

Universell utforming av IKT-baserte løsninger for registrering og autentisering

Resultater fra forprosjekt

Rapportnr

DART/02/09

Forfattere

**Kristin Skeide Fuglerud, Arthur Reinertsen
Lothar Fritsch, Øystein Dale**

Dato

31. januar 2009

ISBN

ISBN-13 978-82-539-0531-0

Norsk Regnesentral

Norsk Regnesentral (NR) er en privat, uavhengig stiftelse som utfører oppdragsforskning for bedrifter og det offentlige i det norske og internasjonale markedet. NR ble etablert i 1952 og har kontorer i Informatikkbygningen ved Universitetet i Oslo. NR driver anvendt forskning innen statistikk og informasjons- og kommunikasjonsteknologi. Innen statistikk jobbes det med svært mange forskjellige problemstillinger slik som estimering av torskbestand, finansiell risiko, beskrivelse av geologien i petroleumsreservoarer og overvåking av klimaendringer. Innen IKT jobbes det med problemstillinger knyttet til bruk av IKT i samfunns- og næringsliv. For eksempel sikkerhet og personvern, IKT-støtte til læring i skole og næringsliv, multimedia på forskjellige plattformer, universell utforming samt tilrettelegging av IKT for funksjonshemmede. NRs visjon er forskningsresultater som brukes og synes.

Tittel	Universell utforming av IKT-baserte løsninger for registrering og autentisering: Resultater fra forprosjekt
Forfattere	Kristin Skeide Fuglerud, Arthur Reinertsen Lothar Fritsch og Øystein Dale
Dato	31. januar
År	2009
ISBN	ISBN-13 978-82-539-0531-0
Rapportnummer	DART/02/09

Sammendrag

For å kunne bruke elektroniske tjenester må man ofte gjennom ulike sikkerhetsprosedyrer. Brukernes behov for enkle og tilgjengelige løsninger har ofte kommet i skyggen for behovet for teknisk og logisk sikre løsninger. Dette kan føre til at mange brukere blir utestengt allerede ved innloggingen.

Forprosjektet har studert ulike utfordringer knyttet til universell utforming og tilgjengelighet i deltakernes løsninger for pålogging. Det er gjennomført brukertester av en prototype for pålogging til Storebrand nettbank med autentisering med tale via mobil. Denne prototypen ble utviklet i forprosjektet. Prosjektet har også sett på brukervennlighets- og tilgjengelighetsutfordringer ved pålogging til to offentlige tjenester, Altinn og MinID. 5 synshemmede og 5 dyslektikere var med på brukertestene. I tillegg er det gjort en analyse av henvendelser til brukerstøtte for tjenestene. Det pekes på en del konkrete utfordringer og behov for videre arbeid.

Det er også gjennomført en kartlegging av utfordringer for personer med nedsatt funksjonsevne ved bruk av en ulike autentiserings- og registreringsløsninger. Her påpekes en rekke utfordringer. Videre diskuteres problemstillinger når det gjelder tilgjengelighet i forhold til sikkerhet og personvern.

Forprosjektet mener at det er gjort lite forskning på området, peker på noen konkrete problemstillinger hvor det er behov for videre arbeid og forskning. Det er gjennomført en workshop og forprosjektet utarbeidet et forslag til et hovedprosjekt. Søknad om støtte til dette ble sendt til Verdikt programmet i Norges forskningsråd 15. okt. 2008.

Emneord	digital inkludering, tilgjengelighet til IKT, brukervennlighet, universell utforming, autentisering, IDM, sikkerhet synshemmede, dyslektikere
Målgruppe	Alle
Tilgjengelighet	Åpen
Prosjektnummer	191944/I40
Satsningsfelt	Digital inkludering, universell utforming av IKT
Antall sider	60
© Copyright	Norsk Regnesentral

English Summary

Currently a large number of public and private services are made fully automatic. Examples are ticket systems, ATMs, web-shops, and public services on net. In order to use electronic services the user must be authenticated and their user accounts must be managed. A basic requirement is therefore that authentication and identity management methods can be used by a broad range of users, with different skills, at different age and various (dis)abilities – ideally by all possible users. Common authentication methods include passwords and PINs, tokens and smart-cards, and use of third party channels such as one-time codes transmitted to cell phones.

This half year project has studied usability and accessibility aspects of various security mechanisms. The project has performed a short literature review, interviews with the help desk of a large Norwegian public service, analysis of help desk calls and interviews and user tests with five visually impaired users and five dyslectic users. The project found that there has been done relatively little research on accessible security mechanisms. Some examples of security mechanisms specifically designed to be accessible for various user groups is identified and presented in this report.

An authentication mechanism using a prototype mobile phone application was developed and tested with the ten users. The prototype mobile phone application provided both text and audio instructions to the users. Although there were some usability and accessibility issues with the prototype, the overall evaluation were positive and the conclusion is that such a mobile authentication mechanism, including audio instructions, would increase the accessibility of the Internet bank service. The test users also tried to log in to a large Norwegian e-Government service. One other public service was analyzed by an accessibility expert. The project identified several usability and accessibility challenges connected to the use of these public services.

With basis in the collected literature and empirical material, the project has identified many usability and accessibility problems with common security mechanisms. The project concludes that low usability and accessibility of security mechanisms may be a major source of exclusion from the use electronic services and a source of flaw, risk and barrier to secure and proper use. At the same time, it must be recognized that the security and privacy requirements of security mechanisms put demanding restrictions to user interface design of such systems.

More research is needed in order to be able to develop more inclusive security mechanisms. In cases where authentication methods are inaccessible for certain user groups, one should strive to provide alternative authentication methods. Is it possible to personalize the provision of authentication methods without compromising usability, security and privacy? An important research objective is to create authentications methods with *universal design*, i.e., authentication methods that can be used by as broad a range of users as possible. This may be achieved by user centred research and development, including diverse user groups, such as elderly and people with disabilities or special needs.

Key words: e-Inclusion, e-accessibility, usability, universal design, design for all, authentication, security mechanisms, identity management, visually impaired, dyslectic

Innhold

1	Innledning	9
1.1	Målsetninger	9
1.2	Prosjektets organisering og deltakere	10
2	Bakgrunn	12
3	Relatert arbeid	13
4	Undersøkelser av ulike sikkerhetsløsninger	15
5	Analyse av henvendelser til brukerstøtte ved Brønnøysundregistrene	16
5.1	Bakgrunn	16
5.2	Undersøkelse og analyse av henvendelser til ABS	17
5.3	Analyse av innloggingsproblematikk	18
5.4	Andre utfordringer knyttet til å ta i bruk en tjeneste.	19
5.5	Ulike brukergrupper – ulike utfordringer?	20
5.6	Oppsummering og konklusjoner	21
6	Intervjuer og brukertester	21
6.1	Uvalg	21
6.2	Tekniske forhold	22
6.3	Intervju- og testopplegg	22
6.4	Resultater fra brukertest	23
6.5	Pålogging til Storebrand nettbank vha. Encap's autentiseringsløsning på mobil	23
6.5.1	Installasjon av enCap sikkerhetsprogram på mobilen	23
6.5.2	Prosedyre	23
6.5.3	Advarsler og spørsmål på mobilen	25
6.5.4	Layout	27
6.5.5	Tale	27
6.5.6	Storebrand nettbank	28
6.6	Pålogging til offentlige tjenester via www.altinn.no	29
6.7	Pålogging til offentlig tjeneste via Min ID	33
6.7.1	Tilgjengelighetsaspekter ved MinID	36

6.8	Diskusjon og konklusjon fra brukertestene	37
6.8.1	Pålogging til Storebrand nettbank vha Encap mobil autentisering med tale	37
6.8.2	Altinn	37
6.8.3	MinID	37
7	Kartlegging av sikkerhetsmekanismer og utfordringer for ulike brukergrupper.....	38
7.1	Bruk av taleteknologi	39
7.2	Bilder og symboler istedenfor tall og bokstaver	41
7.3	Near field communication (NFC).....	43
7.4	Biometri	43
8	Sikkerhet og personvern.....	44
8.1	Er det mulig å lage en universelt utformet sikkerhetsløsning?	45
8.2	Klassifisering av sikkerhetsmekanismer	45
9	Oppsummering og forslag.....	46
9.1	Konklusjoner fra prosjektet.....	46
9.2	Behov forskning og videre arbeid.....	47
9.3	Hovedprosjektsøknad.....	48
10	Litteratur	48
Vedlegg A:	Guide for intervju og brukertester	51
Vedlegg B:	Informantenes erfaringer med ulike sikkerhetsløsninger ..	56

Forord

En stor takk til alle som har deltatt i prosjektet, og til de som har bidratt til å finansiere prosjektet: Programmet IT-funk i Norges forskningsråd, og de deltagende virksomhetene NR, Karde, Tellu, Encap, Storebrand, Brønnøysundregistrene, og Norge.no, Dysleksiforbundet og Norges Blindeforbund. Alle de deltakende virksomhetene og organisasjonene har bidratt med egeninnsats.

En spesiell takk til Dysleksiforbundet og Norges Blindeforbund som har bidratt med kunnskap og ved å skaffe informanter til brukertester i prosjektet, og ikke minst til de av deres medlemmer som velvillig stilte opp i undersøkelsen og delte sine erfaringer og synspunkter.

Takk også for godt samarbeid med Storebrand, Encap og Tellu som utviklet en prototype på en elektronisk autentiseringsløsning med tale for mobil og tilrettela denne for test. Det at Brønnøysundregistrene skaffet oss testkonto på www.altinn.no var også et viktig bidrag i prosjektet. Karde har spilt en nøkkelrolle i forhold til organisering og analyse.

Tusen takk også til Lars Bjørndal og Handytech som skaffet oss prøvelisens på Talks, skjermleser og tekst-til-tale programvare for mobiltelefon.

Oslo 31. januar 2009

Kristin Skeide Fuglerud

1 Innledning

For å få tilgang til en rekke elektroniske tjenester krever systemet ofte at brukeren identifiserer seg ved hjelp av koder, passord, smartkort og lignende. Det kan dreie seg om å logge seg på ulike elektroniske tjenester med brukernavn og passord, bruk av PIN koder og kort for å kunne benytte minibanker og betalingsterminaler, og andre kombinasjoner av kort og koder for å benytte nettbank, automater, døråpnere osv. Før man kan begynne å bruke tjenestene må man ofte registrere seg. Dette kan innebære at brukeren må gå gjennom en prosedyre for å få brukernavn og passord. I denne rapporten bruker vi begrepet autentisering i vid forstand om det et system gjør for å identifisere en person.

Forprosjektet tok utgangspunkt i følgende spørsmål knyttet til bruk av sikkerhetsmekanismer i elektroniske tjenester:

- Hvor egnet er ulike registrerings- og autentiseringsmekanismer for brukere med ulike former for nedsatt funksjonsevne?
- Hvordan er sikkerhet/personvern ivarettatt i praksis?
- Hvilke nye typer registrerings- og autentiseringsløsninger finnes?
- Hvordan kan personalisering og spesiell tilrettelegging utnyttes?

1.1 Målsetninger

Prosjektets hovedmålsetning var å identifisere og beskrive ulike utfordringer, suksessfaktorer og forskningsbehov knyttet til universell utforming, tilgjengelighet, sikkerhet og personvern i aktuelle sikkerhetsmekanismer for registrering og autentisering. Med bakgrunn i dette og undersøkelser av bedriftspartners sikkerhetsløsninger, ønsket vi å danne grunnlag for utvikling av et hovedprosjekt innen dette området.

Delmål:

- Kartlegge og beskrive ulike sikkerhetsløsninger for registrering og autentisering. Prosjektet skulle se på vanlige løsninger, samt nye og mindre brukte alternativer. Videre skulle vi beskrive hvilke problemer disse kan skape for personer med ulike funksjonsnedsettelse (for eksempel syn, hørsel, bevegelse, kognisjon), samt vurdere utfordringer knyttet til sikkerhet og personvern.
- Undersøke og analysere deltakerbedriftenes autentiseringsløsninger med hensyn til bruk og tilgjengelighet for ulike grupper, samt tilhørende personvern- og sikkerhetsutfordringer.
- Presentere resultater fra kartlegging og brukerundersøkelse i en workshop. I workshoppen vil deltakerbedriftenes behov for kunnskap og videre arbeid bli diskutert. Målsetningen med workshoppen vil være å etablere et grunnlag for en videreføring av arbeidet, for eksempel i form av søknad om et større forskningsprosjekt rettet mot Norges forskningsråd og/eller EU.

- Etablere et konsortium med norske og utenlandske aktører for å søke om et hovedprosjekt innen autentisering og universellutforming.

1.2 Prosjektets organisering og deltakere

Norsk Regnesentral (NR) og Karde har vært forskningspartnere i forprosjektet. NR har også vært prosjektleder og kontraktspartner i forhold til forskningsrådet. Prosjektet har involvert sluttbrukere (Norges Blindeforbund, Dysleksiforbundet), tjenestebukere (Storebrand) og tjenestetilbydere (Norge.no, Brønnøysund registrene og Encap), samt en teknologiutviklingsbedrift (Tellu AS).

Norsk Regnesentral (NR) er en forskningsstiftelse med flere tiårs erfaring innen IKT-forskning. NR har både teknologikompetanse og metodekompetanse. NR har tre hovedsatsingsområder innen IKT forskning; 1. Sikkerhet og personvern, 2. multimedia/multikanal og 3. e-inkludering/universell utforming. Således passer prosjektets tema svært godt med NR's forskningskompetanse og strategi innen IKT.

Karde AS (org.nr. 986 429 360) er en leverandør av teknologisk spisskompetanse om digitale tjenester på web, mobil og digital TV. Karde fungerer som brobygger mellom anvendt forskning og industri som satser på IKT-relatert innovasjon. Prosjektet vil bygge på og videreutvikle Karde's kompetanse innen universell utforming. Denne kompetansen vil gi Kardes rådgivningstjenester en vesentlig merverdi. Karde vil pga. kompetanseutvikling og posisjonering gjennom prosjektet kunne oppnå et mersalg av rådgivningstjenester relatert til universell utforming.

Tellu AS (org.nr. 989743295) er en knoppskyting fra Ericssons forskningsvirksomhet i Norge. Tellu leverer tjenester relatert til bruk av mobilteknologi og samspill mellom mobilteknologi og andre teknologier. Tellu vil være hovedleverandør av teknologikunnskap i det foreslåtte forprosjektet. Løsningene vi ser for oss i fremtiden, vil kreve samspill av mange ulike teknologier. Dette er Tellu spesialist på. Tjenestene vil også kreve organisatorisk samordning av mange aktører, og samspill av deres produksjonsteknologier. Det å kunne tilby universell utforming av slike tjenester vil være et viktig suksesskriterium for Tellus framgang i markedet. En del av Tellu's visjon er å gjøre tjenestene tilgjengelige for alle typer brukergrupper (for eksempel funksjonshemmede og eldre), og Tellu deltar for tiden i flere prosjekter med denne målsetning. Tellu har bidratt til og utviklet en vesentlig del av Encap's autentiseringsløsning for mobile tjenester. For tiden tilbyr Tellu konsulent tjenester til Encap for å vedlikeholde og videreutvikle Encap's produkter.

Brønnøysundregistrene (BR) er en forvaltningsetat med ansvar for en rekke nasjonale kontroll- og registreringsordninger. Etatens overordnede mål er å bidra til økt økonomisk trygghet og effektivitet både for næringslivet og i samfunnet generelt. eBR-programmet (elektronisk Brønnøysund) tar sikte på å gjøre nettet til "hovedinngangen" gjennom en målsetting om at 95% av all kommunikasjon til og fra BR skal være elektronisk innen år 2010. BR forvalter blant annet Altinn (www.altinn.no) som er nettstedet for elektronisk

innrapportering til det offentlige. Prosjektdeltakelse kan stimulere og bidra til konkrete framskritt i realiseringen av eBR-programmets (elektronisk Brønnøysund) målsettinger.

Encap utvikler og leverer programvare på mobiltelefoner til sikker autentisering av brukerne. Med Encaps programvare kan banker og andre tjenesteleverandører erstatte kodekalkulatoren med kundens mobiltelefon som sikkerhetsmekanisme. Kunden slipper å forholde seg til ulike "dingser", og kan bruke samme mobiltelefon for autentisering til flere ulike tjenester. Encap gjør det mulig å utnytte mobiltelefoner som sikkerhetsmekanisme for tjenester i flere elektroniske kanaler som mobiltelefon, web, digital tv etc. Teknologien gjør det mulig å opprette en sikker knytning mellom en bruker og en mobiltelefon og å etablere en mobiltelefon som en brukers personlige ID-terminal. Mobiltelefonen er en "online" terminal som har innebygde muligheter for å kunne tilpasses ulike brukerkrav, f. eks. ved kombinasjon av lyd, bilde, bevegelse og ulike radioteknologier. Dette gjør at mobiltelefonen er en god kandidat til å imøtekomme krav til universell utforming. Encap har som målsetning å tilby et produkt som imøtekommer kravene til universell utforming.

Storebrand er en ledende aktør i det nordiske markedet for langsiktig sparing og forsikring. Storebrand tilbyr produkter til privatpersoner, bedrifter, kommuner og offentlige virksomheter. Storebrand-konsernet er opptatt av samfunnsmessige forpliktelser og konsekvenser av virksomheten. Tilgjengelighet og universell utforming av de elektroniske tjenestene er både en mulighet og en forpliktelse. Storebrand har et forretningssamarbeid med Encap om autentiseringsløsninger.

Norge.no sin viktigste oppgave er å være en veiviser for brukere av offentlige tjenester. Norge.no skal gjøre det lettere å finne fram til offentlig informasjon og sikre at du som bruker får en enkel tilgang til å utføre offentlige tjenester. Ansvaret for Norge.no ligger hos Direktoratet for forvaltning og IKT (DIFI). Direktoratet er underlagt Fornyings- og administrasjonsdepartementet.

Dysleksiforbundet er en landsomfattende interesseorganisasjon for alle med lese- og skrivevansker. Dysleksiforbundet ble etablert i 1976 og har nå ca 5000 medlemmer og 43 lokallag rundt om i landet. Forbundet arbeider blant annet for å skape økt forståelse for dysleksi og dyslektikernes problemer.

Norges Blindeforbund (NBF) er en landsdekkende interesseorganisasjon for svaksynte og blinde. NBFs hovedmål er å skape samfunnsmessig likestilling for svaksynte, blinde og andre grupper av funksjonshemmede. Organisasjonen er opptatt av å arbeide for å bedre synshemmedes situasjon og rettigheter på ulike områder.

2 Bakgrunn

Stadig flere private og offentlige tjenester blir automatisert. Eksempler er minibanker, nettbanker, billettautomater, netthandel og utfylling av selvangivelse. Slike tjenester forutsetter ofte at systemet kan være sikker på en persons identitet, med andre ord at personen kan bli autentisert. Vanlige sikkerhetsmekanismer er bruk av PIN-koder, engangskode (f.eks. på SMS), kodekort eller kodekalkulator (nettbank), eller smartkort (Norsk Tipping) og kombinasjoner av dette. Felles for de fleste sikkerhetsløsninger er at de har en forholdsvis høy brukerterskel, f.eks. må koder huskes og instruksjoner fra systemet følges nøye. Vanligvis må man gjennom en registreringsprosess før man kan begynne å bruke tjenesten. Brukernes behov for enkle og tilgjengelige løsninger har ofte kommet i skyggen for behovet for teknisk og logisk sikre løsninger. For mange personer med nedsatt funksjonsevne kan terskelen være uoverstigelig og tjenesten blir utilgjengelig.

For offentlige tjenester på nett, slik som MinSide og Altinn, har tilgjengelighet en meget klar prinsipiell side, siden alle deler av befolkningen skal ha tilgang til offentlig informasjon og tjenester. Samtidig er det klare politiske og etter hvert juridiske føringer om at elektroniske tjenester rettet mot allmennheten må utformes på en måte som gjøre dem tilgjengelige for alle:

Stortingsmelding nr. 17 (2006-2007), "Eit informasjonssamfunn for alle" gir et relativt bredt og helhetlig bilde av Norges IKT-politikk. Blant regjeringens satsingsområder er digital inkludering, døgnåpen forvaltning ved hjelp av elektronisk selvbetjening samt personvern og sikkerhet. Dersom målsetningen om økt elektronisk selvbetjening skal nås, er det viktig at tjenestene er tilgjengelige og enkle å bruke. I samme dokument er universell utforming av IKT nevnt som et av hovedvirkemidlene for å sikre digital inkludering.

Universell utforming betegner både en strategi og prinsipper for å lage produkter og tjenester som er tilgjengelige for flest mulige. En definisjon av universell utforming er "Utforming av produkter og omgivelser på en slik måte at de kan brukes av alle mennesker, i så stor utstrekning som mulig, uten behov for ekstra tilpassing og en spesiell utforming" (MD 2007). Universell utforming trekkes i økende grad inn som en grunnleggende premiss i samfunnsutformingen. På overordnet nivå er det en klar politisk målsetting at all teknologisk utvikling innen IKT og media skal bygge på prinsippet om universell utforming (ref. Soria Moria erklæringen).

Det å inkludere flest mulig i informasjonssamfunnet er også et av hovedpunktene i EUs strategiske plan for informasjonssamfunnet, i2010. Dette gjenspeiles også i nyere direktiver, slik som i direktiver om offentlige anskaffelser (2004/17/EC og 2004/18/EC). I følge disse direktivene skal tekniske spesifikasjoner så langt det er mulig utformes slik at det tas hensyn til tilgjengelighet eller universell utforming (design for all). Den norske lovgivingen om offentlige anskaffelser ble revidert våren 2006, og trådte i kraft 1. januar 2007. Både i loven om offentlige anskaffelser og i forskriften er det en

bestemmelse om at oppdragsgiver allerede under planleggingen av anskaffelsen skal ta hensyn til universell utforming der hvor det er mulig.

Den 10. juni 2008 ble en ny diskriminerings- og tilgjengelighetslov vedtatt (Ot.prp.nr. 44 2007-2008). Her stilles det krav om universell utforming av IKT-tjenester rettet mot publikum. Nye tjenester må følge kravene til universell utforming innen 1. juli 2011, mens eksisterende løsninger må i følge forslaget være universelt utformet innen 2021. Svært mange tjenester, f.eks. e-handel og nettbank vil således være omfattet av denne loven.

Fordi mange elektroniske tjenester krever registrering og identifisering (autentisering), vil universell utforming av slike løsningene spille en svært viktig rolle i forhold til tilgjengeliggjøring av elektroniske tjenester generelt.

Dagens sikkerhetsløsninger kan utestenge enkelte grupper fra ulike tjenester. For eksempel kan behovet for å gjenta kompliserte koder føre til problemer for dyslektikere, mens behovet for å tyde visuell informasjon kan utestenge synshemmede. Måten ulike autentiseringsmekanismer er utformet på, kan også skape utilsiktede sikkerhets- og personvernproblemer. Spesielt vil dårlig tilgjengelighet kunne skape sikkerhetsutfordringer for personer med nedsatt funksjonsevne. F.eks. skjer det ofte at personer med nedsatt hukommelse (for eksempel eldre) skriver ned minibankkoden. Dermed kan sjansen for misbruk øke. Synshemmede vil ofte spørre andre om å lese koder og beskjeder i forbindelse med autentisering, noe som svekker både sikkerhet og personvern.

Samtidig som overgang til elektroniske tjenester kan skape utfordringer i forhold til tilgjengelighet, kan man også finne eksempler på at ny teknologi og nye anvendelser av gammel teknologi gir nye muligheter for inkludering. I kap. 7 presenterer vi noen eksempler på slike teknologier.

3 Relatert arbeid

Problemstillingen «autentisering og universell utforming» trenger forståelse av både sikkerhet og hvordan utforming påvirker tilgjengeligheten og brukervennligheten for ulike grupper. Prosjektet vil naturlig komplementere eksisterende prosjekter som tar for seg universell utforming uten å ta spesielt for seg de spesielle utfordringene som er knyttet til sikkerhetsløsningene.

DIADEM er forskningsprosjekt med støtte fra EU's 6 rammeprogram innen IST/e-inclusion. Prosjektet går fra 2006-2009. Hovedmålet i DIADEM er å utvikle retningslinjer og teknologi som skal øke tilgjengeligheten av elektroniske skjemaer for eldre og personer med kognitive funksjonshemninger. Hovedfokus er adaptasjon og personalisering av brukergrensesnittet i skjemaene. Selv om autentisering ofte er en forutsetning for bruk av elektroniske skjemaer har man valgt å avgrense seg noe fra denne problemstillingen i Diadem. Ut fra de foreløpige brukertester og erfaringer i prosjektet er det imidlertid på det rene at universell utforming av pålogging og autentisering er en viktig problemstilling.

UNIMOD prosjektet er støttet av Verdikt programmet i Norges forskningsråd (2007 – sommer 2009). UNIMOD står for Universell Utforming i Multimodale Grensesnitt. Hovedmålet er å utvikle kompetanse om og løsninger som bidrar til å gjøre elektroniske tjenester vesentlig mer tilgjengelig og enklere i bruk. Løsningene skal bl.a. generere brukerprofiler vha. IKT-støttet kartlegging av brukernes ferdigheter. Også i dette prosjektet ser man at autentisering er viktig og at dette utgjør en potensiell barriere. I UNIMOD prosjektet er det gjort en undersøkelse av henvendelsene til brukerstøtte i Brønnøysundregistrene. Denne undersøkelsen viste at pålogging utgjør en betydelig barriere ved bruken av denne tjenesten:

“Selv etter flere år med stadig fokus på brukere og brukervennlighet i løsningen, dreier fortsatt rundt en tredjedel (33%) av henvendelsene til Altinn brukerstøtte seg om å komme innenfor døren, altså pålogging til portalen www.altinn.no.” (Udjus 2007).

Synshemmedes IKT-barrierer: Dette prosjektet avdekket at svært mange synshemmede hadde problemer med registrerings og påloggingsløsninger samt betalingsløsninger i forbindelse med en rekke ulike netttjenester. Dette skaper barrierer i forhold til bruk av ulike tjenester, som nettbank, e-handel og deltagelse i en rekke ulike fora og nettsamfunn (Fuglerud, Kristin S. & Solheim 2008). Rundt halvparten av Norges Blindeforbunds medlemmer behersker nettbank i liten grad og 44% har problemer med elektroniske skjemaer (Synnovate 2008).

Ved søk i EU's prosjektdatabase (<http://cordis.europa.eu/ist/projects/projects.html>), fant vi ingen lignende prosjekter. Det er imidlertid flere prosjekter som omhandler bruk av mobile løsninger for mobile arbeidstakere og sikkerhetsløsninger for dette. Så langt vi kan se, nevner ingen av disse prosjektbeskrivelsene behovet for å lage løsninger som kan brukes av alle brukere.

Det er også gjort en del arbeid når det gjelder sikkerhet og brukervennlighet. Se for eksempel (Adams, A. & Sasse 1999; Braz & Robert 2006; Dhamija & Dusseault 2008; Garfinkel 2005; Halpert 2005; Jendricke & Gerd tom Markotten 2000; Whitten & Tygar 1998). Det ser altså ut til at det er gjort svært lite arbeid når det gjelder universell utforming av sikkerhetsløsninger.

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 brukernes muligheter og funksjonsevne, brukssituasjon og behov, og man må se på hvordan brukere løser problemer med nåværende og framtidige sikkerhetsmekanismer i praksis. Det er derfor også nødvendig å involvere brukere med svært ulike behov og nedsatt funksjonsevne i denne forskningen. Flere argumenterer for at fokus på og involvering av brukere med nedsatt funksjonsevne kan medføre radikal nytenking, noe som kan være en verdifull kilde til innovasjon, og som kan føre til bedre løsninger for alle. Også EU påpeker mulighetene som ligger i

brukerdrevet innovasjon, "user driven innovation" eller "co-creation", som de også kaller det (EC 2006; ODPM 2005).

Mange forskere understreker nødvendigheten av å lage fleksible løsninger som kan tilpasses den enkelte for å oppnå universell utforming (Adams, R. 2004; Cremers & Neerincx 2004; Erra et al. 2007; Lines et al. 2006; Petrie, Weber & Fisher 2005). Flere prosjekter innen universell utforming forsøker også å bruke personalisering og profiler som et virkemiddel for bedre tilpassede tjenester (slik som Diadem og Unimod over). Sikkerhets- og personvern-utfordringene knyttet til dette er imidlertid lite undersøkt (Fritsch, Fuglerud & Solheim 2008). Forskning på universell utforming av sikkerhetsløsninger vil være viktig for muligheten til å lage grensesnitt som er bedre tilpasset den enkelte brukers behov, såkalte adaptive eller personaliserte elektroniske tjenester.

Videre er det behov for å formidle eksisterende og ny forskning til aktører som tilbyr automatiserte, personlige tjenester. Det vil også være behov for utveksling av forskning mellom utenlandske og norske aktører, samt videreutvikling av forskning knyttet til sikkerhet, personvern, og universell utforming.

4 Undersøkelser av ulike sikkerhetsløsninger

Det første delmålet i forprosjektet var å gjøre en kartlegging av ulike sikkerhetsløsninger med hensyn på utfordringer for personer med ulike funksjonsnedsettelse, samt å vurdere sikkerhet og personvern for disse.

På bakgrunn fra innspill fra Dysleksiforbundet og Norges Blindforbund og andre deltakere i prosjektet ble det laget en liste over ulike identifiserings- og autentiseringsmekanismer. Denne listen ble gjennomgått i intervju med de 10 informantene i prosjektet, synshemmede og personer med dysleksi, for å høre deres erfaringer med de ulike variantene. En oppsummering av dette finnes i kap. 7. Kartlegging av sikkerhetsmekanismer og utfordringer for ulike brukergrupper, mens en mer detaljert oppsummering av kommentarer fra informantene i forprosjektet finnes i Vedlegg B: Informantenes erfaringer.

Vi har også fått innspill på alternative og mer tilgjengelige løsninger både fra prosjektdeltakere, vår tidligere forskning og søk i litteraturen og på nettet. Videre fant vi noen eksempler nye og mindre vanlige sikkerhetsløsninger. Et sammendrag av kartleggingen sammen med eksempler på alternative og nye autentiseringsmetoder er presentert i kap. 7. Problemstillinger i forhold til sikkerhet og personvern er omtalt i kap. 8. Sikkerhet og personvern.

Det andre delmålet i forprosjektet var å undersøke autentiseringsløsningene til partnere i prosjektet. Disse ble undersøkt med hensyn på tilgjengelighet. Dette var:

1. Pålogging til www.altinn.no. Det ble foretatt intervju med brukerstøtte i Brønnøysund samt en analyse på bakgrunn av dette og en tidligere undersøkelse i regi av Unimodprosjektet (se kap. 5 Analyse av henvendelser til brukerstøtte ved Brønnøysundregistrene). Videre fikk vi tilgang til en testbruker og testversjon av løsningen, og denne ble undersøkt gjennom brukertester (se kap. 6).
2. Pålogging til Storebrand nettbank med Encap's løsning for mobil autentisering. Teknologiutviklingsbedriftene Encap og Tellu utviklet her en prototype for løsningen med tale for opplesning av sikkerhetskoden. Videre bidrog Storebrand, Encap og Tellu med teknisk tilrettelegging, tilgang til testkontoer, teknisk support osv. Denne ble undersøkt gjennom brukertester. (se kap. 6)
3. Pålogging med MinID (Norge.no). Denne påloggingsløsning er også omtalt i dette kap. 5 Analyse av henvendelser til brukerstøtte ved Brønnøysundregistrene. Videre ble løsningen gjennomgått av en prosjektmedarbeider, og kommentarer med tanke på mulige tilgjengelighets- og brukervennlighets utfordringer ble gitt. (Se kap. 6.7 Pålogging til offentlig tjeneste via Min ID).

I forprosjektet har vi ikke gjort en systematisk tilgjengelighetsvurdering i forhold til retningslinjer slik som WAI og Difis "Kvalitet på nett". Dette anbefaler vi alle tjenesteleverandører å gjøre. Det å følge retningslinjer for tilgjengelighet er svært viktig, og man kan luke ut mange tilgjengelighetsproblemer på den måten. Det at man følger slike retningslinjer sikrer imidlertid ikke praktisk brukervennlighet og tilgjengelighet for ulike grupper fullt ut. Derfor anbefaler vi å gjøre brukertester med ulike grupper. Når det gjelder pålogging dukker det opp spesielle problemstillinger på grunn av kombinasjoner av programvare og kort og koder/passord etc. samt at noe av informasjonen blir gjort utilgjengelig for annen programvare på grunn av sikkerheten. Dette kan kreve at man løser tilgjengelighetsutfordringene på andre måter.

5 Analyse av henvendelser til brukerstøtte ved Brønnøysundregistrene

5.1 Bakgrunn

Som et ledd i arbeidet med å forstå hvor egnet ulike registrerings- og autentiseringsmekanismer er for brukere med nedsatt funksjonsevne, har man i prosjektet analysert henvendelser til Altinn brukerservice (ABS). ABS er førstelinje brukerservice for alle etater som har tjenester mot innbyggere og næringsliv og omfatter på den måten tjenester både fra Brønnøysundsregistrene og DIFI som begge er deltakere i prosjektet.

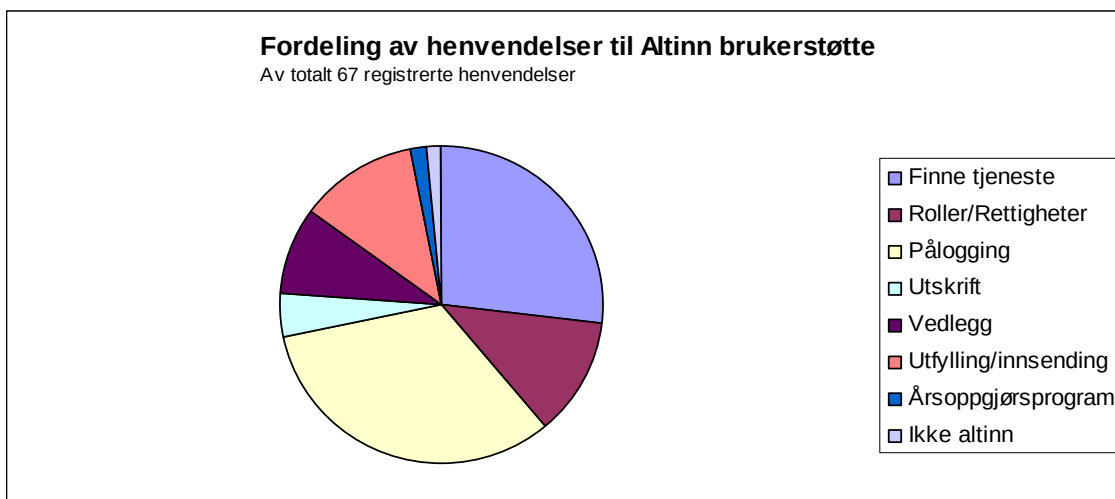
Vi ønsket spesielt å fokusere på brukere med lese- skrivevanskeligheter og synshemmede (blinde/svaksynte). Det eksisterer dessverre ingen logger eller statistikk som kan benyttes til å belyse dette temaet. Imidlertid viser en tidligere undersøkelse gjennomført i regi av et annet forskningsprosjekt, UNIMOD, at

kognitive ferdigheter i stor grad utfordres. Særlig viser det seg vanskelig å orientere seg og finne frem til riktig tjeneste. Det må kunne antas at brukergruppene vi fokuserer på ikke skiller seg vesentlig ut. Dette ble også bekreftet i samtaler med nøkkelpersonell i ABS.

5.2 Undersøkelse og analyse av henvendelser til ABS

Statistikk fra de første 8 mnd. av 2007 samt andre undersøkelser som er gjennomført ble benyttet som grunnlag for arbeidet. Basert på denne informasjonen gjennomførte vi samtaler med nøkkelpersonell fra brukerservice for å sjekke ut eventuelle endringer i 2008. Statistikken som ble bekreftet i samtalene viser at innloggingsproblemer relativt konstant i 2007 og frem til desember 2008 har stått for ca. 30 % av det totale antallet henvendelser til brukerservice.

I Unimod prosjektet lyttet man til brukerstøtte (ABS) og registrerte følgende fordeling av henvendelser (Udjus 2007):



Figur 1: Fordeling av henvendelser til Altinn brukerstøtte.

Tallene fordeler seg slik:

Kategori	Antall	Prosentvis
Finne tjeneste	18	26,87 %
Roller/Rettigheter	8	11,94 %
Pålogging	22	32,84 %
Utskrift	3	4,48 %
Vedlegg	6	8,96 %
Utfylling/innsending	8	11,94 %
Årsoppgjørprogram	1	1,49 %
Ikke altinn	1	1,49 %
Sum	67	100,00 %

Påloggingsproblemene står altså for 32,84 % av henvendelsene. Det er også viktig å legge merke til at før en bruker kan gjøre det han/hun ønsker så må man også finne frem til tjenesten eller skjemaet som skal benyttes. Statistikken viser at dette også står for en stor del av henvendelsene.

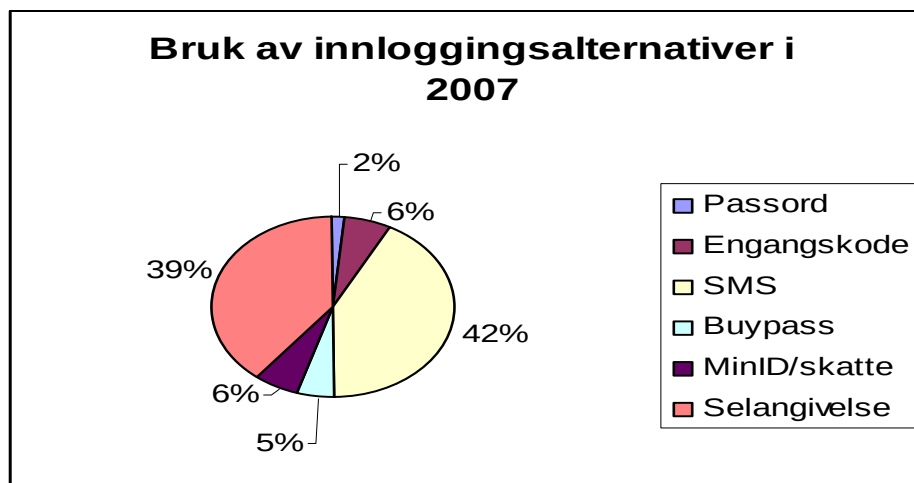
5.3 Analyse av innloggingsproblematikk

Det er en rekke utfordringer knyttet til innlogging. Det kan synes å være en utfordring at det er så mange valgmuligheter. Imidlertid viser statistikk fra Danmark at det er omtrent samme fordeling på henvendelsene knyttet til innlogging der, til tross for at det kun finnes et innloggingsvalg.

En annen utfordring kan være å velge rett sikkerhetsnivå. Det synes ikke å være mange henvendelser relatert til dette, men det skaper i følge bruker-service, ofte lett diskusjon fordi man ikke er enig i sikkerhetsnivåene. For eksempel, hvorfor har koder på skattekortet høyere sikkerhetsnivå enn koder på selvangivelsen og koder på SMS osv.

Det er en god del henvendelser knyttet til at bestilte koder ikke kommer fram. I gjennomsnitt kommer ca. 22 kodebrev hver dag i retur pga. at bestiller har feil/utgått adresse i folkeregisteret.

Det er også noen henvendelser på D-nummer, som er et midlertidig fødselsnummer (gis for eksempel til innvandrere). Det er mange som blir sperret (2630) og det skyldes i de fleste tilfellene at man taster feil passord (1090) som også har mange henvendelser. Bruken av de forskjellige innloggingsalternativene fordeler seg som følger:



Figur 2: Bruk av innloggingsalternativer i 2007.

Innloggingsalternativet der en benytter koder fra Skattekort (nå MinID), er en av de minst brukte valgene, men står for ca. 30 % av alle innloggings-henvendelser. Det har faktisk siden slutten av januar 2008, etter at ny versjon av innlogging med PIN - koder fra skattekort kom i desember 2007, blitt anbefalt at brukerne benytter andre løsninger.

De siste ukene før skatteetaten sendte ut nytt kodebrev (MinID) den 8. desember 2008 lå henvendelser angående innloggingsløsningen med koder fra skattekort på 7 % av totalt antall henvendelser til ABS. Dette økte så til 16 % i uke 50 og 20 % i uke 51. Det nevnes i kodebrevet at man ikke lenger får koder på selvangivelse og skattekort, derfor ser mange bort fra disse 2 innloggingsvalgene og kobler ikke MinID med skattekort. Mange bruker kodene på Altinns innloggingsvalg: "Jeg har engangskoder på brev bestilt på Altinn" (og blir sperret 1 time). Det er noen henvendelser på engelsk/tysk fra utlendinger (fra ulandet) om hva dette er for noe (de har kanskje hatt sommerjobb i Norge?).

5.4 Andre utfordringer knyttet til å ta i bruk en tjeneste.

For å benytte en tjeneste rettet mot næringslivet må man være registrert med en rettighet/rolle i Enhetsregisteret. Dette skaper behov for henvendelser til ABS om roller (340 henvendelser i de 35 første ukene av 2007), delegering av rettigheter (4470) og om hvilke rettighetskrav som gjelder (220) for å kunne fylle ut et skjema.

Det er også som nevnt tidligere vanskelig for mange brukere å orientere seg og finne frem til ønsket tjeneste. Dette fikk vi bekreftet fra våre informanter. I vår brukertest plukket vi ut ett (mer eller mindre tilfeldig) scenario for å skulle benytte www.altinn.no. Informantene ble fortalt at de kunne tenke seg at de hadde byttet bank, og ville gå inn på Altinn for å endre sitt kontonummer for utbetalinger fra det offentlige. Det var svært få av våre informanter som fant fram til dette, både synshemmede og dyslektikere hadde store problemer.

Det eksisterer som nevnt ikke statistikk som spesielt er fokusert på å vise utfordringer for brukere med lese- og skrivevansker og/eller blinde/svaksynte. Ved å lytte til henvendelsene til ABS fikk man i Unimod undersøkelsen imidlertid registrert på hvilken måte kognitive ferdigheter ble utfordret (Udjus 2007). Man fant følgende fordeling:



Figur 3: Henvendelser fordelt i forhold til kognitive utfordringer.

Tallene fordeler seg slik:

Kognitive utfordringer	Antall	Prosentvis
Orientering	51	76,12 %
Begrepsforståelse	5	7,46 %
Hukommelse	3	4,48 %
Annet	8	11,94 %
Sum	67	100,00 %

Så mange som 76% av henvendelsene hadde et vesentlig element av problemer med å finne frem eller orientere seg i tjenesten. Dette området kunne kanskje ha vært brutt ned i underliggende kategorier, slik som å kunne, lese, resonnere, lære eller navigere i tjenestene. Nyansene blir likevel vanskelige å skille mellom, så "orientering" ble valgt som et dekkende begrep.

Videre dreide 7- 8 % seg om begrepsforståelse hos brukeren. Flere brukere har problemer med for eksempel tekniske begreper, som andre tar som en selvfølge. Enkelte brukere har problemer med å huske hvordan de gikk inn i løsningen sist, selv om dette kan ha vært kun kort tid i forveien (samme dag eller noen dager tidligere).

5.5 Ulike brukergrupper – ulike utfordringer?

Gjennom kartleggingen av de forskjellige utfordringene i forbindelse med innlogging gjorde vi en grov vurdering av hvorvidt det var noen bestemte mønstre i hvordan ulike brukergrupper fordeler seg i dette bildet.

Det synes ganske opplagt å være et skille mellom ung og gammel bruker i deres evne til å tilegne seg og å bruke de elektroniske løsningene, uten at vi definerer noe bestemt skille mellom ung og gammel. Tilsvarende synes det også å være et ganske klart skille mellom de som bruker de elektroniske tjenestene ofte (ofte profesjonelle brukere) og de som kun bruker tjenestene en gang i blant (ofte uprofesjonelle brukere). Det er stort sett den siste gruppen som henvender seg til brukerstøtte.

Det kan også være et relativt stort mørketall, dvs. at det reelle antall personer som har vansker med disse tjenestene i virkeligheten er høyere. Også det man tenker på som profesjonelle brukere, dvs. brukere som bruker tjenesten i forbindelse med sitt arbeid, kan ha problemer med tjenestene. Som Dysleksiforbundet påpeker, det finnes for eksempel svært mange gründere med dysleksi. Likeledes finnes det selvfølgelig mange synshemmede arbeidsgivere og arbeidstakere. Disse vil i ulike sammenhenger kunne ha behov for å bruke de offentlige tjenestene. Med bakgrunn i vår brukertest, er det ikke usannsynlig at mange dyslektikere og synshemmede på grunn av dårlig tilgjengelighet blir tvunget til å betale andre for å gjøre disse oppgavene for seg.

Dette er en ganske grov analyse, og antakelser og resultater fra denne må benyttes med forsiktighet.

5.6 Oppsummering og konklusjoner

På bakgrunn av gjennomgåtte materialet er det åpenbart at:

1. Det er ganske komplisert for vanlige brukere å bruke Altinn tjenesten. Tjenesten er i praksis nesten utilgjengelig for brukere med kognitive eller andre utfordringer. (Dette bekreftes også av brukerundersøkelsen).
2. Mange opplever Altinn som lite intuitiv, men samtidig er svært mye vanskelig inntil man har lært det. Man kan anta at det er stort behov for brukeropplæring.
3. Det kan også være et behov for forenkling av Altinn tjenesten.
4. Mange brukere er i utgangspunktet ikke veldig motivert for å ta i bruk Altinn. Hvordan innvirker det på henvendelsene til ABS?
5. Mange valgmuligheter for innlogging kan synes problematisk. På den andre siden viser erfaring fra Danmark at kun ett alternativ også fører til mange henvendelser.
6. Både statistikk og samtaler med ABS indikerer at det er mange og relativt store utfordringer i forbindelse med pålogging til MinID.

Det er et stort behov for videre forskning omkring årsaker til utfordringene og mulige løsninger.

6 Intervjuer og brukertester

6.1 Uvalg

Dysleksiforbundet og Norges Blindforbund har stått for rekruttering av informanter til intervju og brukertest. Informantene ble rekruttert med utgangspunkt i organisasjonenes medlemsregister og nettverk. Vi endte opp følgende fordeling:

- Alder fra 17 til 66 år
- 7 kvinner og 3 menn
- God spredning på formell utdanning, fra en person med ungdomsskole til et par med høyere utdanning.
- 5 dyslektikere
- 5 synshemmede hvorav to var nesten blinde

Alle informantene var erfarne PC og mobil brukere. De fleste bruker PC til kontorapplikasjoner, e-post og Internett. Bare noen få brukte MSN og Facebook og en hadde utdanning innenfor IKT. Fire av informantene var ikke nettbankbrukere i utgangspunktet.

6.2 Tekniske forhold

De fleste brukte nettleseren Internet Explorer, men det var også et par som brukte Opera og et par som brukte Firefox. En av dyslektikerne brukte IKT-hjelpemidler på PC spesielt regnet på dyslektikere, og ingen med dysleksi hadde ekstra hjelpemidler på mobilen. Blant de synshemmede informantene var det 4 som brukte IKT-synshjelpemidler (skjermleser, tekst til tale, leselist, og/eller forstørrelse), mens kun en brukte tilgjengelighetsinnstillinger i operativsystem og nettleser. Fire av de fem synshemmede hadde hjelpemidler på mobilen (tre hadde skjermleser med tekst til tale og en hadde forstørrelse).

Vi testet på

- 6 Nokia-telefoner, alle med Symbian operativsystem (N73, N82, 6290, 6110, 5500).
- 4 Sony Ericsson telefoner, alle med proprietært operativsystem (K750, W890, K800i, W660).
- Informantene hadde forskjellige mobiloperatører (Telenor, Netcom, OneCall, Ventelo og TalkMore).

6.3 Intervju- og testopplegg

Det ble utarbeidet en intervjuguide med test scenario for pålogging til Storebrand bank og www.altinn.no. Videre fikk vi tilgang til testbrukere slik at ingen av informantene brukte egne personopplysninger under testen. Brukernavn, passord og pinkoder ble opplest for informantene.

Dysleksiforbundet og Norges Blindeforbund rekrutterte personer til undersøkelsen. Det var en forutsetning at brukeren som brukte hjelpemidler hadde tilgang til eget utstyr og internett samt en max 3 år gammel Sony Ericsson eller Nokia mobiltelefon med mulighet for nedlasting av programvare.

Forskerne tok deretter kontakt og informerte om opplegget og avtalte tid og sted. Deltakerne fikk tilsendt et informasjonsskriv per e-post. De som ønsket det fikk dette skrevet opplest i forkant av intervjuet. Det ble til sammen gjennomført intervju og test med 10 brukere, 5 rekruttert fra Norges Blindeforbund og 5 rekruttert fra dysleksiforbundet. Vi reiste hjem til 7 av informantene, mens 3 intervjuer/brukertester ble gjennomført på et møterom/kontor.

Vi ønsket at informantene skulle bruke sitt eget utstyr/telefon. I noen tilfeller fikk vi tekniske problemer og testtelefoner fra prosjektet ble brukt, men da la vi vekt på at brukeren fikk en telefon som var mest mulig lik den de var vant med. Under brukertesten ble informanten bedt om å "tenkte høyt". Intervju og test tok til sammen rundt 1 ½ til 2 timer (i ett tilfelle mye lengre tid pga av at nettforbindingen ble borte i lang tid). Det ble etter samtykke fra deltakerne brukt digital lydopptaker for videre bearbeiding. Hver deltaker fikk kr. 500 som takk for hjelpen og til å dekke eventuelle reisekostnader og kostnader ved bruk av tellerskritt og nedlasting til telefonen. Intervjuguide og testoppgaver finnes i Vedlegg A: Guide for intervju og brukertester.

6.4 Resultater fra brukertest

Det ble skrevet referat på bakgrunn av notater gjort under hvert intervju/ brukertest. På grunn av rammene i prosjektet ble lydopptak i liten grad brukt.

Det ble gjort en enkel versjon av tematisk analyse, hvor utsagn og observasjoner fra alle informantene ble samlet og sortert i henhold til temaer som stod fram som viktige. Resultatene kunne kanskje vært mer detaljerte og nyanserte dersom vi hadde hatt tid til å transkribere alle intervjuer/observasjoner, men vi mener å ha fanget opp de viktigste poengene og problemstillingene.

Nedenfor gjennomgås de to påloggingsprosedyrene som ble testet gjennom 10 brukertester.

6.5 Pålogging til Storebrand nettbank vha. Encap's autentiseringsløsning på mobil

6.5.1 Installasjon av enCap sikkerhetsprogram på mobilen

For å kunne bruke EnCap sin mobile autentiseringsløsning må man laste ned et sikkerhetsprogram på mobilen. Dette er noe brukeren gjør en gang, før man begynner å ta i bruk tjenesten. Vi valgte å hjelpe informanten med dette, og i de fleste tilfeller ble installasjon og oppsett gjort av intervjuer.

Prototypen på sikkerhetsprogram med tale ble altså installert på informantens mobil. Installasjonen av EnCap prototypen fungerte stort sett greit. Prosedyren varierte noe på de ulike telefonene avhengig av nettforbindelse/operatør, type telefon og oppsett på telefonen.

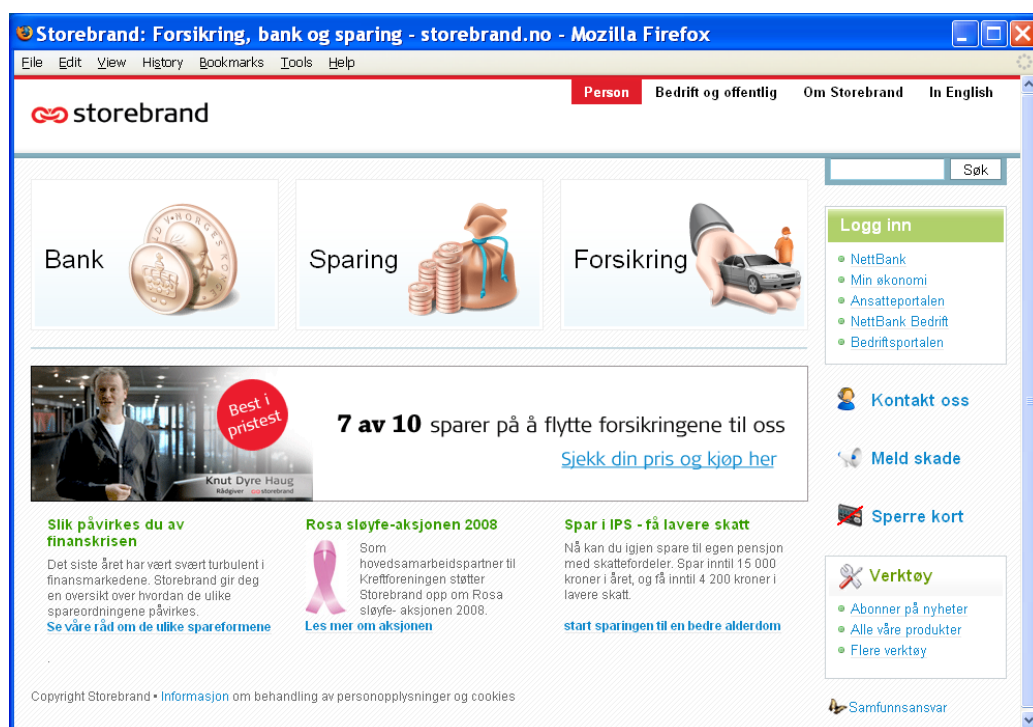
Ettersom vi skulle bruke testkontoer i testen, ble det i tillegg til installasjon av prototypen også foretatt noen tilleggsoperasjoner for å overføre en testbruker til informantens mobil. Denne overføringen av testbruker tok imidlertid ganske lang tid. Dette var litt uheldig da informanten ble sittende passive og vente en stund. For de informantene som brukte testtelefonen slapp vi dette og merket oss at det var en stor fordel å kunne gå rett på sak.

6.5.2 Prosedyre

1. går inn på www.storebrand.no (se skjermbildet under)
2. finn Nettbank (i meny til høyre)
3. taste inn brukernavn (personnr) + passord
4. i det passordet godkjennes, startes mobil-applikasjonen
5. tast inn pinkode på mobilen
6. man får deretter en engangskode lest opp fra mobilen
7. denne engangskoden tastes så inn i nettbanken, og dersom alt stemmer er man da logget inn.

Prosedyren ble i grove trekk forklart til informantene, og de ble bedt om å finne menyvalg for Nettbank (til høyre i skjermbildet). Tre av informantene var brukere av Storebrand nettbank fra før. For dem gikk dette raskt og greit. Fire av informantene var ikke nettbank brukere.

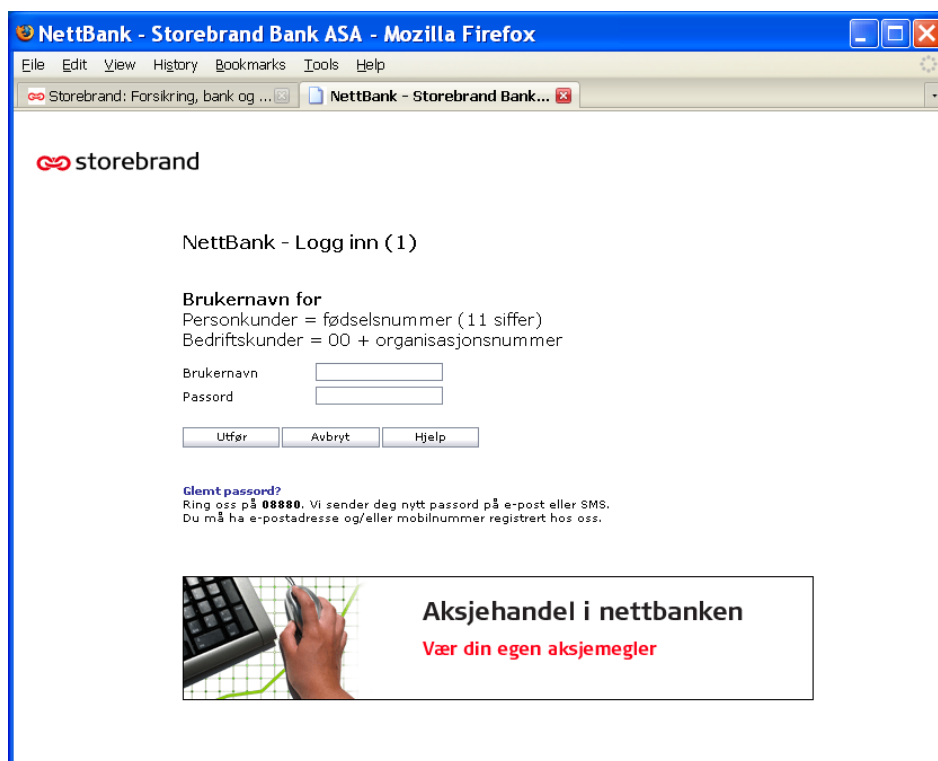
Flere av de synshemmede, kanskje spesielt leselistbrukerne, men også brukere av forstørrelsesprogram brukte tid på å finne menyvalget "Nettbank". Det ble kommentert at de hadde forventet dette mye lengre til venstre i skjermbildet (det vil si mye tidligere i sekvensen av lenker og menyvalg for leselistbrukere). Noen prøvde å klikke på "Bank", som er et av de mest sentrale valgene på forsiden, men dette ble bare en omvei. Det ble kommentert at kontrastene på nettbankvalget (lys blå skrift på hvit bakgrunn) lett kan bli for dårlig for svaksynte brukere.



Figur 4: Forsiden til www.storebrand.no.

Storebrand nettbank sin påloggingsside fungerte greit med leselist. (Noen Informanter forsøkte å trykke Enter-tasten etter brukernavn, og fikk da feilmelding om at passordet ikke kunne være tomt. Man må bruke tabulator eller mus for å gå videre til Passord).

Etter inntasting av brukernavn og passord ble sikkerhetsprogrammet på mobilen automatisk startet. Det var imidlertid et gjennomgående problem at informantene ikke helt forstod hva som skulle skje. De forstod ikke at sikkerhetsapplikasjonen på mobilen ble startet automatisk ved godkjent brukernavn og passord.



Figur 5: Skjerm bilde fra pålogging til Storebrand nettbank.

6.5.3 Advarsler og spørsmål på mobilen

På en del av informantenes mobiltelefoner kom det opp noen advarsler eller spørsmål som måtte besvares før selve sikkerhetsprogrammet kunne starte. Noen ganger kom dette opp på tross av at intervjuer på forhånd hadde forsøkt å stille inn mobilen til å vise færrest mulig av slike advarsler. Måten å skru av disse advarslene på varierte fra modell til modell også mellom modellene fra samme merke.

Disse spørsmålene eller advarslene var som oftest lydløse, og brukeren ble dermed ikke klar over at noe skjedde på mobilen. Dette kan være et problem for alle brukere, men kanskje særlig for de med synshemming som heller ikke har mulighet til å se spørsmålene.

Et eksempel på dette var spørsmålet om man ville tillate programmet enCap å starte. Det at innlegging av bruker og passord starter mobilapplikasjonen vil de fleste brukere lære seg, men det vil antagelig uansett være en fordel dersom brukeren får et tilleggssignal (pip, vibrasjon etc.) om at noe skjer på mobilen.



Figur 6: Skjerm bilde fra mobiltelefon – enCap oppstart.

For synshemmede brukere kan det være et problem at selv om man har tekst-til-tale programvare på mobilen, er det ikke sikkert at man får lest opp denne type advarsler og spørsmål. Det ser ut til å avhenge av type mobil, operatør? og av innstillinger i tekst-til-tale programvaren.

Det kan være at brukeren har satt opp tekst-til-tale programvaren til ikke å lese opp absolutt alt på skjermen da dette kan være svært forstyrrende og upraktisk ved vanlig mobilbruk. Det å skulle endre innstillinger i tekst-til-tale programvaren hver gang man skal bruke nettbanken vil også være tungvint.

(Mange synshemmede brukere er vant til å måtte lære tastesekvenser utenat for å svare på spørsmålssekvenser som for dem er utilgjengelige, men dette er langt fra ideelt).

Å få satt opp den enkelte brukers mobil riktig er med andre ord en utfordring som vil kreve grundig gjennomgang testing og dokumentasjon.

6.5.3.1 Påloggingssekvens

I det enCap sikkerhetsprogram starter blir man bedt om å taste PIN kode. Dette kom også som lydmelding. Nedenfor vises skjermbildene på mobilen før og etter inntasting av PIN kode.



Figur 8: Skjermbilde fra mobil - tast PIN.



Figur 7: Skjermbilde fra mobil: PIN tastet.

De fleste informantene ble litt usikre på rekkefølgen i sikkerhetsprosedyren. Selv om mobilen ba om PIN-kode, var det ikke helt klart for alle at PIN-koden skulle tastes inn på mobilen.

Deretter kom en engangs- sikkerhetskode på mobilen som også ble opplest (to ganger). Denne sikkerhetskoden skulle så tastes inn i nettbanken. Usikkerheten med hensyn på rekkefølgen i prosedyren, hva som skulle tastes hvor, var et gjennomgående problem. Men dette kan sikkert avhjelpes en del med bedre ledetekster.

Man må også ta i betraktning at brukere vil lære en slik prosedyren etter hvert og at dette var første gang for alle informantene.

Dessuten, som noen av informantene påpekte, vil det antagelig være en fordel å ha en punktvis instruksjon ved siden av seg de første gangene. Dette hadde ikke informantene våre.



Figur 9: Sikkerhetskode fra mobil

Et par av informantene opplevde timeout i nettbanken. Det vil si at påloggingen ble stoppet fordi det gikk for lang tid mellom inntasting av brukernavn/passord og sikkerhetskode fra mobiltelefon. Noen brukte litt ekstra tid antagelig fordi alt var nytt, på grunn av at de var usikre på sekvensen, eller fordi de tastet feil kode. Det ble påpekt at man kanskje burde ha fått et spørsmål om man trenger mer tid før det blir timeout. En informant ville hatt litt lengre tid, og en annen ville hatt informasjon på forhånd om tidsbegrensingen.

Videre kan sikkerhetsprogrammet forbedres med hensyn på robusthet: Noen opplevde at applikasjonen lukket seg fordi de kom borti feil taster på mobiltelefonen. De måtte da starte det hele på nytt, og det var selvsagt irriterende.

6.5.4 Layout

Det var stort sett positive tilbakemeldinger på størrelse på tallene og skrifttype på mobilen. For brukere med forstørrelsesprogram kan det være et problem at de ikke ser menyvalgene nederst (Gjenta, Avslutt). En informant kommenterte at bakgrunnslyset på skjermen forsvant litt fort. Han ble da usikker på om han ville miste koden hvis han beveget på tastene for å få tilbake bakgrunnslyset. Hvis mulig, kunne det være en ide å stille inn bakgrunnsbelysning til å vare inntil man lukker skjermbildet med koden.

6.5.5 Tale

Det er viktig å påpeke at uten talefunksjonalitet i prototypen ville ikke de sterkt synshemmede informantene hatt tilgang til informasjonen i prototypen. På grunn av sikkerheten får ikke tekst-til-tale programvaren deres adgang til det som skjer i sikkerhetsprogramvaren (da kunne spionprogramvare også fått tilgang til denne informasjonen).

De fleste var positive til tale i prototypen, men noen mente man burde ha mulighet til å skru denne funksjonen av og på. De som ikke ser innholdet på skjermen er som forklart avhengige av å ha talefunksjonen. En av informantene uttalte at hun håpet løsningen ble tilgjengelig snarest mulig, da hun håpet at dette ville øke hennes muligheter til å velge bank betraktelig. Hun ønsket også å kunne velge ut fra priser, og ikke bare som i dag, ut fra hvilken bank som har talende kodekalkulator.

Noen av dyslektikerne likte også bruk av lyd. Da slapp de å flytte blikket mellom mobilen og PC-skjermen. Noen ble imidlertid forvirret av at de leste tallene fortere med blikket enn de ble opplest med talefunksjonaliteten. Dette skapte forvirring, men ville kanskje vært bedre med raskere opplesning.

Noen ønsket mer lydinformasjon om hva som skjedde underveis, ved oppkobling til nettbank etc. Det ble også påpekt at det kan bli mindre behov for lydinformasjon etter hvert som man lærer seg prosedyren. Det kan derfor kanskje være aktuelt å la brukeren kunne velge mellom noen nivåer av mengde lydinformasjon, for eksempel alt, middels eller lite.

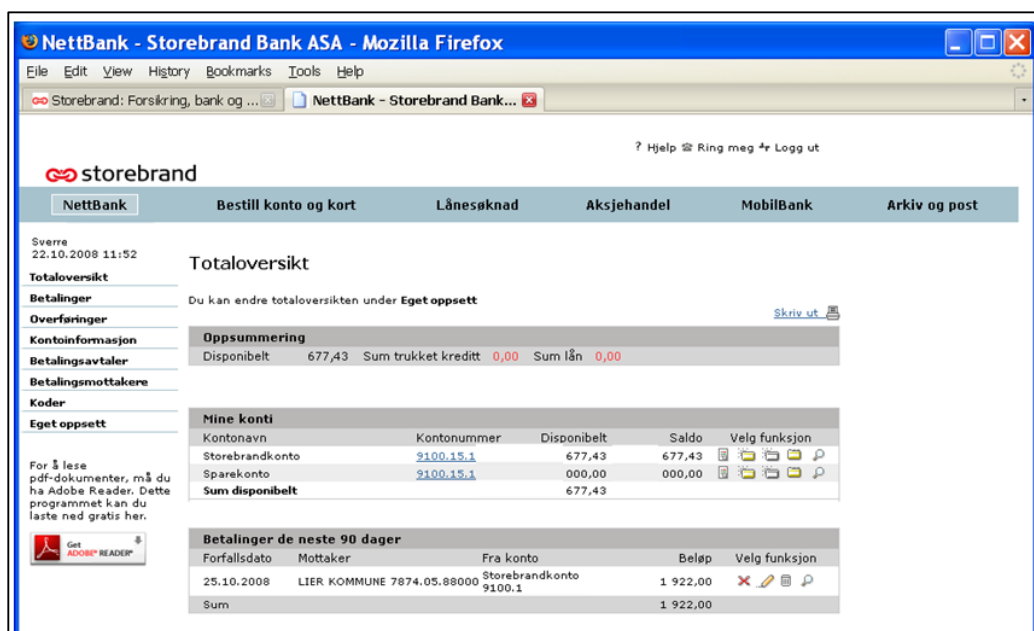
Dette var en prototype, så lydkvaliteten var ikke helt på topp, men god nok til at informantene fikk med seg informasjonen. På en av mobilene var lydstyrken for lav (K750i) og på en annen mobil (W980) fungerte ikke lyden (uten at vi kunne avdekke årsaken til det der og da). De fleste syntes hastigheten på opplesning av tallene i prototypen var for sakte.

Omtrent halvparten av informantene mente det var greit med opplesning av et og et tall, mens de andre mente at det hadde vært greit med opplesning av to og to tall om gangen. Det ble allikevel påpekt at det for dyslektikere vil være best med opplesning av et og et tall for å unngå å bytte om sifrene.

I denne prototypen ble sikkerhetskoden repetert en gang automatisk, det vil si den opplest to ganger på rad. Noen informanter brukte repetisjonen da de ikke fikk med seg hele koden første gang, mens de fleste syntes det var irriterende med denne gjentakelsen, kanskje spesielt fordi de fleste syntes det gikk for sakte. Det ble kommentert at siden man hadde ett tastevalg for å gjenta, så behøvde man ikke en automatisk repetisjon.

6.5.6 Storebrand nettbank

Når man så kom inn i selve nettbanken er det nok et forbedringspotensial for å gjøre denne mer brukervennlig og tilgjengelig, men dette gikk vi i liten grad inn på. Et par informanter mente at enkel pålogging i forhold til andre banker, samt lavt gebyrnivå, var viktige årsaker til at de var kunder i Storebrand nettbank. Det så ut til at tilgjengeligheten for leselistbrukere i selve nettbanken var relativt dårlig. Et tips til forbedring for Storebrand bank er å sørge for at det er fornuftige og forklarende alternativtekster på alle ikoner. Man bør sjekke at den oppfyller retningslinjene til W3C/WAI og Kvalitet på nett. Flere påpekte at det var vanskelig å finne "Logg ut"-knappen.



Figur 10: Skjerm bilde - pålogget Storebrand nettbank.

6.6 Pålogging til offentlige tjenester via www.altinn.no

Vi presenterte informantene for et tenkt scenario:

Testpersonen vår, Markus Kvinge (en oppdiktet person), har byttet bankkonto og ønsker at utbetalinger fra det offentlige (skatt til gode / tilbakebetaling av for mye betalt egenandeler til helsetjenester etc.) skal overføres til ny konto. Han vil derfor endre kontonummeret for utbetaling fra det offentlige.



Figur 11: Forsiden til www.altinn.no

Vi instruerte informanten til å gå inn på www.altinn.no. (Det vil si, vi gikk inn på en annen URL hvor vi hadde tilgang til en testkonto for en oppdiktet person). De fleste kommenterte at forsiden på Altinn var uoversiktlig og fremstod som rotete med for mye tekst. Informantene syntes det var vanskelig å vite hva de skulle velge ut fra det presenterte scenarioet.

"Man vet ikke hvor man hører hjemme.."

"Jeg blir litt stressa og redd for å gjøre feil."

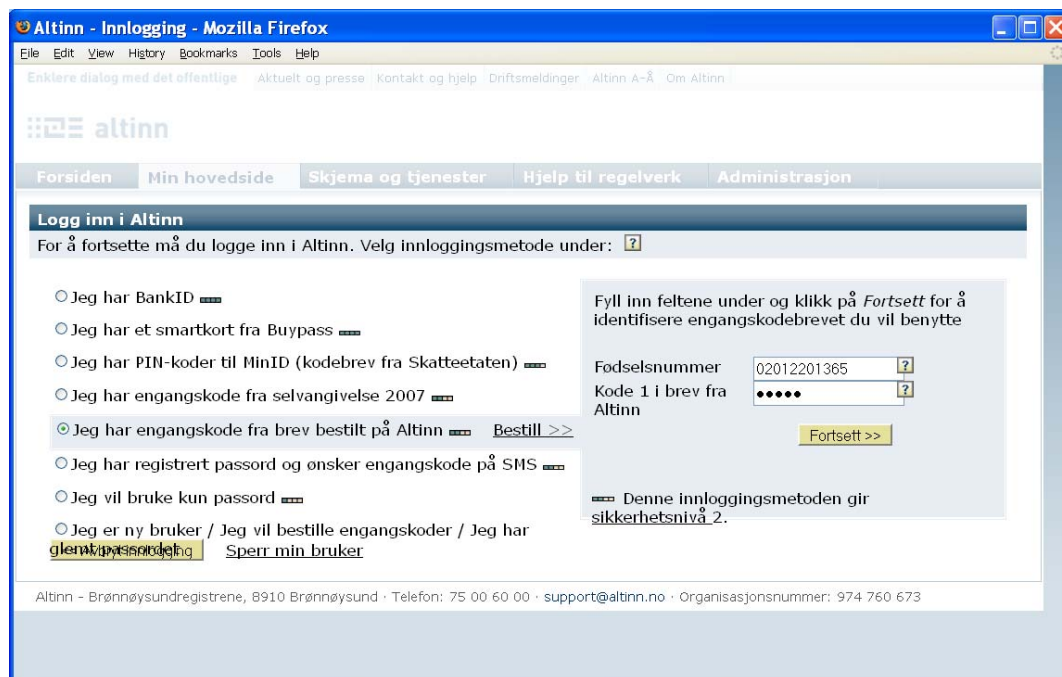
"Det står så mye her, ønsker at det skal være kort og konkret."

"Dette ser forferdelig rotete ut!"

For å hjelpe informantene på vei, ble de instruert i å logge seg inn ved hjelp av logg inn knappen. En av leselistbrukerne fant ikke denne knappen. Det var den første linken på siden, og det var uklart hvorfor han ikke fikk tak i lenken til denne.

Noen kommenterte at det var for mange valg, i alt 8 måter å logge seg inn på (se bildet under). Det ble forvirring rundt hva de forskjellige valgene var, og en kommenterte at hadde det ikke vært for intervjueren, ville hun avsluttet der. Informantene ble instruert i å velge "Jeg har engangskode fra brev bestilt på Altinn". De fleste mente at de ville hatt vansker med å vite hvilket valg de skulle ta hvis ikke dette var blitt oppgitt av intervjuer.

Det ble påpekt at det kunne være vanskelig å oppdage at det skjedde noe til høyre i skjermbildet etter at man hadde valgt et påloggingsalternativ. Man forventet seg et nytt skjermbilde eller en endring til venstre i skjermbildet.



Figur 12: Skjermbilde - Altinn påloggingsalternativer.

Videre var det veldig lett å overse at man skulle legge inn to forskjellige PIN-koder, da det bare var veldig liten endring i skjermbildet, nemlig tallet på koden som tilsa det (og dato på brev).

Figur 13: Skjermbilde - Altinn pålogging – ny kode.

En informant trodde at påloggingen feilet da han ikke la merke til at spørsmålet endret seg fra å be om kode 1 til å be om en annen kode. Teksten og skjermbildet var det samme, og det var bare selve tallet som endret seg til 8. (På Figur 12 bes det om kode 1, mens på Figur 13 bes det om kode 11). Etter å ha bli gjort oppmerksom på at det først ble spurt om kode 1, og deretter i det aktuelle tilfellet kode 8, sier informanten:

"Siden er jo prikk lik, det er jo umulig å legge merke til at den spør om en annen pin...."

Etter pålogging kom det en informasjonsside. De fleste var negative til denne informasjonssiden. Man ønsker ikke å lese og huske masse tekst på forhånd, men heller ha mulighet til å be om hjelp underveis. Det var spesielt dyslektikerne som reagerte på dette. Det ble kommentert at "Videre-knappen" burde være nede til venstre i skjermbildet.



Figur 14: Skjermbilde - informasjonsside om Altinn.

Kommentarer fra informantene:

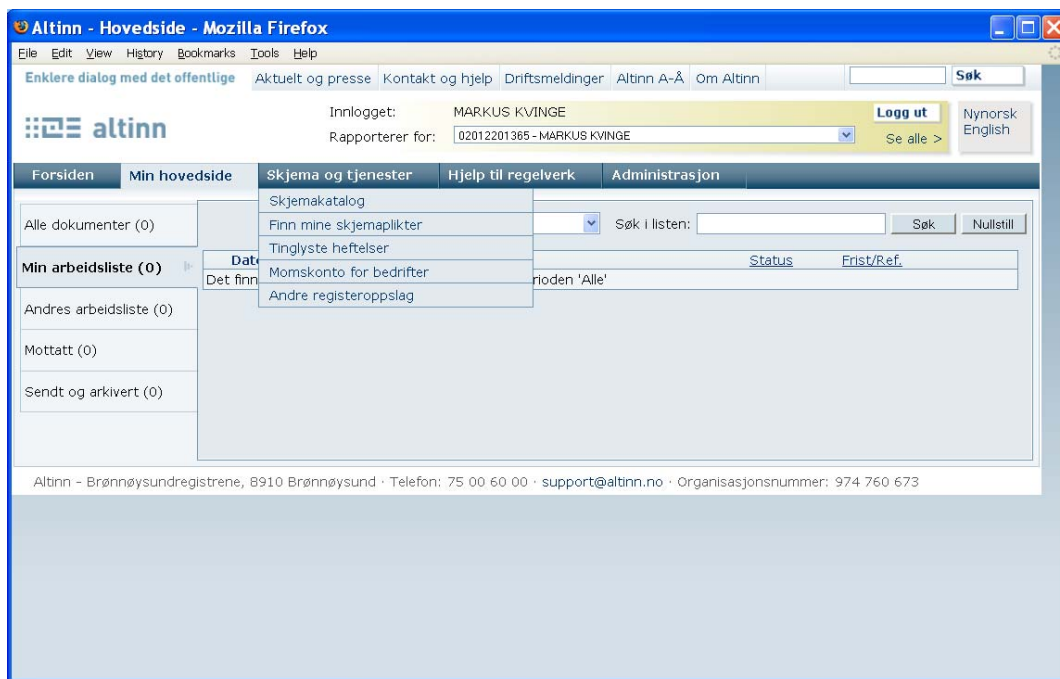
"Instruksjonene ser ut til å relatere seg til en annen side. Istedenfor at man kan søke om hjelp når man først er der, må man huske alt dette på forhånd?..."

"Jeg bruker aldri hjelpesider. Det blir altfor omfattende. Det ville vært bra med konkrete instruksjoner, gjerne som video".

"Her er det mange som ville falt av". Hvis ikke du var her ville jeg gått og satt på kaffen nå. Dette er for innviklet, for tungt språk, for mye."

"Dette er for høyskoleutdannede og mer enn det. Dessuten - disse instruksjonene henviser til knapper og felt og skjemaer, men jeg kan ikke finne dem her. Jeg er avhengig av en oppskrift".

Ved å trykke på Videre-knappen kom man inn i Altinn, og kunne få tilgang til egne dokumenter og skjemaer og tjenester. Ettersom det var pålogging som var fokus i forprosjektet, valgte vi å avslutte etter innlogging.



Figur 15: Skjermbilde - logget inn i Altinn.

6.7 Pålogging til offentlig tjeneste via Min ID

For å få et inntrykk av hvordan påloggingen til offentlige tjenester via MinID fungerer og vurdere eventuell tilgjengelighetsproblematikk, testet en av forskerne en enkel pålogging på denne tjenesten. Testen ble utført på en PC med Windows XP i IE 7 nettleser, samt på en PC med Windows Vista og IE 7. Sekvensen i påloggingen ble som følger:



Figur 16: Skjermbilde - MinID - starter pålogging.

1. Testperson var av den oppfatning at han aldri hadde benyttet MinID før, og valgte å registrere seg som ny bruker idet dette virket som det mest plausible valget ved førstegangsbruk.
2. Oppgav fødsels- og personnummer, etterfulgt av 2 PIN-koder fra det mottatte PIN-kodearket fra myndighetene.

The screenshot shows the MinID login interface. At the top, it says "MinID - felles innlogging til offentlige tjenester" and "MinID". Below this, a box contains the text: "Du er bruker fra før." followed by "Du har allerede registrert deg som bruker. Gå tilbake til Logg inn og bruk ditt selvvalgte passord for å logge deg inn." and a link "Gå tilbake til Logg inn". To the right, there is a list of links: "Hjelp til innlogging", "Personvern og sikkerhet", "Bestill PIN-koder", and "Sperr PIN-koder". At the bottom, it shows the version "Versjon 2.1.0.22 - 28.11.2008" and contact information for the user support.

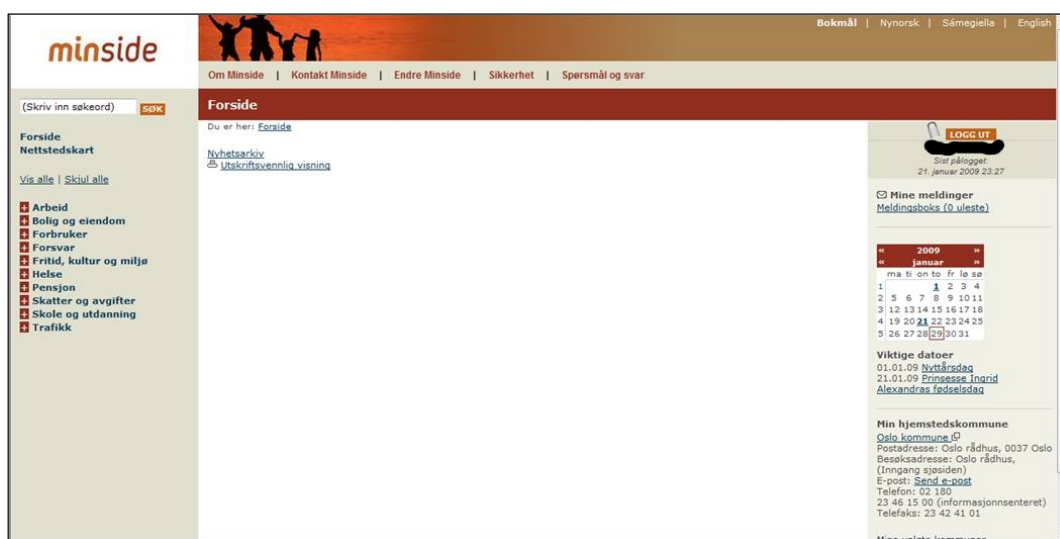
Figur 17: Skjerm bilde - MinID - bruker fra før.

3. Fikk oppgitt at testperson allerede var registrert som bruker, og fikk instruks om å logge på med fødsels- og personnummer og selvvalgt passord. Passordet hadde testpersonen glemt. Dette passordet må antakeligvis stamme tilbake fra en pålogging via Min Side for lang tid tilbake. Måtte følge lenke tilbake til påloggingssiden.
4. Valgte så alternativet for glemt passord. Måtte oppgi ny PIN-kode fra PIN-kodeark, og midlertidig passord skulle sendes per e-post eller sms til testperson – valgte e-post. Det var ikke mulighet for å se hvilken e-post adresse eller mobiltelefonnummer som det midlertidige passordet ville bli sendt til. Måtte også fylle inn captcha.

The screenshot shows the MinID "Forgot Password" page. It is titled "Steg 2 av 4: Midlertidigpassord". The text explains that the user can receive a temporary password either by choosing "Glemt passord" or after three failed login attempts. It instructs the user to provide the "PIN-kode nummer 2" from their PIN card, dated 08.12.08, and to choose how they want the temporary password sent (e-post or sms). There is a text input field for the PIN code and a radio button selection for e-post (selected) and sms. Below this is a captcha image showing the letters "xghkd" and a text input field for the captcha. At the bottom, there are "NESTE" and "AVBRYT" buttons. The footer contains the same version and contact information as Figure 17.

Figur 18: Skjerm bilde - MinID – captcha.

5. Prøvde den lydbaserte versjonen. Et nytt nettleservindu åpnet seg, og lydfilen ble spilt av. Det var imidlertid umulig å høre forskjell på en del av bokstavene – blant annet "m" og "n", slik at testperson var nødt til å tolke det visuelle bildet. Prøvde på en annen PC med annet operativsystem (Vista), og fikk beskjed om lydfilen ikke kunne spilles av fordi det manglet en kodek, eller at Windows Media Player ikke støttet filtypen (Vista). En annen prosjektmedarbeider forsøkte dette på en tredje PC og fikk bare avspilt de to første tegnene i caphca koden.
6. Måtte så legge inn nok en PIN-kode fra PIN-kodearket og midlertidig passord fra e-post som besto av 9 tegn med tall og små og store bokstaver. For å få tilgang til det midlertidige passordet måtte testbruker logge seg på sin e-postklient. Hentet dette og tastet det inn i MiniID-løsningen.
7. Fikk så beskjed om å lage selvvalgt passord på 8 bokstaver og tall, samt å gjenta dette.
8. Dessverre må testperson ha tastet feil ved andregangs bekreftelse av nytt passord, og all informasjon ble slettet i utfyllingsboksene. Måtte tilbake til punkt 5 og finne fram PIN-kode fra tilsendt PIN-kodeark.
9. Etter å ha gjentatt 5 og 6 fikk testeren logget seg på. Kom inn på en side hvor det var en del oversiktsinformasjon om personlig adresse, e-post etc., men det var ingen umiddelbar og intuitiv vei videre for å komme seg til de ulike tjenestene. Trykket på funksjonstast 5 for å oppdatere siden, og kom til forsiden for MiniID hvor det var mulighet for å velge ulike offentlige tjenester.
10. Prøvde pålogging med nytt selvvalgt passord. Fikk tilsendt engangskode på sms til mobil, og pålogging fungerte fint.



Figur 19: Skjerm bilde - logget inn på MinSide.

6.7.1 Tilgjengelighetsaspekter ved MinID

Det er tydelig at det er sikkerhetshensyn som er gitt størst prioritet i denne påloggingsløsningen, og dette går helt klart på bekostning av hensyn til brukervennlighet og brukbarhet – for alle, men spesielt for personer med redusert funksjonsevne. Generelt fremstår løsningen ved førstegangsbruk eller dersom man har glemt selvvalgt passord som komplisert. Løsningen krever veldig mange steg/utfyllingsmomenter. Det er lite informasjon og hjelp/støtte i brukergrensenettet. Idet det ikke er oppgitt hvilket telefonnummer eller e-postadresse midlertidig kode vil bli sendt til, kan man risikere at disse blir sendt til inaktive tjenester dersom man har byttet telefonnummer eller e-postadresse.

Følgende kommentarer kan gjøres i forhold til tilgjengelighet:

- Løsningen er vanskelig å bruke for de som har problemer med å tilegne seg PIN-kodene tilsendt på papir (synshemmede, dyslektikere, personer med kognisjonsutfordringer med flere).
- Bruk av captcha er ekskluderende for synshemmede og for personer som ikke kan lese/tolke tegnene i denne. Lydalternativet kan gjøre pålogging enklere, men idet visse bokstaver høres helt like ut ved opplesing, kan det skape vanskeligheter. Lydfilen ble åpnet i nytt nettleservindu som legger seg oppå påloggingsvinduet. Dette gjør det vanskelig å fylle ut inntastingsfeltet samtidig som man hører på lydfilen. Dessuten får man et ekstra vindu som må lukkes. Dette kan virke forvirrende og det gir unødvendig merarbeid – særlig for bevegelseshemmede som benytter alternativer til vanlig tastatur og mus. På den ene test-PC'en var det ikke mulig å spille av lydcaptcha'en, noe som dermed kan ekskludere både synshemmede og dyslektikere.
- Det at informasjon slettes fra innloggingsfeltene ved feiltasting gir unødvendig merarbeid.
- De mange stegene som kreves for å logge seg på, kan føre til at personer som av ulike årsaker bruker lang tid eller har problemer med å fylle ut hvert enkelt utfyllingspunkt gir opp og lar være å registrere seg og kan dermed ikke bruke tjenesten.
- Vanlig pålogging når man først har registrert seg fungerer greit dersom man kan tilegne seg engangskode tilsendt på sms.

Konklusjon: Førstegangspålogging eller pålogging ved glemt passord som beskrevet over med MinID er ikke brukervennlig og brukbar for personer med redusert funksjonsevne, slik den fremstår per i dag. Den krever stor tålmodighet og motivasjon hos brukeren. Man må nesten regne med å få hjelp/assistanse fra andre for å gjennomføre dette.

Vanlig pålogging etter at man har fått registrert seg og opprettet eget passord fungerte greit dersom man har mulighet for å lese av engangskode tilsendt på sms. Dette kan være et problem for synshemmede.

Det ble ikke gjort noen vurdering av hvorvidt tjenesten oppfyller WAI-kravene til tilgjengelighet til nettsider.

6.8 Diskusjon og konklusjon fra brukertestene

6.8.1 Pålogging til Storebrand nettbank vha Encap mobil autentisering med tale

- Selve testopplegget med flytting av testbruker-id tok for mye oppmerksomhet og forstyrret testopplegget. Det kan ha bidratt til forvirring rundt sekvensen i påloggingen (hva skulle testes hvor – på mobil eller PC). Brukerne ønsket også en kortfattet punktvis instruksjon som viser prosedyren. Det vil være naturlig å utarbeide en slik instruksjon for nye brukere.
- De fleste var positive til tale, og tale er helt nødvendig for blinde eller sterkt svaksynte brukere. Det var ønske om tilpassingsmuligheter både med hensyn til å skru talen av og på og endre opplesningshastighet. Det var ønskelig med raskere opplesning.
- Prototypen var ny for alle brukerne, slik at vi observerte første gang de brukte den. Forvirring med hensyn på rekkefølge ville antagelig blitt mindre etter hvert som man blir vant til løsningen. En del informanter etterlyste mer informasjon underveis, men man kan vurdere om det også bør være mulig å slå dette av og på, eller velge mengde informasjon, da en trent bruker kanskje vil synes at det blir forstyrrende.
- Installasjon og oppsett: Det er mange faktorer som spiller inn på hvordan løsningen oppfører seg, slik som nettleser og sikkerhetsinnstillinger i denne, type mobil og innstillinger på den samt type IKT-hjelpemiddel og innstillinger i dette på både datamaskin og på mobil. Dette er for komplisert for brukere å forholde seg til. Her må det utvikles enkle prosedyrer og veiledninger og mest mulig bør automatiseres. På workshopen ble det kommentert at tilbyder bør gjennomteste og dokumentere noen anbefalte mobiltelefoner først.

6.8.2 Altinn

- På Altinn testet vi kun et tilfeldig scenario, og brukeren ble veiledet en god del under testen.
- Det er behov for mer omfattende testing for å kunne gi konkrete råd til forbedringer.
- Mye informasjon og mange påloggings alternativer gjorde tjenesten svært tung å bruke for våre informanter.

6.8.3 MinID

- På MinID ble det foretatt en enkel gjennomgang av tjenesten av prosjektmedarbeidere.
- Ut fra intervjueren fikk vi bekreftet at det er store utfordring i forhold til bruke av pin-koder som for synshemmede ikke er tilgjengelige og som man ikke nødvendigvis har for hånden. Det kan også lett oppstå forvirring i forhold til ulike versjoner av kodebrev.
- Det kan også oppstå utfordringer i forhold til bruk av lyd-captcha. Få av våre informanter hadde erfaring med det, men oppførsel avhenger av type nettleser, innstillinger i nettleser, og hvilken programvare for lydavspilling brukeren har.

7 Kartlegging av sikkerhetsmekanismer og utfordringer for ulike brukergrupper

Målet var å omtale en rekke løsninger, vanlige og mye brukte løsninger, samt nye og mindre brukte alternativer. Ofte kan behovet for sikkerhet og personvern bli benyttet som argument for at løsningene utformes på en måte som er vanskelig tilgjengelig for ulike grupper. Samtidig kan dårlig tilgjengelighet og brukervennlighet i seg selv føre til sikkerhets og/eller personvernproblemer. Det ble gjort en kartlegging av ulike måter som brukes for identifisering og autentisering, og hvilke utfordringer dette kan skape for personer med nedsatt funksjonsevne (se Vedlegg B: Informantenes erfaringer med ulike sikkerhetsløsninger for detaljer.) Her er en oppsummering av de viktigste utfordringene:

- Bruk av minibanker kan være utfordrende fordi det er ulik layout på tastatur på forskjellige maskiner, og sekvensen i hvordan man betjener dem kan variere. Videre oppleves berøringsskjermer som problematiske av synshemmede. Uheldig fysisk plassering av minibanker kan medføre gjenskinn i skjermen, og kan føre til sikkerhetsrisiko ved å gi innsyn for andre. Flere av de synshemmede informantene benytter minibank med tale, men dette tilbys bare i noen få minibanker. Maskiner uten tale og auditive tilbakemeldinger er et problem idet man ikke får tilbakemelding på hva man har tastet inn eller feilmeldinger med mer.
- Ved bruk av smartkort i betalingsterminaler og automater er det en utfordring å vite hvor og i hvilken retning man skal sette inn kortet, samt å vite hvorvidt betalingsterminalen/automaten kan benyttes med smartkort. Flere av de synshemmede informantene foretrekker allikevel å ta ut penger i butikk. De opplever mange av de samme utfordringene som med minibank, for eksempel ulik utforming av terminaler, mangel på standard layout på tastatur etc. En av forskjellene fra minibanker er at det ofte ikke er auditiv tilbakemelding når man trykker på knapper, noe som kan forårsake feil inntasting. Innsyn fra andre påpekes som en sikkerhetsrisiko, men sikringstiltak av terminaler gjennom deksler over tastatur og lignende gjør betjening ekstra vanskelig.
- Informantene påpekte at manglende standardisering av utforming av terminaler, tastaturer og automater er et problem. Dette skaper også dårlig effektivitet og problemer for folk flest (for eksempel når koden sitter i fingrene og man får problemer hvis tallene på tastaturet går motsatt vei). Manglende standardisering byr på ekstra store utfordringer for enkelte grupper. For personer med kognisjonsutfordringer eller lese- og skrivevansker kan det være et problem å forholde seg til stadig nye prosedyrer. Så lenge automaten/terminalen etc. følger et bestemt mønster kan man lære seg det, men man får lett problemer ved avvik (for eksempel forskjeller mellom leverandører og nye prosedyrer ved oppdateringer etc.). Noen synshemmede lærer seg prosedyrer utenat (f.eks. til minibanker), da ikke-visuelle instruksjoner og tilbakemeldinger ofte mangler. Men manglende

standardisering i tillegg til manglende tilgjengelighet er svært utfordrende, da det er vanskelig å oppdage om noe er feil eller endret, og det er begrenset hvor mange prosedyrer man kan gå rundt å huske.

- Ved bruk av nettbanker er det en stor utfordring at kodegeneratorene ikke presenterer koden på en tilgjengelig måte dvs. store tall, auditivt eller taktilt. Flere av informantene (både synshemmede og dyslektikere) påpekte at tilgjengelighet og brukervennlighet (eller snarere mangel på tilgjengelighet), i minibank og nettbank har vært avgjørende for deres valg av bank. I følge Norges Blindeforbund fungerer ikke internett grensesnittet til BankID sammen med tekniske hjelpemidler som skjermleser med tale/punktskrift, og brukere som er avhengig av slike hjelpemidler blir utestengt fra de bankene som benytter denne løsningen. enCap sin mobile autentiseringsløsning er godkjent for bankID, men tilgjengeligheten avhenger både av tilgjengelighet på mobilapplikasjonen og på grensesnittet i nettbanken.
- Koder, slik som PIN- og PUK-koder fra telefonselskaper og PIN-koder fra det offentlige, tilsendt på papir byr på problemer for informantene. Det er en utfordring å finne de riktige kodene når man trenger dem. Synshemmede er nødt til å be om hjelp fra andre eller bruke tekniske hjelpemidler for å lese dem. Det ble påpekt at banker ofte sender koder på papir som er så tynt at skannere ikke kan lese dem når de prøver å overføre koden fra papir til elektronisk format. Flere er dessuten skeptiske til å bruke skanner fordi de mener at faren for feil er for stor ved bruk av denne teknologien. Synshemmede vil derfor ofte være avhengig av å finne noen de stoler på som kan lese opp sikkerhetsinformasjonen for dem. Flere av informantene, både synshemmede og dyslektikere, kunne tenkt seg å få disse kodene elektronisk hvis det kan gjøres på en sikker måte.
- Det er en generell utfordring at man etter hvert får så mange brukernavn, passord og koder som må huskes. Dette er en utfordring for alle, men våre informanter bekrefter at det kan være en ekstra utfordring for synshemmede og dyslektikere. Dyslektikere vil kunne ha større utfordringer med å huske alle kodene, bruker lenger tid på å taste dem riktig, og kan oftere oppleve å taste feil (noe som medfører mye plunder og heft). Synshemmede har ofte dårlig tilgang på papirbasert informasjon (se forrige punkt). De fleste av våre informanter var allikevel skeptiske til å samle mest mulig under en ID.
- Færre betjente billettkontorer etc. medfører henvisning til selvbetjeningsautomater som er utilgjengelige og vanskelige å bruke. Stadig oftere møter man berøringsskjermer som er utilgjengelig for synshemmede og andre.
- Informantene hadde lite erfaring med biometriske metoder.

7.1 Bruk av taleteknologi

Taleteknologi kan gi økt tilgjengelighet for mange grupper, f.eks. for blinde og svaksynte, for dyslektikere, eldre og for personer med andre fysiske og/eller kognitive funksjonsnedsettelse. Taleteknologi kan brukes på flere måter i forbindelse pålogging og identifisering. For det første kan systemet gi instruksjoner og beskjeder til brukeren i form av tale. For det andre kan stemmegjenkjenning brukes til autentisering.

Det finnes noen eksempler på Norske tjenesteleverandører som jobber med tilgjengelighet av sine sikkerhetsløsninger. Våren 2007 kom Nordea med tale i minibanker og i løpet av høsten 2008 har også Sparebank 1 kommet med talende minibanker i Hedemark.

Minibankkunder som ønsker å få alle instruksjoner opplest benytter egne øreplugger eller hodetelefoner som man putter inn i en minijack-inngang på minibanken. Dette er en ny mulighet som synshemmede er godt fornøyd med (Brenden 2008; Fuglerud, Kristin S. & Solheim 2008).

Som påpekt av våre informanter er kodekort og kodekalkulatorer utilgjengelige for synshemmede og kan være vanskelige å bruke for andre grupper, slik som personer med dysleksi eller eldre. **Error! Reference source not found.**, øverst til høyre, viser et kodekort med mange koder, og to forskjellige kodekalkulatorer. Alle disse tre løsningene krever at brukeren har relativt godt syn.

DNB Nor tilbyr en kodekalkulator med stort display og opplesning av koden med syntetisk tale til bruk sammen med sin nettbank (se Figur 21).

Enkelte banker sender SMS til kundens mobil med en engangskode. Dersom kunden har programvare for tekst-til-tale kan engangskoden i SMSen leses opp. Utfordringer med dette er at det kan være vanskelig å skille på små og store bokstaver. Videre kan det være sikkerhetsutfordringer med denne løsningen.

I vår brukertest har vi sett på et alternativ til denne løsningen. EnCaps mobile autentisering regnes som sikrere enn autentisering ved hjelp av engangskoder på SMS. I denne løsningen er talen innebygd i selve sikkerhetsprogrammet.

Mange nettsteder bruker såkalt Captcha kode for å redusere muligheter for misbruk, spesielt såkalt spam eller automatiserte angrep fra web-roboter (Jameel et al. 2007; May 2005). Dette er en løsning hvor brukeren blir bedt om å tolke en grafisk presentasjon av en kode (ofte tall og bokstaver). Brukeren må deretter skrive denne koden inn i et felt. Enkelte nettsteder tilbyr et lydbasert alternativ til den visuelle koden, men det er fortsatt behov for bedre alternativer til denne typen registreringsløsning (se skjermbildet hentet fra www.dok.no under).



Figur 20: Kodekort og kodekalkulatorer.



Figur 21: DNB kodekalkulator med stor skrift og tale.



Abonner på ukentlig elektronisk nyhetsbrev fra dok.no.

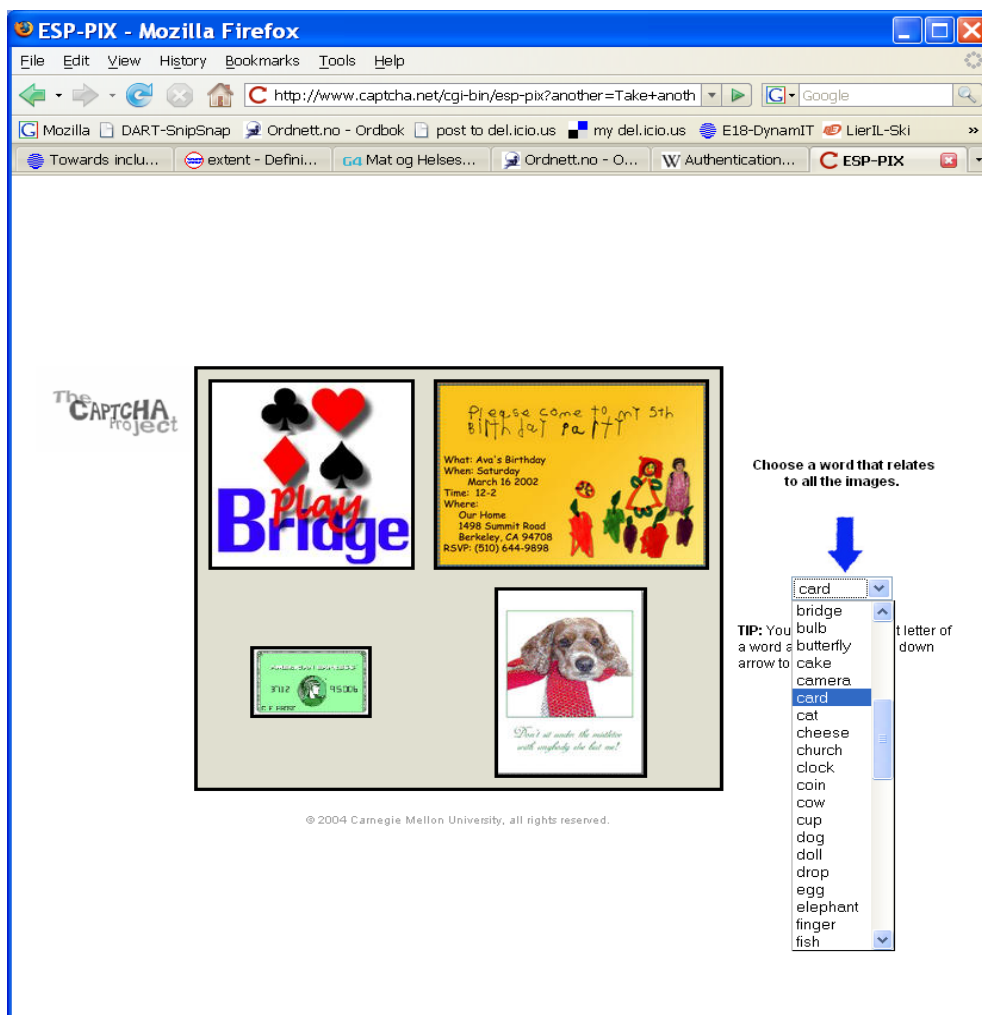
Epostadresse: *

Kode Vennligst skriv inn anti-SPAM-koden du ser nedenfor. [Hør koden.](#)

Figur 22: Skjerm bilde hvor man kan velge å få captcha-koden (anti-SPAM-koden) opplest.

7.2 Bilder og symboler istedenfor tall og bokstaver

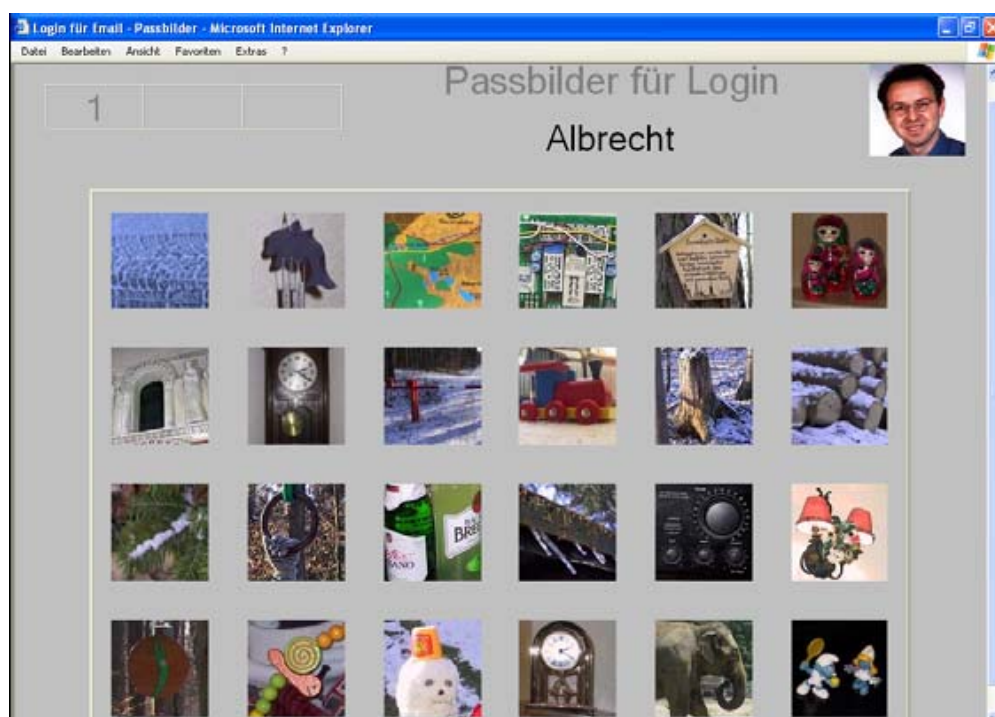
Bruk av symboler og ikoner er svært utbredt i grafiske brukergrensesnitt, og dette kan også være en fordel for personer med lese- og skrivevansker. Men autentiseringen, kan som vi har sett, være en barriere også for denne gruppen.. Nedenfor vises forsøk på å lage alternativer til de vanlige tegnbaserte Captcha kodene.



Figur 23: Skjerm bilde med bildebasert captcha.

Eksempelet er hentet fra www.caphca.net og går ut på at man ser på de presenterte bildene og velger et ord fra en nedtrekksliste. Dette ordet skal relatere seg til alle de presenterte bildene. Vi kjenner ikke til studier som sier noe om dette er et bedre alternativ for personer med lese- skrivevansker.

Også skriving av passord være et problem for personer med lese- og skrivevansker. For det første kan man ofte ikke se hvilke tegn man har skrevet (tegnene blir erstattet med stjerner), og for det andre kan man ikke bruke stavekontroll (Fuglerud, Kristin Skeide 2007). En studie viste at bruk av passord basert på valg av bilder i en bestemt rekkefølge fungerte bedre og raskere enn bruk av tegnbasert passord eller PIN-kode (Schmidt et al. 2004). Dette foregikk på den måten at brukeren først valgte ett av 24 bilder (se figuren under). Deretter kom 24 nye bilder opp, og brukeren valgte neste bilde. Etter valg av 3 bilder på denne måten (13824 muligheter), vil man oppnå omtrent den samme sikkerhet som ved bruk av en PIN kode med 4 siffer.



Figur 24: Skjerm bilde fra bildebasert passord (Schmidt, Kölbl et al. 2004).

I denne studien klarte alle deltakerne å huske bildepassordet sitt, selv etter flere uker. Til sammenligning hadde de fleste store problemer med å huske et vanlig tegnbasert passord eller en PIN kode.

7.3 Near field communication (NFC)

Noen mobiltelefoner kommer nå med en innebygd sensor for såkalt Near Field Communication (NFC). Når NFC-sensoren i mobilen kommer nær en NFC-brikke, vil den kunne lese denne informasjonen sørge for at mobiltelefonen utfører ulike oppgaver.

Ved hjelp av NFC kan man for eksempel bruke mobiltelefonen som adgangskort til en bygning. Man kan bare la telefonen berøre et felt ved inngangsdøren. NFC brikken ved inngangdøren registrerer hvem som eier mobilen, og man kan også tenke seg at telefonen kan laste inn nyttig informasjon som man kunne trenge i den bygningen. NFC - teknologien kan også brukes for å åpne nettsider, overføre data mellom to mobiltelefoner, starte nedlasting av en fil eller overføre data mellom mobiltelefoner. Man kan også bruke denne teknologien for å endre profilen i telefonen etc.

Det er mange muligheter ved bruk av NFC, for eksempel til identifisering, billettkjøp og lignende. Fordelen er at denne teknologien kan gjøre en del ting enklere for brukeren, men samtidig er teknologien ganske ny og det er mange utfordringer når det gjelder personvern og sikkerhet.



Figur 25: Autentisering ved bruk av NFC og mobil.

7.4 Biometri

Noen mener at biometri vil løse mange av problemene vi har med de autentiseringsmetoder som basert på noe brukeren har eller vet. Biometri er basert på brukerens kropp. Noen eksempler på biometriske teknologier er gjenkjenning av

- fingeravtrykk
- iris
- signatur
- tale eller stemme
- ansikt
- måten man går på
- håndgeometri
- blodåregeometri

På samme måte som ved bruk av de foregående autentiseringsmetodene som er basert på noe brukeren har eller vet, kan det for hver av de ulike biometriske metodene være utfordringer for enkelte grupper fordi

- det fysiske kjennetegnet kan være midlertidig eller permanent skadet på grunn av sykdom eller skade.
- etter hvert som man blir eldre, vil de biometriske kjennetegnene endre seg,
- det blir ofte mer feil ved bruk av biometri etter hvert som man blir eldre.
- det er også sikkerhetsproblemer med biometri, for eksempel kan fingeravtrykk kopieres, og i motsetning til bruk av koder eller passord er det problematisk for den egentlige eier å bytte biometrisk informasjon.
- Biometri er vanligvis mindre nøyaktig enn metoder basert på koder og kort.

Det dukker derfor opp mange problemstillinger knyttet til autentisering og tilgjengelighet for ulike grupper. En sentral problemstilling vil kunne være:

Hvordan kan man tilby øket fleksibilitet, slik at hver enkelt bruker kan bruke en sikkerhetsmekanisme som er tilgjengelig og tilpasset vedkommende og samtidig ivareta personvern hensyn?

8 Sikkerhet og personvern

Målsetningen var å gjøre en gradering og vurdering av de ulike sikkerhetsmekanismene både med hensyn på tilgjengelighet og med hensyn til personvern og sikkerhet. Vår hypotese var at dårlig tilgjengelighet og brukervennlighet kunne føre til at brukeren må kompensere på måter som kan gå ut over sikkerhet og personvern. Det å faktisk gjøre denne vurderingen for alle sikkerhetsmekanismer viste seg å være en svært omfattende oppgave. Først må man utarbeide et klassifiseringssystem. Her anbefaler vi videre arbeid i et hovedprosjekt.

Vi stilte informantene noen enkle spørsmål vedrørende personvern/sikkerhet.

De fleste informantene var ganske skeptiske til å skulle gi tjenesteleverandører informasjon om sin funksjonshemming, selv om de ellers ikke legger skjul på det. Det ble bemerket at tjenesteleverandør istedenfor burde opplyse om muligheten til å bruke for eksempel lyd, og så kan den enkelte få velge om man vil bruke dette eller ikke, uten å oppgi noen grunn.

De fleste informantene var også skeptiske til å bruke en ID, for eksempel bank-id som identifikasjon til ulike tjenester, også andre enn banktjenester, slik som e-handel. Tre informanter var positive til dette mens de fleste var svært skeptiske til å samle informasjonen under en felles bruker.

På spørsmål om hvordan informantene så på forholdet mellom tilgjengelighet/brukervennlighet og sikkerhet/personvern, var informantene

ganske klare på at de ønsket sikrest mulige løsninger. En informant mente at man til nød kan bruke en mindre sikker løsning som en overgangsordning. Det ble påpekt at det bør være opp til banken/tjenesteleverandør å vurdere sikkerheten. Tjenesteleverandøren bør kun tilby så sikre løsninger at de selv er villige til å bære eventuelle tap

På den annen side kommenterte flere at de bytter koders å sjeldent som mulig, og kun når man blir tvunget til det. Noen velger å gjenbruke koder i størst mulig grad. Når man først blir tvunget til å endre kode/passord, oppgir en av informantene at hun da velger å forandre alle sine koder til en felles ny kode.

Flere av de synshemmede informantene uttrykte bekymring over at de ikke hadde kontroll på personer som eventuelt forsøkte å se hvilken kode de tastet på terminaler, og bankautomater.

8.1 Er det mulig å lage en universelt utformet sikkerhetsløsning?

Det synes som at 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?

Nedenfor antyder vi hvordan man kan integrere tilgjengelighetsspørsmål i en prosess for sikkerhetsklassifisering.

8.2 Klassifisering av sikkerhetsmekanismer

Det å velge den autentiseringsmetoden som passer best for en spesiell brukergruppe, til sikkerhetsmålene, truslene osv. er en integrert del av det ordinære arbeidet med sikkerhet.

For å kunne tilby flere parallelle og like sikre måter å autentisere seg på for ulike brukergrupper kreves en klassifisering av sikkerhetsegenskaper, sikkerhetsnivåer, og trusler. En slik strategi vil også kreve at man starter med å finne en portefølje av egnede sikkerhetsmetoder som har god nok tilgjengelighet og brukervennlighet til å dekke behovene til flest mulig brukere. Samtidig må man vurdere om de har høye nok sikkerhets nivåer og at de er håndterbare for systemeieren.

En mulig tilnærming er å utarbeide en kunnskapsbase med en portefølje med mulige autentiserings og identifiserings teknologier som blir gradert og klassifisert på bakgrunn av et sett med parametere. Utviklingen av et slikt sett med parametere er ikke triviell, og vil antagelig kreve grundig forskningsinnsats. Et slikt sett med måleparametre bør inneholde alle de viktige sikkerhets egenskaper og potensielle trusler, spesielt med hensyn tilgjengelighet samt

mulighet og sannsynlighet for sikker og potensielle trusler for ulike brukergrupper.

Eksempler på parametere i et slikt klassifiseringssystem kan være

- ⊗ 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

I tillegg til en vurdering av disse egenskapene i forhold til brukervennlighet og tilgjengelighet for ulike brukergrupper, vil det være nyttig med en vurdering av administrasjonskostnader og andre kostnader.

En mulig tilnærming kan være å ta utgangspunkt i metoder for balansert målstyring (balanced scorecard), men dette må det eventuelt forskes videre på.

9 Oppsummering og forslag

9.1 Konklusjoner fra prosjektet

Om de undersøkte løsningene:

- **Storebrand/Encap:** Autentisering ved hjelp av mobil med tale: Løsningen ble godt mottatt av informantene, selv om det er en del forbedringspunkter på prototypen som ble testet (installasjon og oppsett, kvalitet og fleksibilitet/personlig tilpassing). Denne tjenesten vil kunne øke tilgjengeligheten for flere grupper.
- **Altinn:** Antallet henvendelser til Altinn brukerstøtte tyder på at tjenesten er ganske komplisert for folk flest. Mye informasjon og mange påloggings alternativer gjorde tjenesten svært tung å bruke for våre informanter. Vi har pekt på noen problemområder. Det er behov for videre arbeid for å gjøre denne tjenesten mer tilgjengelig og enklere å bruke for alle.
- **MinSide:** Både statistikk og samtaler med ABS indikerer at det er mange og relativt store utfordringer i forbindelse med pålogging til MinID. Statistikk fra henvendelser til brukerstøtte viser at svært mange opplever vanskeligheter

ved pålogging med MinID. Dette prosjektet har pekt på noen konkrete tilgjengelighets- og brukervennlighets utfordringer. Dagens løsning for førstegangs pålogging er ikke brukbar for personer med nedsatt funksjonsevne.

Dette har vært et forprosjekt med begrensede ressurser. Vi har gjort noen relativt enkle undersøkelser av spørsmål knyttet til bruk og tilgjengelighet av noen sikkerhetsløsninger. Dette bør undersøkes nøyere og for flere grupper.

For alle tjenestene anbefaler vi en grundig gjennomgang i forhold til retningslinjer for tilgjengelighet, slik som W3C/WAI og DIFI "Kvalitet på nett" i tillegg til arbeid med forenkling og brukertester med ulike grupper.

På tross av at dette har vært et forprosjekt, har vi pekt på en rekke utfordringer når det gjelder tilgjengelighet og brukervennlighet ved sikkerhetsløsninger. Vi mener et det er et stort forbedringspotensial på dette området, og anbefaler at brukervennlighet og tilgjengelighet blir en integrert del av det videre arbeidet med løsningene.

9.2 Behov forskning og videre arbeid

Mange grupper blir i dag utestengt fra å bruke en rekke digitale tjenester, slik som forskjellige banktjenester og offentlige tjenester, på grunn av manglende universell utforming av sikkerhetsløsningene. Mange sikkerhetsløsninger er utilgjengelige og vanskelige å bruke for ulike grupper, og mylderet av ulike varianter skaper også utfordringer for folk. For å inkludere flere i informasjonssamfunnet, samt å gjøre det enklere for folk flest, er det et stort behov for forskning og videre arbeid med universell utforming av sikkerhetsløsninger. Nedenfor peker vi på noen problemområder:

- Det å huske mange forskjellige brukernavn, koder og passord er en gjennomgående utfordring, spesielt for de man ikke bruker så ofte. Det å få alle disse kodene tilsendt på papir byr også på utfordringer, spesielt for synshemmede, men også for andre. En mulighet er å få tilgang til flest mulig tjenester via en og samme ID, men mange er skeptiske til dette. En annen mulighet er utvikling av systemer som kan hjelpe folk å holde rede på alle sine brukere med tilhørende koder. Det er gjort noe forskning på slike systemer, men det er behov for mer arbeid og spesielt med tanke på at slike systemer selvsagt også må være enkle å bruke og tilgjengelige for alle brukere.
- Manglende standardisering av utforming av terminaler, tastaturer, automater er en utfordring for alle, men kan by på ekstra store utfordringer for enkelte grupper. Det er behov for en klargjøring av hvilke standarder som fungerer best for ulike grupper og å arbeide videre med å utvikle standarder tilgjengelige sikkerhetsløsninger. Videre bør det startes en prosess for å øke oppslutningen om de beste og mest tilgjengelige løsningene.
- Økende bruk av automater er et problem da automatene ofte ikke er tilgjengelige for alle. Økende bruk av berøringsskjermer kan være bra for mange, men medfører store utfordringer for eksempel synshemmede. Det er

nødvendig med alternativer for de som ikke kan bruke dette. Nordeas minibanker og enCaps mobile autentiseringsprototype med tale for mobil er eksempler på hvordan man kan benytte lyd i brukergrensesnittet. Det bør forskes videre på hvordan ulike modaliteter (lyd, bilde, berøring, video etc.) i brukergrensesnittet kan utnyttes. Kan man presentere flere alternativer og modaliteter i den samme terminal/automat uten at den blir for kompleks?

- Det er behov for mer kunnskap om utfordringer ved bruk av de ulike sikkerhetsmekanismene for forskjellige brukergrupper med hensyn til brukervennlighet, tilgjengelighet, sikkerhet og personvern. Brukertesten av EnCaps påloggingsløsning avdekket at brukerne ønsket muligheter for ulike tilpassinger av tjenesten. Et viktig spørsmål er om det er mulig å tilby en sikkerhetsløsning som er tilgjengelig for grupper med ulike funksjonsnedsettelse. Et alternativ kan være å tilby flere parallelle sikkerhetsløsninger slik at grupper med ulike behov vil kunne finne en løsning som er tilgjengelig for seg. Sikkerhet og personvern er en forutsetning for personalisering samtidig som personalisering trolig vil kunne øke tilgjengelighet og brukervennlighet. Det bør forskes mer på hvordan personalisering praktisk og sikkert kan benyttes i sikkerhetsløsninger.

9.3 Hovedprosjektsøknad

En søknad om hovedprosjekt ble sendt til forskningsprogrammet VERDIKT (Kjernekompetanse og verdiskaping i IKT) under Norges forskningsråd (NFR) den 15. oktober 2008. Deltakere i denne søknaden var Norsk Regnesentral, med gjesteforskere fra Karde, Institutt for rettsinformatikk ved UiO, Norges blindeforbund, Dysleksiforbundet og Seniornett. I tillegg knyttet vi til oss Brønnøysundregistrene, Encap og Storebrand som alle sa seg villige til å stille sine systemer til rådighet som case.

Søknaden pekte på behovet for tverrfaglig forskning innen området inkluderende identitets-håndteringssystemer. Prosjektforlaget tittel er "IncludeMeToo - universal design of authentication mechanisms".

Prosjektforlaget bygger på kunnskap fra forprosjektet "Universell utforming av IKT-baserte løsninger for registrering og autentisering". Forprosjektet ble utført høsten 2008, og forutsatt at søknaden blir innvilget vil hovedprosjektet starten i løpet av våren 2009. Det arbeides videre med å få i stand et internasjonalt konsortium som kan utforme en søknad til EU under en aktuell utlysning.

10 Litteratur

Adams, A. & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measure. *Communications of the ACM*, 42 (12): 41-46.

Adams, R. (2004, June 28-29). *Universal Access Through Client-Centred Cognitive Assessment and Personality Profiling*. UI4All 2004, Vienna, Austria. Springer-Verlag Berlin Heidelberg. 3-15 s.

Braz, C. & Robert, J.-M. (2006). *Security and usability: the case of the user authentication methods*. Presentasjon ved Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine. ACM. Montreal, Canada.

Brenden, J. E. (2008, 4. desember 2008). Den talende minibanken er her. *Hamar Dagblad*.

Cremers, A. H. M. & Neerincx, M. A. (2004, June 28-29). *Personalisation Meets Accessibility: Towards the Design of Individual User Interfaces for All*. User-Centered Interaction Paradigms for Universal Access in the Information Society, UI4All 2004, Vienna, Austria. Springer-Verlag Berlin Heidelberg. 119-124 s.

Dhamija, R. & Dussault, L. (2008). The Seven Flaws of Identity Management: Usability and Security Challenges. *IEEE Security and Privacy*, 6 (2): 24-29.

EC. (2006). Analysis of European target groups related to inclusive eGovernment, European Commission, Information Society and Media Directorate-General, eGovernment Unit, eGovernment Action Plan. 60 s.

Erra, U., Iaccarino, G., Malandrino, D. & Scarano, V. (2007). Personalizable edge services for Web accessibility. *Universal Access in the Information Society*, 6 (3): 285-306 Tilgjengelig fra: <http://dx.doi.org/10.1007/s10209-007-0091-y>.

Fritsch, L., Fuglerud, K. S. & Solheim, I. (2008, May 28, 2008). *Towards inclusive identity management*. Presentasjon ved Identity in the Information Society Workshop. Pre-Proceedings of the 1st IDIS workshop 2008. Arona, Italy. Available from: <http://publ.nr.no/4751>.

Fuglerud, K. S. (2007). *Hvordan utforme IKT for personer med kognitive funksjonshendringer – en litteraturgjennomgang*. NR Notat, Dart/05/07. Oslo, Norwegian Computing Center. 16 s.

Fuglerud, K. S. & Solheim, I. (2008). Synshemmedes IKT-barrierer. Resultater fra undersøkelse om IKT-bruk blant synshemmede. *Report number: 1016*. Oslo, Norwegian Computing Center. 91 s.

Garfinkel, L. F. C. S. (2005). *Security and Usability: Designing secure systems that people can use*. Theory in practice, O'Reilly. 714 s.

Halpert, B. J. (2005, September 23-24). *Authentication Interface Evaluation and Design for Mobile Devices*. Information Security Curriculum Development (InfoSecCD) Conference '05, Kennesaw, GA, USA.

Jameel, H., Shaikh, R. A., Lee, H. & Lee, S. (2007, February 5-9). *Human Identification through Image Evaluation using Secret Predicates*. Presentasjon ved To be published in Topics in Cryptology CT-RSA 2007, The Cryptographers Track at the RSA Conference 2007. San Francisco, CA, USA. Available from: http://uclab.khu.ac.kr/usec/publication/hassan_rsa.pdf.

- Jendricke, U. & Gerd tom Markotten, D. (2000). Usability meets security - The Identity-Manager as your Personal Security Assistant for the Internet. *Proceedings of the 16th Annual Computer Security Applications Conference* Tilgjengelig fra: <http://www.acsac.org/2000/papers/90.pdf>
- Lines, L., Ikechi, O., Hone, K. & Elliman, T. (2006, 12 September 2006). *Online form design for older adults: Introducing web-automated personalisation*. HCI, the web and the older population workshop, London, UK. HCI 2006.
- May, M. (2005). Inaccessibility of CAPTCHA. Alternatives to Visual Turing Tests on the Web. I: W3C (red.), W3C Working Group Note, work in progress.
- MD. (2007). *Universell utforming – begrepsavklaring*. Miljøverndepartementet. 16 s.
- ODPM. (2005). Inclusion Through Innovation, Tackling Social Exclusion Through New Technologies. London, Office of the Deputy Prime Minister, Social Exclusion Unit, UK. 83 s.
- Ot.prp.nr. 44. (2007-2008). *Om lov om forbud mot diskriminering på grunn av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven)*. Tilråding fra Barne- og likestillingsdepartementet av 4. april 2008, godkjent i statsråd samme dag. (Regjeringen Stoltenberg II). Barne- og likestillingsdepartementet.
- Petrie, H. L., Weber, G. & Fisher, W. (2005). Personalization, interaction, and navigation in rich multimedia documents for print-disabled users. *IBM Systems Journal*, 44 (3) Tilgjengelig fra: <http://www.research.ibm.com/journal/sj/443/petrie.html>.
- Schmidt, A., Kölbl, T., Wagner, S. & Straßmeier, W. (2004, June 28-29, 2004.). *Enabling Access to Computers for People with Poor Reading Skills*. 8th ERCIM Workshop on User Interfaces for All, Vienna, Austria. Springer-Verlag Berlin Heidelberg. 96–115 s.
- St.meld. nr. 17. (2006-2007: 17). *Eit informasjonssamfunn for alle*. FAD, Fornyings- og administrasjonsdepartementet. 181 s.
- Synnovate. (2008, 14. December). *Rapport Medlemsundersøkelse 2008*. Presentasjon ved Norges Blindforbund.
- Udjus, L. (2007). "Gjør døren høy - gjør porten vid". Offentlige elektroniske tjenester for alle. *Stat og styring*, 2007 (3).
- Whitten, A. & Tygar, J. D. (1998). Usability of Security: A case study, CMU-CS-98-155, Carnegie Melon University, Pittsburgh, PA 15213, USA. 39 s.

Vedlegg A: Guide for intervju og brukertester

Dato:_____, ID:_____

A.1 Informasjon om prosjektet, anonymitet og frivillighet

- Undersøkelsen: Hensikt og gjennomføring. Beskriv hva vi skal gjøre, og hvor lang tid man forventer at dette tar. Spør om det er ønskelig å få opplest informasjonsbrevet?
- Anonymitet i forhold til rapportering og presentasjon av resultater
- Informanten kan fritt velge ikke å svare på enkeltspørsmål.
- Informanten får kr. 500 som takk for hjelpen og til å dekke evt. utgifter
- Informanten kan velge å avslutte samtalen når som helst
- Informanten kan i etterhånd be om at dataene slettes og ikke brukes videre.
- Noe informanten lurer på i forhold til dette?

A.2 Bakgrunnsinformasjon om informanten

- Alder:
- Kjønn:
- Funksjonsnedsettelse:
- Utdanning:
- Data-opplæring/utdannelse:
- Data-erfaring:
- Bruk/Utstyr/Programvare:
- Hjelpemidler:
- Mobil-erfaring:
- Hjelpemidler mobil:
- Mobil type:
- Operatør:

A.3 Gjennomgang av et par påloggingsløsninger

Forklarer informanten at vi nå ønsker å gå litt mer detaljert inn ting som fungerer og ikke, ved å gå gjennom noen IKT baserte oppgaver.

- Vi ønsker å finne ut mer om hva som fungerer bra og hva som fungerer dårlig
- Fortell hva du tenker, gjør og forstår/ikke forstår underveis. Referer gjerne til andre erfaringer du har.
- Ta den tiden du trenger! Det er en fordel hvis du gjør det så langsomt at jeg kan følge med på hva som skjer!
- Det kan hende jeg stiller spørsmål eller ber deg gjenta hvis jeg ikke oppfatter eller klarer å følge med på hva du gjør!

	Oppgave	Kommentar
1.	Pålogging til Storebrand bank med Encap mobil autentisering • Gå til Storebrand bank http://www.storebrand.no/ • Velg nettbank • Legg inn fødselsnummer og passord (opplysninger på en fiktiv bruker oppgis fra intervjuer) • Er instruksjoner forståelige, får man info om hva man skal gjøre? • Hvordan er lyd kvalitet? • Opplesningshastighet? • Ett og ett tall eller to og to? • Annet: • Du har prøvd autentiseringsløsning på mobil. Ville du synes at det er trygt nok? Hva hvis du mister din mobil telefon? • Hvis du skulle miste mobilen, hvor fort trenger du ny løsning? • Er det noen grense for hvor høye beløp du vil overføre med en slik metode?	
2.	Pålogging på www.Altinn.no Scenario: Markus har byttet bank og vil endre kontonummer for utbetaling av tilgodebeløp fra det offentlige. • Gå til www.altinn.no (men siden dette er en test må vi istedenfor gå til en URL for test) (Oplysninger på en fiktiv bruker oppgis fra intervjuer) • Finn skjema for Kontonummerendring (RF-1030-A). Skjema benyttes av privatpersoner som ønsker å endre kontonummer eller utbetalingsmåte av tilgodebeløp.	

A.4 Om bruk av koder for identifikasjon, registrering og pålogging

Hvilken type identifiserings og påloggingsmetoder bruker du og hvilke erfaringer har du i forbindelse med dette? (går gjennom tabellen under)

Type løsning	Kommentarer	Har informant opplevd utfordring i forhold til dette:
Gyldig identifikasjon:		
Pass		
Smartkort med bilde (se neste)		
Smartkort		
Bruk av smartkort i betalings-terminaler og automater, brukes oftest sammen med pinkode.		
Personlig spillkort fra Norsk Tipping (har eID i seg)	Personlig spillkort fra Norsk Tipping (har eID i seg)	
Trådløs identifisering med RFID	(Chip) e-ticket (for eksempel Oslo's sykkelutleie), dør-åpner, pass	
Bankkort med magnetstripe		
Minibankkort med personlig kode til bruk i butikk og minibanker		
Nettbank:		
Ulike nettbankløsninger med kodekort eller kodekalkulator.	Brukes i forbindelse med innlogging til nettbank, men også for å bekrefte en regning som skal betales. (Tilsvarende problemstillinger som BankID)	
Bank ID (engangskode via kodekalkulator)	Kombinasjon av personlig passord, og engangskode som man kan få via en kodebrikke eller via mobil	
Bank ID (engangs kode via mobil)	Kombinasjon av personlig passord, og engangskode man får via mobil. Eksempel: Encap	Skriv kommentarer under oppgaven.
Registrering på internett		
Ved førstegangs registrering og oppretting av brukerkontoer kreves ofte ekstra informasjon, slik som fødselsnumre, adresser og koder.	Ofte krever inntasting av koder fra visuell informasjon, slik som trykt materiell, eller kodekalkulatorer med tekstvinduer. Det er også mange nettsteder som krever en sikkerhetssjekk der man skal identifisere bokstaver og tall	

Vanligst er Brukernavn + passord + e- post-adresse (eller annen ID)	som står på kryss og tvers i et bilde, en såkalt "captcha" kode. Verified visa har kombinasjon av online registrering av et passord + PIN + engangskode. Personvernutfordring: Google prøver å samle alle ID-er ved å spørre brukeren om man ønsker å slå sammen kontoene.	
Passord:		
Passord på elektroniske tjenester (innlogging)	Eksempler: Facebook, mobilabonnement, kundeservice, kjøp av konsertbilletter via billett service, finn.no m.m.).	
Pinkoder:		
Personlige pinkoder til selv- angivelse og skattekort	Man får tilsendt et ark med mange koder	
Personlig kode til mobil (PIN og PUK)		
Talepostkasser og telefon- svarere.	For å lese av beskjeder du har fått på telefonen må man ofte taste inn en personlig kode for å få tilgang til beskjedene, være seg mobiltelefon eller fasttelefon.	
Adgangskontroll	Brukes for eksempel i borettslag for å komme inn inngangsdøren, Kodene er ofte personlige.	
Alarmkoder	Det brukes i økende grad ulike koder for innbrudds- og sikkerhetsalarmer i for eksempel bygninger.	
DigitalTV		
Engangskoder og referansenumre		
Referansenumre og koder man får på nettet	Ved bestilling av varer og tjenester på Internett (til flyreiser, togreiser, kinobilletter, teaterbilletter m.m.) får man ofte referansenumre og koder.	
Koder til selvbetjenings- automater.	Man må ofte bruke kode til selvbetjenings- automater for å hente pakker eller varer som er bestilt). Dette finne bla. på Oslo S og Majorstua T-banestasjon	
Koder til oppbevarings- bokser.	Koder til oppbevaringsbokser, for eksempel på jernbanestasjoner.	
Hotellsafer på hotellrom		
Identifisering i (offentlig) saksbehandling		
Pålogging altinn	Skal undersøkes	Kommentarer skrives under oppgaven.
Biometri		
Fingeravtrykk		
Iris-scan		
Stemme gjenkjenning		
DNA		

A.5 Kommentarer med hensyn på personvern og sikkerhet

- Hva synes du om at navnet ditt knyttes til at du har synsnedsettelse eller lese-skrive vansker?
- Hva synes du om at slike opplysninger kan gis videre til tjenester slik som banken eller minside.no
- Hva synes du om at andre tjenester på internett får vite det?
- Hva synes du om at den samme bank-id brukes som identifikasjon til ulike tjenester, også andre enn bank-tjenester, slik som e-handel.
- Banken eller andre tjenester oppgraderer ofte sine sikkerhetsmetoder, og det fører ofte til at man må gjøre ting på andre måter og lære seg nye prosedyrer. Hva er ditt synspunkt på sikkerhet vs. tilgjengelighet (bank-id vs. gammel metode)? Ville du for eksempel foretrekke å bruke en gammel metode som er tilgjengelig og som du kjenner til tross for at den ikke er like sikker som den nye bank-id metoden?

Vedlegg B: Informantenes erfaringer med ulike sikkerhetsløsninger

	Oppsummering synshemmede	Oppsummering dyslektikere
Smartkort		
Bruk av smartkort i betalingsterminaler og automater, brukes oftest sammen med pinkode.	Det er en utfordring å vite hvor og i hvilken retning man skal sette inn kortet, samt å vite hvorvidt betalingsterminalen/automaten kan benyttes med smartkort. For øvrige kommentarer se bruk av kort til minibank/betalingsterminaler.	For kort og koder som man bruker ofte og daglig går dette greit. Selv om det stort sett går greit for dyslektikere å bruke smartkort sammen med pinkoder, påpekte noen at man ofte setter kortet i feil vei og at man standarder på området.
Personlig spillkort fra Norsk Tipping (har eID i seg)	For lite informasjon til å konkludere noe, men en informant påpeker at det er vanskelig å benytte løsningen, og en annen at det kan oppstå problemer med bruk av hjelpemidler sammen med Java.	Det å huske flere forskjellige pinkoder kan være en utfordring, spesielt for kort man ikke bruker så ofte.
Trådløs identifisering med RFID	Flere bemerket at det ville være en fordel å unngå plunderet med at man drar eller stikker kortet feil vei. Informantene var ikke særlig bekymret for sikkerheten, men påpekte at utfordringen med å huske pinkoder fortsatt vil være der.	
Bankkort med magnetstripe		
Minibankkort med personlig kode til bruk i minibanker	Bruk av minibanker kan være utfordrende fordi det er ulik layout på tastatur på forskjellige maskiner, og sekvensen i hvordan man betjener dem kan variere. Videre oppleves berøringsskjermer som problematiske. Uheldig plassering av minibanker kan medføre gjenskin i skjermen, og føre til sikkerhetsrisiko ved å gi innsyn for andre. Flere av informantene benytter minibank med tale, men dette tilbys bare i noen få minibanker. Maskiner uten tale er et problem idet man ikke får tilbakemelding på hva man har tastet inn eller feilmeldinger med mer. Ønsker standardisering og forutsigbarhet mellom ulike minibanker. Se forøvrig kommentarer om smartkort.	Enkelte av informantene påpekte at brukervennligheten, eller snarere mangel på brukervennlighet i minibank og nettbank var avgjørende i forhold til hvilken bank de ønsket å være kunde hos.

Minibankkort med personlig kode til bruk i butikk	Flere av informantene foretrekker å ta ut penger i butikk. Opplever mange av de samme utfordringene som med minibank, for eksempel ulik utforming av terminaler, mangel på standard layout på tastatur etc. En av forskjellene fra minibanker er at det ofte ikke er auditiv tilbakemelding når man trykker på knapper, noe som kan forårsake feil inntasting. Innsyn fra andre påpekes som en sikkerhetsrisiko, men sikringstiltak av terminaler gjennom deksler over tastatur og lignende gjør betjening ekstra vanskelig. Ønske om standardisering av layout med mer.	Se punktet om smartkort over
Nettbank:		
Ulike nettbankløsninger med kodekort eller kodekalkulator.	To av informantene benytter ikke nettbank idet de oppfatter dette som vanskelig. To benytter nettbank med sikkerhetskode tilsendt via mobil, og en rapporterer at det kan være vanskelig å skille mellom små og store bokstaver. En informant benytter kodegenerator med store tall, og har også mulighet for tale men benytter ikke denne funksjonaliteten. Hovedutfordringen ved pålogging er kodegeneratorer som ikke presenterer koden på en tilgjengelig måte dvs. store tall, auditivt eller taktilt.	Flere av informantene brukte faktisk Storebrand bank. En av informantene oppgav enkel pålogging som en av grunnene til å velge denne banken. Her kan man bruke kodekalkulator uten PIN -kode. Det blir også bemerket at god service og muligheten for å få ordnet ting ved å ringe er viktig. Inntasting av KID-nummere er et slit. En av informantene kommenterer at opplesing av inntastet KID-nummer ville være nyttig. Det vil kunne effektivisere kontrollen. Man vil da slippe å flytte blikket og å holde fingeren på det tallet man har kommet til.
Bank ID (engangskode via kodekalkulator)	Se nettbanker generelt. Ifølge Norges Blindforbund fungerer ikke BankID sammen med tekniske hjelpemidler som skjermleser med tale/punktskrift.	Informantene hadde få kommentarer til dette.
Bank ID (engangs kode via mobil)	Se nettbanker generelt.	På tross av en del kommentarer til prototypen som ble testet, var hovedinntrykket at informantene var positive til bruk av engangskode til mobil. Noen av dyslektikerne syntes det var praktisk at koden ble lest høyt når de skulle dobbeltsjekke at de hadde tastet riktig.

Registrering på internett		
Ved førstegangs registrering og oppretting av brukerkontoer kreves ofte ekstra informasjon, slik som fødselsnumre, adresser og koder. Vanligst er brukernavn + passord + e-post-adresse (eller annen ID)	Foruten generelle navigeringsproblemer og informasjonsinnhenting på de aktuelle nettsidene, rapporterer flere at utfylling stort sett går greit. Uformingen av utfyllingsfelter og sekvens etc. kan forbedres. "Captchas" oppleves som utfordrende.	De fleste forsøker å gjenbruke noen faste koder og passord så ofte som mulig, og ellers brukes muligheten for å få tilsendt passord på e-post flittig.
Passord:		
Passord på elektroniske tjenester (innlogging)	Kun to informanter rapporterer på dette. Det blir mange brukernavn og passord å forholde seg til. NBF melder at det kan være vanskelig å fylle ut, og at krav om kompliserte passord bestående av tekst og tall er en utfordring. Utfylling sammen med tekniske som skjermleser og forstørring hjelpemidler er et problem ved at elementene ikke fanges opp av hjelpemidlene eller at de vises korrekt.	Se over
Pinkoder:		
Personlige pinkoder til selvangivelse og skattekort	Pin-koder tilsendt på papir er et problem, og man er nødt til å be om hjelp fra andre eller bruke tekniske hjelpemidler for å lese de. Forslag om å få dette tilsendt elektronisk.	Det ble påpekt at det var en utfordring å finne de riktige kodene når man trenger de. Flere kunne tenkt seg å få disse kodene elektronisk, mens en var skeptisk til dette pga. sikkerheten.
Personlig kode til mobil (PIN og PUK)	Samme som med personlige pin-koder. Dersom man ikke har tekst-til-tale på mobil får man ingen tilbakemelding på tastetrykk og vet ikke om man har tastet feil.	Enkelte med dysleksi kan ha problemer med at man bytter om rekkefølgen på tallene. Derved kan man være noe mer utsatt for å taste feil tre ganger, og har behov for å sørge for å ha PUK koden tilgjengelig
Talepostkasser og telefonsvarere.	Samme som med personlige pin-koder.	Ingen kommentar
Adgangskontroll	Utfordring er særlig avlesning av liten skjerm, og betjening av tastatur gjerne uten taktil merking.	Faste koder som brukes ofte går stort sett bra.

Alarmkoder	Ikke rapportert som problem av de fleste. For øvrig samme utfordringer som ved adgangskontroll, samt det kan være tidsbegrensning i tillegg.	Det er en fordel når kodene kan defineres selv, og i en husstand er man ofte flere som deler en kode, så flere kan huske den. Også for dyslektikere kan det være en utfordring dersom tallene er små og med har dårlig skrifttype.
DigitalTV	Kun rapportert som problem av en informant. Kun visuelt grensesnitt er en utfordring.	
Engangskoder og referansenumre		
Referansenumre og koder man får på nettet	Utfordring er generell dårlig tilgjengelighet på aktuelle internettsider, samt at det kan være vanskelig å huske lange referansenumre. Referansenumre tilsendt på sms benyttes av flere informanter. Færre betjente billettkontorer etc. medfører henvisning til selvbetjeningsautomater med berøringsskjerm som er utilgjengelig for synshemmede.	For informantene våre går det stort sett greit å ta med seg utskrift med de referansenumre/koder man trenger.
Koder til selvbetjeningsautomater.	Dette er en utfordring, men ingen relevante spesifikke problemer nevnt utover generelle utfordringer ved bruk av automater. NBF påpeker at det kan være vanskelig å finne tastatur på automater, samt problemer med å få ut pakken fra postautomater.	lite erfaring
Koder til oppbevaringsbokser.	Bruk av berøringsskjerm påpekt som utfordring. NBF melder om utilgjengelige tastaturer, samt bruk av kode på papir.	lite erfaring
Hotellsafer på hotellrom	Minibar på hotellrom med utilgjengelig adgangskontroll meldt som problem. Tastatur uten taktil merking.	lite erfaring
Identifisering i (offentlig) saksbehandling		
pålogging (Altinn se over)		
Biometri	For lite informasjon til å rapportere noe på dette.	

Fingeravtrykk		Informantene hadde ikke motforestillinger mot bruk av fingeravtrykk, og mente dette kunne forenkle identifiseringen for dem.
Iris-scan Stemme gjenkjenning DNA		Det var mer skepsis rundt de andre biometriske metodene, men ingen hadde prøvd det.

Brukervennlighet/tilgjengelighet vs. personvern og sikkerhet		
Hva synes du om at navnet ditt knyttes til at du har synsnedsettelse eller lese-skrive vansker?	Tre informanter rapporterer på dette og alle er skeptiske og ønsker ikke å gi slik informasjon.	Fire er skeptiske til dette. Det blir bemerket at banken istedenfor kan opplyse om muligheten til å bruke for eksempel lyd, og så kan man velge om man vil bruke dette eller ikke, uten å oppgi noen grunn.
Hva synes du om at slike opplysninger kan gis videre til tjenester slik som banken eller minside.no	Som over. En informant er positiv, men er betenkt dersom andre opplysninger også kan lekke ut.	-
Hva synes du om at andre tjenester på internett får vite det?	To informanter er positive til dette og to ønsker ikke en slik løsning.	Fire er svært skeptiske til å samle informasjonen under en felles bruker. En syns dette ville være veldig praktisk.
Hva synes du om at den samme bank-id brukes som identifikasjon til ulike tjenester, også andre enn bank-tjenester, slik som e-handel.	For lite informasjon. Se på dette sammen med neste spørsmål.	
Banken eller andre tjenester oppgraderer ofte sine sikkerhetsmetoder, og det fører ofte til at man må gjøre ting på andre måter og lære seg nye prosedyrer. Hva er ditt synspunkt på sikkerhet vs. tilgjengelighet (bank-id vs. gammel metode)? Ville du for eksempel foretrekke å bruke en gammel metode som er tilgjengelig og som du kjenner til tross for at den ikke er like sikker som den nye bank-id metoden?	Ønsker sikrest mulig løsning, men kan til nød bruke mindre sikker løsning som overgangsordning. En informant ville latt være å bruke løsningen. Det bør være opp til banken å vurdere sikkerheten. Det blir kommentert at bør være opp til tjenesteleverandør å kun tilby så sikre løsninger at de er villige til å bære eventuelle tap	Flere kommenterer at de bytter koders å sjeldent som mulig, kun når man blir tvunget til det. Noen velger å gjenbruke koder i størst mulig grad. Når man først blir tvunget til å endre kode/passord, oppgir en av informantene at hun da velger å forandre alle sine koder til en felles ny kode.