en grov oversikt over noen typer nettsider som krever innlogging.Det gir et godt utgangspunkt for å se for seg hvilke sider og hvor mange steder som kan eller som allerede krever innlogging. [5]

2.3.3 Risikopersepsjon, hvordan forstår vi risiko?

De kommende avsnittene om risikopersepsjon, vil for en leser som går meg nøye i sømmene, følge Bruce Schneiers essay fra 2008 [76] både i oppbygging og fokus på innhold. Han har skrevet et innsiktsfullt og lettlest essay som gir oversikt over et fagområde som er mangefasettert og spredt i forskjelige fagdisipliner. Det er et godt utgangspunkt for å kondensere kunnskapen enda noen hakk og tilpasse dem til denne oppgaven.

> «Det finnes ikke noe slikt som absolutt sikkerhet og enhver sikkerhetsgevinst involverer alltid en eller annen form for kompromiss.» [76].

Sikkerhet koster penger, tid, bekvemmelighet, kapasitet, friheter også videre. Du gjør et kompromiss om du bytter bort ekstra sikkerhet i hjemmet mot ulempen i å bære med deg en ekstra nøkkel og låse opp en dør hver gang du skal inn. Bruce Schneier gjør et stort nummer av sikkerheten rundt fly. Dette er også kompromisser, vi bytter blant annet bort tid, penger og bekvemmelighet mot økt sikkerhet på flyet. Slike kompromisser gjør vi hver eneste dag i større og mindre grad. Du gjør det når du setter deg i bilen og kjører fremfor å gå til jobb. Du gjør det når du velger å sykle med eller uten hjelm. Det gir ingen mening å se på sikkerhet i form av effektivitet. Vi kan ikke bare spørre oss «Er dette tiltaket effektivt mot trusselen?» Vi må spørre oss «Er det et godt kompromiss?» [76]. Disse kompromissene er i stor grad basert på følelser og vi gjør dem intuitivt hele tiden. (ibid)

[5] Bonneau og Preibusch har en oversikt over hvilke sider de plasserte i hvilken kategori for spesielt interesserte.

> «But security is also a feeling, based not on probabilities and mathematical calculations, but on your psychological reactions to both risks and countermeasures. (....) Or, more generally, you can be secure even though you don't feel secure. And you can feel secure even though you're not. The feeling and reality of security are certainly related to each other, but they're just as certainly not the same as each other. We'd probably be better off if we had two different words for them.» [76].

Som tidligere skrevet er sikkerhet alltid basert på et eller annet kompromiss. Dette kompromisset kan gå veldig galt dersom vurderingen gjøres på feil grunnlag eller forståelsen er feil. Bruce Schneier trekker frem fem ting som kan føre til at kompromisset blir galt:

1. Alvorlighetsgraden av risikoen.
2. Sannsynligheten av risikoen.
3. Omfanget av kostnadene.
4. Hvor effektiv mottiltaket demper risikoen.
5. Hvor godt ulike risikoer og kostnader kan sammenlignes.

Desto mer vår oppfattelse av virkeligheten avviker fra virkeligheten på hvilket som helst av disse punktene, desto mer vil vår oppfattelse av kompromisset divergere med det virkelige kompromisset. For eksempel dersom du overvurderer risikoen vil du bruke mer resurser enn nødvendig på å minske risikoen. Eller dersom du evaluerer kompromisset feil vil det være en ubalanse mellom kost og nytte [76].

Å forstå hvordan følelsen av sikkerhet «blir til» i oss er grunnleggende for å forstå hvordan vi på en og samme tid kan føle oss sikre men være usikre. I følge Schneier er det spesielt fire forskningsfelt som er interessante i den sammenhengen. Det er *Atferdsøkonomi* (engelsk: behavioral economics) en vitenskap som studerer hvordan individer foretar økonomiske beslutninger i praksis. Det andre er *forskning på psykologien i beslutningsprosesser* (engelsk, psychology of decision-making) nærmere bestemt forskning på hvordan vi foretar avgjørelser. Det tredje området er *forskning på risikopsykologi*, altså forskning som prøver å finne ut når vi overdriver og når vi underdriver risiko. Det fjerde relevante feltet er *nevrovitenskap*, å forstå hvordan hjernen vår fungerer og når den feiler i forbindelse med håndtering av risikoer er kritisk for å forstå følelsen av sikkerhet[76].

Jeg skal forsøke å gjøre en alt for kort oppsummering fra disse fire områdene som kan gi oss et grunnlag å jobbe videre ut i fra for å forstå følelsen av sikkerhet.

Folk overdriver risikoer som er:	Folk undervurderer risikoer som er:
Spektakulære	Kjedelige
Sjeldne	Vanlige
Personifiserte	Anonyme
Utenfor deres kontroll, eller ekstern påtvunget	Mer under deres kontroll, eller tatt frivillig
Snakket om	Ikke snakket om
Forsettlig eller menneskelagde	Naturlige
Umiddelbare	Fjerne eller diffuse
Påvirker dem personlig	Påvirker andre
Nye og ufamiliære	Familiære
Ukjente	Vell forstått
Rettet mot deres barn	Rettet mot dem selv
Moralsk støtende	Moralsk ønskelige
Helt uten forsonende trekk	Forbundet med supplerende nytte
Ikke lik deres nåværende situasjon	Lik deres nåværende situasjon

Tabell 2.1: Konvensjonell kunnskap om mennesker og risikopersepsjon fra [76] oversatt fra engelsk.

Konvensjonell kunnskap om mennesker og risikopersepsjon

På side 31 finner vi Schneiers tabell over konvensjonell kunnskap om mennesker og risikopersepsjon den gir en god oversikt over hvilke typer risikoer vi overvurderer og hvilke vi undervurderer.

Risiko og hjernen

I en av de eldste delene av hjernen vår ligger Amygdala. Den er ansvarlig for å prosessere følselser som kommer fra sensoriske input så som sinne, unngåelse, forsvar og frykt. Når et dyr, eller vi mennesker, ser, hører eller føler at noe er en potensiell fare er det Amygdala som reagerer umiddelbart. Det er den som fører til at adrenalin pumpes ut i kroppen, at du klargjøres for kamp eller for å flykte. Det er omtrent så avansert den er også. Den kan gi deg enormt lav responstid på slike inntrykk. Til gjengjeld vurderer den ikke risikoen i et større perspektiv. Til det har vi Neocortex, som er intelligent og analytisk. Det er der vi vurderer risiko og argumenterer, den kan gjøre mer nyanserte kompromisser. Neocortex er ansvarlig for at vi kan forberede oss og forutse farer som kommer. Men nettopp disse egenskapene gjør også at den er treigere og ikke gir den samme umiddelbare reaksjonsevnen. Der Amygdala er hardkoblet

til nervesystemene våre og er noe vi ikke har kontroll på kan en se på Neocortex som et mer sofistikert område av hjernen som må overbevise oss gjerne på tross av hva Amygdala sier [76].

Vi kan bruke evolusjonen til å forklare en rekke av de «intuitive reglene» hjernen vår har. Disse reglene er gjerne dårlig tilpasset samfunnet vi lever i nå. Det går blant annet på hvordan vi vurderer sannsynlighet og hvilken vekt vi legger på å vinne eller tape noe. Vi har gjerne større aksept for risiko når det gjelder å tape noe enn når det gjelder å vinne noe. Vi tillegger også ting høyere verdi når det er noe vi kan tape fremfor noe vi kan vinne. For eksempel vil vi vurdere en gjenstands verdi lavere når vi ønsker å kjøpe den enn det vi selv er villige til å selge den samme gjenstanden for. En annen vanlig bias når det gjelder risiko er «optimisme biaset». Vi vurderer våre sjanser for å gjøre det bedre enn andre som gjør akkurat det samme som høyere. Dette er en grunn til at vi tror bilulykker kun skjer andre. En forklaring på hvorfor det er slik kan være så enkel at vi har utviklet oss til å undervurdere tap siden mange av de som har opplevd tap opp igjennom evolusjonen har en tendenes til å ikke overleve. Men å finne forklaringer i evolusjonen er ikke så viktig. Det viktige er hvilken effekt disse intuitive reglene gir. Denne biasen fører også til at vi overvurderer sannsynligheten for at noe positivt kommer til å skje. Gitt lik sannsynlighet for to utfall vil vi overvurdere det positive. Vi har en hel rekke slike intuitive regler som gjør det vanskelig for oss å vurdere noe objektivt. Se Schneier for en noe mer utfyllende liste og flere eksempler[76]. Kort fortalt gjør vi hele tiden feilvurderinger basert på erfaringer som er utdaterte. Vi har sterk slagside mot ting som før kunne være praktiske huskeregler, men disse intuitive reglene henger ikke med i samfunnsutviklingen forøvrig. Dette må vi ta hensyn til når vi lager sikkerhetsløsninger slik at folk kan ta de riktige avgjørelsene.

Schneier anbefaler å utnytte disse egenskapene slik at følelsen av risiko og den faktiske risikoen stemmer bedre overens. På den måten kan folk også gjøre bedre kompromisser. Han kaller det å gjøre seg nytte av sikkerhetsteateret.

> «The feeling and reality of security are different, but they're closely related. We make the best security trade-offs—and by that I mean trade-offs that give us genuine security for a reasonable cost—when our feeling of security matches the reality of security. It's when the two are out of alignment that we get security wrong.
>
> In the past, I've criticized palliative security measures that only make people feel more secure as "security theater." But used correctly, they can be a way of raising our feeling of security to more closely match the reality of security. One example is the tamper-proof packaging that started to appear on over-the-counter drugs in the 1980s, after a few highly publicized random poisonings. As a countermeasure, it didn't make much sense. It's easy to poison many foods and over-the-counter medicines right through the seal—with a syringe, for

> example—or to open and reseal the package well enough that an unwary consumer won't detect it. But the tamper-resistant packaging brought people's perceptions of the risk more in line with the actual risk: minimal. And for that reason the change was worth it.» [76]

Flechais et al. [42] Skriver at kontekst er viktig når en skal analysere sårbarhet. Risiko er subjektivt og den relative viktigheten av et system er også subjektiv [42]. I artikkelen rangeres viktigheten som enten høy, medium eller lav. De skiller også mellom tekniske sårbarheter og sosiale sårbarheter.

Stølen [81] kommer frem til at bruk av mønster for å låse mobiltelefonen oppleves av brukeren som mindre sikkert enn passord fordi «det er for enkelt». Hun forklarer at dette er på grunn av brukerens mentale modeller for sikkerhet [81].

2.3.4 Sikkerhet og kostnad

En del av problemstillingen min var å se på kostnaden knyttet opp til informasjonssikkerhet. Utgangspunktet var å sammenligne kostnader mellom forskjellige autentiseringsløsninger. Av praktiske grunner er dette lettere å si at en skal gjøre enn å gjennomføre. Det ville vært et stort studie i seg selv. Men noe kan man si ut i fra andre undersøkelser. Og kanskje det viktigste, kostnadene ligger i dag ikke bare på den som tilbyr tjenesten, men i stor grad på brukeren. Lucidman prosjektet [57] kaller dette «Password Fatigue» og prøver å utvikle løsninger som kan håndtere problemet. Andre tar i bruk begrepet *allmenningens tragedie* om kostnaden som blir pålagt brukeren. Kostnaden er kognitiv og for hver konto en bruker får for hver identitet og for hvert passord må brukeren huske noe nytt. I hvert fall om man følger retningslinjer og råd som sier at passord skal være ulike. Men dette er en usynlig kostnad for tjenestetilbyderen. I den grad man tenker over problemstillingen i det hele tatt blir brukerens hukommelse sett på som en allmenning alle kan benytte seg av.

Bonneau and Preibusch [34] skriver om allmenningens tragedie og passord:

> «Common goods are characterised by an inability to restrict consumption either directly or indirectly through payments. Like public goods there is no exclusiveness, but unlike public goods common goods decline in value as they are consumed more intensively. Classical examples include natural resources such as parks or fishing grounds which tend to be overused and depleted in the absence of regulation. Consumers' finite mental storage capacity for passwords is a common good from the viewpoint of website operators. Asking consumers to remember an additional password comes at no cost to a site operator, but can bring direct financial benefit from increased customer affinity and the ability to gather customer data (§ 5.5). Yet, each additional password places further demands on

> a user's memory, and may not bring real benefits to the user. To prevent depletion of their password memory, consumers must either reduce the burden for each individual password by choosing weaker passwords or reduce the cumulative burden by re-using passwords. The former tactic may have limited applicability as individual sites can enforce password restrictions (§ 4.3.2), but user surveys have revealed that users do consciously make this sacrifice. There is considerable empirical evidence that consumers more often take the latter approach of password re-use (§ 2.2).» [34, side 34].

Også andre forfattere bruker dette begrepet blant annet [30, 79]. I et tradisjonelt syn på dette problemet må man for å få bukt med problemet regulere tilgangen til allmenningen[52]. Siden brukerens hukommelse strengt tatt ikke er en allmenning kan denne reguleringen påtvinges av brukeren. Ellers må dette komme som en tvungen eller frivillig regulering fra de som utnytter allmenningen.

2.4 Autentiseringsmetoder

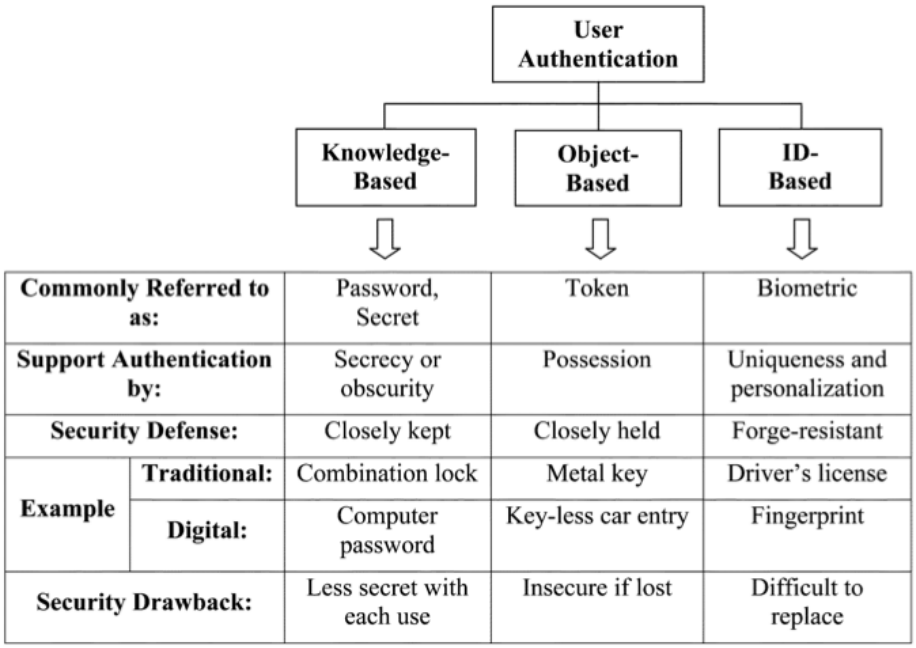
Vi deler vanligvis inn i tre måter å autentisere seg på det er *Noe du har, noe du er* og *noe du vet*. Syta et al. [83], Hulsebosch et al. [54] foreslår i tillegg *stedet du er* som en fjerde kategori. I figur 2.7 på neste side ser vi en oversikt over de tre tradisjonelle kategoriene med eksempler og egenskaper til hver av dem.

2.4.1 Noe du har

Den tradisjonelle måten å få tilgang til noe på. Vi har alle vært i kontakt med nøkler og håndterer daglig disse enten vi skal inn i huset eller kjøre bil. O'Gorman [71] kaller denne kategorien *objektbasert autentikator*. Syta et al. [83] legger vekt på at det er noe du er i besittelse av. Alle nærhetsbaserte autentiseringsløsningene som gjennomgås nedenfor er basert på noe du har og er i besittelse av (Det mest ekstreme tilfellet av å bære med seg tokens finner vi nok i [79]). Med den forskjellen at de ikke trenger fysisk kontakt for å gi deg adgang. Vi kan bruke samlebetegnelsen *tokens* om disse nøklene.

For tradisjonelle nøkler, som husnøkler, er en svakhet at hvem som helst som er i besittelse av nøkkelen kan få tilgang. Det kan gjøre at dersom du mister nøkkelen får noen fremmede adgang til huset. Dette er grunnen til ta mange digitale former for tokens er kombinert med noe du vet. En fordel med fysiske nøkler er at innehaveren på en enkel måte kan sjekke om den er mistet eller ikke[71].

Fysiske tokens så som smartkort brukes gjerne for å skape en sterk autentisering. Det er gjerne forbundet med en tungvindt prosess, men en test av Buypass i E-me prosjektet viste at bruken ikke var det som var mest tungvindt[44]. Det var prosessen med å få kortet og bli innrullert i systemet



		Knowledge-Based	Object-Based	ID-Based
Commonly Referred to as:		Password, Secret	Token	Biometric
Support Authentication by:		Secrecy or obscurity	Possession	Uniqueness and personalization
Security Defense:		Closely kept	Closely held	Forge-resistant
Example	**Traditional:**	Combination lock	Metal key	Driver's license
	Digital:	Computer password	Key-less car entry	Fingerprint
Security Drawback:		Less secret with each use	Insecure if lost	Difficult to replace

Figur 2.7: De tre tradisjonelle Autentiseringsmekanismene med tilhørende egenskaper. Fra [71, side 2024]

som var vanskeligst. I bruk fungerte smartkortet Buypass godt og brukerne var fornøyde[44].

Yubikey[18] som brukes i testen av LastPass i denne oppgaven og blir nærmere beskrevet i kasus kapittelet er også en form for noe du har, en nøkkel eller et token om du vil. Tokens behandles grundigere under nærhetsbasert autentisering.

2.4.2 Noe du vet

En *kunnskapsbasert* autentikator er karakterisert gjennom hemmelighold og «safety through obscurity»[71]. Vanligvis er refereres det til en hemmelighet som passord eller PIN-kode. Men det kan også være noe som er hemmelig for de fleste, altså at sikkerheten ligger mer i at kunnskapen er obskur. Et typisk eksempel på dette er sikkerhetsspørsmål som «Hva het din første lærer» og andre ting man antar få vet[71]. Et studie viste at en typisk nettbruker i 2006/2007 hadde rundt 25 forskjellige kontoer som krever passord og trykker inn omtrent 8 passord daglig [82].

En godt kjent svakhet med passord er konflikten mellom at det skal være noe brukeren husker og det skal være noe som er vanskelig å gjette seg til[39] (med og uten prosessorkraft).

> «However, PINs and passwords proved themselves to be a weak solution that does not provide an adequate level of security. Short, memorable passwords are weak and guessable

> while long, random sets of characters are difficult to remember and increase user inconvenience. The main weakness of this approach is a significant reliance on the user. People tend to choose uncomplicated passwords that often contain easy to obtain information, such as name or age.
>
> (...)
>
> However, a strong password should be long and as random as possible which makes it difficult to remember and inconvenient to use. The problem of convenience becomes significantly more severe taking into account small keyboards available on many mobile devices, not to mention that some of the smart phones do not have full keyboards. As a result, mobile users often choose to deactivate existing authentication mechanisms because they perceived them as cumbersome and inconvenient» [83, side 2]

Bonneau et al. [37] viser hvor enkelt det er å gjette seg frem til PIN-koder som er laget av folk og ikke generert av en datamaskin. Bursdagsdato står her for en av de største årsakene til dette.

> «We find that guessing PINs based on the victims' birthday, which nearly all users carry documentation of, will enable a competent thief to gain use of an ATM card once for every 11-18 stolen wallets, depending on whether banks prohibit weak PINs such as 1234» [37, side 1]

Svakhetene med passord og PIN-koder er godt kartlagt. Herley and Van Oorschot [53] tar et oppgjør med passord:

> «In the past 20 years, little progress has been made in therms of real-world impact of password research. Despite countless attempts to dislodge passwords, they're more widely used and firmly entrenched than ever. The list of new technologies, research efforts, and industry initiatives that have tried to supplant them is impressive in effort burt disappointing in outcome.» [53, side 28]

Men passord har mange styrker også og på tross av de mange ulempene med passord sier de: «*We might say that passwords are the worst possible authentication system, except for all the other systems.*» [53, side 33]

Singel Sign-On (SSO) eller *Federated identity* [34] prøver å begrense behovet for ulike passord og brukernavn ved å benytte den samme identiteten mellom ulike systemer.

> «In this world, your identity provider is your only provider - log in once, and you are automatically logged in everywhere. Log out once, and you are automatically logged out everywhere. No need to keep clicking "log-in" buttons. It has a kind of poetic beauty and simplicity to it.» [73, s29]

Nå har det vist seg at SSO løsninger ikke har fått den utbredelsen man hadde forventet. Det er blitt utbredt i «interne» systemer som for eksempel på universiteter. Eksempel på dette finner vi igjen i kasuset til Stølen [81] hvor Feide er beskrevet. Men SSO systemer har ikke fått den store utbredelsen blant og mellom andre tjenester brukerne benytter seg av[82].

2.4.3 Hvor du er

Hulsebosch et al. [54], Syta et al. [83] introduserer en ny form for autentisering utover de tre tradisjonelle *noe du er, noe du har* og *noe du kan*. De sier stedet du er, når du er der og konteksten du er i har en betydning[54, 83]. Også Tognazzini tar til orde for å gjøre begrepet sikkerhet noe mer elastisk i forhold til situasjonen brukeren befinner seg i. Blant annet trekker han frem mobile systemers evne til å være mer eller mindre stedsbevisste gjennom GPS posisjon. WiFi MAC adressen kan også fortelle maskinen at du sitter på hjemmenettverket. Han foreslår tre nivåer fra lav til høy sikkerhet alt etter hvor du befinner deg som en mer sofistikert tilnærming til sikkerhet [39]. Hulsebosch et al. [54] bruker begrepet «Overall Confidence» og regner ut denne basert på en rekke ulike faktorer.

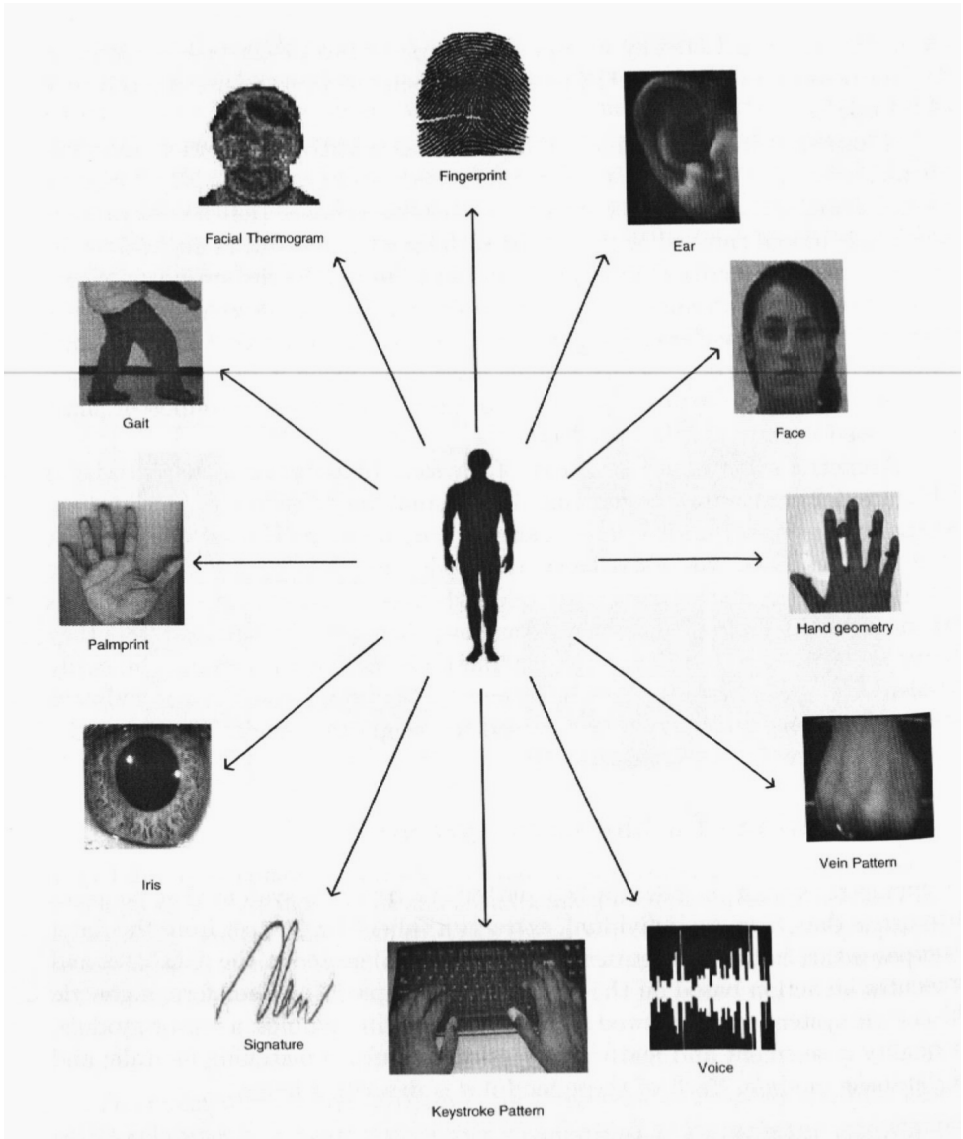
Denne formen for autentisering har også en tett relasjon til forskning gjort på nærhetsbasert autentisering, da de systemene ofte benytter seg av slike terskler for hvor sikker en kan være på at brukeren fremdeles er der (Se for eksempel [31]).

2.4.4 Noe du er

Historisk sett er Biometri den eldste måten vi har å stadfeste en identitet på. Biometri er en interessant vinkling på sikkerhet og jeg tror noe av grunnen til det er at vi bruker biometri hver dag, i hvert eneste møte med mennesker nettopp til å identifisere dem. Det er biometri vi bruker for å skille dyre- og plantearter fra hverandre. Samtidig er det et ømfindtlig tema når en kombinerer bruk av biometri og informasjonssystemer, da det krever at biometriske data om deg lagres.

Tenk bare på hvor lett vi kjenner igjen en stemme i telefonen, mens selve telefonnummeret som også i stor grad kan identifisere avsenderen sjelden sier oss noen ting somhelst. Vi er trente i denne formen for autentisering [60]. Nettopp fordi biometriske kjennetegn, eller ID-baserte som O'Gorman [71] kaller dem, er noe vi kjenner og intuitivt forstår har jeg valgt å se litt nærmere på hva biometri er enn de øvrige autentiseringsmekanismene.

Vi har mange ulike metoder for biometrisk identifikasjon, men de er alle basert på mønstergjenkjenning. Enten det gjelder Fingeravtrykk, ansiktsgjennkjenning, stemme eller DNA. Derfor vil jeg med utgangspunkt i fingeravtrykk, som er det biometriske trekket som først ble gjenstand for automatisert mønstergjenkjennelse belyse biometri og sikkerhet.



Figur 2.8: Eksempel av biometriske trekk som er vanlige å bruke. Fra [55, side4]

Biometri

Et biometrisk identifiseringssystem er i bunn og grunn et mønstergjennkjennings system som ekstraherer biometriske data fra et individ og sammenligner disse med data lagret i en database. De aller fleste biometriske systemer består av fire hoveddeler: en sensormodul, en modul for å bestemme kvaliteten på dataen og trekke ut karakteristikker og trekk, en sammenligning- og bestemmelsessmodul og en databasemodul[55, side 3]. Sensormodulen fungerer som menneske-maskin grensesnittet og er derfor helt sentral for bruken og brukeropplevelsen. Ikke minst er også feilraten avhengig både av bruken av sensoren og på kvaliteten på rådataen som kommer inn. En konsekvens av en dårlig designet sensormodul kan være både dårlig data og lav brukeraksept som en konsekvens av at det biometriske systemet har høy feilfaktor[55, side 3]. Modulen som bestemmer kvaliteten på dataen og trekker ut karakteristikker har algoritmer som forsterker signalene (dataen) som kommer inn fra sensormodulen. Dersom disse dataene er for svake vil den be brukeren om ny data. Er de gode nok vil den ekstrahere fremtredende trekk som representerer den underliggende dataen til et forenklet mønster. De ekstraherte dataene blir sammenlignet med de lagrede mønster-malene i sammenligning- og bestemelsesmodulen. Fra dette får en en sammenlignings poengsum på i hvor stor grad mønstrene stemmer overens. Denne poengsummen kan bli moderert i hennhold til kvaliteten på inndataene. Deretter basert på poengsummen avgjør modulen om identiteten er validert [55]. Databasen fungerer enkelt og greit som en database over mønster-maler. Gjerne kombinert med andre opplysninger knyttet til identiteten, enten det er adresse, kontonummer, e-post adresse eller andre opplysninger. Datainnhenting i det som kalles innrullerings prosessen kan både være med og uten overvåkning av annen person. For eksempel kan det være at banken ønsker at du skal møte opp personlig og kunne identifisere deg på vanlig måte (ID papirer ol.) før du får registrere biometriske data. I andre tilfeller kan det jo tenkes at en registrerer noen andres biometriske data. For eksempel bruker A har logget seg inn på løsning 1 og skal registrere en ny biometrisk adgang men registrerer adgangen på person Bs biometri. I et tenkt system kunne dette blitt gjort for å unngå en kontroll ved hjelp av biometriske data på dupliserte brukere.

En fordel ved bruk av biometri er at en kan tilbakevise at personen faktisk har hatt tilgang[55]. Dette kan en også gjøre uten bruk av biometri, men da vil alltid muligheten for at noen har stjålet eller lånt en annens identitet (nøkler, kort, koder). Videre vil systemet også ha mulighet for å sjekke om det finnes flere registrerte identiteter. I et vanlig IDM vil det være nærmest umulig å kontrollere dette da en person kan ha flere identiteter i systemet. Ved bruk av biometri kan en person kun ha en identitet i systemet. Dette kan være aktuelt i sammenheng med dobbeltregistrering av barn for å få barnebidrag og andre ytelser fra staten. [6] Denne formen for kontroll av dupliserte identiteter kalles negativ gjennkjenning [55, side 6].

Et biometrisk system har to operasjonsmoduser: Verifikasjon og iden-

[6] se for eksempel hvordan barn blir registrert flere ganger på forskjellige mødre: http://goo.gl/eBMIq og http://goo.gl/ByP39 Sist besøkt 16. januar 2012

tifikasjon. I verifikasjonsmodus vil systemet validere at en bruker er den han oppgir. Dette gjøres i kombinasjon med for eksempel adgangskort eller PIN-koder. Den som ønsker å bli verifisert oppgir en identitet til systemet og systemet kontrollerer den lagrede identiteten gjennom biometriske data. Da sammenligner systemet mønstermalen, som er forbundet med identiteten, mot personens biometri. Verifikasjon er ofte brukt for positiv gjennkjenning hvor målet er å forhindre folk fra å bruke samme identitet (F.eks låne bort brukernavn/passord eller adgangskort). Dette er sikrere enn identifikasjon da systemet sjekker en til en fremfor en til mange templates. [55, 71] I identifikasjonsmodus vil systemet sjekke en persons biometriske data mot alle de lagrede mønstermalene for å finne en som er maken. Dette skjer da uten at brukeren trenger å oppgi en gitt identitet.

Ulikt passord-baserte systemer hvor det kun er eksakt likhet mellom passord som gir adgang vil ikke biometrisk baserte systemer få perfekte likheter. Dette har flere årsaker som for eksempel ved ansiktsgjennkjenning har lyset mye å si, vinkelen mot kameraet og ikke minst i hvilken retning hodet står mot kameraet. For fingeravtrykk kan det være skit og andre ting gjør det vanskelig å lese fingeravtrykket. Eller selve avleseren og kameraet ikke har god nok kvalitet. Det er faktisk slik at en eksakt likhet mellom inndata og mønstermal kan være tegn på et forsøk på å omgå systemet, eller bryte seg inn i det. Ved bruk av biometriske data ønsker en seg biometriske egenskaper som har lav varians for hvert individ og stor varians mellom individer[55, side 7].

Som nevnt tidligere er graden av likhet mellom to biometriske mønstre indikert av en likhetspoengsum. Denne poengsummen omtales som en genuin- eller autentisk sum dersom den er et resultat av sammenligning mellom to mønstre fra samme bruker. Mens når en sammenligner to mønstre fra ulike brukere blir den kalt bedragersum (eng: impostor score). En bedragersum som overgår terskel n resulterer i en falsk aksept, mens en genuinsum som er lavere enn n resulterer i en falsk avvisning. Den falske aksept raten (FAR) eller den falske avvisnings raten (FRR)[7] kan bli definert som andelen av genuine poeng som faller under n. Den genuine aksept raten (GAR) er den delen av den genuine poengsummen som overgår n. Derfor er GAR = 1- FRR. En regulering av n vil endre FAR og FFR men for et gitt biometrisk system kan du ikke minke begge samtidig[55, side 8].

Jain et al. [55] refererer til en modell utarbeidet av Jain et. al (1999) som oppgir syv egenskaper ved et biometrisk system en kan vurdere opp i mot egnetheten til det systemet skal brukes til. (Jain et. al (1999) ≪Biometrics: Personal Identification in Networked Society≫ her fra Jain et al. [55, side 15])

Universalitet: Alle individer som skal bruke systemet må ha karaktertrekket som skal måles.

Unikhet: Det gitte trekket må være forskjellig nok mellom individene.

[7]På engelsk False Rejection Rate, jeg velger å beholde den engelske forkortelsen for å unngå misforståelser siden en norsk oversettelse ville vært Falsk Avvisnings Rate (FAR).

Biometric identifier	Universality	Distincitveness	Permanence	Collectabillity	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand Geometry	M	M	M	H	M	M	M
Hand/finger vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Tabell 2.2: Sammenligning av noen vanlige biometriske trekk. High, Medium og Low er annotert med H, M og L Fra [59, side 11]

Uforanderlighet: Det biometriske trekket må være tilstrekkelig uforanderlig over tid. Et trekk som forandres mye over tid er ikke et brukart biometrisk trekk.

Målbarhet: Det må være mulig å tilegne seg, og digitalisere, det biometriske trekket ved hjelp av passende apparater, som ikke medfører unødvendig besvær. Den tilegnede dataen må være mottakelig for prossesering slik at systemet kan ekstrahere representative trekk.

Ytelse: Gjennkjennelses nøyaktigheten og resursene som kreves for å nå den nøyaktigheten må møte begrensningene påtvunget av anvendelsen.

Akseptabiliteten: Personene som skal bruke systemet må være villige til å fremvise deres biometriske trekk til systemet.

Omgåelsen: Dette refererer til enkelheten ved å etterligne et biometrisk trekk ved hjelp av artefakter (for eksempel falske fingre, fotografier) eller ved hjelp av etterligning.

Typer biometrisk identifisering

Fingeravtrykkgjennkjenning

Et fingeravtrykk består av overhuden på det ytterste leddet på fingeren. En sier gjerne at det består av rygger og daler. Det formes gjennom en blanding av DNA og miljø og miljø er så avgjørende at eneggede tvillinger ikke har likt avtrykk grunnet ørsmå forskjeller i fostervannet og stillingen de ligger i. Et fingeravtrykk er stabilt fra et foster er rundt syv måneder gammelt. Etter dette forandres ikke fingeravtrykket gjennom livet, sett bort fra kuttskader eller andre ulykker som kan ha en innvirkning[55, side 23]. Hver finger har også sitt eget unike mønster[55, side 17].

Arkeologiske utgravinger tyder på at mennesket har vært klar over dette unike mønsteret i lange tider. Allikevel var det først på tampen av det nittende århundre Henry Fauld gikk vitenskapelig til verks gjennom empirisk observasjon og forselo at fingeravtrykk er unike. Allerede tidlig i det tyvende århundre ble fingeravtrykk formelt akseptert og brukt til å identifisere personer. Allerede i 1924 ble FBIs avdeling for fingeravtrykk opprettet, da hadde de et kartotek på 810 000 fingervtrykk[55, side 28]. Etter hvert vokste denne databasen seg til 200 millioner avtrykk og selv med gode klassifiseringssystemer vokste behovet for et automatisk system.

Automatisk Fingeravtrykk Identifikasjonssystem (AFIS) ble utviklet så tidlig som på 1960 tallet og spredte seg raskt rundt omkring i verden. Etter hvert har teknologien blitt så tilgjengelig at vi nå i dag finner fingeravtrykksesorer i bærbare datamaskiner og til og med i mobiltelefoner, den første ble vist frem av Siemens på CeBIT i 1999[83]. [8] Det er diskutert hvor stor lit en skal sette til identifisering ved hjelp av fingeravtrykk. Dette er en spesielt viktig diskusjon i forbindelse med bruk av fingeravtrykk som bevismateriale i retten. Og Zabell [89] drøfter utfordringene og svakhetene nettop ved slik bruk av fingeravtrykk. Dette gjelder i stor grad der hvor en ikke har hele fingeravtrykk. se figur 2.9 på neste side. Slike fingeravtrykk og denne problemstillingen rettsvesenet står overfor er ikke tilsvarende innenfor autentisering i informasjonssystemer. For det første kan vi forvente høyere kvalitet på inndataen, for det andre vil en eventuell avvisning ikke nødvendigvis føre til de samme konsekvensene. Men det er et viktig poeng å ta med videre at en falsk avvisning kan få følger dersom tilgang til systemet er prekært Det som er viktig i vårt perspektiv er hvor vidt det er mulig å omgå systemet, og om verdiene for FAR og FFR er på et akseptabelt nivå.

Omgåelsen av fingeravtrykksystemene er flere ganger vist å være ganske enkel. I 2004 viste en gruppe fra Chaoz Computer Club hvordan en kan omgå systemet ved hjelp av enkle midler.[9] Wiehe and Søndrol [88] Inspirert av dette og andre artikler finner at i hvert fall optiske fingeravtrykksleserne kan omgås med enkle midler. Det vi ser er at selv en så gammel teknikk som fingeravtrykksgjennkjenning hvor utvikling av programvare startet allerede på 1960 tallet ligger det mange ubesvarte spørsmål og systemene er langt i fra perfekte.

Andre biometriske alternativer

- Ansiktsgjennkjenning
- Irisgjennkjenning
- Ganglag

[8] Motorola Atrix har en innebygd fingeravtrykksensor fra AuthenTec. http://www.motorola.com/Consumers/US-EN/Consumer-Product-and-Services/Mobile-Phones/Motorola-ATRIX-US-EN og http://www.authentec.com/a/ATRIX.aspx Sist besøkt 17. januar 2012.

[9] http://www.youtube.com/watch?v=OPtzRQNHzl0besøkt 19. januar 2012

Alex Garcia; Chicago Tribune
Fig. 1(a) – Inked print of Richard Jackson

Alex Garcia; Chicago Tribune
Fig. 1(b) – Latent print said to match the print in Fig. 1(a)

Figur 2.9: Til venstre: Fingeravtrykk satt med blekk, til høyre: fingeravtrykk funnet på åsted og angivelig fra samme person. Opprinnelig fra McRoberts et.al.Forensics Under the Microscope: Unproven Techniques Sway Courts, Erode Justice, CHI. TRIB., Oct. 17, 2004, Her fra Zabell [89, side 145]

- Øret som biometri
- Stemmen
- Håndflaten
- Signatur
- 3D ansiktsgjennkjenning
- Tenner
- Hånd vaskulær mønster-gjennkjenning
- Multibiometri
- Multispektral ansiktsgjenkjenning

[55]

Sikkerhet i biometriske systemer

Adler [55, side 383] viser til Maltoni et al. [59] og lister opp følgende svakheter ved biometriske systemer.

Omgåelse: Enten gjennom et angrep på datasystemet (for eksempel endring av FAR) eller gjennom en omspilling (replay) (for eksempel opptak av stemme)

Omgåelse: Enten gjennom et angrep på datasystemet (for eksempel endring av FAR) eller gjennom en omspilling (replay) (for eksempel opptak av stemme)

Skjult tilegnelse: Bruk av biometrisk informasjon innhentet fra legitime brukere uten deres viten og vilje.

Sammensvergelse og tvang: Er biometriske systemsvakheter fra legitime brukere. Enten gjennom en sammensvergelse hvor den legitime brukeren villig gir bort tilgang. Eller ved bruk av makt enten det er gjennom utpressing eller andre måter.

Denial of Service (DoS): Et angrep som kan forhindre legitime brukere tilgang til systemet. Målet er å overbelaste systemet ofte for å tvinge systemet til å gå inn i et annet modus som er lettere å omgå.

Avvisning: Angriperen nekter å ha hatt tilgang til systemet og hevder gjerne at noen har stjålet dennes identitet og misbrukt den (Enten gjennom omgåelse, skjult tilegnelse eller falsk aksept.)

En utfordring med biometriske systemer kontra systemer basert på passord/pin/nøkler er at disse sistnevnte alltid kan byttes ut dersom noen skulle få tilgang til dem. Det er ikke fullt så enkelt å bytte ut fingrene våre. Mønstertemplates kan gjøres om til brukbare fingeravtrykk. Dersom vi bruker fingeravtrykk flere steder vil en inntrenger kun trenge å bryte seg inn i den minst sikre databasen med slike avtrykk. Deretter kan den forfalske avtrykk og bruke det i andre systemer. Eller den kan bruke mønsteret til å koble sammen opplysninger. For eksempel en anonym e-post konto som sikres med fingeravtrykk mot tjenester som Altinn.[59, side 375]. En trenger ikke en gang bryte seg inn i en database, med pass og muligens også identitetskort med biometrisk informasjon kan det være mulig å hente ut informasjonen uten at du vet om det og uten at du har mulighet til å sjekke det [3]

2.5 Nærhetsbasert Autentisering

Her redegjøres det for tidligere forskning som er gjort rundt temaet brukerautentisering gjennom nærhetsteknologi. Jeg vil beskrive noen av disse forsøkene og eksempler på systemer som er basert på et token, flere tokens og en blanding av tokens, biometri og posisjon. Målet med kapittelet er å se om vi kan lære noe fra tidligere forskning og prøve å gi en oversikt over de ulike begrepene som er brukt om disse løsningene. Jeg går ikke nærmere innpå de ulike kommunikasjonsteknologiene eller krypteringsløsningene som mange av forslagene inneholder da det ikke er et mål i denne oppgaven å gå nærmere innpå spørsmål knyttet til sikkerheten i disse.

2.5.1 Hva er nærhetsbasert autentisering?

Å få tilgang til noe gjennom noe du har er velkjent for alle, vi er omgitt av ulike låser med tilhørende nøkkelknippe. Veien derfra til løsninger som ikke krever at det er fysisk kontakt mellom kortet/nøkkelen og låsen er ikke lang. Vi kjenner til dette fra bilindustrien med nøkler som låser opp bilen på avstand. Det er blitt vanligere og vanligere med adgangskort med RFID brikker i for å få adgang til bygninger. Ikke minst har de fleste som

har kjørt ski i alpinanlegg de siste årene ganske sikkert hatt skikort som gir adgang uten at du selv er nødt til å gjøre noe. Skidata er en av flere tilbydere av slike systemer [23]. Vi har også blitt vant med å kjøre rett igjennom bomstasjoner, sannsynligvis uten å tenke så mye på hvordan det er mulig. I Norge er det Autopass som er den store tilbyderen av disse løsningene og med en brikke i ruten og en avleser på bomstasjonen slipper man lange køer for å betale manuelt[19]. Når vi kan betale for bompasseringer, få tilgang til bilen og kjøre på ski uten å måtte ta nøkkelen ut av lommen er det selvsagt flere som har spurt seg hvorfor vi ikke kan bruke det når vi handler også. Telenor hadde høsten 2011 et forsøk blant egne ansatte for å teste betaling gjennom RFID [20] Og i Hol kommune har de allerede tatt NFC basert betaling i bruk i «full skala» [21].

Det er åpenbart at dette også har blitt forsøkt gjort med innlogging til datamaskiner. Og de første forsøkene er gamle.

> «The idea of enabling users to access a computer by simply walking up to it has a long history in ubiquitous computing research. This idea of proximity-based login can be traced back to the pioneering work on the Active Badge System, which could be used to 'teleport' an X window session to a display located in front of the user.» [32]

En av de viktige egenskapene til disse systemene er at innloggingen er så lite påtrengende som mulig [Se for eksempel 83, 31]. Brukeren skal ikke behøve å gjøre noen ting for å logge seg ut, han skal bare ta maskinen i bruk [31]. Et slikt mål høres unektelig fristende ut når det kommer til systemer som skal være universelt utformede. Nå skal vi ta en nærmere titt på noen av de forslagene som er kommet opp igjennom årene til slike systemer.

2.5.2 Nærhetsbasert innlogging

I 2003 testet Bardram et al. [32][Også omtalt i 31] ut et system for brukerautentisering i et sykehusmiljø. Formålet var at systemet skulle støtte opp om arbeidsmåten til sykepleiere og leger. En nærmest nomadisk jobbsituasjon hvor de går fra pasient til pasient og hvor de stadig skifter sted, rom og terminal. I dette studiet bruker de en form for to-faktor autentisering basert på lokasjon og nærhet. Bardram et al. [32] har valgt å kalle denne formen for innlogging *nærhetsbasert innlogging*. Brukbarhetsmålet var at brukeren ikke skal trenge å gjøre noen ting for å logge seg inn, bare ta maskinen i bruk.

Systemet kunne med en viss sikkerhet si om personen som prøvde å autentisere seg trådløst overfor en terminal er registrert i det samme rommet. For å få til dette registrerer systemet personene når de går inn og ut av et rom. Tiden mellom en slik registrering danner grunnlag for en beregning av om systemet stoler på at personen er tilstede. For hvert tidsintervall som går uten at brukeren blir registrert med nytt sted minker sikkerheten på hvor denne befinner seg. Systemet har i dette tilfellet ikke en kontinuerlig overvåkning av personen eller kontakt med denne personens token. Dersom personen både er i rommet og prøver å låse opp en maskin

fikk denne tilgang så lenge antagelsen om at personen fremdeles befant seg i rommet var over en viss terskel. Dette er en såkalt *kontekstavhengig autentisering*[54, 32]. Dersom systemet ikke kunne avgjøre om personen var i rommet eller sannsynligheten for det var under den satte terskelen, ville det når terminalen ble presentert for smartkortet komme opp en passordialog hvor brukeren må taste inn sitt passord. Tilsvarende ville også systemet nekte tilgang dersom personen var registrert også et annet sted. Hulsebosch et al. [54] kaller det «Overall Confidence» (OC) og beskriver en modell for å regne ut denne basert på stedet brukerens tokens sist er registrert tiden som er gått.

> «We argue that security services, like authentication and access control, can be made less intrusive, more intelligent, and able to adapt to the rapidly changing contexts of the environment. To validate this argument we show that by fusing various sources of location information that are available over time, the confidence in the user identity associated to the sensed devices can be increased considerably.»[54, side 107]

Noble and Corner [64] vil at tokenet brukeren har for å autentisere seg overfor en terminal eller enhet skal gjøre en «binding» en sammenkobling som krever brukerens eksplisitte godkjenning for hver terminal. En terminal kan ha bindinger til flere tokens og et token kan være bundet til flere terminaler. I forslaget er tokenet en klokke eller noe tilsvarende. I det tokenet forsvinner ut av rekkevidden vil terminalen sikres og dataen krypteres. Den vil auomatisk låses opp når brukeren nærmer seg igjen. Noble and Corner [64] kaller dette «Transient authentication». De har fire prinsipper for denne type autentisering:

> «Transient authentication consists of four properties. First, users must hold the sole means to access resources on the device. Second, the system ust impose no additional usability burdens. Third, the mechanisms to secure and restore sensitive data on a mobile device need be no faster than the people using it. Fourth, users must give explicit consent to later actions performed on their behalf.» [64, side 25]

De to samme forfatterne bruker også begrepet «Zero-interaction Authentication» om et system som beskrives på samme måte [38]. Her foreslås det at tokenet låses ved hjelp av en PIN-kode. Målet deres er å sikre enheter som for eksempel laptoper slik at det ikke er mulig å hente ut informasjon fra dem dersom de blir stjålet. De skriver at forskjellen mellom noe du bærer med deg (laptopen) og noe du har på deg (tokenet) er at det er mindre sannsynlig at du mister det du har på deg.

Senere kommer Nicholson et al. [63] tilbake til «Transient Authentication» og nå er det mobile enheter som er fokuset. Det å kunne sørge for at også mobile enheter er krypterte og informasjonen sikker så snart de kommer i feil hender, samtidig som enhetene er enkle å bruke og ikke tvinger

brukeren til å autentisere seg hele tiden. Da kan den mobile enheten heller kontrollere at tokenet er i nærheten hele tiden i det mellomrommet som går for hver gang brukeren autentiserer seg overfor enheten gjennom en PIN-kode eller på annen måte.

Ojala et al. [72] kommer med et forslag som skal øke sikkerheten til tokenet ytterligere. I tillegg til en initiell autentisering mellom bruker og token (de foreslår å bruke fingeravtrykk) skal tokenet kontinuerlig kontrollere at det fremdeles sitter på den samme brukeren. Også i dette tilfellet er tokenet noe som bæres på armen i form av et armbånd. Dette armbåndet sjekker kontinuerlig vitale signaler fra kroppen. I deres forslag sjekkes hudtemperaturen, oksygenmetning og puls, bevegelse og kapasitans[10]. De ulike sensorene har terskler for hva de anser som ok med tanke på om brukeren fremdeles har armbåndet på seg. Forslaget kaller de «Transparent Login in Nomadic Applications Environment» [72]. Grunnen til at det brukes armbånd i forslaget er at dette bæres på armen som ansees som et ikke intrengende sted på kroppen. Stajano [79] foreslår at det brukes flere tokens for å øke sikkerheten. Han ser at alt brukeren bærer med seg til vanlig kan være en del av systemet. Enten det er briller, lommebok, sko eller andre ting.

Et annet viktig sikkerhetspoeng i disse siste forslagene [72, 38**?** , 63] er at tokenet vil sørge for kontinuerlig autentisering mot maskinen. Det antas at siden tokenet er noe du har på deg er det større sannsynlighet for at brukeren er den samme under hele sesjonen. Fremfor den vanlige måten å gjøre dette på hvor brukeren autentiseres ved begynnelsen av sesjonen og sesjonen kan vare i lang tid.

En tilsvarende tilnærming som har mange fellestrekk med Ojala et al. [72] er Syta et al. [83] som bruker en RFID-basert kontinuerlig autentitisering i kombinasjon med mobile enheter. Men de har en tilnærming som ligger et sted i mellom Bardram og Ojala. Da brukeren får tilgang til enheten gjennom en ikke nærmere beskrevet autoriseringsprosess (for eksempel brukernavn/passord eller biometri) og RFID brikken sørger for kontinuerlig autorisering og dekryptering av informasjonen. I det øyeblikket kontakten mellom den mobile enheten og RFID brikken er brutt vil systemet logges ut og være kryptert. Brukerautentisering blir her gjort hver gang brukeren logger inn i systemet, skrur enheten på eller enheten har vært inaktiv i en gitt periode[83]. Syta et al. [83] legger vekt på at dette er en ikke-påtrengende måte å sørge for kontinuerlig autentisering på.

2.5.3 Funn og retningslinjer fra forskningen

For Bardram et al. [32] og [31] var et av funnene underveis at utlogging er vel så viktig som innlogging av en bruker, da dette er noe folk ofte glemmer. Dette er en av tingene de mener må være med som en del av en autentiseringsmekanisme.

Bardram [31] bruker også begrepet «silent login» om en sesjon hvor to eller flere brukere er inne i samme system, samme applikasjon, samtidig. I

[10] Kroppens evne til å lede strøm.

stede for at den første brukeren blir logget ut og den andre logger seg inn skjer dette i bakgrunnen og sesjonen fortsetter uten avbrytelse når brukerne bytter på å bruke systemet. Systemet tilpasser seg brukernes forskjellige rettigheter uten å avbryte sesjonen.

Bardram et al. [32] identifiserte fire mulige sikkerhetsutfordringer. (Oversatt fra [32]

1. Dersom inntrengeren klarer å få tak i smartkortet og klarer å forfalske posisjonen til den legitime brukeren (enten gjennom å stjele lokasjons tokenet eller på andre måter lure systemet)

2. Dersom inntrengeren har smartkortet kan denne logge seg inn på terminaler i samme rom som den egentlige eieren.

3. Dersom inntrengeren kan passordet og har smartkortet vil denne kunne logge seg inn.

4. Dersom inntrengeren ikke har smartkortet vil denne ikke kunne logge seg inn da systemet vil ignorere at han står der uten et smartkort til å identifisere seg med.

Av disse anses nummer to som ekstremt lite sannsynlig. Den store svakheten i systemet ligger i lokasjonsdelen. Dette er også noe som blir påpekt av [72]. Om en person klarer å tilegne seg både smartkortet og lokasjonstokenet vil denne ha full tilgang til alle brukerens systemer uten noen gang å trenge å identifisere seg eller autentisere seg på andre måter. Det vil si to tokens er nok for å få tilgang til hele systemet. Det er ikke vanskelig å se for seg at både et slikt smartkort og en lokasjonstoken vil kunne bli oppbevart på samme sted av brukeren. Bardram et al. [32] har noen forslag til mottiltak mot dette. For det første bør systemet sjekke om brukeren er på to steder samtidig. Det bør kontrollere for om brukeren er på arbeid eller ikke. Systemet kan sjekke at brukeren ikke beveger seg for raskt fra ett sted til et annet. Dette blir gjort med skikort i dag, hvor en ikke får adgang til heisen dersom det er for kort tid siden sist gang du ville igjennom porten. Dette har og kan selvsagt skape nye utfordringer igjen, men i forslaget vil systemet falle tilbake til passorddialogen.

For å bøte på svakheten ved at et individ, eller brukeren ikke må identifisere og autentisere seg opp mot sine tokens før disse gir adgang foreslår Ojala et al. [72] et token som bæres på håndleddet. Dette armbåndet sjekker kontinuerlig vitale signaler fra kroppen. I deres tilfelle sjekkes hudtemperaturen, oksygenmetning og puls, bevegelse, kapasitans[11] og bevegelse. Et av kravene deres var at disse dataene måtte kunne samles inn uten å forstyrre brukeren. Forslaget deres utelukker ikke andre typer data. I tillegg til en kontinuerlig sjekk fra armbåndet om det faktisk *er* på brukeren kobles det enkelte token opp mot en spesifikk bruker. Brukeren må ha en *initiell autentisering* når armbåndet ikke har vært i bruk. I tillegg vil systemet kreve reautorisering så snart armbåndet blir tatt av og ikke kan registrere noen av de nevnte dataene lenger. På denne måten økes sannsynligheten

[11] Kroppens evne til å lede strøm.

for at armbåndet blir brukt av en genuin bruker. Armbåndet blir ubrukelig så snart det mistes eller blir stjålet. Måten de valgte å autentisere brukeren på var gjennom fingeravtrykk. Dette fungerer da som en verifikasjon av brukeren, noe som er sikrere enn å bruke biometri i identifikasjonsmodus (se 2.4.4).

Syta m.fl [83, side 4] lister opp noen krav til autentiseringssystemer for mobile enheter:

- Ikke-påtrengende: brukere bør oppfatte autentiseringsprosessen som enkel å bruke.
- Transparent: Noen eller alle stegene i autoriseringsprosessen bør være uten brukerens eksplisitte interaksjon.
- Kostnadseffektiv: Ingen ekstra og/eller dyr hardware bør kreves.
- Kontinuerlig: Autentisering må skje kontinuerlig og ikke stoppe etter den initielle innloggingen (point of entry). Tilstedeværelsen av en autentisert bruker må være sikret til enhver tid.

Mobiltelefonen er foreslått som et slikt token på grunn av deres popularitet og den relativt korte tiden det tar før en oppdager at en mobil er mistet eller stjålet sammenlignet med bankkort

2.6 Rammeverk for sammenligning og evaluering av web-autentiseringsløsninger

Bonneau m.fl [35] har laget et grundig rammeverk for sammenligning og evaluering av autentiseringsløsninger. Dette er først og fremst rettet mot webbaserte løsninger. Men det later til å være et veldig godt utgangspunkt både for å se hvordan eksisterende løsninger gjør det i dag. Dessuten som et utgangspunkt for å se hvor det er forbedringspotensiale og for å sammenligne forslag til nye løsninger. En slik systematisk sammenligning er nok ikke unik, men er så vidt jeg vet det ferskeste eksempelet på en slik sammenligning.

En annen styrke med dette rammeverket er bakgrunnen og agendaen (eller mangelen på en) forfatterne har. De konfontrerer tidlig den vanligvis endimensjonale fremstillingen av sikkerhet og brukbarhet, som gjennomsyrer mye av forskningen rundt sikkerhet og brukervennlighet, når de skriver:

> ≪In the past decade our community has recognized a tension between security and usability: it is generally easy to provide more of one by offering less of the other. But the situation is much more complex than simply a linear trade-off: Wee seek to capture the multi-faceted, rather than one-dimensional, nature of both usability and security in our benefits. We further suggest that "deployability", for lack of a better word, is an important third dimension that deserves consideration.≫ [35]

Se også [53] om passords utholdenhet for større forståelse for forfatternes bakgrunn hvor passord ikke er et stort onde og alle andre løsninger er bedre.

Vurderingskriteriene de har valgt å se nærmere på er gjengitt i en oversatt og til dels forkortet utgave under.

2.6.1 Vurderingskriterier for sammenligning og evaluering

Brukervennlighetsfordeler

B1 Minnemessig uanstrengt: Brukere av løsningen trenger ikke å huske noen hemmeligheter i det hele tatt. Løsningen får en *Kvasi minnemessig uanstrengt* skår dersom brukeren må huske en hemmelighet for alt.

B2 Skalerbar for brukeren: Bruk av ordningen for hundrevis av kontoer øker ikke belastningen på brukeren. Som kategorien antyder, menes skalerbar bare fra brukerens perspektiv, vi ser på den kognitive belastningen, uten perspektiv fra distribusjon av systemet eller fordeling av tekniske resurser.

B3 Ingenting å bære: Brukerne trenger ikke å bære et ekstra fysisk objekt (elektronisk enhet, mekanisk nøkkel, et stykke papir) for å bruke ordningen. *Kvasi-Ingenting å bære* tildeles hvis objektet er et de ville bære med seg uansett, for eksempel mobiltelefonen, men ikke en datamaskin (inkludert nettbrett).

B4 Fysisk uanstrengende: Godkjenningsprosessen krever ikke fysisk (i motsetning til kognitiv) brukerinnsats utover, for eksempel å trykke på en knapp. Ordninger som ikke tilbyr denne fordelen er de som krever å skrive, skrible eller utføre et sett med bevegelser. Vi gir *Kvasi fysisk uanstrengende* hvis brukerens innsats er begrenset til å snakke, på grunnlag av at selv analfabeter finner det naturlig å prate.

B5 Enkelt å lære: Brukere som ikke kjenner løsningen kan enkelt finne ut av den og lære den uten for mye trøbbel og de kan enkelt huske hvordan det brukes.

B6 Effektivt å bruke: Tiden det tar hver gang brukeren skal autentiseres er akseptabelt kort. Tiden det tar å assosieres med en ny verifiserer kan være lenger men må også være rimelig.

B7 Sjeldent feil: Oppgaven brukeren må gjøre for å logge inn må vanligvis være vellykket når den utføres av en legitim bruker. Med andre ord løsningen må ikke være så vanskelig å bruke eller upålitelig at brukeren nærmest rutinemessig blir avvist.

B8 Enkel gjennoppretting fra tap: En bruken kan enkelt få tilbake muligheten til å autentiseres dersom tokenet mistes eller legitimasjonen (brukernavn og tilsvarende) blir glemt. Dette inkluderer brukbarhets aspekter så som: lav ventetid før evnen til å autentiseres er tilbake; lav

grad av ulempe for brukeren ved gjennoppretting (for eksempel ikke noe krav om fysisk måtte stå i kø); og bekreftelse på at gjennopretting er mulig, for eksempel gjennom innebygde sikkerhetskopi eller en sekundær gjennopprettingsløsning. Dersom gjennopretting krever en eller annen form for re-registrering vil dette bli lagt til i vurderingen av ulempe.

Utplasseringsfordeler (Deployability, implementeringsfordeler se aanestad

U1 Tilgjengelig: Brukere som kan bruke passord er ikke forhindret fra å bruke denne løsningen på grunn av funksjonsnedsettinger eller andre (ikke kognitive) grunner. [12]

U2 En uvesentlig kostnad per bruker: Den totale kostnaden per bruker av løsningen, summering av kostnadene både fra den som prøver å bevise og den som verifiserer sin side. Løsningen må være plausibel for oppstartsbedrifter med ingen inntekt per bruker.

U3 Serverkompatibel: På verifiserers side, løsningen er kompatibel med tekstbaserte passord. Tilbyder trenger ikke å endre på eksisterende autentiseringsoppsett.

U4 Nettleserkompatibel: Brukere trenger ikke å endre på klientene sine for å støtte løsningen og kan forvente at løsningen fungerer også på andre maskiner med en oppdatert nettleser uten ekstra mykvare. I 2012 vil dette bety en nettleser som støtter HTML5 med JavaScript aktivert. Løsninger som krever en eller annen form for mykvare hvor installasjon krever administrative rettigheter vil ikke støtte dette kravet. Løsninger får en *Kvasi nettleserkompatibel* skår dersom de benytter seg av ikke-standard men vanlige plugins som for eksempel Flash.

U5 Modent: Løsningen har blitt implementert og utplassert i storskala for faktiske autentiseringsformål som ikke er til forskning. Faktorer å vurdere for å gi full fordel av dette kriteriet er om løsningen har vært testet, om det finnes standarder, om open-source prosjekter har implementert løsningen og om noen andre enn implementererne har adoptert løsningen, mengden litteratur om løsningen og så videre. U6 Ikke-proprietært: Hvem som helst kan implementere løsningen til hvilket som helst formål uten å måtte betale royalties til noen andre. De relevante teknikkene er kjente, publiserte og åpne. De er ikke beskyttet av patenter eller forretningshemmeligheter.

[12] De skriver selv at ideelt sett skulle et system være brukbart av alle uavhengig av funksjonsnedsettinger. Men for alle systemer vil en alltid kunne påberope seg at det ikke er tilgjengelig for alle dermed ville ingen løsninger fått en skår på dette kriteriet. Derfor er det valgt å gi en skår for de systemene som gjør det bedre en dagens de-facto standard nemlig passord, selv om dette heller ikke er perfekt blir det i dag akseptert. Et alternativ til dette tekst-passord baserte grunnmålet kunne en basert målingen på løsningens evne til å være tilgjengelig for en viss prosent av befolkningen.

Sikkerhetsfordeler

S1 Motstandsdyktig mot fysisk observasjon: En angriper kan ikke opptre som en bruker etter å ha observert dem autentisere seg en eller flere ganger. Vi gir *Kvasi motstandsdyktig til fysisk observasjon* dersom løsningen kan bli forbigått bare ved å observere mer enn si 10-20 ganger. Angrep inkluderer å se over skulderen, filme tastaturet, ta opp lyden av tastettrykk, eller å ta termiske bilder av et tastatur.

S2 Motstandsdyktig mot målrettet etterlikning: Det er ikke mulig for en bekjent å etterligne en spesifikk bruker ved å utnytte kunnskap om personlige detaljer (fødselsdato, navn på slektninger og lignende.). Personlige spørsmål er den kanoniske løsningen som feiler på dette punktet.

S3 Motstandsdyktig mot gjentatt begrenset gjetting: En angriper, hvis mulighet til å gjette hemmelighet er begrenset av den som verifiserer, kan ikke gjette seg frem til en signifikant del av brukerne. Begrensningen fra verifisereren kan bli påtvunget fra en online server, en chip som ikke kan tukles med eller andre mekanismer som kan kvele gjentatte forsøk. Et kvantitativt eksempel kan være for eksempel 10 gjettinger per konto/bruker per dag, eller at en angriper høyst kan gjette seg frem til 1% av kontoene på et år. Mangel på denne egenskapen er ment å straffe løsninger hvor det er vanlig at brukeren velger hemmelighet fra en liten og velkjent delmengde.

S4 Motstandsdyktig mot ubegrenset gjetting: En angriper hvis mulighet til å gjette er begrenset bare av tilgjengelig datakraft kan ikke gjette seg frem til hemmeligheten til en vesentlig del av brukerne. Vi vil for eksempel tildele dette kriteriet dersom en angriper kan prøve seg 240 ganger på en konto, men fremdeles bare klarer å gjette seg frem til 1% av kontoene. Mangel på denne egenskapen er ment å straffe løsninger hvor mengden berettigelsesbevis (ID'er) ikke er stor nok til å motstå brute force angrep.

S5 Motstandsdyktig mot intern observasjon: En angriper kan ikke etterligne en bruker ved å avskjære brukerens input fra brukerens enhet (for eksempel ved hjelp av tastaturlogging) eller ved tyvlytting på klartekst kommunikasjon mellom den som beviser og verifisereren (Også TLS er antatt å kunne brytes). Vi gir *Kvasi motstandsdyktig mot observasjon* dersom løsningen kun kan bli brutt ved gjentatt tyvlytting, for eksempel 10-20 ganger. Dette straffer løsninger som ikke er motstandsdyktige mot gjentagelses angrep (Engelsk replay attacks) enten fordi responsen er statisk eller den dynamiske responsen kan bli knekt ved gjentatte observasjoner. Denne egenskapen antar at enheter som brukes til generelle formål så som datamaskiner og mobiltelefoner kan inneholde malware, men at dedikerte hardvare enheter som hører til løsningen kan være fri for slik malware. *Kvasi motstandsdyktig mot intern observasjon* gis til tofaktors løsninger hvor begge fak-

torene må være angrepet av malware for at et angrep skal være vellykket.

S6 Motstandsdyktig fra lekasjer fra andre verifisererere: Ingenting av det en verifiserer kan lekke kan hjelpe en angriper i å etterligne en bruker mot en annen verifiserer. Dette straffer løsninger hvor en inside man eller et vellykket angrep et sted kan sette brukerens kontoer i fare andre steder.

S7 Motstandsdyktig mot Phising: En angriper som simulerer en gyldig verifiserer (inkludert ved hjelp av DNS manipulasjon) kan ikke samle inn berettigelsesbevis som senere kan brukes for å etterligne brukeren mot den virkelige verifisereren. Dette straffer løsninger som er åpne for phising gjennom at brukeren blir presentert for en falsk autentiseringsside som brukes for å høste berettigelsesbevis. Denne egenskapen er ikke ment å straffe løsninger som er sårbare for mer sofistikerte sanntids angrep eller relé angrep hvor angriperen har en kobling til bruker og en til verifisereren.

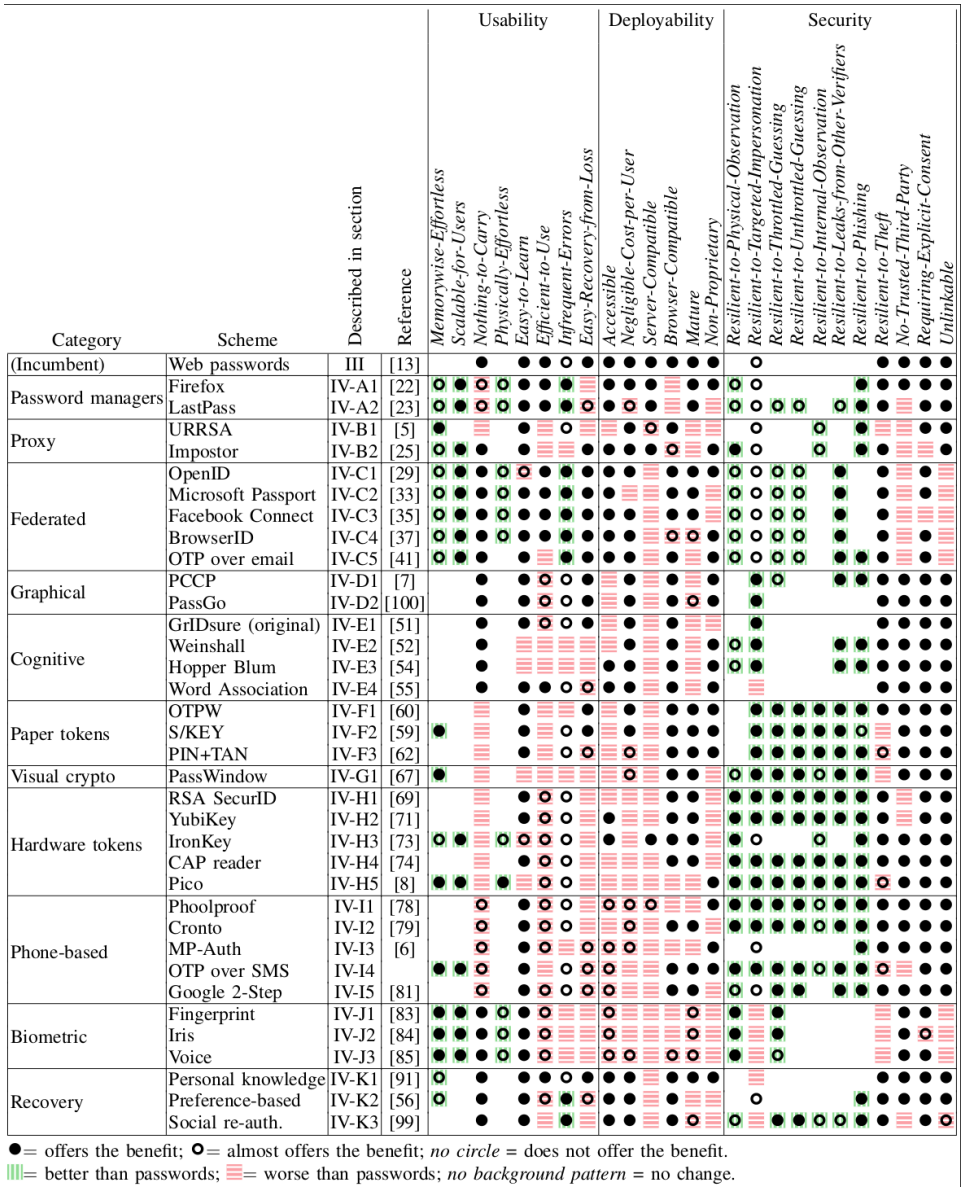
S8 Motstandsdyktig mot tyveri: Dersom løsningen bruker et fysisk objekt for autentisering kan ikke en annen person som får tilgang til dette objektet. Det gis *Kvasi motstandsdyktig mot tyveri* for løsninger som beskytter enheten med enkel styrke, som en PIN-kode, selv om det ikke ligger begrensning i antall gjette forsøk, siden et slikt angrep ikke enkelt skalerer til mange ofre.

S9 Ingen tiltrodd tredjepart: Løsningen baserer seg ikke på en tiltrodd tredjepart (andre enn den som beviser og verifisereren) som kan gjennom et angrep eller på andre måter miste tiltroen kompromitere brukerens sikkerhet eller personvern.

S10 Krever eksplisitt samtykke: Autentiseringsprosessen kan ikke starte uten eksplisitt samtykke fra brukeren. Dette er både en sikkerhets- og en personvernsfunksjon.

S11 Ikke linkbar: Kolliderende verifisererer kan ikke bestemme gjennom autentikatoren alene om brukeren autentiserer seg til begge. Dette er en personvernsfunksjon. For å rangere denne tar vi ikke hensyn til linkbarhet gjennom andre mekanismer (samme bruker ID, IP adresse osv.).

Bonneau med flere legger vekt på at det ville være for enkelt å vekte alle kriteriene likt også summere opp for å sammenligne løsninger. Hvilke egenskaper og kriterier en legger vekt på vil avhenge av hva målet med sammenligningen er. B2 *Skalerbart for brukeren* er for eksempel en viktig egenskap dersom målet er å adoptere en universell løsning, det er mindre viktig dersom målet er å finne et passord alternativ til en enkelt konto. Det foreslås en kvantitativ løsning som kan gi en poengsum, men forfatterne har valgt å gå for en kvalitativ vurdering. En hovedårsak til det er at det er selve evalueringen som gir ny kunnskap om løsningen ikke nødvendigvis



Figur 2.10: Rammeverk for sammenligning og evaluering fra [35]. Diskusjonen for avgjørelsen av hvordan de forskjellige løsningene er dekket finnes i en egen teknisk rapport [36]

en poengsum hvor poengene uansett er avhengig av vektingen og da allikevel ikke vil kunne bli objektive [37]. Det legges også vekt på at det ikke nødvendigvis er dataen de er kommet frem til som er viktig, men metoden å vurdere en ny sikkerhetsløsning på. Med egenskaper som er lette å sammenligne og en relativt grovmasket fordeling. Fordelen med så pass grove masker er at diskusjonen og vurderingen kan ligge på et noe høyere plan før en dykker ned i detaljene og vurderer og tester en spesifik løsning. Bakgrunnen til dette er at mange forslag til nye autentiseringsløsninger tenderer til å være i overkant positive hva gjelder egenskapene til akkurat denne løsningen. Denne måten å evaulere på, med disse kriteriene kan være til hjelp for å hindre en slik bias mot «sin egen løsning».

Kapittel 3

Metode

3.1 Om valg av forskningsmetode

Metodikken som brukes for å komme frem til svar har mye å si for et studie. Uavhengig av om forskningen er kvalitativ eller kvantitaiv har forskeren et filosofisk utgangspunkt for sin forståelse av «gyldig» forskning. Ut i fra dette filosofiske synet følger det naturlig hvordan en angriper spørsmålene og hvilke metoder som er riktige å bruke for å komme frem til svarene. Myers [62] legger vekt på at det er viktig å være bevisst dette utgangspunktet når en utfører forskningen. Våre epistemologiske antagelser legger grunnlaget for hvordan vi vil ta fatt på et spørsmål. Epistemologien referer til hvordan vi forstår kunnskap og hvordan en kan nå frem til denne kunnskapen [62]. Målet med dette kapittelet er å redegjøre for hvordan jeg har angrepet forskningsspørsmålet og hvorfor jeg har valgt å angripe temaet på den måten som er gjort.

Den vanligste måten å skille studier på er mellom kvalitative og kvantitative studier. Men det finnes også andre linjer en kan beskrive studier langs. For eksempel objektive kontra subjektive studier. Studier som prøver å finne generaliserbare lover (nomotetisk) kontra studier som fokuserer på unikheten i en situasjon (idiografisk). En utfordring er at det er store diskusjoner rundt bruken av disse merkelappene [62]. Det kan være vanskelig å plassere en merkelapp på et studie nettopp fordi de grunnleggende forskjellene som virker store i teorien i praksis brukes om hverandre. Som så mange andre steder og i så mange andre situasjoner blir også disse utgangspunktene ofte satt på spissen og nærmest karikert i sort hvitt. Enten er virkeligheten objektiv eller så er den subjektiv. Enten finnes de riktige svarene kun i data som kan generaliseres ut i fra et representativt utvalg eller så ligger den interessante informasjonen i subjektive beskrivelser av virkeligheten fra enkeltpersoner.

Oppå dette kommer ulike tradisjoner i ulike fagdisipliner. Naturvitenskapene er kjent for å holde seg til kvantitative studier, mens de samfunnsvitenskapelige studiene ofte er kvalitative. Dette er selvsagt også en sort/hvitt fremstilling av virkeligheten. Skandinavia er kjent for brukersentrert utvikling av informasjonssystemer (REFERANSE), gjerne gjennom aksjonsstudier. Her brukes kvalitative data for å forme informasjonssyste-

mer som skal passe mange forskjellige brukere. Målet er å skape gode brukeropplevelser. Går vi enda smalere inn og ser på brukbarhetstesting av systemer er det også tradisjon for å teste på et lavt antall brukere. Jakob Nielsen er en av de som skriver varmt om fordelen ved å teste på et lavt antall personer [9]. Samtidig finnes det andre disipliner innenfor utvikling av informasjonsteknologien som gjør dette på andre måter. Studiet kan jo utformes som et etnografisk studie av informasjonssystemet. Plutselig får vi et helt annet utgangspunkt og må gjerne stille andre spørsmål hvorpå også svarene blir annerledes. En kan også teste brukbarhet gjennom så kalt A/B testing for å se hvilke av to alternative design som er mest effektive. Da tester en kvantitativt fremfor kvalitativt og får svar på hva som fungerer best, men kanskje ikke hvorfor det er best.

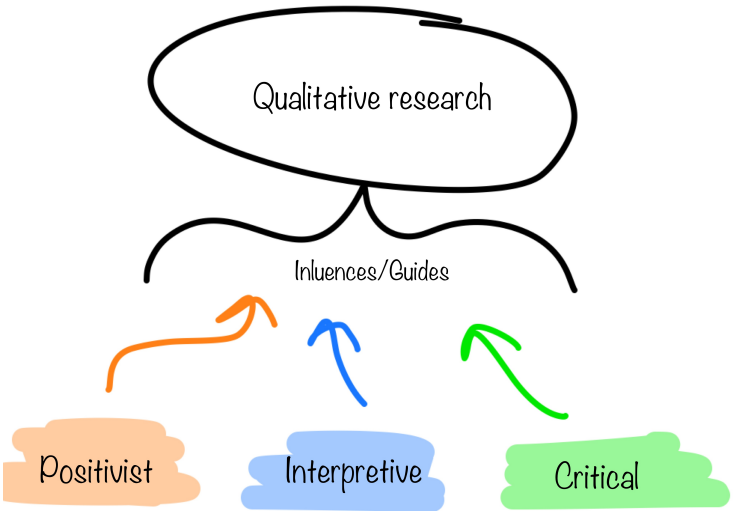
Det er ikke bare enkelt å sette rammene for studiet innenfor disse tradisjonene uten å starte en for lang diskusjon med formål om å tråkke opp grenser. Så vidt jeg kan se av litteratur rundt forskningsmetoder er det aller meste «lov». Hovedutfordringen er kanskje å identifisere hvorfor du gjør det og hvilke styrker og svakheter den måten du har gjort dette på kan spille inn på resultatene. Dersom en klarer å se tydelig hvilket utgangspunkt en har tror jeg det er mulig å utnytte de ulike tilnærmingene slik at en kan bruke den metodologien en tror er best egnet til å komme frem til svar på spørsmålene en har. Nå vil jeg først posisjonere dette studiet faglig og epistemologisk. Deretter redegjøre for metodikken som er brukt. Deretter kommer noen etiske vurderinger i forbindelse med studiet og til slutt noen refleksjoner over mitt ståsted som ikke er ubetydelig for hvordan resultater tolkes.

3.2 Dette studiet

Dette studiet har en faglig forankring i det som kalles interaksjonsdesign. Denne forankringen er befriende tverrfaglig, som vi kan se av figur 2.1 på side 8 har interaksjonsdesign relasjon til mange ulike akademiske disipliner. Denne friheten til å hente inspirasjon fra ulike fagfelt har en pris. På den ene siden er det en styrke å kunne analysere data fra ulike ståsteder. På den andre siden kan mangelen på en tydelig faglig forankring og den ene teorien som binder alt sammen være en svakhet. Det kan være vanskelig å sammenligne studier og resultater. Det kan være vanskelig å vurdere om det faglige tyngdepunktet ligger på riktig sted i forhold til spørsmålene som blir stilt. I det hele tatt er det vanskelig å presist posisjonere studiet innenfor ett felt da det egentlig ligger mellom mange fagfelt.

Slik er det også med denne oppgaven. Teoriene er hentet fra ulike disipliner. Det som binder dem sammen er kanskje mest av alt et fokus på brukersentrert utvikling av informasjonssystemer og et ønske om å forstå brukeren på best mulig måte. Slik at analysen blir tydeligst mulig og kan oppfylle et mål om å bidra til å finne ny viten og øke kunnskapen på det området denne oppgaven undersøker.

På den bakgrunnen er dette studiet blitt et kvalitativt kasusstudie



Figur 3.1: Underlying Philosophical assumptions,[62]. Underliggende paradigmer i kvalitativ forskning.

med formål om å forstå problemområdet rundt universell utforming og brukerautentisering. Den teoretiske forankringen redegjøres for i teorikapittelet.

3.2.1 Paradigme

Kvalitative studier ble utviklet i samfunnsvitenskapen for å sette forskere i stand til å studere sosiale og kulturelle spørsmål. Typiske kvalitative metodologier er aksjonsforskning, kasusstudier og etnografi. De vanligste dataene kommer gjennom dokumenter, intervjuer, notattaking og observasjon[62]. Datainnhentingen kalles gjerne metoder. Som bakgrunn for metodologiene kategoriserer Myers [62] tre paradigmer: positivistisk, fortolkende og kritisk. Dette er illustrert i figur 3.1. Nå gir jeg først en oversikt over de tre paradigmene før jeg diskuterer denne oppgavens ståsted når det gjelder paradigmer.

Positivistisk forskning

I den positivistiske retningen antar man at virkeligheten er objektiv og kan bli beskrevet gjennom målbare egenskaper som er uavhengige av observatøren (forskeren) og dennes intstrumenter. Positivistiske studier prøver gjerne å teste teorier. I positivistisk forskning legger en gjerne vekt på kvantitative data [62, 56]

Kritisk forskning

Innenfor kritisk forskning antar en at virkeligheten er historisk betinget og at denne virkeligheten blir produsert og reprodusert av mennesker. Selv om mennesker bevisst kan handle for å endre sosiale og økonomiske

omstendigheter, har kritisk forskning et fokus på at muligheten til å handle er begrenset av forskjellige former for sosiale, kulturelle og økonomisk dominans fra et annet hold. Hovedoppgaven til kritisk forskning er å kaste lys på disse forholdene med tanke på endring og hjelpe de «svake» gjennom å forstå mekanismene som låser dem i dette systemet av historisk gjentagende dominans. Det fokuseres altså på konflikter og motsetninger i samtiden og forsøker å være frigjørende. [62, 56].

Fortolkende forskning

Fortolkende forskning tar utgangspunkt i at virkeligheten kun er tilgjengelig gjennom sosiale konstruksjoner som språk, bevisthet og delte meninger. Fortolkende studier prøver å forstå fenomener gjennom måten folk tolker dem og meningene deres. Den filosofiske bakgrunnen finner en i hermeneutikken og fenomenologi [62].

Valg av paradigme

Disse paradigmene påvirker også hverandre og lever ikke i et vakum hver for seg. Som vi ser av figur 3.1 på forrige side påvirker de alle den kvalitative forskningen. Denne oppgaven er påvirket av både det kritiske og det fortolkende paradigmet, i mindre grad av det positivistiske. Der det positivistiske slår inn er først og fremst på ting som i hvert fall jeg opplever som objektive. Dette handler blant annet om den objektive risikoen for at noe skal skje med akkurat deg. Risikoen for at A, B, eller C kan skje med deg. Det er ikke noe oppgaven ser veldig nært på, men det kan annerkjennes at dette er viktig når en spesifiserer krav til informasjonssikkerhet. Når det gjelder følt risiko og opplevelsen av hvordan et system er, fungerer eller andre holdninger personen måtte ha med tanke på informasjonssystemet tror jeg det i stor grad er sosialt konstruert og at det er viktigere å forstå hvordan folk tolker dem enn hvordan det (eventuelt) er objektivt sett. Hele tilnærmingen til feltet kan sies å være kritisk. Selve spørsmålsformuleringen impliserer denne holdningen som det står i introduksjonen ønsker jeg å «belyse hvilke rammefaktorer en står overfor i utvikling av universelt utformede autentiseringsløsninger». Nettopp fordi jeg har en forståelse av virkeligheten som at den er styrt i stor grad av ytre omstendigheter.

Dette gjør det vanskelig for meg å si at jeg tilhører et paradigme. Jeg forstår ikke hvorfor jeg skal være «tro» mot kun et av disse paradigmene i forskningen min da de sammen gir en relativt god modell for hvor sannheten ligger. Stake [80] skriver at triangulering i kvalitative studier ikke handler om å bekrefte en hendelse, men om å forstå en hendelse bedre ved å se på den fra forskjellige vinkler. De tre paradigmene er noe helt annet enn det Stake her skriver om, samtidig er min forståelse av dette slik at de funnene jeg gjør blir til gjennom å bruke disse tre utgangspunktene sammen og ikke hver for seg.

3.2.2 Hvorfor et kasusstudie?

Å forme dette som et kasusstudie[1] gir meg mulighet for å få en dypere forståelse for hvilke faktorer som påvirker folks holdninger og for å forstå hvilke behov de har. Det holder ikke å vite at X antall brukere velger å bruke svake passord når en ikke går dypere inn og prøver å forstå hvordan vi kan løse dette på en måte som gjør at de godtar høyere sikkerhet.

Stake [80] skriver:

> «The researcher examines various interests in the phenomenon, selecting a case of some typicality but leaning toward those cases that seem to offer *opportunity* to learn. My choice would to choose that case from which we feel we can learn the most.» [80, side 451]

Også Lazar et al. [58] skriver at et kasusstudie er et dybdestudie av et spesifikt tema [58, side 144]. Objektene som studeres er ofte forsiktig utvalgt med tanke på å generere interessante og nye innsikter (ibid).

Om kasusforskning innenfor HCI og interaksjonsdesign

Lazar skriver følgende om vanlige mål for HCI kasusstudier: «Broadly speaking, HCI case studies have four goals:

- *exploration*, understanding novel problems or situations, often with the hopes of informing new designs;
- *explanation*, developing models that can be used to understand a context of technology use;
- *description*: documenting a system, a context of technology use or the process that led to a proposed design;
- *demonstration*: showing how a new tool was successfully used.»

[58, s 150]

I dette studiet er det de to første punktene utforskning og forklaring som er viktigst.

Kritisk kasus

Jeg har latt meg inspirere av hvordan Flyvbjerg [43] beskriver *kritiske kasuser* eller «black-swans» i min utforming av studiet. Med mål om å forme et kasus som kan bidra til å lære mest mulig slik Stake foreslår over. Denne måten å forme studiet på gjør at jeg undersøker noen ekstreme tilfeller. Nå er ikke studiet formet som en test, mer som en utforskende studie. I den utforskningen har jeg forsøkt å identifisere de brukerne som har de største kravene i en eller annen retning. For dette studiet har det vært førende for hvilke intervjuobjekter jeg har plukket ut og hva jeg har

[1] Jeg har valgt å bruke det norske kasus fremfor det engelske case som benevnelse gjennomgående i denne oppgaven. Jeg håper det ikke forstyrrer leseren i for stor grad.

undersøkt. I intervjuene har jeg vært på jakt etter personer med moderat til lav motivasjon for sikkerhetsoppgaver. Jeg har forsøkt å plukke ut personer som ikke har «noe spesielt å frykte» det vil si de skiller seg ikke ut (så vidt jeg kan bedømme) med tanke på risiko fra den øvrige befolkningen. I testing av LastPass ble det plukket ut en person med høy motivasjon og god innsikt i IKT for at dette ikke skulle være begrensende faktorer. I workshopen ble det igjen lagt vekt på unge personer med antatt mange kontoer og moderat interesse for informasjonssikkerhet. Bakgrunnen for disse valgene ligger i formålet med universell utforming:

> «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 tilpassning og en spesiell utforming.»[5]

Min forståelse for universell utforming er at «uten behov for tilpassning og en spesiell utforming» i aller høyeste grad også gjelder brukere uten spesielle behov. Jeg har antatt at brukere uten spesielle behov er de som setter høyest krav til at et system skal være enklest mulig å bruke. Selv om denne antagelsen skulle vise seg å ikke stemme vil resultatene være interessante fordi de vil vise hvilke behov brukere uten spesielle behov har.

Utvalg og nytte

Ikke-statistisk (Eng:Non-probalistic) utvalg er ganske vanlig innenfor HCI forskning[78]. En viktig grunn er at det ofte ikke er en veldefinert populasjon av respondenter. Det finnes ikke visse egenskaper som gjør det lett å skille ut en gruppe [58]. Sharp et al. [78] bruker også begrepet «bekvemmelighets-utvalg» (Eng: Convenience sampling). Både intervjuobjektene og workshop-deltakerne er plukket ut på en slik måte. Dette omtales nøyere under beskrivelsen av intervjuobjektene.

Kasusstudier blir gjerne beskrevet som enten iboende interessant eller instrumentelle. På mange måter er det fristende å si at mitt kasus er iboende interessant. Men det ville ikke vært iboende interessant dersom jeg ikke så at det ville kunne gi innsikt i noe som kanskje kan gjøre autentiseringshverdagen bedre. Men i mangel av bedre forslag kaller jeg dette et iboende interessant kasus. Både Stake [80] og Flyvbjerg [43] legger vekt på at mye av styrkene til kasusstudier ligger i det Stake kaller *den tykke beskrivelsen* [80]. Kraften i et eksempel skriver Flyvbjerg er undervurdert Flyvbjerg [43].

> «How we learn from the singular case is related to how the case is like and unlike other cases we know, mostly by comparison. It is intuition that persuades both researcher and reader that what is known about one case may very well be true about a similar case (Smith1978)» [80, side 455].

Til forskjell fra Flyvbjerg [43], Stake [80] mener Lazar et al. [58] at et viktig mål med kasusstudier er nettopp å kunne genereralisere. De skriver følgende:

> «An in-depth discussion of one individual (such as Sara) is interesting, but the real value in a study of this sort lies in generating insights that can be applied to a broader class of design challenges.» [58, side 157]

Slik jeg ser det og slik jeg tolker Flyvbjerg og Stake er det mulig å generere slike innsikter Lazar et al. [58] etterspør, også gjennom kasusstudier som er utformet på den måten dette studiet er utformet. Uten at det derved hevdes at de funn som blir gjort i studiet er direkte generaliserbare. Det viktige er at funnene allikevel vil ha en verdi.

3.3 Metoder

Jeg har valgt å benytte meg av intervju og en workshop som de viktigste kildene til innsikt foruten en litteraturgjennomgang. Nedenfor vil jeg redegjøre kort for disse valgene.

3.3.1 Intervju

> «Når folk får muligheten til å prate og spørsmålene åpner og oppfordrer til refleksjon kan intervjuobjektene gå langt i å dele innsikter og ideer som ellers ikke ville kommet frem gjennom spørreskjema» [58, side 178].

Den innsikten man får når intervjuobjekter får tid til å forklare hva de tenker om et tema er helt unik. I dette studiet prøver jeg å forstå ikke bare hvilket behov brukeren har, men like mye prøver å forstå situasjonen de er i. Intervju var et naturlig valg. Dette gav meg muligheten til å i større grad forstå noen av holdningene deres, forstå noen av utfordringene et nytt system må løse. Spesielt når studiet i seg selv ikke er rettet mot å lage en ny løsning og teste den, men å forsøke å forme et konsept til løsning er intervjuet mer nærliggende enn observasjon. For hva skulle jeg observert? Interessen min ligger ikke primært i hvilke problemer et nåværende system har. Og kunnskapen rundt hva et nytt system vil kreve var for lav til å i det hele tatt foreslå et system på forhånd. Det som eventuelt kunne observeres var kjente problemer knyttet til B/P metaforen, disse problemene er relativt godt dokumentert andre steder. I intervjuet får jeg en rik dialog med personer som kan fortelle hvordan de opplever situasjonen i dag og hva de tenker om informasjonssikkerhet. Dessuten var håpet at de kunne reflektere over hvordan andre systemer kunne påvirke dem. Kanskje viktigst var det å få høre selv, og ikke bare lese om, holdningene deres til informasjonssikkerhet. Hvordan opplever de selv risikoen? Hvordan håndterer de denne? Utfordringen med intervjuer er at en har «tatt et skritt bort fra virkeligheten» [58, side 179]. Derfor kan svarene variere fra det som skjer og det en gjerne ville observert dersom en var in situ. En helt naturlig fortsettelse ville være å utvikle et system og deretter teste systemet eller enkeltelementer også observere brukeren.

> «look at behavior, listen to perceptions»[179 58, Refererer til Miller og Crabtree 1999]

Intervjuene ble utformet som semistrukturerte intervjuer slik både Lazar et al. [58] og Sharp et al. [78] anbefaler når målet er å utforske et tema.

Identifisering av intervuobjekter (utvalget)

Utvalget av intervjuobjekter ble gjort med en så kalt ikke-statistisk utvalg som bakgrunn. Denne oppgaven gir ikke svar som er generelle eller ment å være generaliserbare. Når jeg skulle plukke ut personene var hovedkriteriet at de var ordinære brukere av teknologi. I en slik utvelgelse blir det en subjektiv vurdering av hvem som passer inn. Samtidig er det vanskelig å se at dette er så mye mer subjektivt enn å på forhånd definere en gruppe mennesker ut i fra kjønn, alder eller interesser for så å si at en har foretatt et objektivt utvalg av disse objektive egenskapene. Utvalget av objektive egenskaper vil jo uansett være subjektivt og en ender derfor opp med det samme resultate. Siden målet med intervjuene først og fremst var å kaste lys over temaet i oppgaven sett fra noen brukeres ståsted og siden utvalget kunne gjøres ut i fra bekvemmelighet ble det viktigste kriteriet personer som kan reflektere over temaet. Dette kriteriet var mulig å sette da jeg plukket ut intervjuobjekter fra eget nettverk. Det vil si at alt fra nære til fjerne bekjente ble vurdert. Tanken bak et slikt kriterie var at det vil være mer effektivt å intervju fem personer som er flinke å reflektere over problemstillinger enn ti personer som kanskje er det.

Utover kriteriet om at de som ble plukket ut skulle være tilgjengelige og antatt flinke til å reflektere ble de også valgt ut på en slik måte at de vil ha forskjellig bakgrunn. Den norske filosofen Arne Næss skal ha sagt at «alder er den aller minst interessante opplysningen om et menneske». Alder blir ofte brukt som et av de såkalt objektive kriteriene når en skal plukke ut en gruppe mennesker fra en populasjon. Kjønn er et annet kriterie. Disse to kriteriene var nok ikke en del av det jeg vurderte. Jeg forsøke heller å finne noen egenskaper som kunne gi forskjellige syn på temaet. Det var menesketyper og personligheter jeg var på jakt etter ikke grupper av mennesker.

Derfor valgte jeg en person som sent i livet ble kjent med informasjonsteknologi, en dame som fikk sin første datamaskin i en alder av 65 år, men som nå har vært en aktiv bruker i over ti år. For det første er dette en person som kanskje ville kunne trekke linjene fra en analog til en digital verden. Se hvordan ting var før og sette temaet i det perspektivet. For det andre en person som begynner å dra på årene og som kan ha andre ønsker og behov enn unge mennesker.

Jeg valgte meg også ut personer som jeg antok ikke hadde veldig høy motivasjon for å teste ut nye ting. Rett og slett de brukerne som forholder seg til teknologi uten den store «wow» faktoren. De som ikke *må* ha de nyeste dingsene. De som liker teknologi som fungerer. Men det måtte være personer som har et aktivt liv og som oppfattes som vanlig sosiale

mennesker. For på den måten å sikre seg at de også er brukere av IKT. Ikke superbrukerne som må være tilgjengelige hele døgnet kanskje, men gjerne noen som trenger tilgang til kontoene sine også utenfor hjemmet og arbeidsplassen. Med andre ord jeg ville ha en bruker som mest av alt forholder seg til IKT som jeg (og du som leser antar jeg) forholder meg til vann i springen. Som en selvfølge. Som noe som bare er der. Og som noe som bare skal fungere.

Den siste personen jeg så etter var en med god innsikt i IKT og gjerne motivasjon over gjennomsnittet. Dette var helt nødvendig for å få testet LastPass og Yubikey over en lengre periode. Det ville være vanskelig å rekruttere personer med lav motivasjon til å prøve et system jeg antok ville by på mindre og større utfordringer og mest av alt tid. Dessuten måtte det være en person som forstod risikoen denne tok ved å teste systemet. Jeg var ikke ute etter funn på brukbarheten på selve systemet, men mer etter erfaringer i bruken av det.

3.3.2 Workshop

Målet med å arrangere en workshop var å få demonstrere et system for brukerne og deretter spinne videre med det som grunnlag. Deltakerne var altså ikke med på en brukertest men mer på en idèmyldring rundt temaet nærhetsbasert innlogging. I workshopen skulle det demonstreres et system basert på en NFC kapabel telefon, en NFC kapabel Yubikey og programmet LastPass. Sammen gjør disse tre det mulig å logge seg inn på webkontoer uten å trykke inn en kode. Man fører Yubikey NEO til telefonen og logges automatisk inn i LastPass som derfra håndterer brukernavn og passord til kontoene dine. Dette er nærmere beskrevet under kasuskapittelet.

Tanken bak det å arrangere en workshop kom fra tidligere positive erfaringer med dynamikken som oppstår i en gruppe. Det er vanlig å gjøre dette for å teste programvare, men det var som tidligere nevnt ikke formålet med hverken intervjuene eller workshopen. Målet var å få i gang en refleksjon etter at deltakerne hadde fått demonstrert og testet et eksempel på nærhetsbasert autentisering. Den dynamikken som oppstår i slike grupper illustreres godt i dette avsnittet fra Toftøy-Andersen and Wold [84]:

> «Noen grupper samarbeider bedre enn andre, men det som var interessant, var diskusjonen som oppsto mens de klikket seg rundt i løsningen. Brukerne pratet sammen om løsningen uten at vi behøvde å stille spørsmål. Vi fikk høre mye positive tilbakemeldinger, som:"Vi gleder oss til å ta det i bruk, når blir det ferdig!"Vi fikk mange gode innspill som vi tok med oss i den videre prosessen. I etterkant ser jeg at dette ble en mellomting mellom fokusgruppe og en vanlig brukertest.»[84, Side 137].

Dersom det var mulig å skape en slik stemning og en slik dynamikk ville det kunne gi gode innspill til hvilke krav som stilles til systemet og funksjonalitet.

Sharp et al. [78] skriver om «Brainstorming for Innovation». De foreslår en gruppe som er bredt sammensatt fra ulike disipliner. Jeg vil samle deltakere som er potensielle brukere uten spesiell erfaring i feltet. Men jeg har latt meg inspirere av måten de beskriver hvordan dette bør gjøres på, blant annet at alle forslag blir støttet og ikke fokus på kritikk men på å få opp mange ideer[78].Utprøvingen av telefon med LastPass og Yubikey til å logge inn ved hjelp av NFC ble brukt som en slags oppvarmingsøvelse slik Sharp et al. [78] foreslår. I tillegg til dette ønsker jeg å samle en gruppe personer som kjenner hverandre fra før og som er vant til å jobbe sammen for å øke muligheten for at ideer får blomstre og at deltakerne er sosialt trygge på situasjonen. Denne måten å gjøre det på er vel det Sharp et al. [78] beskriver som *fokusgrupper*. Men de legger et fokus på at det skal være en representativ gruppe og de sier også at denne måten å jobbe på er best egnet til å «investigating community issues rather than individual experiences».[78, Side 232]. Det er jeg uenig i for det jeg er ute etter har også Lazar et al. [58] skrevet om:

> «Participants can encourage each other to speak up, either in support of or opposition to earlier statements. This highly dynamic situation can stimulate participants to raise issues that they might not have identified in one-to-one interviews.»[58, Side 193].

I den siste setningen her ligger det jeg er på jakt etter. At deltakerne kan identifisere ting de ikke hadde gjort i et vanlig intervju.

3.4 Etiske vurderinger & mine bias

3.4.1 Etiske vurderinger

Intervjuene

Forskning rundt informasjonssikkerhet kan by på en del etiske problemstillinger. I dette studiet blir intervjuobjekter spurt ut om sine holdninger og tanker rundt dette temaet. Da er det også å forvente at det er en mulighet for at jeg vil få innsikt i hvilket system intervjuobjektene bruker for å holde kontroll på alle kontoene sine. Om de ikke deler dette bevisst vil det kunne være enkelte ting som gjør at jeg kan forstå hvor svakhetene i systemet deres ligger. Det kan til og med være at dette blir et tema de ønsker å utdype nærmere.

For å unngå dette vil det være viktig for meg å gjøre de jeg prater med klar over denne muligheten for at jeg forstår mer enn de hadde planlagt. Dessuten påpeke at jeg ikke ønsker tilgang til, eller passord til kontoene deres. Det skal være unødvendig å samle inn slik sensitiv informasjon i oppgaven og derfor vil jeg aktivt gå i mot det. Under intervjuene vil jeg være ekstra observant på disse temaene og sørge for at intervjuobjektene ikke «forsnakker seg» og sier mer enn det jeg burde høre. Dessuten åpenbart opprettholde strenge krav til datasikkerhet for den informasjonen jeg samler inn. Det er innhentet godkjenning fra

Norsk samfunnsvitenskapelig datatjeneste AS (NSD) om behandling av personopplysninger og elektronisk opptak av intervjuene for å sikre at metodene som brukes er innenfor personopplysningsloven.

Samtidig vil dette være trygge omgivelser for deltakeren å tråkke feil dersom det skulle skje. Alle jeg intervjuer skal være i stand til å håndtere slike opplysninger hver dag, derfor tror jeg også det er noe de vil være bevisst på selv.

Test & workshop

For testen av LastPass blir det noe verre. Til forskjell fra intervjuene er testen av LastPass avhengig av reelle kontoer. Det er en risiko som er vanskelig å se helheten av. Den antas å være lav, men hvem skal bestemme at den er lav nok? Det viktigste i forbindelse med denne testen er at deltakeren skal kunne vurdere dette i størst mulig grad selv. Dessuten må jeg være tydelig på at jeg ikke kan garantere noe for tjenesten utover det jeg har lest om den. I samråd med testeren bør jeg være med å foreslå at kontoer med høyere sensitivitet som bank, tjenester med kredittkortopplysninger og e-post er hvor andre kontoer kan tilbakestilles gjennom bør holdes utfor testen. Da er en stor del av risikoen minimert. Her kan det også legges til at jeg personlig bruker LastPass på det aller meste av webbaserte kontoer og det må igjen legges vekt på, overfor den personen som skal teste systemet, at det ikke nødvendigvis er et kvalitetsstempel. Om ikke annet kan det si noe om at jeg har foretatt risikovurderinger selv og funnet systemet for sikkert nok til min bruk.

I workshopen kan dette fortone seg noe annerledes siden deltakerne her er tilstede samtidig og eventuelle forsnakkelser er noe alle får del i. Igjen er nok det viktigste å styre samtalen i en slik retning at en unngår det. Dessuten stole på at deltakerne selv har et så pass bevisst forhold til informasjonssikkerhet at de ikke deler opplysninger. Dersom så skulle skje vil det være liten sannsynlighet for at de øvrige deltakerne vil utnytte det. I sær før den som har forsnakket seg har fått rettet opp og eventuelt skiftet passord der det er aktuelt.

3.4.2 Refleksjoner over mine bias

Jeg tror min desidert viktigste bias ligger mot at jeg opplever at folk er mindre interessert i i teknologi, datasikkerhet og personvern enn det de burde være. Med andre ord fra mitt ståsted som interessert i disse spørsmålene burde de være mer interessert. Fra et informasjonssikkerhetsståsted vil det ofte bli hevdet at de burde være mer opptatt av det. De er gjerne interessert i resultatene, men har ikke en inngående interesse fra dag til dag. Det handler om å få utført det en ønsker. Det er for så vidt et bias som har støtte fra forskning, men allikevel vil jeg trekke det frem. Spesielt med tanke på en leser som er uenig på dette punktet vil oppgaven virke til å ha en sterk slagside mot at folk mangler motivasjon for å utføre allminnelig vedlikehold av informasjonssikkerheten sin. For meg er det et så pass grunnleggende at det sannsynligvis filtrerer bort informasjon som

motbeviser mitt syn. Det er noe jeg forsøker å være bevisst på, spesielt under intervjuene er det viktig å prøve å se etter om det finnes tegn til det motsatte. Som beskrevet tidligere i dette kapittelet har jeg utformet studiet som et kritisk kasus for å se om de resultatene det gir kan være interessante med tanke på et fremtidig universelt utformet system for autentisering. Det kan være jeg gjennom mitt bias har lett (og funnet) argumentasjon for å sette høyere krav til systemets brukeropplevelse og enkelhet enn det som strengt tatt er nødvendig.

Nå har jeg nok utelatt en hel del biaser leseren vil oppdage selv underveis. Det er dessverre slik at de er lettere å oppdage for andre enn for seg selv. Jeg håper det ikke påvirker oppgaven negativt i for stor grad.

Kapittel 4

Kasus

Universell design er idealet.
Inkluderende design er det praktisk oppnåelige.
(Sagt i E-me møte)

4.1 E-me forskningsprosjektet

Denne oppgaven blir skrevet i tilknytning til E-me prosjektet. E-me prosjektet utforsker temaet «inkluderende identitetshåndtering». Først og fremst med tanke på at «autentiseringsløsninger ikke skal stå i veien for deltagelse i sosiale medier og det digitale samfunnet»[1]. En moderne forståelse for hva funksjonshemning er ligger til grunn for forskningen. «[En] Funksjonshemning oppstår når det foreligger et gap mellom individets forutsetninger og omgivelsenes utforming eller krav til funksjon.»[26] Funksjonshemning er med andre ord ikke en individuell egenskap, men et forhold eller en situasjon som kan oppstå i et individs møte med samfunnet. E-me prosjektets oppgave kan beskrives på følgende måte: Å lage identitetshånteringsløsninger som forhindrer at det oppstår en funksjonshemmning i utgangspunktet.

Prosjektet er finansiert gjennom VERDIKT-programmet i Norges forskningsråd. Det eies av Norsk Regnesentral (NR og Karde AS leder prosjektet. E-me prosjektet startet opp i mai 2010, og varer ut 2013.[1] Det empiriske forskningsarbeidet blir gjort ut i fra organisasjoner som gir konkrete kasuser å jobbe med. De organisasjonene som er en del av E-me forskningen er: Brønnøysundregistrene, Storebrand ASA, Encap AS, Dysleksi Norge, Norges Blindeforbund og Seniornett Norge [1].

Et økende behov for tilgjengelige og brukbare brukerautentiseringsløsninger er bakgrunnen for at prosjektet ble startet. Et forprosjekt viste også at det fantes lite forskning som gikk direkte på inkluderende identitetshåndtering [46]. Det samme viste en senere rapport[50]. Disse rapportene sammen med annen forskninge som er gjort innenfor området inkluderende identitetshåndtering blir behandlet i litteraturgjennomgangen i Teori kapittelet. Forskningen som er gjort i E-me prosjektet er vanskelig å oppsummere før prosjektet er avsluttet. De foreløpige resultatene som presenteres her yter ikke rettferdighet til den forskningsinnsatsen som er gjort og

det anbefales å se selv hvilke resultater E-me prosjektet har publisert etter denne oppgaven ble skrevet De foreløpige resultatene er som følger:

Det er så langt utviklet 3 ulike prototyper i prosjektet[49]:

- Alternative innloggingsmekanismer (lyd, mønster, spørsmål og bilder)
- OpenID: Pålogging ved hjelp av disse mekanismene via OpenID
- Spleiselag: Pålogging vha av OpenID til sosialt nettverk med betalingstjenesten Spleiselag.

Det er også foretatt brukertester av innloggingsmekanismene. Resultatet av disse er ikke publisert enda hverken internt eller eksternt. Foruten flere rapporter som er nevnt tidligere [45, 50] og noen vitenskapelige artikler[47, 69] er det også skrevet tre masteroppgaver i tilknytning til prosjektet [73, 81, 40]. Disse rapportene, artiklene og masteroppgavene og resultatene fra prosjektet så langt behandles andre steder i denne oppgaven.

4.2 Om fokusområdet til dette kasuset

Denne oppgaven fokuserer på universell utforming av brukerautentisering. Kasuset tar utgangspunkt i en bruker uten spesielle behov. Dette valget ble tatt da det antas at en slik bruker vil ha den laveste terskel for hvilke hindringer som er psykologisk akseptable. Siden en universelt utformet løsning skal være en løsning som kan brukes av flest mulig uten spesielle tilpasninger krever det også at brukere uten spesielle behov ønsker å ta i bruk løsningen. Som et anekdotisk «bevis» på at det kan arte seg slik kan vi se tenke oss en situasjon som setter uakseptable krav for en bruker med normalt godt syn: Personer som er avhengige av briller for å kunne lese aksepterer å ta med seg brillene (eller linsene) i nær sagt alle situasjoner hvor det kan være de må lese noe. En person med vanlig syn vil på den andre siden ikke ta med seg egne hjelpemidler for å kunne lese det som står på et skilt, eller i en restaurantmeny. Det vil være vanskelig å se for seg en restaurant som gjør skriften så liten at selv personer med godt syn trenger hjelpemidler for å lese. Sannsynligvis vil ikke kundene akseptere dette og som en ytterste konsekvens gå til andre restauranter. Dersom du er enig i dette, kan en tenke seg at en slik bruker vil ha vanskeligere for å akseptere ekstra hjelpemidler som står i veien for en oppgave personen allerede håndterer uten hjelpemidler. Denne forutsetningen er gjort først og fremst for å skape dette kasuset og gjøre det til et ekstremtilfelle slik det er beskrevet av Flyvbjerg [43]. Kasuset prøver å finne den brukeren som har høyest krav til at brukerautentisering skal gi en god brukeropplevelse. Mer om hvorfor valget er lagt på et ekstremtilfelle finner du i metodekapittelet på side61.

Dette har ført til at intervjuobjektene er plukket ut i fra en tanke om at de skal representere en gjennomsnittsbruker. Jeg har ikke fulgt en spesiell bruker men valgt ut noen få brukere som kan være representanter for

forskjellige behov og krav. Brukeren det blir sett på har heller lave enn høye kunnskaper om sikkerhet og IKT. Ut i fra de beskrivelsene som finnes av brukerens motivasjon som et viktig element i hvordan denne forholder seg til informasjonssikkerhet, har jeg også valgt å se på brukere som oppleves å ikke ha særlig høy, men heller lav motivasjon for å oppfylle sikkerhetskrav. Disse egenskapene har jeg forutsatt at en finner i alle aldersgrupper, derfor er ikke alder en begrensende faktor hverken den ene eller andre veien for kasusets del. Formålet med kasuset er ikke å fremskaffe generelle retningslinjer som kan passe alle, dette er viktig å understreke selv om en har vært på jakt etter en gjennomsnittsbruker. Det er mange faktorer som kan påvirke behovet en bruker har med tanke på tilgang til kontoer, for eksempel ser vi i programvare og løsninger en økende grad av «foreldrekontroller». Altså begrensninger som gjør det tryggere for barn å bruke både internett og spill. Det er bare et eksempel. Noen personer har knapt behov for tilgang til kontoer utenfor sitt eget hjem, atter andre kunne ikke levd uten denne tilgangen. Intervjuobjektene i denne oppgaven bør reflektere noen av disse sidene, men kan umulig reflektere alle. I så måte er kasuset begrenset dithen at det ikke kan testes eller undersøkes for alle mulige situasjoner. Kanskje kan noen få viktige elementer som går igjen hos mange brukere identifiseres og legge grunnlag for videre utvikling og testing av systemer.

Det er autentisering i den private sfæren som undersøkes, dette er i tråd med E-me prosjektets mål om å undersøke temaet nærmere med tanke på nye sosiale medier. Dessuten en praktisk begrensning av omfanget av undersøkelsene. Rent praktisk slipper en da å få tilgang til bedrifter og innsyn i deres systemer, dette er både en stor og krevende oppgave. Rent faktisk er det også to forskjellige domener for brukeren og tjenestetilbyderen. Og i så måte to relaterte men forskjellige felt å undersøke. I et privat perspektiv er det brukeren selv som, så langt det er mulig, tar valgene selv av hvilke tjenester hun tar i bruk og hvilke autentiseringsmekanismer hun aksepterer. I en bedrift kan den ansatte i større grad pålegges sikkerhetsregimer som en del av arbeidet. For tilbyderen betyr det at brukeropplevelsen må være god og at enhver tjeneste som ikke har et de facto monopol også har autentiseringsløsningen som et konkurranseelement. Dessuten vil brukeren i et privat perspektiv ha større kontroll på hvilke sikkerhetsnivåer denne forholder seg til i den praktiske tilnærmingen til sin egen informasjonssikkerhet.

Det som skiller dette kasuset fra mange andre undersøkelser rundt temaet brukeropplevelse og sikkerhet, spesielt de undersøkelsene som fokuserer på tilgjengelighet gjennom universell utforming, er at en ser på hele bredden av brukerens ulike kontoer og passord. Dette skiller også oppgaven fra mye av forskningen som blir gjort i E-me prosjektet. Så lenge funn fra intervjuer og observasjoner kan sies å være en del av den private sfæren vil det være interessant å undersøke i denne oppgaven. Undersøkelsen er derfor åpen og bred i den retning. Dette innebærer å ta høyde for at brukeren opplever begrensninger i hvor mange forskjellige identiteter, kontoer og passord denne kan holde orden på uten hjelpemidler.

Da kasuset ikke har som mål å erstatte brukernavn/passord metaforen men undersøke hvordan en kan lage en universelt utformet autentiseringsløsning vil løsningen som foreslås antagligvis måtte være kompatibel med dagens systemer. Det er viktig å understreke at utforskningen av temaet ikke har en agenda mot brukernavn/passord metaforen som har en så vid utbredelse i dag. Et viktig delmål er å forstå hva bakgrunnen for denne utbredelsen skyldes. Hvilke styrker har B/P metaforen som gjør den så utbredt? I dette ligger også å utforske hvilke rammevilkår en må forholde seg til dersom en skal foreslå nye løsninger. Enkelt sagt, undersøkelsen må finne ut hva spillereglene for autentisering er.

Selv om oppgaven ikke har en agenda mot B/P metaforen har den en annen agenda. Det er å undersøke spesielt hvordan en kan benytte nærhetsbasert autentisering for å få til en universelt utformet løsning. Prototyping og testing av systemer er derfor naturlig å gjøre i en retning som kan gi mer kunnskap på dette området. Bakgrunnen for å teste ut nærhetsbasert autentisering er den økende graden av brukerautentisering mot ulike terminaler som viker fra den tradisjonelle skrivebordsbaserte skjerm/tastatur dialogen. Enheter uten skjerm og uten tastatur, eller med bare nummeriske taster setter nye krav til brukeren og autentiseringen mellom bruker og maskin. Termen *en maskinlesbar hverdag* er brukt om for eksempel utbredelsen av QR-koder. Vi bruker visakort til å betale med, vi får adgang gjennom smartkort og PIN-koder, ikke tradisjonelle nøkler. Månedskortet for kollektivtrafikk, for eksempel i Oslo, kan ikke lenger leses direkte av kontrollørene men må sjekkes ved hjelp av et apparat. Dette er bare noen få eksempler på hvordan hverdagen vår i større og større grad dreier seg om å identifisere og autentisere seg overfor «noe» som ikke er et menneske.

Hvilken enhet som brukes for å få tilgang til en konto er interessant men ikke avgjørende. Et tidlig utgangspunkt for denne oppgaven var å undersøke mobile enheter. Men mobile enheter innebærer også laptoper, tablets og andre enheter som inneholder og gir tilgang til et bredt spekter av kontoer. Siden oppgaven ser bredt på problemstillingen rundt brukerautentisering blir hvilken type enhet brukeren benytter underordnet. I det perspektivet som er lagt opp i dette kasuset skal en se på det totale bildet for en brukers behov for autentisering. Da kan en ikke begrense seg til enkeltenheter før det er gjort intervjuer og foretatt observasjoner og brukertester.

Enheter uten tastatur og gjerne uten en tradisjonell skjerm gir nye utfordringer med tanke på B/P metaforen, hvor det kreves input i form av tegn. Derfor *er* typen av enhet interessant i oppgaven, men ikke først og fremst om den er mobil eller stasjonær, heller om den har en mulighet for å taste inn B/P for å kunne identifiseres og autentiseres. I en slik hverdag med flere enheter som kanskje bør autentiseres men vanskelig kan gjøre det ved hjelp av B/P og hvor enheten i seg selv er så liten og fysisk utilgjengelig at det i det hele tatt vil være upraktisk, er tanken at den kan kommunisere trådløst med en annen enhet hvor brukerautentiseringen er praktisk mulig. Med dette som bakgrunn vil kasuset utforske nærhetsbasert autentisering som en del av en universelt utformet autentiseringsløsning

4.2.1 Avgrensning

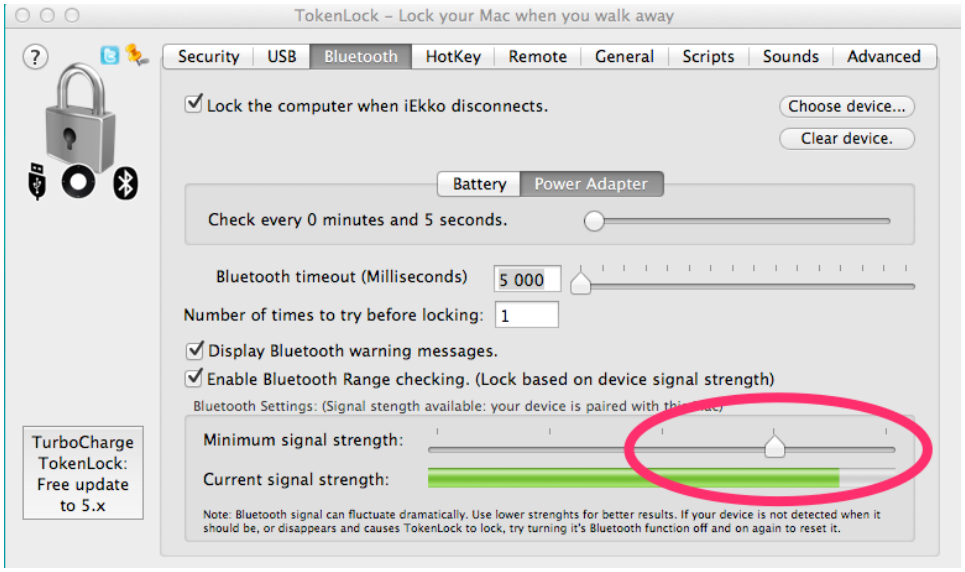
Når kasuset nå er beskrevet i bredde, dybde og omfang kan det være en fordel å se på hvor grensene trekkes. En viktig begrensning som er gjort er å utelukke den tekniske siden. Den tekniske sikkerheten er interessant, men det ligger utenfor denne oppgaven å vurdere denne. Dette innebærer også at drøftinger rundt kryptering og ulike krypteringsalgoritmer ikke er en del av denne oppgaven. For en leser som først og fremst er interessert i disse spørsmålene vil dette kanskje virke som en stor svakhet. Det får så være. Enkelte tekniske sider kan bli drøftet i oppgaven, men det er ikke noe mål at også denne siden av et sikkerhetssystem skal være besvart gjennom denne oppgaven.

Teknologien som brukes i oppgaven er først og fremst et verktøy for å teste konsepter. I det oppgaven skrives er nærfelts-kommunikasjon gjennom NFC standarden mye omtalt i media og på vei inn i mange mobile apparater. I brukerdemonstrasjonen og testene er det brukt NFC og blåtann for å illustrere nærhetsbasert autentisering. Det betyr ikke at det er tatt stilling til *om* det er akkurat disse to teknologiene som egner seg best i en slik løsning.

Oppgaven har heller ikke som mål å komme med et forslag til en ferdig løsning. Det gjenstår mange spørsmål før en er kommet så langt at prototyper av en universelt utformet løsning kan testes på brukere. Målet er å øke kunnskapen rundt dette temaet og forhåpentligvis komme et lite skritt videre i utforskningen av dette problemområdet.

4.3 Prototyping og testing

Det har vært et eksplisitt mål å ikke bruke tid på egenutvikling av systemer. Oppgaven har handlet mer om å demonstrere for brukeren hvordan system basert på nærhet mellom to enheter kan fungere enn en testing av løsningene. Siden den antatt viktigste kunnskapen som kan komme fra dette kasuset er å utforske hvilke innspill brukeren har til et konsept som baserer seg på nærhet mellom to apparater som en form for autentisering. Det er ikke en ferdig løsning som presenteres for brukeren, men de aller tidligste demonstrasjoner av hvordan noe kan bli. Disse demonstrasjonene vil være begrenset i omfang og ikke håndtere alle aspekter et ferdig system må kunne håndtere. I så måte vil brukeren kunne sies å bli skjermet for en del konfigurering og tilpasninger som hun i et ferdig system nødvendigvis må kunne håndtere selv. Slik testing blir gjerne gjort med såkalte «low fidelity prototypes» for eksempel gjennom papirskisser. Dette var et reelt alternativ også i denne oppgavens tilfelle. Samtidig ville det være spennende å se om eksisterende teknologi kunne brukes i demonstrasjon for brukeren og på den måten være nærmere en reell situasjon. Når det viste seg at noen slike programmer fantes ble disse tatt i bruk, fremfor papirprototyper, for å demonstrere konseptet. En viktig grunn for å demonstrere systemene for brukeren var å hjelpe brukeren i gang med å forestille seg hvordan dette kunne brukes andre steder og



Figur 4.1: Skjermskudd fra TokenLock konfigureringsskjerm. Sirkelen i rødt viser hvor en stiller terskelen for styrken på blåtannsignalet. Styrken på signalet indikeres her i grønt og det er en laptop med mobiltelefon tilkoblet og enhetene har en avstand på ca 30cm.

hvilke resonnnementer denne ville ha rundt det.

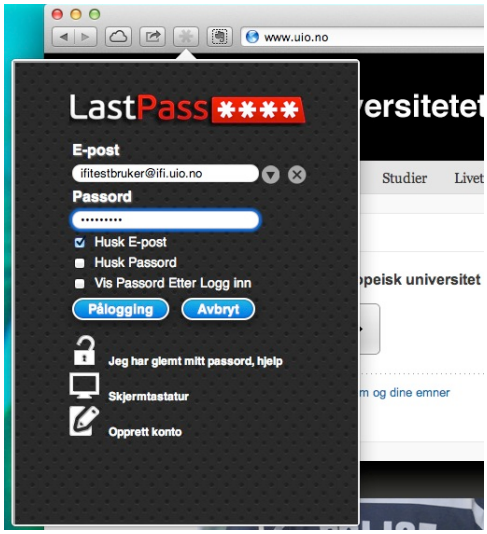
De systemene som er blitt brukt i brukertester er: *LastPass, Yubikey* og *Token Lock*. Testingen eller demonstrasjonen ble gjennomført en til en i forbindelse med intervju. Det ble også arrangert en workshop med flere deltakere på én gang. I intervjuene lå fokuset på å forstå brukerens situasjon og behov. Det ble brukt en del tid på å oppklare brukerens tanker om sikkerhetsnivåer for de ulike kontoene og tingene sine. Deretter ble TokenLock demonstrert og deretter testet av intervjuobjektet. Også fortsatte en en liten drøfting rundt hvordan og til hva dette kunne brukes og hva en da måtte ta hensyn til. I workshopen var fokuset hovedsaklig på hva deltakerne kunne se for seg denne type teknologi kan brukes til og hvordan det måtte fungere for at de selv skulle ønske å ta det i bruk.

Nå følger en nærmere beskrivelse av de tre systemene som er brukt.

4.3.1 TokenLock

TokenLock er et program til Mac OSX som blant annet kan brukes til å låse ned og -opp datamaskinen ved hjelp av den innebygde sikkerhetsmekanismen. Opp/nedlåsingen kan som navnet tilsier gjøres ved hjelp av en gjenstand (token) i stedet for et passord. Dette tokenet kan være en USB-brikke, eller en enhet tilknyttet via blåtann [14]. I testene ble dette programmet brukt sammen med en blåtantilknyttet enhet. Når en benytter blåtann i TokenLock kan en også justere følsomheten eller hvor sterkt signalet mellom enhetene skal være. Denne ble finjustert slik at mobiltelefonen måtte være innenfor en rekkevidde på noen få meter.

Som en forberedelse til intervjuene ble et annet program kalt Proximity



Figur 4.2: Skjermskudd fra LastPass innlogging gjennom en plugin i Safari.

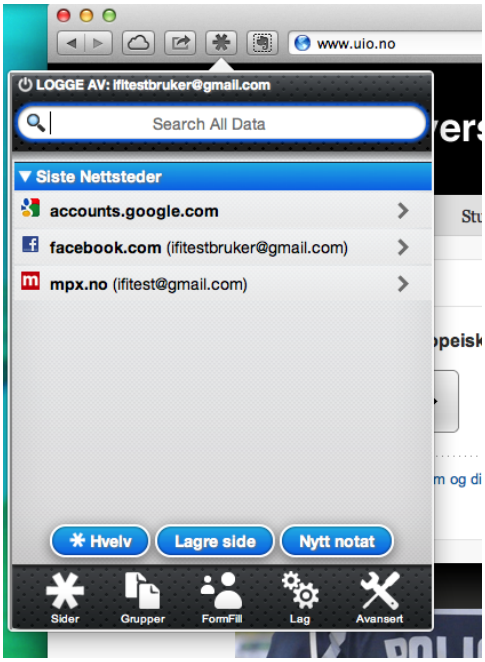
[11] vurdert. Dette programmet tillater brukeren å kjøre egne applescript ved til- eller frakobling av en blåtannhenhet. Men det fantes ingen enkel måte å kontrollere terskelen for signalstyrke på apparatet og allerede i initielle forsøk for å se om programmet kunne egne seg til brukerdemonstrasjon viste det seg at blåtannrekkevidden var for stor til å kunne vises i et rom eller hus med normal størrelse. Den totale rekkevidden på blåtanntilknytningen kan i gitte tilfeller være over 15 meter.

Token lock ble brukt for å illustrere hvordan nærhet mellom to apparater kan fungere. Programmet ble ikke testet med tanke på hvilken sikkerhet det tilbyr i dag. Heller ikke brukeropplevelsen av selve programmet ble testet.

4.3.2 LastPass

LastPass fungerer som en nøkkelring for de digitale, web-baserte kontoene dine. En passordhåndterer som vil gjøre det lettere for brukeren å manøvrere seg gjennom utallige kontoer på nett [8]. Det finnes flere forskjellige typer slike passordhåndterere. Noen er integrert i operativsystemet mens andre installeres på maskinen. LastPass lagrer en kryptert kopi av alle passordene dine på web og brukeren har mulighet for å logge inn gjennom et webbasert grensesnitt, plugin i nettleseren og gjennom en mobilapplikasjon. Passordene blir synkronisert sømløst mellom disse. Den viktigste grunnen til å velge LastPass var at det støtter nærhetsautentisering gjennom NFC. For workshopens del var det et viktig poeng å demonstrere to ting: Hvordan nærhetsautentisering kan fungere og hvordan passordhåntering kan fungere.

I to typer tester ble programmet brukt. Den ene testen ble gjort på én bruker over en periode på 20 dager. Denne brukeren sa seg villig til å bruke systemet «på seg selv». Det innebar å legge inn sine egne kontoer på tjenesten. Denne testen ble gjort for å prøve å forstå hva et system som



Figur 4.3: Skjermskudd fra LastPass «hvelv» med en oversikt over de registrerte kontoer.

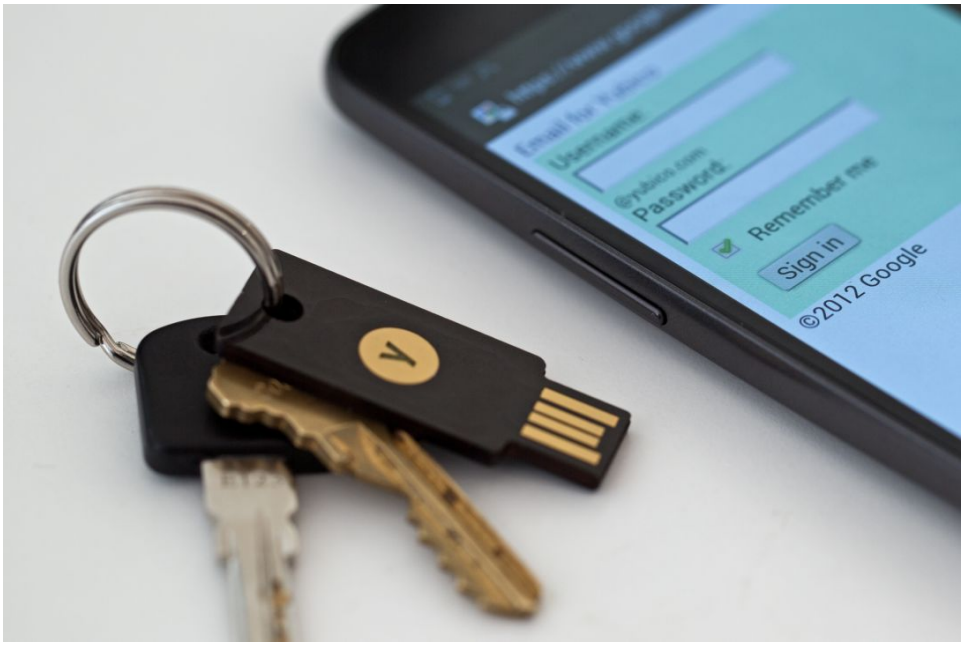
håndterer passordene til brukeren må levere av funksjonalitet. På grunn av den betydelige innsatsen som må til fra brukeren for å teste dette ble det valgt å teste på kun én bruker.

I den andre testen hvor LastPass ble brukt, ble det satt opp egne testkontoer på LastPass.com, Gmail.com, Facebook.com og nettbutikken MPX.no. Passordene til disse tjenestene var noe forskjellige, et kort passord med tilfeldige tegn, et langt passord med tilfeldige tegn og en passfrase. Det ble gjort slik for å illustrere for brukeren hvordan typisk «sikre» passord kan være dersom en følger de strengeste passordkravene. LastPass applikasjonen for Android ble lastet ned til en Samsung S3 telefon for å teste LastPass sammen med nærfelts kommunikasjon gjennom en Yubikey NFC kapabel nøkkel.

4.3.3 Yubikey

Yubikey fra selskapet Yubico var i utgangspunktet en USB nøkkel som kan generere OTP koder eller statiske passord. Selve USB nøkkelen registreres som et standard tastatur og er kompatibelt på tveers av plattformer [18]. Yubikey er ment å brukes i en to-faktor løsning hvor OTP koden som genereres skal sikre høyere sikkerhet. Heller ikke her var det et mål å teste sikkerheten i selve løsningen med Yubikey, men å bruke den sammen med LastPass for å demonstrere for brukeren og la brukeren teste nærhetsbasert autentisering.

Brukeren som testet LastPass i 20 dager fikk benytte en original utgave av Yubikey som plugges inn i USB-porten og sørger for to-faktor



Figur 4.4: Et pressebilde fra Yubico som viser Yubikey NEO som har NFC kapabilitet og ble brukt i testing sammen med en Samsung S3 og LastPass

autentisering i LastPass.

I workshopen ble det benyttet en Yubikey NEO som er i «pre-production» når denne oppgaven blir skrevet. Det betyr at det var en tidlig NFC kapabel utgave som ble brukt. Denne er kompatibel med LastPass på Android telefoner med NFC kapabilitet. Måten det fungerer på er at OTP koden blir generert og sendt gjennom NFC fremfor en fysisk tilkobling. Brukt på denne måten blir LastPass appen automatisk startet når en fører Yubikey NEO i nærheten av NFC brikken på telefonen. Deretter kan en logge inn med eller uten passord. Det er mulig å be LastPass huske passordet, dermed vil det være nok å presentere Yubikey NEO for telefonen. I brukerdemonstrasjonen ble denne innstillingen brukt.

Kapittel 5

Funn

Jeg skal nå redegjøre for de funnene som er kommet frem i gjennom intervjuer, demonstrasjoner, tester og observasjon. Vi begynner med de funnene som er gjort i forbindelse med Diskriminerings- og tilgjengelighetsloven.

5.1 Funn i forbindelse med Diskriminering- og tilgjengelighetsloven

Det var en erkjennelse av at forskningsprosjekter gjerne glemmer «verden utenfor» som fikk meg til å ta kontakt med de berørte etater og organisasjoner for å finne ut hva deres tanker rundt universell utforming og autentisering er. Det startet som en planløs jakt etter noen som visste noe om eksisterende praksiser, erfaringer, ideer og diskusjoner. Håpet var å finne kunnskap som kunne komme til nytte i denne oppgaven. Enten for å sammenligne med innspill fra forsøkene eller justere tanker og ideer til det arbeidet som blir gjort utenfor akademia. Jeg begynte med det som føltes mest naturlig og med den etaten som jeg trodde ville stå nærmest kunnskapen nemlig Deltasenteret som tidligere nevnt er statens kompetansesenter for universell utforming og tilgjengelighet. De anbefalte meg å ta kontakt med DIFI som har tilsynsmyndighet. Dessuten FAD, selskapet MediaLT, teknologirådet og Standardisering Norge. Jeg fikk et innskudd til å ta kontakt med LDO etter jeg så at de engasjerte seg for å få norske apoteker og Posten Norge til å akseptere signaturstempel under overskriften «Frå enkeltsak til strukturendring» legges det vekt på at IKT tjenester må være tilgjengelige for alle og at LDO ønsker å ta tak i problemstillingen rundt autentisering gjennom underskrift på digitale enheter for alle apotekene i Norge [12]. Jeg forsøkte også i samme runde å ta kontakt med noen banker for å høre hvordan de jobbet med dette. Og når jeg først hadde ringerunder var det naturlig å ta en prat direkte med noen få interesseorganisasjoner. Dette var blindeforbundet, Dysleksi Norge, unge funksjonshemmede og Funksjonshemmedes fellesorganisasjon.

Det viktigste funnet fra alle disse telefonene var at ingen egentlig jobbet med denne problemstillingen. Igjen ønsker jeg å legge vekt på at dette må leses med de forebeholdene som hører til denne formen for informasjonshenting. Hvem du får kontakt med på telefon kan være

tilfeldig og det kan være jeg har pratet med feil person.

Videre er det helt klart at samtlige av de statlige organisasjonene venter på at forskriften skal komme på høring. I kontakten med LDO var det et håp at de hadde noen interne retningslinjer for dette. Men så var ikke tilfellet. Nå i ettertid har Likestillings- og diskrimineringsombudet Sunniva Ørstavik selv etterspurt forskriften slik at LDO kan gjøre jobben sin[7].

Heller ikke interesseorganisasjonene har jobbet med akkurat denne problemstillingen rundt autentisering. Selv om blindeforbundet spesielt har jobbet mye med universell utforming var tilbakemeldingen at problemstillingen var interessant, men de hadde ikke noen konkrete innspill eller erfaringer på området. Ingen av interesseorganisasjonene jeg var i kontakt med hadde egne retningslinjer eller vedtatt politikk som gikk på IKT og autentisering spesielt. På generell basis ble det vist til WAIs retningslinjer[16]. Blindeforbundet har utarbeidet informasjon om tilgjengelighet som er tilgjengelig på nettsiden deres [2]. Men disse retningslinjene sier ikke noe spesifikt om autentisering.

5.2 Funn fra intervjuene

Intervjuene varierte både i innhold og lengde. Felles for alle intervjuobjektene var at temaet vekket oppmerksomhet. Selv om den umiddelbare tilbakemeldingen jeg fikk fra Gustav var helt typisk å få når jeg spurte om de kunne stille som intervjuobjekt. Han sa at han nok ikke hadde så mye å si om «passord og sånn». I intervjuet viste det seg imidlertid at samtlige hadde mye å si om dette temaet. Lengden på intervjuene var fra en time til to og en halv time. Under presenterer jeg funnene fra de fire første intervjuene. Intervjuet etter testingen av LastPass i 20 dager kommer under egen overskrift. Intervjuene startet med en runde med enkle spørsmål for å sette i gang intervjuobjektet og gjøre denne trygg på situasjonen. Et av spørsmålene var hvilke elektroniske enheter du har og bruker. Og hvilke tjenester du bruker på nett som krever en eller annen form for innlogging. Formålet her var ikke å grave så lenge at en får fullstendige lister. Heller å få et overblikk og ha noen konkrete enheter eller tjenester å ta utgangspunkt i under resten av intervjuet. Resultatet er samlet i tabell 5.1 på side 81. Noen av tjenestene er samlet i én kategori, for eksempel nettbanker og nettbutikker. Tabellen gir først og fremst en enkel oversikt over ting som kan kreve innlogging.

5.2.1 Om «passord og sånn»

På spørsmål rundt hva de tenkte om brukernavn og passord var svarene forholdsvis samstemte men enkelte var mer tydelige enn andre. Jane sa for eksempel:

> «[Passord er] kødd, som du må ha for å komme inn over alt på pc'en. Det beste er Google Chrome som har sånn at du kan lagre automatisk. Det liker jeg.»

Fysiske enheter	**Tjenester og enheter som krever innlogging**
DVD spiller	Altinn
iPad	Amazon
Ipod	Aviser
Kamera	Bankkort
Kodelås koffert	Bilioteket (PIN+bib.kort)
Kodelås sykkel	eBay
Mobil	Facebook
Pc	Mail
Playstation	Mobil
Printer	Nettbank
Pulsklokke	Nettbutikker
TV	Nettpanel (TNS)
Visakort	NRK
	PayPal
	Reise (flyselskap, tog, buss)
	Skolemail
	Strømleverandør
	Studentweb
	TV2

Tabell 5.1: Oversikt over personlige enheter og tjenester som kom frem under intervjuene

Margrethe mente hun opprettet en ny konto minst en gang i måneden. Hun har tre-fire forskjellige passord som gjenbrukes på alle kontoer. Det er ikke passordet som er vanskelig å huske, men hvilket brukernavn som hører til hvilken konto.

> «Noen ganger er det mail andre ganger noe jeg bare har laget. Jeg husker jo mailen min.»

(Margrethe)

Karl Gustav utvidet problemstillingen ytterligere. Han har opplevd flere ganger å forsøke å opprette nye kontoer for å oppdage at han allerede har en konto på det aktuelle nettstedet. På spørsmål om han har kontroll på brukernavn og passord sier han:

> «Nei, finnes ikke. Det er noen jeg bruker ofte som jeg klarer å huske.»

Guri tenker først og fremst på nettjenester når hun tenker på brukernavn og passord. Men så kommer hun på at både husnøkkelen og alarmen nå bruker PIN-kode. De benytter seg av en nøkkelboks med kode på som henger utenfor husdøren.

I alle intervjuene er det tydelig at kontrollen på de mest brukte kontoene er god for alle. Det er kontoer som er brukt sjeldnere som er det store problemet. Dessuten bruker samtlige den samme strategien for passord, de rullerer på noen få passord til alle tjenestene. Ikke alle har en bevisst holdning til hvilke passord de bruker til hvilke typer tjenester. Dette er noe vi prater om i sammenheng med sikkerhetsnivåer.

Noen av intervjuobjektene er inne på dette med deling av passord.

> «Tenker at det er litt stress [med passord.]. Men skjønner at det må til. (...) Men om typen har passordet til min facebook eller til min mail, så gjør ikke det meg noe. Og jeg har passordet til hans mail. For av og til er jeg kanskje utenfor dekningsområde, da kan jeg ringe han og be han sjekke det og det.» (Margrethe)

Margrethe mener altså at fordelen med at typen kan sjekke e-posten hennes dersom hun ikke har tilgang til internet langt overgår ulempen med at han har tilgang. Hun legger vekt på at det kun er privat e-post og at dette kanskje ville endret seg dersom det var en jobb-konto.

> «Veldig mye kjedelig mail. Tror den er fra 2000 eller noe, og det er veldig mye mail. Og viss han da skal lete etter en spennende mail tror jeg han må lete et år etter det.»

Dette med at innholdet er kjedelig eller relativt betydningsløst er noe flere nevner og dette påvirker definitivt hvordan risikoen og sikkerhetsnivåene vurderes.

5.2.2 Risiko & sikkerhet

Dette lille utdraget fra intervjuet med Karl Gustav illustrerer godt hvordan intervjuobjektene vurderer risiko:

> «Jeg føler meg trygg på at det er mitt, og at det kommer til å være mitt. Det som er på mailen er på en måte ingen andre som får tilgang til når jeg har brukernavn og passord. Også er det vel litt sånn, sånn som på Norwegian for eksempel, jeg har ikke noe å skjule der. Selv om jeg sikkert har noe kredittkortinformasjon. Men jeg tenker liksom at Norwegian ikke er noe farlig. I forhold til mailen min for eksempel der jeg har en del forskjellig eller facebook med private bilder og den slags. Så på mange av de andre nettbutikkene så tenker jeg liksom at jeg har ingenting å skjule. Men har vel noe kredittkortopplysninger og sånne ting som ikke alle trenger å få tak i muligens. Men du vet nå ingenting om det på en måte. Hvor lett det er å få tak i. Om folk kan få tak i det. Så, mest sannsynlig kan de få tak i alt.
>
> [Også om ID tyveri]Jeg føler at den kjangsen er så minimal at det skjer ikke. Jeg kjenner ingen andre som har opplevd ID tyveri, som jeg vet om i hvert fall. Hadde jeg hatt en venn eller veninne som hadde blitt frastjålet dette hadde det kanskje vært noe annet.
>
> Føler det er MPX.no sin skyld om kredittkortopplysnigner kommer på avveie. Om jeg hadde hatt passord 12345 så hadde det vært min skyld, men om jeg har det passordet jeg har nå er det deres skyld. Da må det være et eller annet dårlig system inni der.» (Karl Gustav)

Generelt føler intervjuobjektene at banken er sikker og de stoler på banken og løsningene den har. Noen av intervjuobjektene er klar over at banken vil dekke eventuelle tap som følge av innbrudd i systemet.

I mange tilfeller viser det seg at fysisk tilgjengelighet i manges øyne er nok når det gjelder enheter. Dessuten at de aller fleste kontoer på webbaserte tjenester egentlig ikke inneholder kritisk informasjon og dermed får et lavt behov for sikkerhet. Brukeren opplever risikoen for misbruk av deres konti som særdeles lavt «det er jo bare lille meg, uten noen store verdier». I ytterste konsekvens mener Karl Gustav at han kan miste alt, det er kanskje først og fremst bilder gjennom bildearkivet som er det som er surest å miste «alt annet kan erstattes». Men det vil være «kjipt» og «kjedelig» ikke katastrofalt om informasjon ble spredt eller mistet.

«Jeg stoler like mye på banken som jeg gjør på et legekontor for eksempel. Veldig lite redde for at, og kanskje litt farlig lite redde, at noen skal gå inn og gjøre noe. Og en annen ting er at vi har ikke de store verdiene, vi har ikke den redselen for [at noe skal skje]. Mye reddere for brann. Da er vi hjelpeløse.» (Guri)

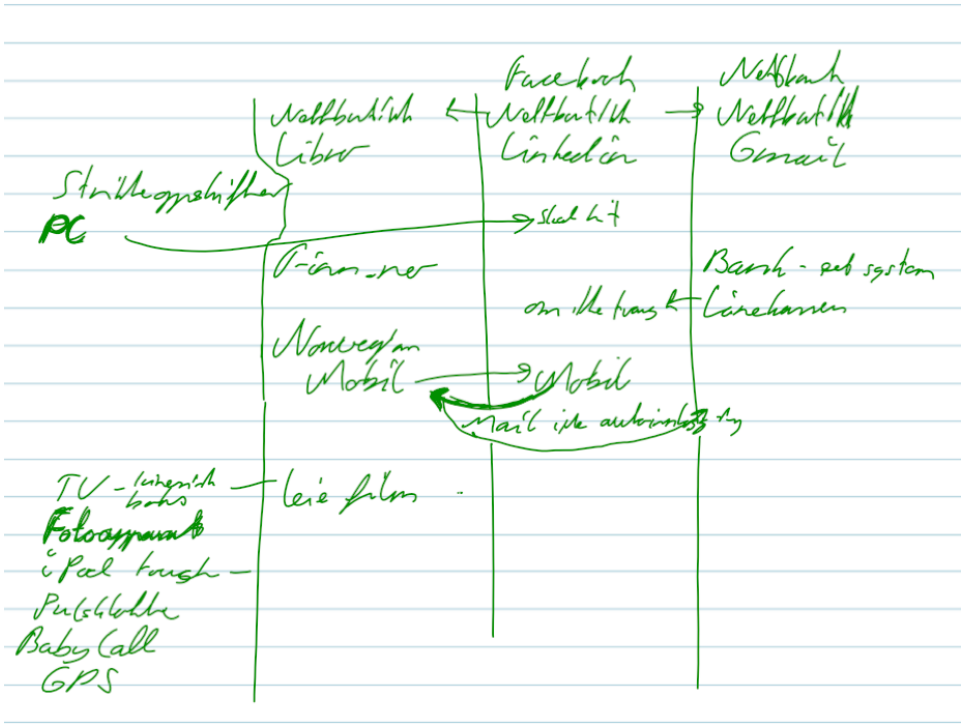
Når det gjelder helseopplysninger er det noe annet. Thea påpeker at opplysninger som er flaue eller negative eller som kan ha en økonomisk

konsekvens for eksempel gjennom dyrere helseforsikring ikke må slippe ut.

5.2.3 Sikkerhetsnivå

I intervjuene ble risikonivåer fra 1-4 brukt for å ha noe å diskutere ut i fra. Det ble tatt utgangspunkt i statens *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor* [41]. Det kom imidleritid frem i intervjuene at denne kanskje ikke er så godt egnet for å bestemmme risikonivåene. Noen av uttrykkene virker litt voldsomme i privat sammenheng for eksempel nivåene for liv og helse hvor det på øverste nivå står: «Det kan forekomme tap av liv og/eller store helseskader» [41]. Men i manglene av bedre utgangspunkt gir rammeverket et brukbart bilde for intervjuobjektet å diskutere ut i fra. Funnene rundt sikkerhetsnivå gjengis derfor med vekt på hvordan brukeren resonnerte, ikke hvilket nivå de forskjellige tjenestene ble satt på. Det er mange forskjellige perspektiver intervjuobjektene trekker frem når de skal vurdere sikkerheten. Avsnittet under demonstrerer hvordan Thea vurderer nivået laptopen bør ligge på:

> «Har ikke behov for at absolutt alle kommer inn og ser alt på pc. Har jo veldig mye forskjellig der. Men det verste hadde vært om alt ble slettet. Vet ikke om jeg har backup av alt. Så da vet jeg at ting blir mistet, men kanskje ikke akkurat hva. Men det ville blitt en del bryderi. Men ser ikke for meg noen økonomiske tap. Men personlige tap.. Ville kanskje hatt pc'en på nivå tre, men tenker at de som er proffe vet en måte å bryte seg inn på uansett. Så er først og fremst ute etter å beskytte meg mot uproffe folk. Passordmessig slik jeg har nå, har et passord, vurderer å ta ned passordet til bare en bokstav. For det er en del som, jeg vil heller at folk skal ha, et passord jeg ikke har andre plasser, som jeg kan rope ut [når maskinen blir lånt ut]. Og de, jeg stoler jo på hele klassen at de ikke vil rassere den. Så den personen som vil rassere den tror jeg ikke jeg ville kjent [visst hvem var fra før], så da betyr det ikke så mye om passordet er 'm' eller lengre. Og de som kan det får sikkert tilgang uansett. Viss alt ble slettet ville det vært veldig dumt.
>
> (...)En pc er en personlig ting, men det er gjerne en ting mange andre er inne på også. Sånn som de nærmeste vennene dine. De gir du jo passordet til, ellers er du helt snål, viss du hele tiden må bort og skrive passordet hver gang de skal skrive passordet. Du har jo venner hjemme[på besøk] som skal sjekke når bussen går eller andre ting. Men de er jeg ikke redd for skal gå og herje på pc'en min. Men jeg har jo bare et visst antall passord og gir jeg dem et av de så har de tilgang til mange andre tjenester også. Så da er det bedre å bare ha en bokstav. Det gjør pc'en mindre sikker, men det svekker ikke de andre tjenestene som bruker det samme passordet.»



Figur 5.1: Fra notatet som ble gjort under intervjuet om risikonivå på ulike tjenester og enheter. Notatet ble aldri fullført, men figuren illustrerer hvordan intervjuobjektene endret mening underveis etterhvert som de kom på flere brukscenarier.

Denne måten å tenke på går igjen også hos de andre. De veier sikkerhet mot nytte og bekvemmelighet. Figur 5.1 på side 85 er hentet fra intervjuet med Jane og er en skisse som ble gjort under intervjuet. Den ble aldri ferdig, men pilene illustrerer godt hvordan ting ble flyttet på etterhvert som intervjuobjektet fikk reflektert og pratet seg igjennom ulike scenarier.

Nivået intervjuobjektene plasserte de ulike tjenestene på varierte en del. For noen var nesten alle enheter og tjenester på nivå 1, for andre var for eksempel banktjenester oppe i nivå 4, mens dette var et nivå noen ikke engang benyttet. På bakgrunn av intervjuene er det laget en tabell (tabell 6.1 på side 114) som foreslår noen sikkerhetsnivå og plassering av enheter og tjenester under disse.

Intervjuet med Karl Gustav viser også hvordan han resonnerer seg frem til sikkerhetsnivåer. Jeg trekker her frem fem utdrag fra intervjuet og prøver å kondensere det til selve resonnementet:

> ≪[Kommer plutselig på at mail er en del av telefonen og tenker tilbake på det han har sagt tidligere om mailen. Lurer derfor på om den bør heves.] Viss en normal person finner mobilen på gata klarer de ikke omgå den firesifrede koden. Så på den måten er mailtilgangen låst. Men viss du ikke har det, da ligger jo mailen og facebooken veldig åpen. Litt skremmende hvor mye som går via telefonen.

(...) Viss konsekvensene hadde vært større ville jeg plassert ting høyere. Knapt plassere noe på nivå tre. Kanskje nettbank. For det er en større økonomisk ulempe.

(...)Sykkelen min, sånn, viss jeg ikke hadde hatt forsikring på sykkelen og noen hadde tatt den ville jeg kanskje hatt den på tre, men siden jeg har forsikring som dekker det meste så er det bare veldig kjedelig å miste sykkelen. Ikke noen stor økonomisk belastning.

(...)Bildene på tre siden de ikke kan erstattes, men de har jo ingen økonomisk belastning, eller ødelagt renommé. Men de kan jo ikke erstattes.

(...)Leilighet, inbrudd. Alt er forsikret, men det er jævlig kjipt. Bilen på tre. Kommer litt ann på. Relativt i forhold til egen inntekt osv.»

Karl Gustav er en av de som påpeker svakheten i å kunne få nye passord gjennom e-posten. For hans del brukes den samme e-post adressen til alt i privat sammenheng.

5.2.4 Krav til systemet

Å definere krav til systemet er ikke brukerens ansvar. Det var heller ikke målet at brukeren skulle gjøre i intervjuene. Men de følgende funnene kan relateres til krav systemet må håndtere og er plassert under denne overskriften. Dette er elementer som kom frem enten under intervjuet eller etter test og demonstrasjon av TokenLock.

Betalingsvilje for systemet var ikke et eget tema i intervjuene da det er vanskelig å svare på et så abstrakt spørsmål, men vi var innom det og Thea svarte følgende:

«Risikoen min er så liten for at jeg skal oppleve økonomisk tap derfor kan jeg ikke tenke meg å betale så mye. Folk som føler de har mer å tape ville nok vært interessert i å betale mer. I tillegg har jeg så få passord at jeg klarer å huske det.» (Thea)

Thea var også inne på dette med konfigurasjon av systemet. Samtlige intervjuobjekter berørte denne tematikken med at systemet måtte være enkelt å bruke og enkelt å forstå. Karl Gustav sier det enkelt og greit:

«Systemet må være enkelt og raskt. Sånn som dette her virket fort.»

Thea utdyper det noe:

«Det må ikke være vanskelig å laste ned eller installere. 5-10 minutter. Ikke komplisert. Ikke enda en dings. Om jeg måtte gå igjennom 10 sider med forskjellige ting å taste inn så hadde jeg vært litt sånn off, for å sette i gang med det. Men hadde det vært enklere...» (Thea)

Stabilitet og terminologi

I samtalen med Guri kom vi i prat om merking av fysiske nøkler for å huske hvor de hører til. Derfra kom vi over på en samtale om de systemene hun forholder seg til både fysiske og virtuelle:

> «Der er det noe, for foreløpig er vi ganske oppegående. Det systemet vi arbeider etter nå det må vi ha slik at vi kan bruke når vi ikke er så oppegående. Og det gjelder alt, enten det er elektronikk eller data eller hva det gjelder. For til lenger vi har et system som er så enkelt så kan vi gå inn i neste fase og bli ganske, vi kan bli ganske reduserte og allikevel greie å komme inn, om det er enkelt nok. Det er derfor vi sier at når vi har koder og passord og sånn noe. De skal være sikre, men de skal og være så enkle at de skal kunne brukes av oss. Inn i den fasen vi er på vei inn i. For når du snakker om funksjonshemning, må du huske at jeg allerede er funksjonshemmet på grunn av alder. Men den funksjonshemningen forsvinner ikke eller er statisk, den forandrer seg fra måned til måned og det må vi ta hensyn til i alt vi gjør. For vi har lyst å fungere 100% eller så nærme 100% som vi klarer. Derfor er det viktig at jeg fremdeles kan gå inn på datamaskinen. Jeg irriterer meg jo grenseløst når jeg ikke kommer meg inn på noe. Det er da jeg roper på hjelp.
>
> Det er da det er fantastisk når jeg gikk over til den nye maskinen. Jeg var så irritert, hvorfor skulle jeg over på dette nye systemet? Til denne apple driten! Sønnen hjalp meg gjennom dette. Men sant ikke forstår jeg ordbruken. Ikke forsår jeg systemene. Jeg er bare bruker. Og jeg må være bruker på det enkleste enkleste nivået.
>
> Og du trenger rådgiver på et enkelt plan. Fordi jeg ikke forstår terminologien, jeg forstår ikke hvordan det virker og dermed stopper det. Så når, viss jeg går inn og leser. For jeg prøver jo av og til å gå inn og lese. Men når jeg ikke forstår det som står skrevet for jeg forstår ikke de ordene som står skrevet.
>
> Det er det samme som ordet «app» app [sies med klar og tydelig A ikke Æ], hva er det for noe? Hadde de enda brukt applikasjon, men app. «du må ha app», det har ikke vært i vår terminologi i det hele tatt i de 80 årene vi har levd. Det finnes enormt mange spesialord som dere tar som en selvfølge som for meg er helt hebraisk. Selv om jeg fikk det på engelsk, så ville jeg ikke vite hva bruken var.
>
> Ord setter seg dårligere nå også. Det er det samme med brosjyrer (brukermanualer), bruksanvisninger, de er oversatt av folk som kan språket eller terminologien. Med sin ordbruk av nyere dato, mye av ordbruken er ukjent for oss. Det er et nytt språk for oss, ikke sant!» (Guri)

Dette er tydelig et tema som engasjerer og etter å ha sagt dette vil hun vise noen eksempler fra brukermanualer både på datamaskin og andre

produkter.

Plan B og utlån av enheten

Det kom flere tilbakemeldinger på at systemet måtte ha noe å falle tilbake på dersom den enheten som autentiserte deg opp mot resten skulle feile.

> «Om det så er bilen du skal starte, så må du ha en plan B, og jeg vet ikke hva plan B skal være. Viss det kun hadde vært telefonen hadde jeg vært litt bekymra. Det hadde vært dritkult. Enkelt, men viss noen tar telefonen din så har de kanskje tilgang til alt i livet ditt. Så du er veldig sårbar hvis det skulle skjære seg.» (Karl Gustav)

Grunnen til at bil blir nevnt her er at jeg i intervjuene oppmuntret til å tenke på andre ting enn bare datarelatert for å få brukerne til å tenke videre enn bare ting de forbinder med en skjerm og et tastatur.

Det var ikke bare i forbindelse med feil i den enheten som er ment å autentisere deg som ble nevnt. Også tilfeller hvor du må låne noen midlertidig tilgang. Vi så tidligere hvordan Thea vurderte sikkerheten på pc. Nå skal vi se på et utdrag fra utlån av visakort:

> «Hva om jeg skal kjøpe noe for deg? Da MÅ jeg legge ut for deg da. For det må være mulig å låne bort. For eksempel visakortet lånes jo bort om du skal kjøpe noe for meg.»

Hennes forslag er å tilby tradisjonell autentisering gjennom PIN-kode slik at det er mulig å låne bort kortet. Hun foreslår også at enkelte personer kan forhåndsgodkjennes for bruk av enheten også i tilfellet med visakort får eier beskjed og må godkjenne dersom beløpet er høyere enn en gitt terskel. Hun forteller også hvordan en venninne lånte bilen av faren, men det var Thea som var sjåfør. I den forbindelse kommer vi også inn på nødtilgang. På mobiltelefoner kan en uansett kode og andre begrensninger slå inn nødnummer. Hun under på om dette kan være noe å tenke på i forbindelse med bil og andre ting, at det kan gis nødtilgang til dem. Det må selvsagt ikke føre til at folk kan stjele fra bilen. Så hun konkluderer med at det er noe vanskelig å gjennomføre i praksis.

Andre tilfeller av bortlåning er når hun er på skolen og samboeren er hjemme og ønsker tilgang til laptopen. Da ønsker hun å kunne gi tilgang til den. Langtidslåning blir også nevnt, for eksempel at hun skal på ferie og en venn får låne laptopen eller andre ting over lengre tid. Her kom hun også med innspill på at tilgangen kunne være geografisk betinget, at den som lånte enheten kun hadde tilgang til den innenfor kommunen eller fylket. Eller på tid. For eksempel når du låner bort telefonen din vil hun ha mulighet for å begrense ringing til innenlands og kanskje også på samtalelengde.

Autentiseringsmekanisme og hva skal du bære?

Intervjuobjektene hadde også innspill når det gjelder sikkerheten og hvilken enhet som bør brukes. Karl Gustav mente at det ville føles tryggere

med fingeravtrykk enn med en dings som gav deg tilgang:

> «Om det hadde gått på fingeravtrykk, da hadde jeg følt meg trygg. Jeg vet nå at fingeravtrykk kan kopieres på en måte, men da er vi der at kjangsen er veldig liten igjen da. Så da hadde jeg følt meg veldig trygg igjen da. Men det er klart det er mange fingeravtrykk på telefonen din da. Men det er et eller annet med fingeravtrykk som jeg hadde følt meg trygg på.» (Garl Gustav)

På spørsmål om hvilke enheter som kunne fungert og som han kunne tenke å bære med seg var en innebygdt chip det han hadde mest tro på.

> «Det kunne vært genialt. Tenker jeg. Hatt en innebygd chip en eller annen plass, som du da kunne. Du måtte kunne programert den mot huset, bilen eller dataen. som da kanskje kan stjeles på en måte [det du programmerer mot]. Med chipen føler jeg at det er noe jeg alltid har med meg, ja det kan sikkert stjeles på en eller annen måte, men det er en mindre kjangse en at det kan stjeles via den chipen siden den alltid er med. Det er så utrolig lite kjangse da for at noen er ute etter deg da tror jeg jeg hadde følt meg veldig trygg.» (Karl Gustav)

Andre tilbakemeldinger

Guri var ikke så fascinert av systemet. Hun skjønte ikke hva hun skulle med noe slikt da hun opplever at hun takler sitt system relativt godt nå. Kanskje det kunne være mer aktuelt dersom systemet virket på iPaden siden den blir brukt mer enn datamaskinen. The mente derimot at systemet kunne virke aller best på «dumme innlogginger». Med det mente hun alle innlogginger som var vanskelige å huske og som hadde et lavt sikkerhetsnivå.

5.3 Workshopen

Workshopen var ikke umiddelbart en suksess da vi opplevde problemer med tilknytning til Wifi og dårlige 3G signaler. Dette løste set etter hvert gjennom å låne en annen telefon som også hadde NFC funksjon. På mange måter demonstrerte dette godt hvordan passordene kunne hentes frem på en helt ny enhet. I begynnelsen var også deltakerne noe korte i tilbakemeldingen. Men etter hvert begynte samtalen å flyte og det ble en veldig god meningsutveksling mellom deltakerne. Mange av de tingene som ble nevnt i workshopen er også nevnt tidligere i intervjuene, derfor gjengis kun det som er nytt eller som har nye innfallsvinkler.

Vi begynte med at noen av deltakerne fikk logge seg inn på de tre nettsidene MPX.no, Gmail.com og Facebook.com på vanlig måte med passord. Deretter brukte vi Yubikey NEO mot LastPass og gruppen fikk prøve dette hver sin gang. Det som skjer da er at appen LastPass åpnes på telefonen og han får opp en liste med de kontoene han har registrert der. Når han så trykker på et av objektene i listen får han valget om å

gå direkte til nettsiden. Når en så kommer til nettsiden er brukernavn og passord ferdig utfyllt og brukeren kan logge seg direkte inn.

Deltakerne var enige i at dette virket mye enklere og var et praktisk system. De var litt nølende i begynnelsen da det virket som om de ikke så for seg brukerscenarier utover mobiltelefonen. Også når de fikk prøve systemet selv krevdes mye forklaring på hvordan systemet hang sammen, sikkerhet var tidlig et tema. Men også hvordan kontoene ble registrert i LastPass. Etter hvert løsnet gruppen mer, de forstod konseptet bedre og det virket som om de klarte å se for seg flere brukscenarier. Etter hvert begynte de å diskutere hva systemet kunne brukes til.

En diskusjon som dukket opp var at noen kontoer, i dette tilfellet AppleID og noen nettbanker, krever at et nytt passord må være ulikt det en tidligere har brukt. En av deltakerne påpekte at dette var en stor ulempe når hun måtte be om nytt passord etter å ha glemt passordet til kontoen. For da måtte hun komme på et nytt passord igjen og dette passet dårlig med hennes passordhåntering ellers som gikk ut på å ha et lite knippe passord til alle de forskjellige kontoene. Et nytt passord som var «utenfor» dette systemet ble fort glemt ut.

> «Det må jo være enkelt å bruke, bare det å skifte passord må være enkelt». (Workshopdeltaker)

Dette ble også nevnt senere, at det måtte være enkelt å endre passord på de tjenestene en allerede hadde registrert seg på.

Deltakerne tok litt av når de tenkte på hvordan alt kunne henge sammen på denne ene brikken, enkelt. Legge inn ting fortløpende. Men når alt er samlet er det veldig viktig å ikke miste den, en fordel som ble trukket frem var at du hadde bare én dings å tenke på. Som å miste veska. Men veska kan ikke sikres, det kan en slik dings ved å ringe et nummer og gjøre den ubrukelig. De var veldig interessert i hva som skjedde dersom en mister Yubikey NEO. Et eksempel som ble kastet frem av en var hvordan bankene håndterer mistede bankkort. Hvor en bare kan ringe inn for å sperre alle kortene sine. En enhet som gir tilgang til alle kontoer og eventuelt også utvides til betaling og fysisk adgang, må ha en mulighet for å sperres var gruppens konklusjon. Også foreslo en av deltakerne at en kunne sperre én brikke og deretter bare gå på nærmeste 7 eleven for å hente en ny brikke og få registrert den på deg igjen. Da ville den gamle brikken være låst og den nye gi deg den tilgangen. i forbindelse med dette foreslo en annen av deltakerne at brikken eller dingsen som hadde blitt stjålet kunne melde fra om hvor den var på og eventuelt bruke innebygde kameraer i laptoper og mobiler til å ta bilde av den personen som prøvde å logge seg inn med feil PIN-kode.

Gjestekonto eller mulighet for å låne bort apparatet ble også tatt opp. En av deltakerne viste til eksempelet med når en skal låne bort telefon eller pc til å spille av musikk på fest. Da hadde det vært fint med en egen konto. Hun hadde selv laget en egen konto for å dele musikk på fest, for å unngå at alle hadde tilgang. Også når en skal låne bort telefonen hadde det vært fint å hindre folk fra å gå inn på bilder eller sms'er.På spørsmål om de kjenner

noen som ikke låner bort tingene sine svarer de fleste kjapt nei. De var enige om at det ikke helt akseptert å ikke låne bort dingsene sine til venner. Å låne bort til venner så de fleste på som helt naturlig. Men de kunne godt tenke seg å gi begrenset tilgang gjennom en gjestekontoprofil som bare har tilgang til å ringe for eksempel. Eller med mulighet for å definere rammene på gjestekontoen. Kan den ha tilgang til internett, tilgang til passord og kontoer? Ikke alle så problemet om venner så igjennom bildene på telefonen selv om de fleste virket enige i at det hadde vært greit å kunne forhindre. En av deltakerne kom med flere eksempler på hvorfor han ikke vil at folk skal se bildene sine.

> «[For eksempel om en] har bilder av en person en har hatt en liten "romanse" med kan det bli litt kleint å forklare».

Andre eksempler han trakk frem var internetthistorikk. Bare «småting» egentlig, men fint å hindre folk i å få den tilgangen. Et annet eksemplel som alle nikket gjenkjennende til var «Facerape»[1] et velkjent fenomen og ikke uvanlig etter at folk har lånt bort mobilen på fest i følge deltakerne på workshopen.

Flere var opptatt av at det måtte være noe mer enn bare tilgang til denne nøkkelen, en eller annen form for PIN-kode, passord eller andre grensenitt for autentisering virker det som er viktig for å øke følelsen av sikkerhet, siden det å miste noe som gir lett tilgang til «alt» uten øvrig sikkerhet føltes for usikkert. Når vi diskuterte hvilke dings det kunne vært ble det tidlig nevnt å operere den inn. Dette var flere av deltakerne veldig positive til med tanke på enkelhet. Dette ble diskutert i sammenheng med å miste enheten. En av deltakerne nevnte faren for at en bankterminal plukket opp flere signaler samtidig. Da må en vite at personen foran seg ikke kan betale med din konto. Eksempelet var en ansatt i en butikk som holdt frem bankterminalen til kunden og dermed ble trukket på sin egen konto dersom hun hadde en innebydg chip i fingeren. Det ville være mulig å løse gjennom å måtte taste PIN-koden sin mente hun.

For at systemet skal bli tatt i bruk mente den ene deltakeren at en måtte tro på at dette var fremtidens system. Med andre ord at dette var et system som ville kunne brukes i noen år og ikke bare var en døgnflue. Dersom dette kriteriet var oppfyllt mente flere av deltakerne at de kunne tenke seg å betale for et slikt system. Alle var enige om at de hadde betalingsvilje for brukervennlighet. Om en kunne plusse på backup av filer som en tilleggstjeneste og alt fungerte sømløst mente de at det var noe de selv kunne tenke seg å betale for. En annen funksjonalitet de så for seg var å koble en slik brikke eller enhet opp i mot dokumenter, kontakter, instillinger med mer som kunne ligge i «skyen» for så å hentes frem uansett hvilken terminal du benyttet. På den måten ble terminalen du brukte

[1] Ukjent begrep? Det er altså at noen får tilgang til facebook kontoen din, vanligvis gjennom å låne laptopen/telefonen også skrive noe på tidslinjen som blir flaut for deg eventuelt gjøre andre ting som blir sett på som rart og muligens flaut. Eksempelet til han som deltok på workshopen var en veninne som hadde fått skrevet på tidslinjen sin at hun var gravid og ikke ante hvem som var faren. Hvorpå hun måtte forklare dette for familie og venner når hun selv oppdaget dette dagen etter.

personlig tilpasset selv om du aldri før hadde vært på den. Mobiltelefoner du lånte kunne ha dine kontakter på også videre.

5.4 Test av LastPass

5.4.1 Sikkerhet

Denne brukeren fikk teste LastPass over lengre tid for å komme med tilbakemeldinger til bruken og hvordan det føltes å ta i bruk. På spørsmål om han følte det var sikkert å bruke LastPass til å håndtere passord:

> «Ja, men vanskelig å beskrive hvorfor. Du har gått god for det. På nettsidene har de en del awards som de har fått fra andre nettsider, de har fått annerkjennelse fra andre nettsider om at dette er et bra produkt som anbefales. Googlet også om det var sikkert eller ikke. Der kom en historie om at de mistet passord, men at passordene var saltetslik at det ikke var korrespondanse mellom brukernavn og passord og den biten der. Tror nok det er ganske safe». (Birger)

Samtidig gir Birger uttrykk for at det er vanskelig å ha helt kontroll med sikkerheten. Han er usikker på hvordan informasjonsutvekslingen mellom LastPass og nettleseren er. Men han innbiller seg at passordene er lagret sikkert og kryptert. Spesielt utvidelsen med å bruke Yubikey slik at en får en to-faktor autentisering gav ham en økt følelse av sikkerhet. Det at han kan gå inn på en ukjent terminal og logge inn i webgrensesnittet til LastPass også sette Yubikey inn i maskinens usb-port for å få OTP koden virker som en sikker løsning. Men han har ikke helt god erfaring med å bruke plugin i Safari da det virker som om noen sider «henger igjen», det vil si han kan logge ut av LastPass og fremdeles være innlogget på disse tjenestene. Blant annet nevner han Facebook og Linked in som steder hvor han fortsatt er logget inn.

Birger har benyttet kjangsen når han begynte å bruke LastPass til å knytte e-post kontoene og øvrige kontoer sammen på en smartere måte. Slik at det ikke er hoved e-posten som brukes til å generere nye passord. Det gir også en trygget.

Sikkerhetsnivåer

Også Birger kommer innpå temaet sikkerhetsnivåer. Han ser at det trengs gode passord på LastPass og de e-post kontoene som er knyttet opp til LastPass eller de øvrige kontoene LastPass hånterer. Vi prater litt om muligheten for å inkludere flere ting på én enhet. Også Birger gir uttrykk for at det er skummelt å samle så mye informasjon ett sted.

Med tanke på forskjellige brukscenarier ser han for seg at betaling og adgang til kontoret må kreve PIN-kode. At et system som håndterer flere slike kontoer også håndterer ting som kollektivbilletter er ikke utenkelig og da behøver en ikke kode. Det er jo begrenset hvilken skade det kan gjøre om noen bruker det uten ditt samtykke.

På samme måte kunne han tenke seg at bruken av Yubikey med LastPass, altså to-faktor autentisering, var noe en kunne velge ut i fra tjeneste. For eksempel nettsteder med kredittkortinformasjon burde ha to-faktor autentisering, også e-posten. Men ikke mindre viktige kontoer.

> «Sider som facebook er ikke kritisk. Bare ubehagelig, ubekvemt [om andre får tilgang til]»

5.4.2 Nytt passord

Han gir uttrykk for at det er en viss fare for å bli låst opp i et hjørne. Hva skjer for eksempel dersom han mister Yubikeyen? Eller glemmer passordet til LastPass? Man må ha et system å falle tilbake på og faren er at en lager en sirkel hvor LastPass husker passordet til e-posten som kan gi tilgang til LastPass dersom du mister Yubikeyen. Systemet må være motstandsdyktig mot slike feil. Når du mister BankID brikken din får du en ny som rekommendert post. Som et sidespor der undrer han på om rekommendert post blir låst inne eller står i de vanlige posthyllene. For det er mange forskjellige personer som jobber på posten. På samme måte som du kan få ny BankID brikke ved å signere hos posten mener Birger det bør være mulig å hente en ny brikke. Men det beste hadde kanskje vært om posten har bilde av deg eller noe slik at du ikke er avhengig av å ha med visakort eller andre former for ID. For om en trekker systemet langt nok vil jo den daglige IDen din være det systemet du nettopp har mistet tilgang til. Men om posten har bilde eller eventuelt fingeravtrykk kan du møte opp der uten noen ting og komme ut med en ny enhet som gir deg tilgangen tilbake mener han.

5.4.3 Erfaringer fra bruken

Birger brukte allerede et passordhånteringssystem fra før. Men dette krevde at han kopierte passord og brukernavn fra det systemet og over til tjenesten han skulle ha tilgang til manuelt. Man kan nok derfor anta at Birger hadde bedre kontroll over kontoene sine med tilhørende brukernavn og passord enn det mange andre har. Han sier om prosessen med å legge inn alle brukernavnene og passordene:

> Veldig ålright å legge inn [passord/brukernavn], selv om det tok litt tid. brukte sikkert en time å fikle med det da jeg startet med det. Også har noe blitt tatt underveis.» (Birger)

Om systemet i bruk sier han kort og greit:

> «Noen ting er mer tungvindt mens andre ting er lettere.» (ibid)

For eksempel når han jobber er det greit for da har han gjerne nøkkelknippet tilgjengelig. Men i situasjoner hvor det egner seg dårlig å rasle med et nøkkelknippe er det verre å ta frem Yubikeyen for å autentisere seg og logge inn på LastPass. I andre situasjoner trekker han frem denne

ulempen som en fordel. Det blir høyere terskel for å logge seg inn på facebook når du må hente nøkkelknippet for å gjøre det. LastPass var enklere i bruk uten Yubikey, men det føles sikrere å bruke det sammen med Yubikey.

Det er også enkelte tjenester som ikke fungerer sammen med LastPass, da må han taste inn passordene manuelt.

> «På en slik tjeneste er det kløne te når en lager et vanskelig passord siden en må inn på LastPAss og deretter taste det manuelt inn i den andre tjenesten.»

På spørsmål om hva som skal til for at et slikt system skal få større utbredelse svarer han at folks bevissthet rundt det er høyt nok for å ta det i bruk.

> «Tror det er vanskelig å få mor til å bruke det. Er ikke noen som vil hacke facebookkontoen hennes. Og hun har for få tjenester til at dette er nyttig nok for henne.»

På oppmuntring fra meg beskriver han morens utgangspunkt ytterligere:

> «Mor har én datamaskin med mail på og den har hun ikke satt opp selv engang. Hun skjønner ikke behovet for ekstra autentisering. MAnge som ikke bruker det i det daglige så har det eller gir det ikke så mye verdi. For folk som bruker det på jobb tror jeg det kan være nyttig.(...) Liker tanken på at mor kunne tatt mobilen over pc for å få tilgang. Men hun bruker ikke facebook utenfor huset og hun har ikke tatt i bruk nettbank.»

Alt i alt virker Birger skeptisk til innføring av et nytt system. Han nevner spesielt kostnad og konkurrerende tjenester som to viktige faktorer til dette:

> «Kostnad står i veien for at menigman tar det i bruk. Tviler på at det er mange som går til innkjøp av Buypass til flere hundre kroner for å se pasientjournalen sin.
>
> (...) På samme måte som man bruker BankID kan man innføre nye systemer. De fleste er jo vant med BankID i dag. Men det blir en konkurranse mellom systemet og ett system som er enkelt å bruke eller som folk forstår, som gir tilgang til flere ting kan fungere.»

Kapittel 6

Diskusjon

> «In this world, your identity provider is your only provider - log in once, and you are automatically logged in everywhere. Log out once, and you are automatically logged out everywhere. No need to keep clicking "log-in" buttons. It has a kind of poetic beauty and simplicity to it.»
> [73, side 29]

6.1 Rammefaktorer

Spørsmålet jeg stilte i introduksjonen var:

> «Hvilke rammefaktorer står en overfor i utvikling av universelt utformede autentiseringsløsninger?»

Jeg sa jeg ønsket å se nærmere på retningslinjer, lover, incentiver og nåværende kunnskapsnivå som rammefaktorer. I denne delen vil jeg diskutere de rammefaktorene jeg har identifisert og deres påvirkning og betydning. Jeg diskuterer først krav fra myndighetene, deretter den nåværende kunnskapen

6.1.1 Krav fra myndighetene

Diskriminerings- og tilgjengelighetsloven legger kanskje det viktigste grunnlaget og er den viktigste rammefaktoren for å få større utbredelse av universelt utformede IKT løsninger. Bakgrunnen for loven finner vi i flere ulike stortingsmeldinger [28, 26] og offentlige utredninger [25, 27]. Det kan være verdt å merke seg at Norge ikke har ratifisert FNs konvensjon om rettighetene til mennesker med nedsatt funksjonsevne[5]. Selv om Norge ikke har gjort det så har vi altså en lov som sier at IKT løsninger skal ha universell utforming.

I hvert fall i fremtiden. For så lenge det ikke eksisterer noen forskrift til loven så er det tydelig at ingen heller vet hvordan loven skal følges opp. I hvert fall ut i fra de funnene jeg har gjort gjennom enkle ringerunder rundt til de involverte partene er dette tilbakemeldingen som går igjen. Ingen vet

hvordan loven skal følges opp fordi det ikke eksisterer en forskrift som forteller hvordan en kan oppfylle loven.

Det er derfor vanskelig ut i fra dagens situasjon å si noe om hvilken betydning DTL vil ha for IKT systemer. Så lenge ingen vet hvor strenge kravene vil bli. Eller hvilke krav som skal gjelde. Ser vi på brukerautentisering spesielt er spørsmålet om det i det hele tatt finnes et godt grunnlag å lage krav på. Dette går jeg nærmere inn på under 6.1.2. Selv som det er vanskelig å anslå hvor avgjørende DTL med tilhørende forskrift vil bli, er er det tydelig ut i fra den øvrige politikken på området i form av utredninger og stortingsmeldinger vanskelig å konkludere med noe annet enn at det er et sterkt politisk ønske om å gjøre noe på feltet. Spørsmålet blir da om kunnskapen vår ligger til rette for å lage tilgjengelige autentiseringsløsninger. Dette drøftes videre i neste avsnitt.

6.1.2 Nåværende kunnskap om universell utforming & autentisering

Etter å ha nøstet opp i hvordan DTL og ansvaret for universell utforming henger sammen i de statlige organene var det den manglende erfaringen med, og manglende innspill på temaet som slo meg. Lenge hadde jeg et håp om at noen kunne peke meg i riktig retning til de personene som jobber med forskriften. Men selv om jeg er blitt møtt med vennlige ord og hjelp har dette foreløpig ikke lykkes. Samtidig var dette en avsporing fra selve oppgaven. Som jeg beskrev under Kasus kapittelet ligger det ikke innenfor oppgavens grenser å grave dypt inn i politikken på området. Det var begrenset med ressurser jeg kunne legge i å forfølge spørsmålet. Som funn i en vitenskapelig kontekst er dette ytterst svake funn og med de nødvendige forbehold om at jeg *kan* ha pratet med feil person vil jeg allikevel si at det er en viktig indikasjon når ingen av de etatene og organisasjonene jeg var i kontakt med jobber aktivt med problemstillingen så vidt jeg kunne bringe klarhet i. Det kan være et tegn om at forskning og virkelighet stemmer godt overens.

Fuglerud et al. [46], Fritsch et al. [45] har i sine undersøkelser funnet at det «eksisterer svært lite forskning rundt universell utforming av sikkerhetsløsninger». De viser til undersøkelser som for eksempel DIADEM prosjektet som melder tilbake at «universell utforming av pålogging og autentisering er en viktig problemstilling». Og til UNIMOD prosjektet hvor det viste seg at opptil så mye som 1/3 av alle henvendelser til helpdesk gjaldt innloggingsproblemer og at innlogging var «en betydelig barriere i bruken av altinn.no. Ut i fra det jeg har klart å finne og lese meg frem til av litteratur virker det ikke som det finnes noen gode retningslinjer på krav til en universelt utformet autentiseringsløsning.

Det er også interessant at interesseorganisasjonene til funksjonshemmede i den grad jeg har fått belyst det heller ikke virker til å være spesielt opptatt av dette temaet. De henviser til WCAG, men WCAG sier ikke noe spesielt om innlogging. På grunnlag av at det finnes lite forskning på området. Og at det tilsynelatende finnes få eller ingen retningslinjer som er allment kjent blant interessentene som her inkluderer myndigheter, bedrif-

ter og interesseorganisasjoner. Kan det vise seg at kommende forskrift til DTL ikke vil kreve annet enn det standard tekniske retningslinjer allerede gjør om tilgjengelighet av autentiseringsmekanismer. Det viser seg også at ingen av de involverte partene så langt har kunnet bekrefte at de jobber med reelle alternativer på dette punktet. Det gjelder BLD, FAD, DIFI, LDO, Deltasenteret og interesseorganisasjonene som ligger under funksjonshemmedes forbund. Det inkluderer tilsynelatende også bedrifter som MediaLT som jobber med universell utforming. Ingen vet hva en universelt utformet autentisering er. Det er en vågal påstand, men jeg vil la den stå frem til det motsatte er bevist. En oppgave som ikke burde være veldig vanskelig dersom jeg tar feil på dette punktet. Ikke minst vil det være til stor glede om dette er et punkt hvor jeg tar feil for det er bekymringsfullt dersom det er slik at vi ikke vet hvordan vi kan inkludere flest mulig ikke bare i løsninger men også på vei inn til løsningen.

6.2 Universell utforming og autentisering

I introduksjonen stilte jeg spørsmålet:

> «Hva kreves av en universelt utformet autentiseringsløsning?»

Jeg skrev at jeg ønsket å finne ut av følgende: «Hva ligger i begrepet universell utforming? Hva krever en løsning med tanke på brukeropplevelse og tilgjengelighet? For å kunne svare på det må jeg finne ut av hvilke krav folk har både til funksjonalitet og til bruk. Det vil også være essensielt å vite hvordan brukeren vurderer risikoen og sikkerhetsbehovet til ulike enheter og tjenester.»

Denne delen skal gi svar på disse spørsmålene.

6.2.1 En tilgjengelelig løsning

Beskrivelse av problemet

Det er ikke rett frem å svare på hva som kreves av en universelt utformet autentiseringsløsning. Som vi ser i gjennomgangen av relatert forskning på inkluderende identitetshåndteringssystemer later det til å være en kunnskapsmangel til hvilke krav som stilles til slike løsninger. Fritsch et al. [45] skriver at de ikke finner noen slike retningslinjer, heller ikke W3Cs Web Security Context workin group [17] adresserer selve problemstillingen de viser bare til at det er en problemstilling. For i det hele tatt å kunne svare på hvilke krav som stilles til en universelt utformet autentiseringsløsning må vi først vite omfanget av en slik løsning.

Igjennom denne oppgavens utforming kommer det tydelig frem en forståelse for at universell utforming og brukeropplevelse må sees i helhet fra brukerens ståsted. Ikke som små øyer av tilgjengelige tjenester eller gode brukeropplevelser. Som vi ser av diskusjonen over om hvor kostnaden ligger er det i dag en betydelig kostnad som ligger på brukeren i løsninger som baserer seg på noe du husker. Selv to-faktor løsninger

som krever en ekstra dings blir omtalt som «allmenningens tragedie av lommene» [1].

Om vi så ser på definisjonen av en funksjonshemning eller forklaringen på hvordan en funksjonshemning oppstår gjennom GAP-modellen (se figur 2.3 på side 16. Ser vi at en funksjonshemning oppstår i gapet mellom den enkeltes forutsetninger og de krav samfunnet stiller [75, 26]. Dette «samfunnets krav» må jo omhandle den totale mengden krav som stilles til brukeren like mye som enkeltkravene denne møter. I intervjuene fant jeg at samtlige av intervjuobjektene opplevde problemer med håndtering av brukernavn og passord. Karl Gustav sa blant annet på spørsmål om han hadde kontroll på brukernavn og passord:

> «Nei, finnes ikke. Det er noen jeg bruker ofte som jeg klarer å huske.»
> (Karl Gustav i intervju)

Til disse funnene kommer at dette studiet ikke undersøker personer med funksjonshemninger eller funksjonsnedsettelser. De personene som er intervjuet vil bli oppfattet som normalt fungerende mennesker på alle områder så langt jeg kan forstå.

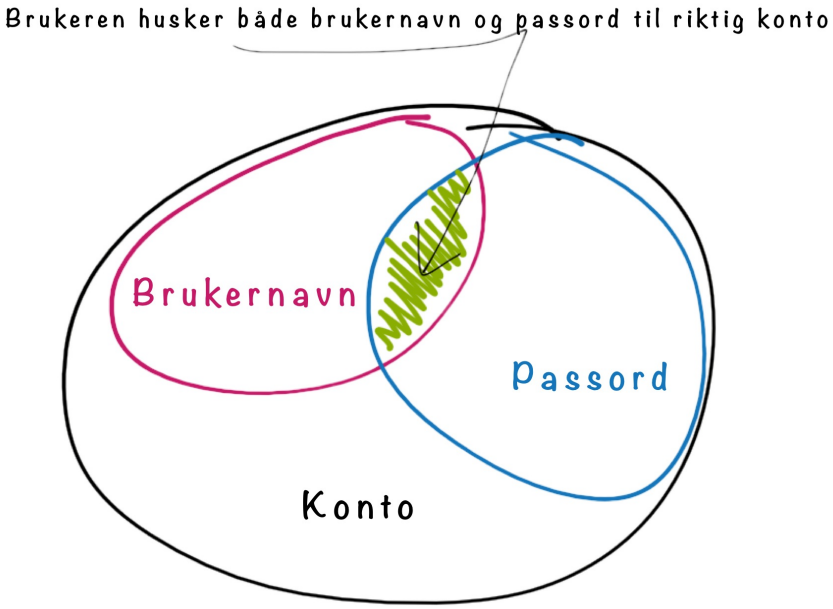
Om vi kombinerer et syn om at «samfunnets krav» ikke er begrenset til enkeltkrav men at det i universell utforming også må handle om det store bildet er det Karl Gustav her beskriver en funksjonshemning slik den forklares av GAP-modellen. Samfunnets krav om å ha kontroll på brukernavn og passord er høyere enn hans forutsetninger for å huske disse, eller lage et system for seg selv som fungerer i praksis. Dersom vi velger å se det på denne måten vil antagligvis de aller fleste av oss oppleve en funksjonshemning i vårt møte med kravene til å ha kontroll på alle kontoene vi har. Sandnes [75] skriver følgende:

> «Dersom noen ikke får tilgang til en tjeneste, vil de oppleve utestengning eller diskriminering. Når samfunnet forventer at borgerne skal benytte en tjeneste, blir det også en folkerett å kunne benytte tjenesten. Målet er derfor å bevege seg fra tilgjengelighet via spesialløsninger tilpasset spesielle brukergrupper til universalløsninger utformet for alle.»[75, side 27]

Med et syn om at de fleste av oss opplever en funksjonshemning i møtet med kravet til å holde kontroll på alle kontoer vil løsningen allerede ha et bredt nedslagsfelt og ikke være en spesialløsning for de få. Dette er selvsagt ikke nok, men som vi ser kan problemet med tilgjengeligheten til autentiseringsløsninger ha et bredere nedslagsfelt enn det vi først antar når vi hører universell utforming.

Problemet ligger så vidt jeg har klart å forstå ikke først og fremst på enkeltkontoer men på den totale belastningen brukeren opplever. Derfor må det første kravet til en universelt utformet løsning være at

[1] Per Torsheim under foredrag på «Open Workshop. Security-usability and biometric» Universitetet i Oslo 28. september 2012



Figur 6.1: Sammenhengen mellom passord, brukernavn og kontoer. Det grønne området illustrerer hva brukeren husker. Figuren er ment som illustrasjon ikke som en gjengivelse av faktiske størrelser.

den klarer å håndtere i hvert fall en større andel av totalen enn bare én enkelt konto. Det er ikke bare en «Passord Fatigue»[57] men en «Konto Fatigue». Allmenningens tragedie oppi dette handler om mer enn bare passord. Det er summen av identiteter, passord og kontoer som er den største utfordringen for brukerne. Men jeg tror det er et godt bilde å bruke bildet av hukommelse som en allmenning som er blitt utnyttet av tjenesteleverandørene slik [34, 30, 79]. Det er her kostnaden med B/P metaforen blir lagt, på brukeren. Og enten må brukeren regulere dette selv og dermed kreve av tjenesteleverandørene at kostnaden blir lagt et annet sted eller så må tjenesteleverandørene frivillig være med på en regulering [52].

Skal vi fortsette å kalle dette en funksjonshemning? Spørsmålet i overskriften gir egentlig svaret. Ut i fra de problemene man står overfor med tanke på tilgjengelighet er de problemene du og jeg og Karl Gustav og de andre intervjuobjektene opplever små. Vi blir ikke nødvendigvis stengt ute av løsningen. Vi opplever bare en dårlig brukeropplevelse. Har du glemt et passord tar det som regel bare mer tid å finne riktig. Enten slik Thea beskriver i intervjuet, om å bare prøve seg frem med forskjellige passord og brukernavn eller be om nytt passord. Vi blir ikke stengt helt ute og det er mulig å håndtere problemet. For det ligger en fare i å vanne ut funksjonshemning helt når det beskrives på denne måten. Jeg har tidligere nevnt Normans uttryk *handlingsgap*[65]. Så langt jeg har sett er dette kun blitt brukt i forbindelse med brukeropplevelse ikke om

funksjonshemning. Selv om begrepet og modellen Norman tegner er veldig lik GAP-modellen[75, 26]. Jeg tror det vil være lurt å ikke bruke ordet funksjonshemning om dette problemet. Først og fremst i respekt for alle de som virkelig opplever en funksjonshemning. Men vi ser at det kan være en sterk sammenheng mellom handlingsgapet og GAP-modellen for funksjonshemning.

Jeg er usikker på hvor denne problemstillingen bør plasseres og hvordan den bør omtales. For det er helt klart en utfordring dersom løsningene vi har i dag for autentisering fører til funksjonshemning for store deler av befolkningen, selv om det er i mindre grad og mindre alvorlig er det fremdeles alvorlig nok. Men bør problemet plasseres under fanen brukeropplevelse eller universell utforming? Kanskje kan figuren Pettersen [73] omtaler og som er gjengitt i denne oppgaven figur 2.4 på side 21 gi oss en mulig tilnærming. Bør vi plassere problemet under fanen «Universall usabillity»? Jeg er redd vi ved å plassere problemet der med den fanen vil plassere det midt mellom de to stolene det egentlig bør sitte på. At problemet plasseres i et ingenmannsland. Vi ser at rammevilkårene for universell utforming av IKT tjenester allerede faller mellom ansvarsområder, vi trenger ikke gjøre det problemet større. Derfor vil jeg ikke benytte begrepet «universal usabillity» om dette problemet men si at det hører hjemme både innen universell utforming og under brukeropplevelse.

Krav til systemet

Nå når jeg har definert inn problemstillingen med at folk flest opplever problemer med å ha kontroll over kontoer og at vi må se autentisering som en helhet og ikke stykkevis og delt vil det resultere i økte krav til et universelt utformet system. Det jeg vil gjøre videre er å beskrive hvilke andre krav som må settes til et universelt uformet system. Det jeg ikke kommer til å skrive om er ulike modaliteter for spesifikke funksjonsnedsettelser. Det er også en viktig problemstilling og under diskusjonen om nærhetsbasert autentisering vil du se at det trengs ulike former for initiell brukerautentisering også i et slikt system. Men hvilken form for grensesnitt og utforming den initielle brukerautentiseringen har blir undersøkt nøye i E-me prosjektet hvor det er utviklet en prototype med ulike grensesnitt som skal testes. Derfor konsentrerer jeg meg i det videre om andre problemstillinger og krav systemt må håndtere.

Stabil utforming

I intervjuet påpeker Guri noe med systemet som per i dag ikke dekkes direkte av designretningslinjene for universell utforming så vidt jeg kan se. At systemet må være stabilt og likt over tid. I intervjuet omtaler hun det om hele systemet deres (hun og ektemannen) for låser, nøkler og koder. Dessuten alle andre ting det være seg matlaging eller å skru på tv. Dette er et krav som muligens kan relateres til kravet om «Enkel og intuitiv bruk»[15, 85, 75].

> «Der er det noe, for foreløpig er vi ganske oppegående. Det systemet vi arbeider etter nå det må vi ha slik at vi kan bruke når vi ikke er så oppegående. Og det gjelder alt, enten det er elektronikk eller data eller hva det gjelder. For til lenger vi har et system som er så enkelt så kan vi gå inn i neste fase og bli ganske, vi kan bli ganske reduserte og allikevel greie å komme inn, om det er enkelt nok.»
> (Guri i intervju)

Slik Guri beskriver dette ligger det intuitive her i at de har gjort det før og kjenner godt til systemet. Dette kravet om at løsningen skal ha et *stabilt design* eller kanskje man skal kalle det *stabile metaforer* for IKT-systemer kan være veldig viktig med tanke på den kognitive belastningen som legges på brukeren. Slik Guri beskriver det her kan det i motsatt fall være slik at endringer i metaforer, designet eller i brukerinteraksjonen (systemet som hun kaller det) fører til at de blir stengt ute fordi de har sluttet å lære[2]. Et praktisk eksempel er nettbanken. Guri er en aktiv bruker av nettbank, men hva skjer den dagen banken endrer systemet slik at hun ikke lenger forstår det? Enten dette er innloggingsløsningen eller det er i selve nettbanken hvor overføringer og betalinger gjøres, en dag kan resultatet av endringene være at hun blir utestengt fra systemet.

Det jeg kaller metaforer her kan like så godt være det Norman [65] omtaler som designkonvensjoner. I følge ham finnes det ikke noe slikt som naturlige grensesnitt [68] alt er tillært. Med en slik forståelse av at de metaforene, de designkonvensjonene vi forholder oss til i et grensenitt, er tillærte, ikke naturlige er det lettere å se sammenhengen mellom kognisjon og endringer. En dag vil læringen ta slutt og før den tid vil det bli tyngre for oss å lære nye ting etter hvert som vi blir eldre. Også for folk som har en kognitiv funksjonsnedsettelse kan dette være en relevant problemstilling. Hvordan skal vi forstå et slikt krav til stabile metaforer? Funnene i denne oppgaven gir ikke grunnlag for å forstå dette problemet fullt ut. Jeg foreslår allikevel to tilnærminger basert på min forståelse for problemet Guri beskriver og forklarer bakgrunnen for de.

Slik jeg forstår Guri vil dette være et tidsbestemt kriterium, eller et historisk betinget krav. Dersom vi nå forholder oss til at det er aldring som gir den kognitive funksjonsnedsettelsen vil det i en gitt brukermasse, for eksempel til en nettbank, være en demografisk fordeling hvor et visst antall av brukerne er over, la oss si 70 år. Da vil det hele tiden vil være brukere som har behov for å «låse» løsningen slik den fremstår i dag. Dersom det hadde vært et krav som var slik og dette kravet settes ut i fra en viss alder eller et tidspunkt hvor brukeren ikke lenger klarer å lære nye metaforer eller interaksjoner, da vil de metaforene måtte «henge igjen» med den brukeren til det siste. Om vi fortsetter eksempelet med

[2]For enkelhetsskyld og for eksemplenes skyld illustreres dette her som om brukeren plutselig en dag mister evnen til å lære. Det er selvsagt ikke slik. I hvert fall ikke for de fleste. Jeg håper leseren kan være overbærende med en slik forenkling. Beskrivelsen av utfordringen er langt i fra ferdig undersøkt og i hvor stor grad brukeren mister evnen til å lære nye ting er en av mange interessante problemstillinger i forbindelse med dette funnet.

banken måtte denne praktisk sett sette en alder eller på et vis gi brukeren mulighet til å fryse interaksjonen på et visst tidspunkt og sørge for at utviklingen som skjer derfra kun tilfaller de brukerne som faller under grensen for «stabile metaforer». Systemene trenger i et slikt tilfelle ikke å fryses på den tekniske siden. Det brukerne ser og jobber med er jo gjerne det grafiske grensesnittet. Man kan si at det settes en dato hvor pikslene fryses for brukeren men systemet får utvikle seg videre i bakgrunnen. Dette er en noe ekstrem beskrivelse av hvordan en kunne brukt et prinsipp om stabile metaforer.

En annen og noe mindre ekstrem måte å forstå dette på er å begrense behovet for å lære nye ting til et minimum. Det kan innebære å sørge for at stabiliteten ikke handler om å fryse metaforer og design helt, men at det innebærer å la det gå lang tid mellom hver gang noe endres for å minske den kognitive belastningen. Igjen må vi se på problemet fra brukerens ståsted og som et system ikke som enkelthendelser. Dersom Guri bruker for eksempel Altinn.no, nettbank.no, nettbutikk.no, nettavis.no, lokalavis.noogfacebook.com og disse tjenestene hver for seg endrer deler av grensesnittet slik at Guri må lære noe nytt bare en gang hver tredje måned for hver tjeneste vil hun fremdeles måtte lære seg noe nytt 24 ganger på et år[3]. Det blir en endring i en av tjenestene hun bruker daglig annenhver uke. Et forslag til hvordan dette kan implementeres i praksis er at eksisterende brukere av slike tjenester får «lov å slippe» å få oppdateringer oftere enn for eksempel en gang i året. Samtidig kan nye løsninger nye design og nye metaforer rulles ut til nye brukere fortløpende, siden disse ikke har noe grunnlag for å si hvordan siden var fra før.

Problemet er to-delt. Det ene er å lære seg hvordan et system fungerer og det systemets metaforer og arbeidsflyt det kan for eksempel løses ved å «fryse» grensesnitt eller begrense antall oppdateringer. Den andre utfordringen handler om hvilke metaforer som er universelt utformet ut i fra den beskrivelsen Guri gir vil det til enhver tid være behov for å lage en oversikt over hvilke metaforer som har vært tilstede lenge nok til at de på en gitt alder kjenner til de og har lært dem. En slags oversikt over konvensjoner som er kommet til etter brukeren har behov for å begrense læringen og konsentrere seg om å beholde det de allerede kan. Et slikt skille kan enkelt forklares på følgende måte: Dersom vi er enige om at Norman [65] at vi bør i så stor grad som mulig holde oss til konvensjoner når vi designer løsninger vil det med den forståelsen jeg har forklart over bli en forskjell på konvensjoner som er universelt utformede og konvensjoner som ikke er det. De konvensjonene som ikke er universelt utformet har ikke hatt lang nok tid blant brukerne til å få det historiske fotfestet som skal til for å også bli forstått av brukere som har sluttet å lære. Ergo er de konvensjonene eller metaforene ikke intuitive for den brukeren. Forstår vi dette slik hører dette kravet til under kravet om «Enkel og intuitiv bruk».

[3] 6 tjenester * 4 endringer i året.

Tilpasset terminologi

Guri snakker også om et annet viktig kriterium og det er språket som brukes for å forklare løsningene.

> «Det er det samme som ordet «app» app [sies med klar og tydelig A ikke Æ], hva er det for noe? Hadde de enda brukt applikasjon, men app. «du må ha app», det har ikke vært i vår terminologi i det hele tatt i de 80 årene vi har levd. Det finnes enormt mange spesialord som dere tar som en selvfølge som for meg er helt hebraisk. Selv om jeg fikk det på engelsk, så ville jeg ikke vite hva bruken var.
>
> Ord setter seg dårligere nå også. Det er det samme med brosjyrer [brukermanualer], bruksanvisninger, de er oversatt av folk som kan språket eller terminologien. Med sin ordbruk av nyere dato, mye av ordbruken er ukjent for oss. Det er et nytt språk for oss, ikke sant!»
> (Guri i intervju)

Dette med terminologi passer godt inn i designretningsnlinjen *Forståelig informasjon: Utformingen skal kommunisere nødvendig informasjon til brukeren på en effektiv måte*. Det kan være et vanskelig krav å følge opp. For det første trengs det en oversikt over hvilke ord som er nye etter den beskrivelsen Guri har. Hun har jo lært seg noen nye ord, hvor går grensen for at hun lærte seg terminologi? Også må en finne andre ord som beskriver funksjonalitet og systemet på en måte som også hun kan forstå. Vi ser at dersom terminologien ikke følger dette prinsippet så stenges Guri ute av systemet. I intervjuet gir hun uttrykk for hvor totalt det stopper opp for henne når hun ikke forstår systemdialoger eller andre meldinger fra systemet.

Universell utforming og å designe for «alle» Det er vanskelig å si om det er riktig å ta det utgangspunktet denne oppgaven gjør ved å samle krav fra brukere uten spesielle behov. Som man ser ovenfor er den personen som har gitt flest innspill som går direkte på universell utforming Guri som er en eldre dame på over 80 år og som strengt tatt har noen spesielle behov ut i fra alderen. Samtidig har jeg gjennom intervjuene identifisert problemet med innlogging til å gjelde personer også uten spesielle behov. På den måten har jeg vist at økt fokus på tilgjengeligheten i autentiseringsløsninger kan hjelpe de fleste av oss. Et annet viktig funn er det at vi må se det totale bildet for brukeren når vi lager tilgjengelige løsninger. Og i dette bildet er det den totale belastningen av alle kontoene som er det første og største problemet. Derfor blir retningslinjene til en viss grad overordnede og ikke spesifikke. Ikke uventet ut i fra måten vi skiller universell utforming og brukeropplevelse på kommer de fleste kravene fra de som er intervjuet i denne oppgaven under kategorien brukeropplevelse. Jeg har valgt å dele det inn på den måten siden det tradisjonelt sett deles mellom universell utforming og brukeropplevelse.

Det er også et poeng med oppgavens design at en løsning ikke kan være universelt utformet og passe «alle» dersom «de fleste» ikke ønsker å bruke den på grunn av for dårlig brukeropplevelse. Nå skal jeg ta for meg de kravene som stilles til løsningen og som passer best inn under fanen brukeropplevelse.

6.2.2 Brukeropplevelse

Om begrepsbruken

Jeg har valgt å bruke ordet brukeropplevelse fremfor en smalere betegnelse som for eksempel brukskvalitet. I følge Sharp et al. [78] bruker den siste internasjonale versjonen av «standard for human-centered design» (ISO 13407) *brukeropplevelse* som en samlebetegnelse som dekker nytte (usefulness), attrådverdighet (desirability), kredibilitet (credibility) og tilgjengelighet (accessibility). Det er et begrep som er bredere enn det tradisjonelle brukervennlighet (usability) og tar i større grad hensyn til at disse begrepene henger uløselig sammen [78]. Allikevel er begrepet skilt ut i fra universell utforming i denne oppgaven slik at tilgjengelighet til dels blir behandlet for seg. Denne inkonsekvente bruken fortjener en kort kommentar. Det finnes forskjellige definisjoner av hva brukskvalitet er. Det finnes mange designretningslinjer og i litteraturen er det forskjellig bruk av begrepene og forskjellige fokus. Dette er nok naturlig. Det fører også til at det i oppgaver som denne, hvor hovedpoenget ikke er å problematisere *hva* interaksjonsdesign er eller likheten og forskjellen mellom begreper som brukes og sammenhengen mellom fagområder, så blir begrepsbruken noe inkonsekvent. Jeg har valgt å skille på de to da jeg opplever at universell utforming er et begrep som har fått sterkt fotfeste og at det er et begrep folk kjenner til spesielt når det gjelder arkitektur. Det er et begrep som dekker helt konkrete problemstillinger. På den måten hjelper det leseren å forstå den sentrale problemstillingen i oppgaven, hvordan kan vi lage inkluderende autentiseringsløsninger?

Når jeg så har valgt å bruke brukeropplevelse som en samlebetegnelse, fremfor å fokusere for eksempel på brukervennlighet, er det fordi jeg tror det er et begrep som dekker de problemstillingene vi står overfor og som oppstår mellom bruker og maskin bedre. Som Sharp et al. [78] skriver er nytte, attrådverdighet, kredibilitet og tilgjengelighet uløselig knyttet sammen. Når Norman [66] dedikerer en hel bok for å rette opp sitt tidligere inntrykk av at brukbarhet var nok og omtaler i hvor stor grad følelsene våre spiller en rolle viser det godt at gode løsninger må være mer enn bare brukbare, mer enn bare brukervennlige. Vi ser også at tilgjengelighet og brukervennlighet er uløselig knyttet sammen Pettersen [73] bruker begrepet universell brukbarhet om de fellesutfordringene som ligger mellom brukervennlighet og tilgjengelighet.

Systemet skal være trygt å bruke: Om å skape en trygg følelse

Sharp et al. [78] skriver at et system skal være «Trygt å bruke». Dette er

et av flere brukervennlighetsmål. Jeg forstår trygt å bruke som at systemet skal være trygt å bruke, men også at brukeren skal *føle* seg trygg når han bruker systemet. I teorikapittelet så vi nærmere på hvordan vi opplever sikkerhet.Schneier [76] skriver

> ≪(...)you can be secure even though you don't feel secure. And you can feel secure even though you're not. The feeling and reality of security are certainly related to each other, but they're just as certainly not the same as each other. We'd probably be better off if we had two different words for them.≫ [76].

Det er et behov for å skille mellom de to, det å være sikker og føle seg sikker. Jeg prøver meg nå på å bruke trygg om følelsen og sikker om bruken av systemet. Med andre ord et system skal være sikkert å bruke og føles trygt for brukeren. En bruker som ikke føler seg trygg vil antagligvis heller ikke ha en god opplevelse. Sharp et al. [78] skriver om brukbarhet at systemet skal gi en gledelig[4] opplevelse foruten å være enkelt å lære og effektivt å bruke. Derfor må en løsning også oppleves som trygg for å gi en god brukeropplevelse.

I intervjuene ser vi at flere av personene opplever at systemene er trygge når de må igjennom flere sikkerhetsdialoger. Under funn skrev jeg følgende om brukernes beskrivelse av den trygge følelsen:

> ≪Det virker som det handler om en blanding av hvem som tilbyr sikkerheten. Bankvesenet blir for eksempel sett på som trygt. Karl Gustav stoler på BankID-løsningen og mener den virker sikrere fordi det er flere ledd. Som vi ser over sier også Guri at hun stoler både på banken og legekontoret.≫
> (Fra Funn)

Også i testen med LastPass påpeker Birger at det ekstra leddet med Yubikey føles tryggere. Det kommer ikke frem i intervjuet om denne sikkerheten kommer av en faktisk økt sikkerhet gjennom OTP løsningen Yubikey gir eller tryggheten i et ekstra ledd.

Et av funnene Stølen [81] gjør er at brukerne føler seg mindre trygge på bruk av mønster i stede for PIN-kode som sikkerhet på mobiltelefonen. Hun antyder at dette kan komme av vane. Noe som stemmer godt overens med det Schneier [76] skriver, at vi undervurderer risikoen på kjente ting og overdriver risikoen for ukjente. Tar vi dette litt lengre ser vi at Guri stoler på banken og legen. Dette *kan* ha noe med vane å gjøre, at det er noe kjent eller noe trygt. Uansett om det er sånn eller sånn har vi noen institusjoner vi stoler mer på enn andre. Kombinerer vi disse funnene ser vi at en følelse av trygghet kan komme fra institusjoner vi stoler på, kjente metaforer for sikkerhet og flere sikkerhetsledd. Det er helt sikkert flere kilder til en trygg følelse men dette er de som er kommet frem i mine funn. Hvordan skal vi så bruke dette i en autentiseringsløsning?

Går vi tilbake til det Schneier [76] skriver om risikopersepsjon gir han oss svaret.

[4]Engelsk: Enjoyable

> «The feeling and reality of security are different, but they're closely related. We make the best security trade-offs —and by that I mean trade-offs that give us genuine security for a reasonable cost— when our feeling of security matches the reality of security. It's when the two are out of alignment that we get security wrong.»
> [76]

Løsningen må prøve å utnytte måten vi opplever risiko på slik at sikkerheten kan utlignes med tryggheten. På den måten kan brukeren føle seg så trygg som systemet er sikkert. Som vi skal se under kan dette bli en utfordring dersom grensesnittene blir mer og mer usynlige. Jeg tror en måte å håndrere dette på er å utnytte «sikkerhetsteateret»[76] og prøver å lage løsninger som klarer å ballanserer sikkerhet og trygghet. Ut i fra kunnskap om risikopersepsjon som vi ser i tabell 2.1 på side 31. Der kan vi velge å få brukeren til å dempe følelsen av risiko (med andre ord øke tryggheten) for eksempel gjennom å gjøre systemet *vell forstått* for brukeren. Eller at brukeren føler at risikoen er *under deres kontroll* og at *den er tatt frivillig*.

Mange passord, virkelig?: Avlivning av en myte

I intervjuene og under workshopen får jeg inntrykk av at personene gir et delt inntrykk av sitt forhold til brukernavn og passord. De fleste gir samtidig uttrykk for at de misliker det sterkt og at de klarer å håndtere det så noenlunde. I intervjuene ser vi at det er kontoer som er mindre brukt som er vanskelige å håndtere. Kontoer som ofte er i bruk for eksempel e-post og facebook er enkle å huske.

Det jeg tror skjer her er at den kontrollen personene oppgir at de har er reell når det kommer til ofte brukte kontoer. Der bruker de en miks av tre-fire passord de kjenner godt. Dette er viktig, for i litteraturen blir brukernavn/passord «problemet» gjerne fremstilt som et problem med at brukerne må huske så utrolig mange forskjellige passord. Reellt sett virker det som om brukerne på de kontoene de bruker hver dag ikke opplever det på denne måten. Der har de passord som de husker godt og som gjerne «sitter i fingrene». For disse kontoene opplever jeg at de presenterer et annet syn, nemlig at B/P fungerer godt, enkelt og raskt.

Grunnen til at dette er et viktig funn er at det er disse kontoene og den holdningen brukerne har til den ikke gjenspeiler noe behov for å endre dagens praksis. Det er enkelt å huske for de fleste brukere. De føler ikke at det er et stort problem. En alternativ løsning må håndtere dette på en måte som oppleves som minimum like enkel, fleksibel og rask. I testen av LastPass og i intervjuet med Birger opplever jeg at så ikke er tilfelle. Han sier om erfaringer til bruken av LastPass:

> «Noen ting er mer tungvindt mens andre ting er lettere.»
> (Birger i intervju)

Det mer tungvindte blir eksemplifisert med Facebook hvor han ikke gidder å hente yubikeyen i jakka for å logge seg inn.

Et brukeropplevelseskrav til en alternativ løsning konkurrerer derfor ikke med en opplevelse brukeren har om at det er helt umulig å forholde seg til B/P metaforen. Slik jeg forstår tilbakemeldingene i intervjuene opplever brukerne at det er enkelt å holde kontroll på de mest brukte kontoene. Det er fleksibelt, effektivt og velkjent. En alternativ løsning må være tilsvarende enkel eller enklere (i følge Schneier om hvordan vi forstår verdien av noe nytt må det være mye enklere eller ha mye høyere verdi for at vi skal være villige til å bytte det ut[76]).

Systemet skal være enkelt å bruke, lett å lære og enkelt å huske: Om å skjule kompleksitet

Vi beygnner å se konturene av de kravene som settes til en universelt utformet løsning. At det skal være lett å bruke og intuitivt å ta i bruk er noen av kravene. I følge Matt Bishop[39] begynner problemene her å tårne seg opp. For å gjøre sikkerheten enklere og bedre lager vi gjerne løsninger som er mer komplekse.

> «So the more complex a system is, the more secure it should be–yet the less secure it is likely to be, because of the complexity designed to add security!»
> [39, side 1]

Den psykologiske akseptabiliteten av systemet må være riktig. Gutmann and Grigg [51] skriver at sikkerhet må følge brukervennlighet, ikke den andre veien. Brukeren er villig til å akseptere noe høyere kompleksitet dersom verdien oppleves som høyere. Sikkerhet oppleves stort sett ikke som å ha høy nok verdi[51].

Det er spesielt konfigurasjon jeg ønsker å trekke frem her. Dersom systemet skal være fleksibelt og tilby brukeren både størst mulig grad av selvråderett over sikkerheten og systemet skal være fleksibelt med tanke på sikkerhetsnivåer vil det bli komplekst. Vi kan ikke forvente at brukeren selv skal akseptere å konfigurere systemet. Hverken med tanke på innsatsen som må legges inn i det eller med tanke på at systemet må konfigureres «riktig» for å være sikkert.

Fra intervjuene vil jeg trekke frem det Thea sier om konfigurasjon:

> «Det må ikke være vanskelig å laste ned eller installere. 5-10 minutter. Ikke komplisert. Ikke enda en dings. Om jeg måtte gå igjennom 10 sider med forskjellige ting å taste inn så hadde jeg vært litt sånn off, for å sette i gang med det. Men hadde det vært enklere...»
> (Thea i intervju)

En mulig løsning er å sørge for at store deler av kompleksiteten blir skjult for brukeren. Tognazzini skriver:

> The ideal interface is no interface at all, and most of the complexity of a multilayered security scheme could and should be

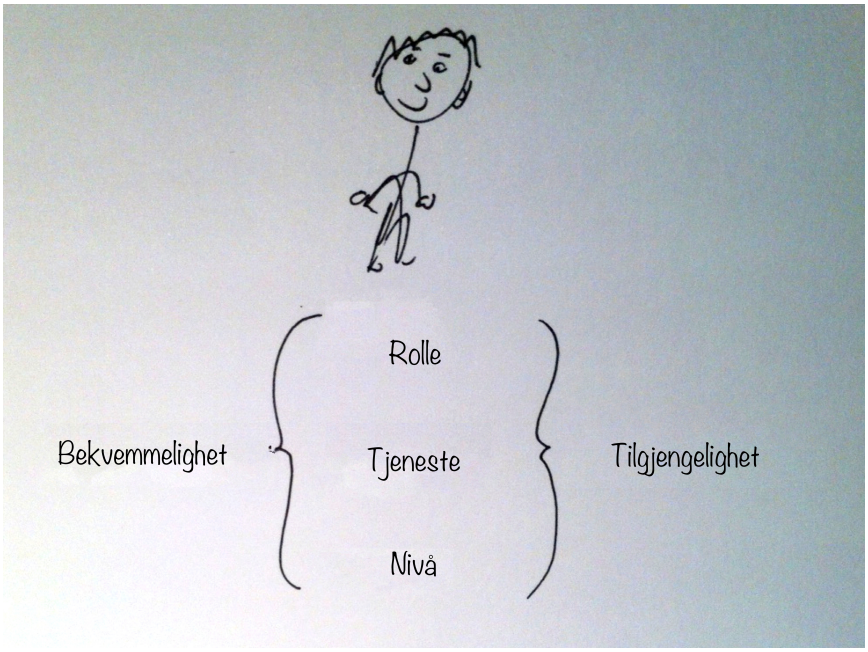
> hidden from the user. Those parts that are visible should enable the user to simply and flexibly change security parameters. [39, side 45]

På mange måter tar en bort mer av det grafiske grensesnittet i løsninger som baserer seg på nærhet. Målet er at brukeren skal kunne gå bort til terminalen og så bare ta den i bruk [31]. I de fleste systemene som beskrives under nærhetsbasert autentisering ser vi at brukerens interaksjon med selve innloggingen blir mindre. Tydeligst trer dette frem i begrepet «Zero-interaction Authentication»[38]. Dette gir noen utfordringer for hvordan vi håndterer designretningslinjer som for eksempel *synlighet, tilbakemelding, restriksjoner, overensstemmelse og ytelse*[78, side 26] I flere av de foreslåtte systemene for nærhetsbasert autentisering er det nettopp kravet til at brukeren eksplisitt ønsker å logge seg inn som er et av problemene [For eksempel 64]. Dersom kompleksiteten skal skjules må det ikke bli så lite interaksjon igjen at brukeren ikke er klar over at hun logges inn. Dette var en av de tingene også deltakerne på Workshopen var bekymret for. De lurte på om det kunne være en fare for at man for eksempel kunne risikere å betale varene til noen andre dersom betalingen var basert på nærhet. Dette kan igjen sees i sammenheng med trygghet. Brukeren må være trygg på når hun logges inn og ut av systemene. Også i testen av LastPass er vi at det er en mangel på tilbakemelding og at handlingene ikke er synlige nok når Birger er usikker på om han blir logget ut av tjenestene eller ikke når han går ut av nettleseren.

For å få bukt med konfigurasjonsproblemet samtidig som man iverater den psykologiske akseptabiliteten tror jeg mye må skje i bakgrunnen. Samtidig må brukeren få være aktivt med selv og bestemme hvordan sikkerheten skal være. Ellers vil brukerne bare finne snarveier rundt løsningen [86, 29]. Vi ser i funnene hvor ulikt brukerne vurderer risikoen. Risiko og viktigheten av et system er i stor grad en subjektiv vurdering [42]. For å få til dette må man lage en god modell som gir grunnlag for å automatisere og hjelpe brukeren å konfigurere systemet uten å måtte konfigurere for mye og uten at konfigurasjonen kan sørge for sirkelsvakheter slik Birger påpeker i intervjuet. En slik modell må være godt gjennomarbeidet og testes utførlig. Ut i fra de funnene jeg har gjort må det være en modell som tar høyde for at brukeren trenger å holde oversikt over kontoene sine altså en løsning og en modell som tar høyde for flere tjenester og ikke bare én og én konto. På den måten kan løsningen klare å hjelpe brukeren med å konfigurere riktig. Et forslag til en slik modell gjennomgås under.

En konseptuell modell for brukerautentisering

I figur 6.2 har jeg gjort et forsøk på å illustere en begynnelse på en konseptuell modell for brukerautentisering. Denne er basert på de inntrykkene jeg har fått i intervjuene og fra workshopen for hvilke vurderinger og i hvilken rekkefølge brukeren vurderer sikkerheten. Dette er ikke et forsøk på å representere brukerens mentale modeller. Det er mer



Figur 6.2: En konseptuell modell for brukerautentisering med bakgrunn fra intervjuene og workshopen

å betrakte som en slags «supermodell» for hvordan brukeren kan hjelpes til å forstå og bestemme riktig sikkerhet på tjenesten. En begynnelse på noe som kan representeres i en algoritme som kan hjelpe brukeren til å vurdere sikkerheten. Slik min forståelse for hvordan hvilke ting brukeren vurderer når han vurderer sikkerhet er hvilken *rolle* han har i forbindelse med den *tjenesten* han vurderer. Jeg tror ikke brukeren ser kontoer men heller tjenester når han logger seg inn eller får adgang til ulike ting. Ved å bruke tjenester åpner en også for muligheten til å dele løsninger, for eksempel nettbank, opp i ulike mindre tjenester. I nettbanken kan en tjeneste være å overføre penger internt mellom egne kontoer, en annen tjeneste kan være å betale regninger. Allerede i dag ser vi mobilapplikasjoner hvor nettbankene skiller på disse to tjenestene. Dette åpner også for muligheten for delte tjenester. Enten tjenesten deles innad i en familie eller med venner (for eksempel medietjenester som musikk, film og bøker). Det gir mulighet til å definere hva en gjestekonto skal få tilgang til av tjenester. Når rolle og tjeneste er vurdert kommer *nivået* altså en subjektiv vurdering av behov for sikkerhet for den tjenesten med den rollen. Det som påvirker alle disse vurderingene er *bekvemmelighet* og *tilgjengelighet*. For eksempel ser vi at intervjuobjektene kan ha en lavere sikkerhet dersom de føler at behovet for bekvemmelighet eller tilgjengelighet er større enn behovet for sikkerhet.

Denne modellen jeg presenterer her er brukt for å demonstrere hvordan og hva et system må vurdere for å hjelpe brukeren å sette riktig nivå. Dersom man hadde klart å få for eksempel facebook til å gi beskjed til brukerens autentiseringsløsning om hvilke tjenester de tilbyr gjerne etterfulgt av noen anbefalte nivåer for hver tjeneste (antagligvis

noen minimumsnivåer) ville det vært en god start for at brukerens autentiseringsløsning ut i fra tidligere definerte nivåer klarte å sette riktig nivå for brukeren. Eventuelt gjennom en dialog med brukeren klarte å hjelpe brukeren på en enkel måte å konfigurere sikkerheten basert også på egne preferanser. Denne modellen er langt i fra ferdig, men den er allikevel tatt med som et skrit på veien mot løsninger som kan hjelpe brukeren å velge riktig og i retning av å lage systemer hvor brukeren får være med på sikkerhetskonfigurasjonen uten å bryte med den psykologiske akseptabiliteten.

Hva med resten av brukeropplevelsesmålene?

Nå har jeg trukket frem de viktigste funnene jeg har gjort i forbindelse med krav fra brukerne som jeg ønsker å plassere inn under brukeropplevelse. Vi skal ta en nærmere titt på sikkerhetsrelaterte krav nedenfor. Men først, det kom frem flere ønsker og innspill i intervjuene. Mye av det går på at systemet skal «være enkelt å bruke» og lignende. Jeg diskuterer ikke disse kravene noe videre da jeg føler de blir dekket i de retningslinjene som er nevnt i teorikapittelet. Kjente retningslinjer og kjente problemstillinger for hva brukerne krever av et system. Jeg opplever det som krav som bør testes direkte på brukerne gjennom prototyping og brukbarhetstesting i en utviklingsprosess. Med det sier jeg ikke at dette er krav som er enkle å finne ut av eller som har mindre betydning. Men måten denne oppgaven er gjort på legger ikke et grunnlag for å analysere slike krav. Da er brukertesting bedre egnet.

6.2.3 Sikkerhet

En ny form for autentiseringsmekanisme(?): Stedet du er

Hulsebosch et al. [54], Syta et al. [83] introduserer en ny form for autentisering utover de tre tradisjonelle *noe du er, noe du har* og *noe du kan*. De sier stedet du er, når du er der og konteksten du er i har en betydning[54, 83]. Også Tognazzini tar til orde for å gjøre begrepet sikkerhet noe mer elastisk i forhold til situasjonen brukeren befinner seg i. Blant annet trekker han frem mobile systemers evne til å være mer eller mindre stedsbevisste gjennom GPS posisjon. WiFi MAC adressen kan også fortelle maskinen at du sitter på hjemmenettverket. Han foreslår tre nivåer fra lav til høy sikkerhet alt etter hvor du befinner deg som en mer sofistikert tilnærming til sikkerhet [39].

I intervjuene kommer det frem at personene bruker fysisk tilgang som et sikkerhetsnivå. Eksempler på dette er mobiltelefoner de har på seg, nettbrett de bruker hjemme, tv og filmleie gjennom dekoder. Tilgang til disse tingene krever at personer er der fysisk. Under diskusjonen om sikkerhetsnivåer sidestiller blant annet Thea fysisk tilgang med å ha et passord på enheten. Hun problematiserer også hvordan det å gi noen tilgang til for eksempel kameraet sitt for at de skal få se bildene derfra automatisk gir dem tilgang til å kunne slette bilder.

Norman [67] illustrerer godt hvordan stedet du er kan bestemme om du har tilgang til en ressurs. Toalettene er innenfor en lukket sone som ikke er åpen uten egen tillatelse. For besøkende er det, i hans beskrivelse, ikke adgang til dette området og besøkende kan dermed ikke benytte seg av toalettene. Dersom en er innenfor denne sonen har en tilgang. Jeg er ikke sikker på om dette er det beste eksempelet, men jeg tror det er slik intervjuobjektene opplever dette. At ting som er i hjemmet deres er noe kun venner har adgang til og da under oppsyn. Så på den måten tror jeg opplevelsen av *stedet du er* fungerer som en egen autentiseringsmekanisme.

Spørsmålet er om denne formen for autentisering kan plasseres inn under en av de tre vanlige formene for autentisering. Så vidt jeg kan bedømme kan vi ikke gjøre det. Det er ganske åpenbart ikke *noe du kan*. Det kunne jo vært *noe du er*. Spesielt med tanke på hvordan Hulsebosch et al. [54] ønsker å bruke en form for mønstergjennkjenning basert på om du skulle vært på jobb, hvordan du vanligvis oppfører og beveger deg og en rekke andre kriterier som de samler til en «Overall confidence» skår og som gir grunnlag for å gi deg tilgang eller ikke. Det er også nærliggende å si at det er akkurat noe du er som gir deg adgang til venners boliger og slipper deg i nærheten av dingsene deres. Det er i kraft av hva du er som gir deg tilgang til kameraet til Thea. Det kan være noe du har også. Dersom du har nøkkelen som gir adgang til de ikke åpne delene av en bygning så har du tilgang for eksempel til toalettet Norman viser til. Men i forbindelse med nærhetsbasert autentisering (som er noe du har) er kanskje en av de viktige tingene systemet kan vite om deg hvor du ikke er. At du er et sted gjør at du ikke kan være et annet sted og dermed kan systemets kunnskap om hvor du befinner deg nå være en viktig faktor. Kanskje en faktor som fortjener sin egen kategori. Jeg går ikke særlig inn på kontekst i denne oppgaven, men kontektsten har åpenbart også en betydning. I workshopen ser vi hvordan konteksten å være på fest og gi tilgang til mobiltelefonen for å spille av musikk er helt forskjellig fra konteksten å være alene hjemme med mobiltelefonen. På bakgrunn av det har jeg valgt å bruke dette som en egen fjerde autentiseringsmekanisme i denne oppgaven. Men jeg ser ikke bort i fra at dette begrepet burde vært diskutert ytterligere i en egen studie[5].

Sikkerhetsnivåer

Når det gjelder sikkerhetsnivåer er det to temaer jeg ønsker å diskutere. Det første er behovet for sikkerhetsnivåer det andre er hvor mange nivåer og hva de bør inneholde ut i fra de funnene jeg har gjort.

I intervjuene og workshopen er det to ting som kommer helt klart frem, den ene er at de fleste brukerne ressonnerer godt når det gjelder sikkerhetsnivåer. Ingen av de jeg var i kontakt med reagerte på at det burde finnes ulike nivåer, selv om dette i seg selv ikke nødvendigvis er åpenbart. Som vi ser av figur 5.1 foretar Jane en drøfting nærmest med seg selv for å komme frem til hvor ulike tjenester og enheter bør plasseres. Dette var helt typisk. I intervjuet med Karl Gustav endret hele bildet

[5]For alt jeg vet kan det godt være dette er gjort også. Jeg har bare ikke kommet i kontakt med den studien/de studiene så langt

seg i det han kom på at det på mobiltelefonen var tilgang til e-post og gjennom e-post kan man be om nytt passord på mange av webtjenestene han bruker. Han virket nærmest overrasket når han selv så hvor stor denne svakheten var. Vurderingene av nivå var forskjellig fra person til person. Det var resonnementet rundt hvor tjenester bør plasseres jeg var ute etter. Jeg tror intervjuene viser med all tydelighet at sikkerhetsnivå også er en subjektiv vurdering hvor konteksten til brukeren må tas med [42]. Jeg tror en viktig del av konteksten er det flere av intervjuobjektene trekker frem at de opplever at de ikke er så viktige, eller har store verdier og at «det bare er lille meg». En annen viktig faktor er bekvemmelighet og tilgjengelighet. Sikkerhetskompromisset gikk i de fleste tilfeller, untatt ting som bank og helseinformasjon, i favør av økt bekvemmelighet og tilgjengelighet. Da høyere sikkerhet innebærer høyere ulempe for brukeren [76].

Selv om brukerne ikke var helt enige om nivå var vurderingene de gjorde ganske like. Og en ting er helt klart de har alle et forhold til fysisk tilgang til enheter. Dette beskriver alle som en begrensende faktor for hvem som kan få tilgang og som en faktor som begrenser risikoen for den enheten. Jeg opplever også at den fysiske tilgangen er noe intervjuobjektene har en god konseptuell forståelse for. Naturlig nok siden dette er et konsept vi alle har vokst opp med og har et daglig forhold til. Det er noe som bør utnyttes i utvikling av systemer.

Et tema som var viktig for de fleste personene er muligheten til å låne bort enhetene sine. Å ha en gjestekonto slik at det er mulig å låne bort telefonen for å spille av musikk på fest. Eller låne bort telefonen slik at noen kan ringe. Andre eksempler var om man har venner på besøk og de ønsker å vise noe eller sjekke noe på internett. Thea sier det må være mulig å låne bort visakort og at det må være mulig å låne bilen bort. Vi var også inne på hus- og hyttenøkler med Guri. Men dette trenger ikke begrense seg til enheter og fysiske ting. Thea beskriver hvordan hun gir typen tilgang til e-post kontoen sin for at han skal kunne hjelpe henne dersom hun ikke har tilgang til internett. Også i slike tilfeller kunne det vært aktuelt å ty til gjestetilgang i stede for full tilgang til hele kontoen.

Jeg opplever at behovet for sikkerhetsnivået i aller største grad er tilstede ikke bare som et sikkerhetskrav men også fra brukerens side er det ønsket med ulike nivåer. Fysisk tilgang oppleves av personene som en sikkerhetsfaktor og dette bør utnyttes i en løsning. Dessuten vil gjestetilgang til enheter være en velkommen funksjon. Men hvilke nivåer bør en velge?

Flechais et al. [42] bruker tre nivåer for sikkerhet i sin studie (low, medium high). Jeg valgte å ta utgangspunkt i statens*Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor* [41]. I løpet av intervjuene viste det seg at dette ikke var et galt utgangspunkt men at beskrivelsene rammeverket gir passer dårlig til hvordan intervjuobjektene opplever risikoen. For eksempel under «konsekvenser for liv eller helse» står det følgende under risikonivå 3 «Det kan forekomme mindre helseskader». Kategorien «Hindring i straffeforfølgelse» og «Uaktsomt bidrag til lovbrudd» virker på intervjuobjektene helt fremmed. Nå har ikke disse retningslinjene blitt laget for å passe til denne bruken heller og i etter-

tid kunne det vært lurt å tilpasse nivåene og kategoriene. For noen av beskrivelsene i rammeverket kan virke noe ekstreme på intervjuobjektene og det kan ha påvirket hvilket nivå de plasserte tjenester på. Men rammeverket ble tatt med som et utgangspunkt å diskutere rundt og det fungerte mer enn tilfredsstillende.

Ut i fra intervjuene kan det se ut som om det vil være passelig med fire nivåer men at det overfor brukeren virker som tre nivåer. Dersom nivå 0 er for tjenester som kun krever å kjenne brukeren igjen, altså kun identifisering. Dette kan for eksempel på webbaserte tjenester være *innholdssider*[34] hvor målet med identifiseringen (og ofte i dag autentiseringen) er å tilpasse sidens innhold til brukerens ønsker, eller å fylle inn skjemaer. Andre sider som faller inn under beskrivelsen *identitetssider* eller *netthandel*[34] og som vil kreve en autentisering plasseres på en skala fra 1-3. En forenklet fremstilling med utgangspunkt i de løsningene vi har i dag ville da plassert en-faktor løsninger i kategori 1, to-faktor løsninger i kategori 2. Det tredje og siste nivået må bestå av den høyeste sikkerhetsløsningen som er akseptert for tilgjengelighet på høyeste nivå for offentlig kommunikasjon. En slik kategorisering vil kunne være med å støtte opp om brukerens konseptuelle modell av sikkerheten. I en slik inndeling vil jeg foreslå at fysisk tilgang til en enhet sidestilles med øvrige en-faktor løsninger for å passe inn med brukerens forståelse av sikkerheten. Her må det understrekes at dette er nivåene brukeren må forholde seg til. Det blir en helt annen sak hvordan systemet håndterer dette i bakgrunnen. Med en slik inndeling vil det helt sikkert også dukke opp hybrider og bastarder som er vanskelige å plassere innenfor en av disse kategoriene. Men intervjuene gir meg inntrykk av at flere nivåer vil bli uoversiktlig for brukeren. I tabell 6.1 har jeg forsøkt å illustrere hvordan fordelingen av noen enheter og tjenester kunne blitt i et slikt system ut i fra de diskusjonene som ble foretatt i intervjuene.

Gjennopprette tilgang til en konto

Gjennoppretting av tilgang til en konto og en «plan B» trekkes frem spesielt i forbindelse med å knytte opp tilgangen til noe fysisk som en Yubikey. Systemene i dag gjennoppretter i stor grad tilgang gjennom å sende en e-post til brukeren. Samtidig er e-post noe av det for eksempel Karl Gustav har tilgjengelig på telefonen uten passordlås. Det er dette han oppdager når han i intervjuet endrer hvilket nivå mobiltelefonen bør ligge på. Birger beskriver det som et «sirkelproblem» i testen av LastPass. For hva skjer om han glemmer passordet til LastPass og gjennom LastPass har lagret passordet til e-posten? Man risikerer å bli låst ut fra sitt eget system. Løsningen må altså ha en god måte å gjenopprette tilgang på som forhindrer dette.

For en løsning som baserer seg på en fysisk «nøkkel» som yubikey eller tilsvarende som i Lucidman prosjektet [57] er både deltakerne i workshopen og intervjuobjektene enig om at det er en stor utfordring uten umiddelbar løsning. Siden det var Yubikey som ble demonstrert er også forslagene til løsning knyttet til at det er en liten brikke. I workshopen

0 **Identifikasjon**	1 **En-faktor**	2 **To-faktor**	3 **Høyeste nivå**
Nettaviser	Nettbutikker uten kred. info	Nettbutikker med kred. info	Altinn
Reise (fly, tog, buss)	Nettbank interne transaksjoner	Nettbank eksterne transaksjoner	Kommunikasjon med lege
	Kamera	Kamera (slette bilder)	
	Mobil (ringe, sende sms innenlands)	Mobil (andre tjenester)	
	Gjestekonto	E-post	

Tabell 6.1: Forslag til sikkerhetsnivåer for brukerautentisering. Sett fra brukerens ståsted hva denne må forholde seg til.

og intervjuet med Birger blir det foreslått at dersom en mister brikken kan en stenge dennes tilgang til kontoene og deretter gå til nærmeste butikk/bank/postkontor for å kjøpe en ny brikke. I bank og på postkontor finnes det allerede rutiner for å kontrollere identitet, det er bakgrunnen for å foreslå en slik løsning. Thea foreslår at man faller tilbake på B/P dersom man mister brikken. Nå er ikke sikkerheten *i* passord behandlet i denne oppgaven. Men en fordel med en passordhåndterer er lange og vanskelige passord. Disse er så og si umulige å huske for brukeren, spesielt dersom denne ikke bruker det ofte noe som ville vært tilfelle dersom passordet vanligvis blir håndtert av en annen tjeneste. Men passord skrevet på papir er en løsning, men ikke en fullgod løsning. Spesielt om en utvider dette til å gjelde andre apparater uten mulighet for å taste inn B/P. Gjennoppretting og en god B-plan er nødvendig å ha i en brukerautentiseringsløsning dette er også noe Fuglerud [48] påpeker som en oppgave systemet må håndtere.

Maskin-maskin autentisering

Denne oppgaven behandler ikke maskin-maskin autentisering. Men i litteraturen rundt brukeropplevelse og sikkerhet blir ofte mennesket beskrevet som det svake leddet. Passordlengde og kompleksitet er en av de tingene som påvirker sikkerheten. Dersom en universelt utformet autentiseringsløsning også håndterer kontoer for brukeren og ikke bare enkeltautentiseringer over en lignende lest som LastPass og tilsvarende løsninger trenger ikke kompleksiteten i passord å være en begrensning lengre. Man kan også se for seg andre og sterkere typer maskin-maskin autentisering slik Lucidman prosjektet foreslår[57] dersom brukeren har en enhet som håndterer og autentiserer brukeren videre mot tjenestene. I så måte har en slik løsning noen likhetstrekk med Single-Sign On

løsninger[73, 81] og andre former for «Federated identity»[34]. Dette er ikke et krav til en universelt utformet løsning, men kan komme som en heldig bivirkning av å gjøre brukerautentisering tilgjengelig for flere.

6.3 Forslag til retningslinjer for universelt utformede autentiseringsløsninger

Nå kommer en samlet oversikt som oppsummerer de kravene som er kommet frem i denne oppgaven med tanke på å utvikle universelt utformede autentiseringsløsninger. Dette blir skrevet som et forslag på de retningslinjene man ut i fra mine funn bør ha med i utvikling av et slikt system. Det er ikke en fullstendig liste over krav som sier at ved å følge dette vil du få en tilgjengelig løsning. Det er heller ikke sagt at punktene under er «nye», mange av dem er allerede ivaretatt eller nevnt i andre retningslinjer og forslag. Dette er retningslinjer som kan peke ut en vei videre til utvikling av en løsning. Noen av disse retningslinjene kan virke litt vell spisset i forhold til grunnlaget de er diskutert på. Det anbefales å se retningslinjene i sammenheng med beskrivelsen tidligere i diskusjonen for å forstå bakgrunnen for de. Det er vanskelig å ta alle forbehold når en skal oppsummere slike retningslinjer.

Følg gjeldende retningsnlinjer for teknisk tilgjengelighet: Universell utforming er mer enn teknisk tilgjengelige løsninger. Men et minstemål er at retningslinjer for tilgjengelighet følges slik at brukeren kan bruke støttende teknologi som for eksempel leselist og opplesning av tekst.

For brukeren er det helheten som teller: Brukeren lever ikke med én og én tjeneste. Det er den totale belastningen som er hovedproblemet, spesielt med tanke på kognisjon. Universelt utformede systemer må ta høyde for dette gjennom å forhindre en allmenningens tragedie på brukerens kognisjon og lommer (en dings for hver konto legger for store krav på hva brukeren må bære med seg).

Kompatibilitet med eksisterende infrastruktur: Man kan ikke forvente at alle leverandører klarer å tilby brukeren universelt utformede systemer på egenhånd. I dag er incentivene for små til at det kommer til å skje. En løsning som tar som mål på seg å hjelpe brukeren med den totale belastningen må være kompatibelt med eksisterende infrastruktur.

Sammenlign kostnaden for alle innvolverte: Kostnaden med en autentiseringsløsning ligger ikke bare hos leverandør brukeren tar også en betydelig del av kostnaden ved å måtte forholde seg til mange ulike kontoer, brukernavn og passord dette må være med i regnestykket.

Stabile metaforer: Også forandringer i systemet må sees i en helhet for brukeren. Det som enkeltvis oppleves som små forandringer kan legge for store krav til å lære seg noe nytt for ofte når en ser på

det totale antall endringer. Universell utforming handler også om å dempe kravet til at brukeren skal lære seg nye grensesnitt.

Bruk tilgjengelige konvensjoner: Konvensjoner er historisk betinget. Vær bevisst på hvilke konvensjoner du kan forvente at brukerne dine kjenner, det er forskjell på etablerte konvensjoner og nye konvensjoner ikke alle brukere kan forventes å kjenne til de nye konvensjonene.

Tilpasset terminologi: Språket skal være enkelt, men det må også tas høyde for at brukeren ikke er kjent med terminologien og dermed ikke har grunnlag for å forstå beskrivelser og hjelpetekster. Også terminologi er historisk betinget og man kan ikke forvente at alle brukere kjenner til ny terminologi.

Attrådverdig: Å designe «for alle» inkluderer de brukerne med høyest krav til brukeropplevelse. Universelt utformede løsninger må også være attrådverdige og gi en god brukeropplevelse.

Effektivitet: Brukeren opplever ikke hverdagen å bestå av uttallige passord og brukernavn. De mest brukte kontoene håndteres relativt godt med brukernavn/passord metaforen gjennom å gjenbruke passord. En universelt utformet løsning som håndterer flere kontoer må ikke føles mer tungvindt eller mindre fleksibel enn dette.

Brukeren krever en uforholdsmessig høyere verdi: Brukeren må oppleve en ny løsning til å ha en uforholdsmessig mye høyere verdi for å finne det bryet verdt å bytte fra løsninger denne kjenner. Denne uretten må en ny løsning håndtere dersom en ikke har mulighet til å påtvinge løsningen på brukeren.

Gi brukeren en trygg følelse: Løsningen må føles trygg å bruke for at brukeren skal ha en god brukeropplevelse. Det holder ikke at systemet er sikkert. Trygghetsfølelsen er en vell så viktig del av sikkerheten.

Utlign trygghet med risiko: Løsningen må utligne forskjellen mellom trygghet og risiko på en sånn måte at brukeren kan foreta riktige og gode sikkerhetskompromisser.

Systemet må være enkelt å konfigurere: Kompleksitet må håndteres på en slik måte at brukeren klarer å konfigurere systemet selv og i høyest mulig grad etter egne preferanser for å unngå at han heller velger å omgå systemet for å få jobben gjort.

Brukeren må få bevissthet om handlingene sine: Gjør løsningen enkel å håndtere men ikke så enkel at brukeren ikke får tilbakemeldinger om inn- og utlogging.

Gjør oversikten over sikkerhetsnivåer enkel å forstå: Gi brukeren mulighet til å forstå ulike sikkerhetsnivåer slik at det er praktisk gjennomførbart for henne å forstå hvilket nivå en tjeneste bør ligge på. Et

forslag er å bruke sikkerhetsnivåer fra 0-3 for å forklare sikkerheten for brukeren.

Utnytt ulike sikkerhetsnivåer: En konto eller enhet kan ha mange tjenester. Sørg for at sikkerheten står i forhold til tjenesten som skal brukes og ikke kontoen/enheten som helhet.

Gjestekonto og utlån: Løsningen må håndtere utlån av tjenester og enheter. Det må være mulig å gi en annen part tilgang til enkelttjenester uten å gi denne full tilgang til hele kontoen/enheten.

Gjennoppretting: Løsningen for gjennoppretting må fungere slik at det ikke er mulig å «låse seg ute fra eget system». Gjennoppretting må være relativt enkel og brukeren må ikke ha følelsen av at det er en risiko for å miste tilgangen helt ved en feil. Det må være tydelig for brukeren hva plan-B er for å komme inn i løsningen.

Utnytt mulighetene som ligger i stedet brukeren er: Fysisk tilgjengelighet er et konsept brukeren forstår godt. Dette kan fungere som en autentiseringsfaktor og kan i mange tilfeller være nok.

6.3.1 Benytt et rammeverk når du analyserer løsningen

Jeg vil trekke frem noen få, men viktige funn fra Bonneau et al. [35]. Den første er at passord ikke gjør det så dårlig totalt sett.

> «Almost all schemes do better than passwords in some criteria, but all are worse in others: as Table 1 shows, no row is free of red (horizontal stripes). Thus, the current state of the world is a Pareto equlibrium. Replacing passwords with any of the schemes examined is not a question of giving up an inferior technology for something arguably better, but of giving up one set of compromises and trade-offs in exchange for another. For example, arguing that a hardware token like RSA SecurID is better than passwords implicitly assumes that the security criteria where it does better outweigh the usability and deployability criteria where it does worse.» [35]

Den andre at grafiske og kognitive løsninger bare har små fordeler sammenlignet med en tekstpassordløsning.

Helt sentralt ligger utplasseringsfordeler (deployability).

> «But *every* scheme does worse than passwords on deployability. This was to be expected given that the first four deployability benefits are defined with explicit reference to what passwords achieve and the remaining two are natural benefits of a long-term incumbent, but this uneven playing field reflects the reality of a decentraliced system like the Internet. Marginal

> gains are often not sufficient to reach the activation energy necessary to overcome significant transition costs, which may provide the best explanation of why we are likely to live considerably longer before seeing the funeral procession for passwords arrive at the cemetery.» [35]

Formålet med rammeverket er å kunne sammenligne forslag til autentiseringsløsninger og for å hindre for sterk bias mot egne løsninger citeBonneau2012a. Jeg tror dette rammeverket kan brukes til dette og at det gjennom å bruke dette er mulig å identifisere styrker og svakheter når man utformer løsninger som også innebærer ikke web-baserte tjenester. Men det siste kan kreve noen tilpasninger.

Rammeverket til [35] viser sin verdi bare i det at biasen *mot* passord kanskje blir lettere å håndtere. Vi ser at den ledende metaforen for autentisering har mange styrker som er vanskelig å gjenskape i nye løsninger.

Ser vi på kravene som stilles i rammeverket har de en sterk tilknytning til brukeropplevelses retningslinjer. Det er bra. Men de stiller for lave krav til tilgjengelighet i løsningen. Minstekravet er at løsningen skal være tilgjengelig for brukere som kan bruke B/P metaforen. Dette kan ha en så praktisk og enkel bakgrunn at vi faktisk ikke vet hvilke krav man må sette for å lage tilgjengelige autentiseringsløsninger. Samtidig har de i brukervennlighetskravene (B1-B) dekket mange tilgjengelighetskrav. Men det er ikke nok. Retningslinjene jeg har foreslått over i kombinasjon med de funn som blir gjort på ulike autentiseringsmodaliteter i E-me prosjektet kan være et skritt i riktig retning for å stille høyere krav til tilgjengelighet som en del av rammeverket.

6.4 Nærhetsbasert autentisering i lys av universell utforming & autentisering

I innledningen stilte jeg spørsmålet:

> «Hvordan kan nærhetsteknologi brukes for å skape en universelt utformet autentiseringsløsning?»

Jeg skrev videre: «Teknologi basert på kort og mellomkort kommunikasjon er i vinden. Hva er nærhetsteknologi? Kan det brukes? Og i tilfelle hvordan kan det brukes for å skape universelt utformede løsninger for brukerautentisering? Her vil det være spesielt interessant å se på tidligere forskning og forsøk rundt temaet.»

6.4.1 Hvorfor nærhetsbasert autentisering?

I litteraturen ser vi at det som jeg her beskriver som nærhetsbasert autentisering er basert på autentiseringsmetoden *noe du har*. Det er det du har som kommuniserer med autentiseringsløsningen ved hjelp av nærfeltskommunikasjon. Det finnes ulike målsettinger for å utvikle

nærhetsbasert autentisering. Vi ser for eksempel i [83, 31] hvor målet er å gjøre innloggingen så lite påtrengende som mulig. For noen er målet å støtte opp om arbeidsmetodene i et nomadisk miljø enten det er enbruker eller flerbruker grensesnitt [31, 32]. Andre har en målsetting om å øke sikkerheten blant annet gjennom å sørge for en kontinuerlig autentisering [72, 38, 63**?**].

Dersom en kan få til både økt sikkerhet, trygghet og tilgjengelighet er det veldig bra. Jeg har sett nærmere på denne formen for autentisering først og fremst med tanke på om det kan være en del av en løsning til en universelt utformet autentiseringsløsning. Det å overføre autentiseringen til noe du har på deg minsker i stor grad den kognitive belastningen på brukeren. Dette er også en metafor vi er godt kjent med og har vært kjent med lenge i form av nøkler. Overføringsverdien burde derfor være stor i så måte.

En annen fordel med å benytte nærhet til og ikke en nøkkel eller et kort som må settes inn i en lås er at kravet til nøyaktighet minskes, man slipper å være i direkte kontakt med autentiseringsmekanismen. Dette kan ha en stor fordel for personer som har nedsatt motoriske evner. Om vi strekker fantasien litt er det heller ikke vanskelig å se for seg at ganske mange av oss ville nytt godt av en løsning hvor ytterdøren låste seg automatisk opp, tenk på alle de gangene du kommer hjem med hendene fulle av handleposer eller bagasje. Aldri måtte rote i lommer for å finne frem nøkler og visakort. Dette var en av de tingene deltakerne i workshopen begynte å fantasere om. I nærhetsbasert autentisering ligger et håp om enklere autentisering.

Det er også en utvikling som gjør nærhetsbasert autentisering interessant. Det er utviklingen vi ser med stadig økende del av prosessorer og tilkobling til internett. Enten det gjelder smart TV, sensorer eller nettbrett, mobiltelefoner, lesebrett, laptoper med mer.Bell and Dourish [33] mente i 2007 at vi allerede var kommet til Weisers fremtid [87] med allestedsnærværende prosessering, med den forskjellen at bruken ikke var slik Weiser forutså. At fremtiden ble litt annerledes enn de han forutså. Det vi ser er en økende grad av krav til autentisering og en økende mengde enheter og tjenester som krever autentisering uten å tilby en tradisjonell desktopinteraksjon med skjerm, tastatur og mus. En nærhetsbasert løsning er ikke avhengig av tastatur, skjerm eller mus. Mellom den enheten brukeren bærer på seg og enheten brukeren autentiseres mot er det ikke engang nødvendig med et tradisjonelt grafisk grensesnitt. Dette legger til rette for enkel autentisering mot enheter vi ikke kan ta og føle på. Enheter som er innebygd eller fysisk utilgjengelige.

Disse fordelene eller antatte fordelene er det som gjør nærhetsbasert autentisering interessant. Spesielt med tanke på de kravene jeg har funnet til universelt utformede løsninger. For etter det jeg skriver om at en universelt utformet løsning skal ta høyde for alle brukerens interaksjoner må det også inkludere disse enhetene uten skjerm og tastatur. Og som funnene mine viser opplever brukerne at det er et sammensatt problem mellom passord, brukernavn og kontoer og ikke bare én av de tre som må håndteres. I omtalen av Singel-Sign On løsninger fra [73, 81] loves det en enkelhet som er vanskelig å matche. Men så vidt jeg kan se av

funnene mine for rammevilkår ligger ikke forholdene helt til rette for at vi kan håpe på at de fleste leverandører kommer til å endre systemene sine for å tilfredsstille et problem og en kostnad brukerne til nå har båret. Incentivene for det virker foreløpig for svake. Dette kan endre seg når forskriften til DTL kommer, men når det så langt jeg har kunnet se ikke finnes gode retningslinjer og generelt lite forskning på universelt utformede autentiseringsløsninger ville det vært en positiv overraskelse om forskriften vil inneholde mer enn tekniske retningsnlinjer.

Et alternativ til SSO løsninger er systemer som håndterer kontoene for deg slik for eksempel LastPass gjorde i forsøket med Birger. Og her tror jeg Lucidman prosjektet[57] kan gi mange interessante funn og forslag på den tekniske siden spesielt til hvordan det kan fungere. For om vi holder fantasien og sinnet åpent og ønsker å håndtere ikke bare autentisering på web, men også på enheter og fra enheter går vi til andre fysiske ting som betaling, dørlåser med mer. Akkurat slik deltakerne i workshopen fantaserte om. Da virker en løsning basert på nærhet i kombinasjon med kontohåndterer fristende og lys for autentisering. Både for økt tilgjengelighet, en bedre brukeropplevelse og økt sikkerhet gjennom maskin-maskin autentisering fremfor menneske-maskin autentisering[60]. I en slik løsning er den initielle autentiseringen mellom bruker og maskin viktig og i et slikt system er det kanskje først og fremst denne dialogen som må tilby ulike modaliteter som er tilpasset brukerens spesielle behov ut i fra brukerens evner.

Med de forventningene skal jeg diskutere kort hva mine funn sier om krav til en slik fremtidig løsning.

6.4.2 Hva kan brukeren bære med seg?

Vi kan begynne med den delen av nærhetsbasert autentisering som på brukerne virker å stå i veien det er hva de skal bære med seg. For Karl Gustav og flere av workshopdeltakerne var det å implementere en chip under huden en fristende løsning de så for seg kunne virke. Dette var spesielt med tanke på ta de var redde for å miste den dingsen som skulle autentisere dem opp i mot alt annet. Her dukket det opp flere utfordringer, spesielt med tanke på å skape en trygg opplevelse. Det ene var at de var redde for at man kunne ende opp med å betale for personen forann seg i butikkøen. Det andre er dersom enheten skulle være noe annet enn en chip i fingeren måtte det også være en annen form for autentisering. Dette er den initielle autentiseringen for eksempel [72**?**] argumenterer for må være på plass for å sikre at det er riktig person som får tilgang.

I intervjuene og workshopen spurte jeg etter hvilken dings som kunne brukes til dette formålet, til å bæres med seg hele tiden. Og utover chip i fingeren peker mobiltelefonen seg ut som et godt alternativ. Thea var tydelig på at hun ikke ønsket «nok en ting å ha med seg». Dette var også deltakerne i workshopen enige om, men det virket som holdningen til dette endret seg i takt med antall tjenester en slik enhet kunne gitt dem tilgang til. Antagligvis kommer personalisering og tilpasning inn i bildet her slik at noen foretrekker å bruke noe annet enn mobiltelefonen.

Vi skal også ta disse tilbakemeldingene fra brukerne med en klype salt. Viljen til å bære med seg ting som autentiserer oss henger nok tett sammen med den opplevde nytten. Vi bærer daglig rundt på lommebok,nøkler, mobiltelefon, laptop, nettbrett, vesker med mer. I tilfellet med hva brukeren skal eller ønsker å bære med seg tror jeg vi må:

> «look at behavior, listen to perceptions»[179 58, Refererer til Miller og Crabtree 1999]

Jeg tror altså vi kan få brukerne til å bære med seg en enhet som autentiserer dem opp i mot noe. Men det vil antagligvis være lettere å få dem til å fortsette å bære med seg mobiltelefon enn å introdusere en ny enhet.

6.4.3 Hvem skal bære kostnaden?

Når det gjelder kostnader har Birger noen interessante betraktninger. Han tror ikke disse kostnadene kan legges på brukerne.

> «Kostnad står i veien for at menigman tar det i bruk. Tviler på at det er mange som går til innkjøp av Buypass til flere hundre kroner for å se pasientjournalen sin.»
> (I intervju med Birger)

Priselastiteten til et slikt system er helt klart en problemstilling som ikke har en åpenbar løsning.

I workshopen sa deltakerne seg villige til å bruke mange hundre kroner dersom et slikt system fungerte smertefritt. Men disse svarene har begrenset verdi uten å observere hva de faktisk er villige til.

Men jeg tror nok folk er villige til å betale for bekvemmelighet. Dessuten er det flere aktører som har i interesse å levere sikre løsninger til brukerne sine og som har og allerede bruker en del på dette. Eksempler er staten i sin kommunikasjon med innbyggerne, enten det er gjennom Altinn eller kommunikasjon mellom lege og pasient. Bankene har en interesse både i nye betalingsløsninger og i sikker kommunikasjon i nettbanken. Som funnene mine antyder kan trygghetsfølelsen til brukeren økes dersom slike institusjoner står bak en løsning. Dersom også forskriften til DTL skulle komme til å kreve tilgjengelige løsninger fra nettbutikker og andre aktører som krever autentisering fra brukerne sine vil også disse kunne få et større incentiv for å implementere universelt utformede løsninger. Men den største kostnaden som må tas er forskning og utvikling av slike løsninger, så lenge kunnskapen er så begrenset som den er [46, 45]. Det er noe som kan ligge lenger fremme enn det burde da det ut i fra de undersøkelsene jeg har gjort ikke virker som det er noe ulike interesseorganisasjoner til funksjonshemmede jobber med eller er spesielt opptatt av. Og dersom det også er slik at de statlige institusjonene som burde jobbet med dette ikke gjør det eller gjør det i for liten grad vil den forskningen og utviklingen som trengs for å lage løsninger som er tilgjengelige ikke bli gjort. Da er det ikke kostnaden med implementering, heller ikke kostnaden med utvikling

som står i veien for universelt utformede løsninger, men interessen for problemstillingen.

Kompatabilitet

I de forslagene jeg har referert til om nærhetsbaserte autentiseringsløsninger brukes flere ulike teknologier for å registrere nærhet. Et viktig krav til et slikt system må være at det fungerer uten å bytte ut all eksisterende infrastruktur helt. Kanskje kan interkompatabilitet være en løsning. At man kan utnytte ulike nærhetsteknologier ikke bare NFC eller bare blåtann men kombinere dem og prøve å inkludere flest mulig apparater. Foruten kostnadssiden for utvikling av en nærhetsbasert autentiseringsløsning som kan implementeres i apparater og tjenester tror jeg kompatabiliteten og de kravene som vil settes til brukernes eksisterende infrastruktur vil være en formidabel hindring for utbredelse av et slikt system.

6.4.4 Konfigurasjon

Konfigurasjonen av systemet kan by på store utfordringer. Funnene mine antyder at systemet må håndtere ulike sikkerhetsnivåer til ulike tjenester innenfor den samme kontoen, dessuten åpne for deling av tjenester både med gjester og mer fast deling med familie og venner. Dessuten at den fysiske plasseringen av enheten som får tilgang til en tjeneste har en stor betydning. Det betyr kanskje at sikkerhetsnivået må endres etter om brukeren er hjemme eller ikke. Men ikke hver situasjon hjemme tilsvarer at en er trygg. Man kan ha folk på besøk eller barn i huset eller det er andre ting som gjør at konteksten endrer seg. Systemet må sørge for at brukeren kan konfigurere løsningen på en sikker måte slik at han unngår å låse seg ute fra sitt eget system eller åpne for store svakheter i systemet. Oppå dette må systemet støtte en plan-B for autentisering. Den må være like fleksibel som det brukerne oppfatter B/P metaforen å være på sine mest brukte kontoer i dag. Det betyr antagligvis at brukeren forventer å kunne få tilgang til web-baserte tjenester på fremmede terminaler. Til slutt ser vi av Birgers erfaring med Yubikey at den ikke alltid er der han er. Dersom det vi skal bære på oss ikke er noe vi alltid bærer på oss, men heller noe vi som regel har med oss og som regel bærer på oss blir det ytterligere innviklet.

Bare det å lage et system som håndterer konfigurasjonen av alle de mulige brukerscenariene som må til for å skape en løsning som er minst mulig påtrengende som veksler mellom sikkerhetsnivåer ut i fra stedet brukeren er, kanksje konteksten brukeren er i og som gir brukeren mulighet til å konfigurere på en sånn måte at han ikke føler for å omgå systemet samtidig som han er trygg på løsningen virker som en for stor oppgave.

Det blir et komplekst system og jeg er redd vi ender opp akkurat på den måten Matt Bishop beskriver sikkerhetsløsninger, at kompleksiteten gjør det nær sagt umulig å implementere riktig, konfigurere riktig og vedlikeholde riktig[39].

Med andre ord kravene som settes til et system basert på nærhet kan være for store til at det kan gjennomføres. Spesielt dersom en ønsker å

samle alle kontoer og tilgang til tjenester gjennom et apparat. Vi risikerer å ende opp med et for komeplekst og for rigid system hvor brukeren ender opp med å gjøre de samme tingene han alltid har gjort i møtet med informasjonssikkerhet. Å omgå det som ikke fungerer og som står i veien for de oppgavene han skal gjøre. Og uten denne kompleksiteten og interkompatabiliteten vil vi kanskje måtte ha mange ulike enheter som autentiserer oss opp i mot de ulike tjenestene trådløst. Og da går vi bare fra en allmenningens tragedie for kognisjonen til en allmenningens tragedie for lommene våre.

Kapittel 7

Konklusjon

7.1 Rammefaktorer

Jeg sa jeg ønsket å se nærmere på retningslinjer, lover, incentiver og nåværende kunnskapsnivå som rammefaktorer for å utvikle universelt utformede autentiseringsløsninger. Funnene viser at vi har lovgivning på plass for å kreve tilgjengelige informasjonssystemer. Samtidig vet ikke de organene som skal følge opp loven hvilke retningslinjer som må følges for å oppfylle lovens krav. På grunn av manglende retningslinjer er det vanskelig å forutsi hvor stor innflytelse DTL får med tanke på universell utforming i IKT systemer. Men dette er bare én av rammefaktorene.

Et annet funn er at de få frivillige organisasjonene jeg var i kontakt med og som ligger under Funksjonshemmedes forbund ikke jobber med problemstillingen. Dette er organisasjoner som ofte fungerer som viktige talsrør for sine medlemmer og kan påvirke politisk agenda.

Når vi ser på kunnskapsnivået og eksisterende forskning rundt temaet passer dette godt overens med lav interesse fra de frivillige organisasjonene og lav kunnskap i de offentlige institusjonene. For det finnes lite forskning på temaet. I hvert fall forskning som går direkte på temaet universell utforming og autentisering. Flere forskningsprosjekter peker på at dette er og *kan* være en betydelig problemstilling for brukerne. Det vi har er mye forskning på informasjonssikkerhet og brukeropplevelse, temaet universell utforming av informasjonssystemer er heller ikke uutforsket. Jeg tror man vil komme lengst fortest dersom man kombinerer disse feltene i utvikling av tilgjengelige systemer. Men det vil antagligvis gjenstå en rekke problemer i det vi for illustrasjonens skyld kan kalle *universelle brukeropplevelses problemer* (se figur 2.4 på side 21.

Incentivene for å utvikle tilgjengelige og inkluderende autentiseringsløsninger har ikke blitt vurdert nøye med tanke på kostnadene ved utvikling og implementering. Men vi har sett at kostnaden med dagens løsninger som baserer seg på brukernavn/passord metaforen og som resulterer i en mengde kontoer brukeren må håndtere i stor grad legges på brukeren. I så stor grad at det hindrer brukere uten spesielle behov å ha kontroll. Dette er en kostnad som må tas med i regnestykket. Allikevel virker det ikke som om det er et stort nok problem for at brukerne kommer til

å kreve andre løsninger med det første. Dette kan ha en sammenheng med at brukerne klarer å håndtere de mest brukte kontoene godt. Om det er manglende forskning som er årsaken til manglende interesse fra organiasjonene og manglende fokus hos myndighetene eller om det er omvendt har ikke vært en målsetting å si noe om. Men at noe må gjøres for at vi skal se tilgjengelige og inkluderende løsninger komme er helt sikkert. Det må mer forskning til, det må legges press på politikerne fra interesseorganisasjonene og de statlige institusjonene må arbeide med problemstillingen.

7.2 Universell utforming og autentisering

7.2.1 Universell utforming

Jeg skrev at jeg ønsket å finne ut av hva som ligger i begrepet universell utforming. Hva krever en løsning med tanke på brukeropplevelse og tilgjengelighet?

Hva en legger i begrepet universell utforming er ikke et eget diskusjonstema i oppgaven. Begrepet er enkelt og tydelig og kommer godt frem i teorikapittelet. Men i møtet med brukerautentisering har jeg identifisert en problemstilling som må håndteres av et tilgjengelig system.

Funnene mine viser at alle jeg har vært i kontakt med opplever problemer med håndtering av brukernavn og passord. Men det er ikke bare det å huske passord som er problemet, selv om det ofte i litteraturen blir omtalt som en allmenningens tragedie og «password fatigue» er det kombinasjonen mellom brukernavn, passord og kontoer intervjuobjektene opplever som problemet. Å få disse tre til å stemme oppleves ikke som noe problem for de kontoene de bruker ofte. Problemet er de kontoene som brukes sjeldnere. Jeg hevder ikke at det er feil å skylde på passord eller bruke begreper i den retning, men brukeren opplever dette ikke bare som et passordproblem og da kan det være mer presist å se på de tre sammen.

Jeg tøyde GAP-modell metaforen for å vise at det disse brukerne opplever kan forstås som en funksjonshemning. Men det kan også, og gjerne heller, forstås som et handlingsgap. Ikke overraskende ligger utfordringen til brukere uten spesielle behov først og fremst i antallet kontoer, brukernavn og passord de må håndtere. Dette problemet antar jeg gjelder uavhengig av hvilke behov eller funksjonsnedsettinger brukeren ellers har. Derfor må universell utforming i møte med brukerautentisering håndtere denne utfordringen og løsningen må ta høyde for summen og ikke bare enkeltdelene for å kunne være tilgjengelig og inkluderende.

Vi ser at autentiseringsløsninger er noe som kan stenge personer helt ute fra tjenester, enten det er bank, offentlige tjenester eller sosial kommunikasjon. Derfor er det viktig at slike løsninger så langt det er mulig lar personer få tilgang til disse tjenestene. Stabil utforming er helt sentralt for å minske kravet som settes til brukere om å lære og huske nye ting. Stadige forandringer i design og metaforer kan stenge brukere ute fra løsningen og gjøre den utilgjengelig for dem. Et forslag er å «fryse løsningen» å beholde grensesnittet likt så lenge som mulig for personer

som har kognitive utfordringer.

Det er kjent at designkonvensjoner og terminologi er viktig for å inkludere brukeren. Jeg diskuterer her at disse må sees på i et historisk perspektiv hvor det til enhver tid vil være personer som ikke lenger tilegner seg nye konvensjoner eller terminologi. På grunn av dette vil det være forskjell på universelt utformede konvensjoner og terminologi og på nyere designkonvensjoner og terminologi.

Når det kommer til universell utforming har jeg ikke diskutert begrepet direkte. Men i hele oppgaven har jeg lagt til grunn at det å designe for alle også inkluderer de brukerne som har høyest krav til brukeropplevelse. Funnene i oppgaven er ikke noe bevis på det. Men ved å hevde dette har jeg indirekte diskutert begrepet universell utforming og antydet at universell utforming er mer enn beslektet med brukeropplevelse. Det er to begreper som henger uløselig sammen. For kommersielle tjenester som ikke oppererer i et monopol er det åpenbart at brukeropplevelsen er et konkurransefortrinn i kampen om brukerne.

7.2.2 Brukeropplevelse

En god brukeropplevelse er avhengig av at brukeren føler seg trygg. Vi ser at trygghetsfølelsen ikke nødvendigvis trenger å være samstemt med risikoen brukeren faktisk tar. Vi kan bruke ulike virkemidler for å få brukerens følelse av trygghet til å bli god. Funnene mine tyder på at avsender og antall sikkerhetsledd har en viktig betydning for brukerens trygghetsfølelse. Også kjente metaforer for sikkerhet føles tryggere enn nye og ukjente metaforer.

For at brukeren ikke bare skal føle seg trygg men også ta riktige sikkerhetskompromisser kan vi utnytte virkemidlene nevnt ovenfor med sikkerhetsteater. I sikkerhetsteater får en brukeren til å føle seg mer eller mindre trygg alt etter hva en er ute etter å oppnå. Man gjør dette gjennom å utnytte brukerens persepsjon av sikkerhet.

Selv om vi står overfor en utfordring når det gjelder antall kontoer, passord og brukernavn en vanlig person må forholde seg til er det fra dag til dag ikke dette brukeren opplever. De mest brukte kontoene har de god kontroll på og der fungerer B/P metaforen godt og i stor grad problemfritt. Dette setter høye krav til nye systemer som foreslås å erstatte B/P metaforen. I testen av LastPass kommer det frem at brukeren ikke bare sammenligner hvordan det er å håndtere alle passord og brukernavn, han sammenligner også de få kontoene han håndterer godt til vanlig. Og for disse kontoene er det mer tungvindt med LastPass. Alternative systemer må være mer effektive, mer fleksible og lettere å bruke for at brukeren skal ønske å gå over fra B/P til et alternativ.

Sikkerhetsløsninger blir komplekse, spesielt dersom man skal håndtere alle brukerens krav til fleksibilitet. Mye av denne kompleksiteten må skjules for å gjøre systemet enkelt nok å bruke. Men dersom vi skjuler for mye av systemet vil brukeren ikke være i stand til å ta de riktige sikkerhetskompromissene og vi kan risikere at han omgår hele systemet. Det er vanskelig å få til en god ballanse mellom psykologisk akseptabilitet

og konfigurasjon og bruk av systemet. Konfigurasjon av systemet er vanskelig å håndtere på en måte som gjør systemet lett å bruke og samtidig sikkert og uten svakheter.

Jeg har foreslått en konseptuell modell for hvordan brukere kan ta valg om sikkerhet og hva som påvirker valget (se figur 6.2 på side 109). Det er en skisse som må videreutvikles men som kan fungere som et innspill på hvordan man kan automatisere konfigurasjonen av systemet og samtidig hjelpe brukeren å ta de riktige valgene.

7.2.3 Sikkerhet

Jeg har diskutert og kommet frem til at stedet du er og konteksten du er i kan og bør være en del av autentiseringsmekanismene. Det er et konsept intervjuobjektene allerede har et forhold til og benytter seg av mer eller mindre bevisst. Fysisk tilgang til enheter er et eksempel på hvordan personer regulerer andres tilgang til noe. I denne oppgaven er *stedet du er* tatt med som en egen autentiseringsmekanisme utover de tre klassiske *noe du har, noe du er og noe du kan*.

Ut i fra funnene mine er det åpenbart også for brukerne at det må eksistere ulike sikkerhetsnivåer. Hvilket nivå som passer til de ulike tjenestene og enhetene er en subjektiv avgjørelse. Et krav trer tydelig frem og det er at enheter og tjenester bør være mulig å låne bort. Enten det gjelder å få noen til å handle dagligvarer for seg eller utlån av datamaskin er det behov for en form for gjestekonto med begrenset tilgang.

I tabell 6.1 på side 114 foreslår jeg at vi bør holde oss til fire nivåer for sikkerhet når vi henvender oss til brukeren. Det laveste nivået, nivå 0 er et nivå for identifisering, ikke autentisering. De tre nivåene over representerer økende grad av sikkerhet. Dette vil gjøre det enklere å forklare for brukeren de metaforene som brukes, det er foreslått en viss sammenheng mellom antall autentiseringsfaktorer og nivå, for eksempel vil en to-faktor løsning ligge på nivå to. Dette tror jeg vil være enklere for brukeren å forstå. Dette er hva brukeren ser og opplever i forgrunnen, hva som skjer i bakgrunnen av systemt for å opprettholde sikkerheten er i denne sammenheng ikke vurdert.

Gjennoppretting av konto og en B-plan for tilgang til tjenester er viktig og her gjenstår mye arbeid. Dersom en skal baserer seg på fysiske tokens for tilgang til virtuelle tjenester må man ha et system som ikke stenger brukeren ute helt dersom tokenet mistes. Muligheten for gjennoppretting må ikke føre til svakheter i systemet.

7.2.4 Retningslinjer for universelt utformede autentiseringsløsninger

Basert på diskusjonen rundt rammevilkår, universell utforming, brukeropplevelse og sikkerhet kommer jeg med 19 forslag til retningslinjer for tilgjengelige autentiseringsløsninger. Mange av disse er som diskusjonen forøvrig en presisering av eksisterende generele retningslinjer.

Jeg konkluderer også med at man når man kommer med nye forslag til autentiseringsløsninger må ha et rammeverk for å sammenligne det nye

forslaget med allerede eksisterende løsninger og eksisterende forslag for å finne styrker og svakheter. Jeg viser til et rammeverk som kan brukes til dette formålet, men er åpen for andre forslag.

7.3 Nærhetsbasert autentisering

Nærhetsbasert autentisering går ut i fra autentiseringsmekanismen *noe du har*. Det er noe du har på deg som kommuniserer trådløst og uten direkte kontakt med noe annet. Forventningene til en slik løsning er at autentiseringen skal skje i bakgrunnen og automatisk uten å avbryte den oppgaven brukeren skal få utført. Siden et er kontaktløst settes det ikke de samme kravene til nøyaktighet fra brukeren for å plassere det man har i en lås eller kortleser. Dette er kanskje spesielt interessant for de med motoriske og sensoriske funksjonsnedsettinger. Også overgangen fra det tradisjonelle skjerm, tastatur og mus grensesnittet vi har levd med så lenge datamaskinen har vært allemannseie til touchgrenseflater og enheter helt uten grafiske brukergrensesnitt er relevant med tanke på nærhetsbasert autentisering. Men dersom hver enhet og hver tjeneste skal ha sitt eget token brukeren må bære for å få tilgang overfører man bare problemet fra en allmenningens tragedie på hukommelsen til en allmenningens tragedie på lommene.

Derfor diskuterer jeg hvor vidt man kan ha én enhet som brukes til å autentisere brukeren opp i mot andre tjenester og enheter. Dette kan ligne noe på Singel Sign-On løsninger. Problemet er å håndtere ulike sikkerhetsnivåer, stedet du er, kontekst og en rekke andre faktorer som må konfigurereres. Kompleksiteten i et slikt system kan føre til at systemet blir enten ubrukelig eller usikkert, ikke usannsynlig begge deler. Men det ligger en forventning om at det kan være mulig å løse. Denne oppgaven gir ikke svaret på hvordan man kan løse det og det virker nær sagt umulig. Men jeg tror det er mulig å løse disse utfordringene. Og kanskje har denne oppgaven vært et lite skritt på veien for å identifisere hvilke problemstillinger et slikt system må håndtere.

7.4 Fremtidig forskning og veien videre

Det er vanlig å foreslå hvilke problemstillinger jeg har støtt på som kan være interessante å se på for andre. Med fare for å overdrive hvor viktig problemstillingen rundt tilgjengelige autentiseringsløsnigner er og i hvor stor grad jeg har klart å peke på det som er sentrale utfordringer og ikke bare perifære utfordringer i denne oppgaven, nesten hvert eneste tema jeg har vært borti ville vært interessant å undersøke nærmere og analysere hver for seg. Innenfor de temaene jeg har berørt bør det være interessante problemstillinger uansett hvilke fagfelt du kommer fra. Du kan undersøke nærmere hvordan politikerne forholder seg til problemstillingen og stille spørsmål med hvorfor forskriften til DTL ikke er kommet etter så lang tid. Er det politisk betinget eller har det andre årsaker? Hvorfor er interessen fra interesseorganisasjonene tilsynelatende så lav på et område som i praksis

kan stenge medlemmene deres ute fra å fungere i det digitale samfunnet? Man kan grave seg dypt inn i hvordan rammevilkårene burde vært for å raskest mulig få løsninger som er tilgjengelige.

De 19 retningslinjene jeg har foreslått kan være et godt utgangspunkt for videre arbeid. Dersom man snur på hvert av disse og gjør dem om til problemstillinger eller til hypoteser har man mer arbeid og flere spørsmål enn det finnes personer som leser denne oppgaven.

En ting er helt sikkert. Nesten uansett hva en undersøker rundt temaet universell utforming og autentisering vil en ha en unik mulighet til å bidra til å øke kunnskapen rundt temaet. Forhåpentligvis er det noe som vil endre seg i løpet av den nærmeste fremtid.

Bibliografi

[1] E-me prosjektets nettsider. URL http://goo.gl/kx22Y. Besøkt 17.04.2012.

[2] Blindeforbundet tilgjengelighet, . URL http://goo.gl/kTsDd. Besøkt 09.10.2012.

[3] Steve boggan, the guardian. cracked it!, . URL http://goo.gl/WC7c5. Besøkt 05.02.2012.

[4] Om deltasenteret, . URL http://goo.gl/3uRqA. Besøkt 29.09.2012.

[5] Fn: Conventions and optional protocol signatures and ratifications, disabilities, . URL http://goo.gl/VYNyo. Besøkt 10.09.2012.

[6] Fakta om likestillings-og diskrimineringsombudet, . URL http://goo.gl/SW3x3. Besøkt 29.08.2012.

[7] Nyheter fra likestillings- og diskrimineringsombudet. «regjeringen somler», . URL http://goo.gl/GFlnA. Besøkt 06.10.2012.

[8] Lastpass, . URL http://goo.gl/P4Bcm. Besøkt 15.09.2012.

[9] Jacob nielsen, accuracy vs. insights in quantitative usability, . URL http://goo.gl/FTM4F. Besøkt 10.10.2012.

[10] Jacob nielsen, usability 101: Introduction to usability, . URL http://goo.gl/x3Hal. Besøkt 19.10.2012.

[11] Proximity, . URL http://goo.gl/A9qlC. Besøkt 15.09.2012.

[12] Nyheter fra likestillings- og diskrimineringsombudet. «frå enkeltsak til strukturendring», . URL http://goo.gl/QugwV. Besøkt 17.08.2012.

[13] Bruce tognazzini, first principles of interaction design, . URL http://goo.gl/NQyor. Besøkt 04.03.2012.

[14] Map pin software, token lock, . URL http://goo.gl/kMgfs. Besøkt 15.09.2012.

[15] Universell utforming i offentlige anskaffelser, . URL http://goo.gl/o5F4j. Besøkt 20.08.2012.

[16] Web accessibility initiative, . URL http://goo.gl/quqqd. Besøkt 11.09.2012.

[17] Web security context: User interface guidelines, . URL http://goo.gl/2DX71. Besøkt 10.09.2012.

[18] Yubikey fra yubico, . URL http://goo.gl/gmnfA. Besøkt 15.09.2012.

[19] Autopass, . URL http://goo.gl/laAIQ. 27.01.2012.

[20] Computer world: Slik gikk telenors test, . URL http://goo.gl/VgzPf. Besøkt 27.01.2012.

[21] Computer world: Her betaler de med nfc i dag, . URL http://goo.gl/Cszow. Besøkt 27.01.2012.

[22] Norsk senter for informasjonssikring (norsis) leksikon, . URL norsis.no/leksikon. Besøkt 24.10.2012.

[23] Skidata.no, . URL http://goo.gl/y70Mr. Besøkt 27.01.2012.

[24] Diskriminerings- og tilgjengelighetsloven §11 lovdata.no. URL http://goo.gl/y7cCf. Besøkt 17.04.2012.

[25] NOU 2001:22 Fra bruker til borger, 2001. Tilgjengelig fra http://goo.gl/iz8aw.

[26] St.meld. nr. 40 (2002–2003) Nedbygging av funksjonshemmende barrierer, 2002.

[27] NOU 2005:8 Likeverd og tilgjengelighet. Tilgjengelig fra http://goo.gl/FdePl, 2005.

[28] St.meld. nr. 17 (2006–2007) Eit informasjonssamfunn for alle. Tilgjengelig fra http://goo.gl/H3tWD, 2006.

[29] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, December 1999. ISSN 0001-0782.

[30] Dirk Balfanz, Richard Chow, Ori Eisen, Markus Jakobsson, Steve Kirsch, Scott Matsumoto, Jesus Molina, and Paul van Oorschot. The future of authentication. *Security Privacy, IEEE*, 10(1):22 –27, jan.-feb. 2012. ISSN 1540-7993.

[31] E. Bardram. The trouble with login: on usability and computer security in ubiquitous computing. *Personal Ubiquitous Comput.*, 9:357–367, November 2005. ISSN 1617-4909.

[32] Jakob Bardram, Rasmus Kjær, and Michael Pedersen. Context-aware user authentication – supporting proximity-based login in pervasive computing. In Anind Dey, Albrecht Schmidt, and Joseph McCarthy, editors, *UbiComp 2003: Ubiquitous Computing*, volume 2864 of *Lecture Notes in Computer Science*, pages 107–123. Springer Berlin / Heidelberg, 2003.

[33] Genevieve Bell and Paul Dourish. Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. *Personal and Ubiquitous Computing*, 11(2):133–143, November 2007. ISSN 1617-4909.

[34] Joseph Bonneau and S Preibusch. The password thicket: technical and market failures in human authentication on the web. *Proc.(online) of WEIS*, 2010.

[35] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, 2012:553–567, May 2012.

[36] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes. Technical Report UCAM-CL-TR-817, University of Cambridge, Computer Laboratory, March 2012. URL http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf.

[37] Joseph Bonneau, Sören Preibusch, and Ross Anderson. A birthday present every eleven wallets? the security of customer-chosen banking PINs. In Angelos D. Keromytis, editor, *FC 2012, 16th International Conference on Financial Cryptography.*, Lecture Notes in Computer Science, Heidelberg, Germany, March 2012. Springer-Verlag. URL http://www.cl.cam.ac.uk/~{}jcb82/doc/BPA12-FC-banking_pin_security.pdf.

[38] Mark D. Corner and Brian D. Noble. Zero-interaction authentication. In *Proceedings of the 8th annual international conference on Mobile computing and networking*, MobiCom '02, pages 1–11, New York, NY, USA, 2002. ACM. ISBN 1-58113-486-X.

[39] Lorrie Faith Cranor and Simson Garfinkel, editors. *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, illustrated edition edition, 2005. ISBN 0596008279.

[40] Hans Joachim Desserud. Mange veier inn - en studie av alternative innloggingsmekanismer. Master thesis, Universitetet i Oslo, 2011.

[41] *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor*. Det kongelige fornyings og administrasjonsdepartement, april 2008.

[42] Ivan Flechais, M. Angela Sasse, and Stephen M. V. Hailes. Bringing security home: a process for developing secure and usable systems. In *Proceedings of the 2003 workshop on New security paradigms*, NSPW '03, pages 49–57, New York, NY, USA, 2003. ACM. ISBN 1-58113-880-6.

[43] B. Flyvbjerg. Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, 12(2):219–245, April 2006. ISSN 1077-8004.

[44] Lothar Fritsch. Utprøving av buypass e-id og altinn.no resultat av smartkort-studie i e-me prosjekt. Prosjektinternt notat fra E-me prosjektet., april 2011.

[45] Lothar Fritsch, Kristin Skeide Fuglerud, and Ivar Solheim. Towards inclusive identity management. *Identity in the Information Society*, 3(3): 515–538, October 2010. ISSN 1876-0678.

[46] Kristin S. Fuglerud, Lothar Fritsch, and Ø ystein Dale. Universell utforming av IKT-baserte løsninger for registrering og autentisering. Technical report, Norsk Regnesentral, 2009.

[47] Kristin Skeide Fuglerud. The challenge of diversity in universal design of ict. Upublisert artikkel, juni 2012.

[48] Kristin Skeide Fuglerud. Accessibility of registration and authentication. Presentasjon på E-me seminar. Tilgjengelig fra http://goo.gl/FMek0, Mars 2012.

[49] Kristin Skeide Fuglerud. Foreløpige resultater fra e-me prosjektet. E-post, september 2012.

[50] KS Fuglerud and TH Røssvoll. Previous and Related Research on Usability and Accessibility Issues of Personal Identification Management Systems. 2010.

[51] P Gutmann and I Grigg. Security usability. *Security & Privacy, IEEE*, 3(4):56–58, 2005. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1492344.

[52] Garrett Hardin. The Tragedy of the Commons. *Science*, 162(3859): 1243–1248, December 1968. ISSN 1095-9203. doi: 10.1126/science.162.3859.1243. URL http://dx.doi.org/10.1126/science.162.3859.1243.

[53] C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. *Security Privacy, IEEE*, 10(1):28 –36, jan.-feb. 2012. ISSN 1540-7993.

[54] R. Hulsebosch, M. Bargh, G. Lenzini, P. Ebben, and S. Iacob. Context sensitive adaptive authentication. In Gerd Kortuem, Joe Finney, Rodger Lea, and Vasughi Sundramoorthy, editors, *Smart Sensing and Context*, volume 4793 of *Lecture Notes in Computer Science*, pages 93–109. Springer Berlin / Heidelberg, 2007. ISBN 978-3-540-75695-8.

[55] A.K. Jain, P. Flynn, and A.A. Ross, editors. *Handbook of Biometrics*. Springer, 2008. ISBN 9780387710402.

[56] H.K. Klein and M.D. Myers. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS quarterly*, 23(1):67–93, 1999.

[57] Henning Klevjer. Invention disclosure: Automatic authentication with never-present user credentials. Iternt dokument for Lucidman prosjektet, April 2012.

[58] Jonathan Lazar, Jinjuan Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Wiley, 1 edition, 2010. ISBN 0470723378.

[59] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer professional computing. Springer, 2009. ISBN 9781848822535.

[60] Geraint Price Marcelo Carlomagno Carlos. Understanding the weaknesses of human-protocol interaction. Financial Cryptography and Data Security 2012. International Financial Cryptography Association, 2012.

[61] Miljøverndepartementet. Universell utforming begrepsavklaring. PDF på web, http://goo.gl/KO6Bl, August 2012.

[62] M.D. Myers. Qualitative Research in Information Systems. *MIS quarterly*, 2:241–242, June 1997. MISQ Discovery, archival version, June 1997, http://www.misq.org/supplements/. Association for Information Systems (AISWorld) Section on Qualitative Research in Information Systems, updated version, last modified: September 5, 2012 www.qual.auckland.ac.nz.

[63] Anthony J. Nicholson, Mark D. Corner, and Brian D. Noble. Mobile device security using transient authentication. *IEEE Transactions on Mobile Computing*, 5(11):1489–1502, November 2006.

[64] Brian D. Noble and Mark D. Corner. The case for transient authentication. In *Proceedings of the 10th workshop on ACM SIGOPS European workshop*, EW 10, pages 24–29, New York, NY, USA, 2002. ACM.

[65] Donald Norman. *The design of everyday things*. Basic Books, 2002. ISBN 0465067107.

[66] Donald Norman. *Emotional Design: Why We Love (or Hate) Everyday Things*. Basic Books, 1 edition, 2005. ISBN 0465051367.

[67] Donald A. Norman. The way i see it: When security gets in the way. *interactions*, 16:60–63, November 2009. ISSN 1072-5520.

[68] Donald A. Norman. Natural user interfaces are not natural. *interactions*, 17(3):6–10, May 2010. ISSN 1072-5520. doi: 10.1145/1744161.1744163.

[69] Maryke Silalahi Nuth. Legal considerations for inclusive identity management system in new social media. PDF på web, Måned 2012. Tilgjengelig fra http://goo.gl/b5HkP.

[70] Barne og likestillingsdepartementet. Norge universelt utformet 2025 regjeringens handlingsplan for universell utforming og økt tilgjengelighet 2009-2013. PDF på web, 2009. Tilgjengelig fra http://goo.gl/vAX9j.

[71] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, dec 2003.

[72] S. Ojala, J. Keinanen, and J. Skytta. Wearable authentication device for transparent login in nomadic applications environment. In *Signals, Circuits and Systems, 2008. SCS 2008. 2nd International Conference on*, pages 1 –6, nov. 2008.

[73] Ø ystein Pettersen. *Inclusive identity management A case study*. Master thesis, Universitetet i Oslo, 2011.

[74] Graham Pullin. *Design Meets Disability*, volume 1. MIT press, 2011.

[75] Frode Eika Sandnes. *Universell utforming av IKT-systemer: Brukergrensesnitt for alle*, volume 1. Universitetsforlaget, 2011.

[76] Bruce Schneier. The psychology of security, Februar 2008. URL http://goo.gl/qVFqc. Besøkt 10.08.2012.

[77] E.Eugene Schultz. *Handbook of Human Factors and Ergonomics*, chapter Human-computer Interaction. Human factors and ergonomics. John Wiley & Sons, 3rd edition, 2006. ISBN 9780471449171.

[78] Helen Sharp, Yvonne Rogers, and Jenny Preece. *Interaction Design: Beyond Human Computer Interaction*. John Wiley & Sons, 2007. ISBN 0470018666.

[79] Frank Stajano. Pico: no more passwords! In *Proceedings of the 19th international conference on Security Protocols*, SP'11, pages 49–81, Berlin, Heidelberg, 2011. Springer-Verlag. ISBN 978-3-642-25866-4.

[80] Robert E. Stake. *The SAGE handbook of qualitative research*, chapter 17 Qualitative Case Studies, pages 443–463. Sage Publications, 3rd edition, 2005. ISBN 0761927573.

[81] Siri Bergman Stølen. The first meeting: Authentication on touch phones. Master's thesis, Universitetet i Oslo, mai 2012.

[82] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. What makes users refuse web single sign-on?: an empirical investigation of openid. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 4:1–4:20, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0911-0.

[83] Ewa Syta, Stan Kurkovsky, and Bernardo Casano. Rfid-based authentication middleware for mobile devices. In *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences*, HICSS

'10, pages 1–10, Washington, DC, USA, 2010. IEEE Computer Society. ISBN 978-0-7695-3869-3.

[84] Eli Toftøy-Andersen and Jon Gunnar Wold. *Praktisk brukertesting*. Cappelen Damm Akademisk, 1. utgave, 1. opplag edition, 2011.

[85] North Carolina State University. The principles of universal design. URL http://goo.gl/VkFel. Besøkt 04.03.2012.

[86] Catherine S. Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers*, 22 (3):153–164, May 2010. ISSN 09535438.

[87] Mark Weiser. The computer for the 21st century. *Scientific American*, 3 (3):3–11, 1991.

[88] Anders Wiehe and Torkjel Søndrol. Attacking fingerprint sensors. Studentoppgave. Tilgjengelig fra http://goo.gl/LLXEY. Besøkt 11.10.2012, 2004.

[89] Sandy L Zabell. Fingerprint evidence in England and Wales–the revised standard. *Journal of law and policy*, 13(1):143–179, January 2005. ISSN 0025-8024. URL http://wwy.brooklaw.edu/students/journals/bjlp/jlp13i_zabell.pdf.

Tillegg A

Samtykkeærklæring

Forespørsel om å delta i et intervju i forbindelse med en masteroppgave

Informasjonsskriv

Jeg er masterstudent i informatikk ved Universitetet i Oslo og jobber nå med den avsluttende masteroppgaven. Temaet for oppgaven er universelt utformet autentisering på mobile enheter. Jeg ønsker å undersøke hvordan vi kan lage universelt utformede autentiseringsløsninger til bruk på mobile enheter.

I den forbindelse ønsker jeg både å finne ut av holdninger til datasikkerhet og mobil datasikkerhet. Holdninger til sikkerhet på fysiske eiendeler så som bil, visakort med mer. Og jeg ønsker å få testet en prototype på nærhetsbasert, situasjonsbestemt og fleksibel autentisering. Dette vil jeg gjøre gjennom intervjuer, observasjoner og spørreskjema.

Jeg ønsker å bruke lydopptak og ta notater mens vi snakker sammen, men det er ikke noe krav.

Det er frivillig å være med og du har mulighet til å trekke deg når som helst underveis, uten å måtte begrunne dette nærmere. Dersom du trekker deg vil alle innsamlede data om deg bli anonymisert. Opplysningene vil bli behandlet konfidensielt, og ingen enkeltpersoner vil kunne gjenkjennes i den ferdige oppgaven. Opplysningene anonymiseres og opptakene slettes når oppgaven er ferdig, senest innen utgangen av 2013.

Dersom det er noe du lurer på kan du ringe meg på 47623114 eler sende e-post til olanb@ifi.uio.no. Du kan også kontakte min veileder Jo Herstad ved institutt for informatikk på telefon 22840051 eller på e-post johe@ifi.uio.no.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste (NSD).

Med vennlig hilsen
Ola Njå Bertelsen
Stemholen 16
4025 Stavanger

Samtykkeerklæring

Jeg har mottatt skriftlig informasjon og er villig til å delta i studien.

Signatur …….Telefonnummer ……..

Tillegg B

Intervjuguide

Versjon: tirsdag 14. august 2012

Tematisk intervjuguide bruker

Innledende for «oppvarming»

Informasjon om studiet, hva jeg ønsker å finne ut av med mer. Ikke vær redd for å si for mye om passord og slikt ingenting som kan være risikabelt å skrive om vil bli skrevet i oppgaven.

GAP-modellen og universell utforming.

Autentisering, noe man har, noe man kan, noe man er.
En-faktor og to-faktor autentisering.

Forhold til teknologi

- Hvilke typer digitale enheter har du eller bruker du jevnlig (bærbare og mobile)?
- Om jeg sier brukernavn og passord hva tenker du da?
- Hvilke tjenester bruker du på datamaskinen som krever en form for innlogging eller autentisering?

  (denne listen brukes senere til klasifisering)?
- Hvilke tjenester bruker du på mobil/nettbrett som krever en form for innlogging eller

  autentisering? (denne listen brukes senere til klasifisering)?
- Hvordan vil du beskrive ditt forhold til teknologi?
  - Er du positiv og tar i bruk det nyeste eller har du et avslappet forhold til det og bruker det

    som fungerer?

Versjon: tirsdag 14. august 2012

Forhold til datasikkerhet

- Hva tenker du når du hører datasikkerhet?
- Er opplysninger og informasjon du har på enhetene dine sikre?
- Mentale modeller for sikkerhet og risiko
    - Fortell litt om hvordan du opplever risikoen for å miste data og informasjon.
    - Hvordan opplever du at disse tingene er sikret i dag?
- Følelsen av sensitive opplysninger
    - Personlige opplysninger hva er farlig at andre får vite?
    - Hvordan forholder du deg til slike opplysninger når du bruker digitale tjenester?
- Forhold til passord og PIN koder
    - Når du mister eller glemmer passord og PIN hva gjør du i dag og hva bør skje?
    - Hvordan forholder du deg til forskjellige passord, PIN-koder og brukernavn?
- Sammenligning av sikkerhet mellom fysisk og virtuelle eiendeler og tjenester.
    - E-post, nettbank, visakort, bolig, bilder, facebook, sms, mobil.

Versjon: tirsdag 14. august 2012

Brukertesten

1. *Finn et sted i hjemmet hvor det er sansynlig at avstanden til laptopen kan bli stor nok.*
2. *Start lydopptak i nærheten av laptop.*
3. *Ta opp laptopen og start den.*
4. Vis hvordan innlogging vanligvis fungerer (som på en vanlig maskin).
5. *Token Lock skal allerede være startet, ellers må det startes.*
6. *Sjekk at mobil og laptop er paret via BT. og at tokenlock har signalet.*
7. Vis ikonet til tokenlock
8. Forklar hvordan det fungerer. Demonstrer en gang når tester sitter foran laptop.
9. Få tester til å bevege seg utenfor rekkevidde slik at maskinen slås av.
10. Gå tilbake mot maskinen slik at den låses opp.
11. Gjenta en gang dersom det føles nødvendig.
12. Få tilbakemeldinger se egen liste med spørsmål

Spørsmål etter testing

- Hva synes du?
- Hvordan oppleves det?
- Er det noe du kan tenke deg å bruke?
- Hva skal til for at du skal bruke det?
- Hva tenker du om en slik teknologi på andre steder enn bare på laptopen om du ikke tenker på sikkerheten i det?
    - Hus, bil, visakort, nettjenester som e-post, facebook?
    - Hva om det ikke var mobilen, hva kunne det vært for en token du har som gir tilgang til alt?
        - Hadde det vært bedre om det ikke var mobilen?
- Dersom du mister mobilen eller tokenet, hva bør skje da?
- Scenarier:
    - Noen skal låne huset ditt hvordan kan de få tilgang til det da?
    - eller laptopen,
    - eller bilen,
    - eller visakortet
    - eller mobilen (SMS, ringing).

Versjon: tirsdag 14. august 2012

Enheter som brukes jevnelig og tjenester som krever innlogging.

Digitale enheter	Tjenester på maskin	Tjenester på mobile enh.

Versjon: tirsdag 14. august 2012

	Risikonivå 1 ingen	Risikonivå 2 liten	Risikonivå 3 moderat	Risikonivå 4 stor
Konsekvenser for liv eller helse	Det kan ikke forekomme fare for tap av liv og/eller helseskader	Det kan forekomme mindre helseskader	Det kan forekomme mindre helseskader	Det kan forekomme tap av liv og/eller store helseskader
Økonoisk tap/økte kostnader	Intet økonomiske tap/merarbeid/økte kostnader	Det kan føre til et mindre økonomisk tap/merarbeid/økte kostnader	Brudd kan føre til moderat økonomisk tap/merarbeid/økte kostnader	Brudd kan medføre store økonomiske tap/merarbeid/økte kostnader
Tap av renommé (anseelse, tillit og integritet)	Ingen skade på renommé	Eventuelle skader på renommé anses bagatellmessige	Renommé kan bli noe svekket i et kortere tidsrom	Renommé kan bli svekket i et lengre tidsrom, eventuelt varig
Bryderi/ ulempe	Ingen ulempe eller bryderi	Det kan forekomme noe ulempe eller bryderi	Ikke relevant	Ikke relevant
Hindring i straffe-forfølgelse	Ingen bidrag til hindring av straffeforfølging	minimalt bidrag til hindring av straffeforfølging	moderat bidrag til hindring av straffeforfølging	det kan forekomme hindringer i straffeforfølging
Uaktsomt bidrag til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	det kan ikke forekomme uaktsom bistand til lovbrudd	det kan ikke forekomme uaktsom bistand til lovbrudd	Brudd kan bidra til uaktdsom bistand til lovbrudd

Versjon: tirsdag 14. august 2012

	Risikonivå 1 ingen	Risikonivå 2 liten	Risikonivå 3 moderat	Risikonivå 4 stor
Konsekvenser for liv eller helse	Det kan ikke forekomme fare for tap av liv og/eller helseskader	Det kan forekomme mindre helseskader	Det kan forekomme mindre helseskader	Det kan forekomme tap av liv og/eller store helseskader
Kommentar				
Økonoisk tap/økte kostnader	Intet økonomiske tap/ merarbeid/økte kostnader	Det kan føre til et mindre økonomisk tap/ merarbeid/økte kostnader	Brudd kan føre til moderat økonomisk tap/merarbeid/økte kostnader	Brudd kan medføre store økonomiske tap/ merarbeid/økte kostnader
Kommentar				
Tap av renommé (anseelse, tillit og integritet)	Ingen skade på renommé	Eventuelle skader på renommé anses bagatellmessige	Renommé kan bli noe svekket i et kortere tidsrom	Renommé kan bli svekket i et lengre tidsrom, eventuelt varig
Kommentar				
Bryderi/ ulempe	Ingen ulempe eller bryderi	Det kan forekomme noe ulempe eller bryderi	Ikke relevant	Ikke relevant
Kommentar				
Hindring i straffe-forfølgelse	Ingen bidrag til hindring av straffeforfølging	minimalt bidrag til hindring av straffeforfølging	moderat bidrag til hindring av straffeforfølging	det kan forekomme hindringer i straffeforfølging
Kommentar				
Uaktsomt bidrag til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	det kan ikke forekomme uaktsom bistand til lovbrudd	det kan ikke forekomme uaktsom bistand til lovbrudd	Brudd kan bidra til uaktdsom bistand til lovbrudd
Kommentar				

Versjon: tirsdag 14. august 2012

Risikonivå 1	Risikonivå 2	Risikonivå 3	Risikonivå 4