

eID – for meg og for oss

Riitta Hellman (Karde AS)



e-Me i et nøtteskall

- Inclusive identity management in new social media.
- Prosjekt finansiert av Verdiktprogrammet i Norges forskningsråd.
- Løper fra 2010 til 2013.



e-Me i et nøtteskall

- Målet er å framskaffe ny kunnskap om inkluderende identifiserings- og autentiseringsmekanismer i sosiale medier – altså eIDer.
- Tverrfaglig:
 - IKT
 - Jus
 - Sikkerhet og personvern
 - Brukervennlighet og tilgjengelighet



e-Me-partnere

- Norsk Regnesentral (prosjekteier)
- Karde AS (prosjektleder)
- Tellu AS
- Institutt for informatikk (UiO)
- Institutt for privatrett, Senter for rettsinformatikk (UiO)



e-Me-brukere og -partnere

- Dysleksi Norge
- Norges Blindeforbund
- Seniornett Norge

- Brønnøysundregistrene
- Encap
- Storebrand



Diskriminerings- og tilgjengelighetsloven – formål

- Trådte i kraft 1. januar 2009.
- Formål: Sikre like muligheter og rettigheter til samfunnsdeltakelse for alle uavhengig av funksjonsevne og hindre diskriminering på grunn av nedsatt funksjonsevne.
- Håndheves av Likestillings- og diskrimineringsombudet (LDO).
- FAD tar sikte på at forskriften trer i kraft i 2013.
- Difi etablerer tilsynet når forskriften trer i kraft.



Loven og universell utforming

- Utforming eller tilrettelegging av hovedløsningen ... slik at virksomhetens alminnelige funksjon kan benyttes av flest mulig.
- Gjelder for offentlige virksomheter og for privat virksomhet rettet mot allmennheten.
- Viktig utgangspunkt for FoU-arbeidet i e-Me.



Kilder

Regjeringen

- <http://www.regjeringen.no/nb/dep/bld/dok/rundskriv/2010/nytt-rundskriv-om-universell-utforming/universell-utforming-i-diskriminerings--.html?id=611202>

Lovdata

- <http://www.lovdata.no/all/hl-20080620-042.html>



Oversikt

- I. **Grunnbegreper** – Knut Eilif Husa (Tellu AS)
- II. **Tilgjengelighetsutfordringer i eID** – Kristin Skeide Fuglerud (Norsk Regnesentral)
- III. **Alternative eksperimentelle løsninger** – Ivar Solheim (Norsk Regnesentral)
- IV. **Rettslige utfordringer i eID** – Maryke Silalahi Nuth (Institutt for privatrett, Senter for rettsinformatikk)
- V. **e-Me-tutorial** – Riitta Hellman (Karde AS)



I Grunnbegreper

Knut Eilif Husa (Tellu AS)

E-post: knut.eilif.husa@tellu.no



Logg på!

Autentiser deg!

Signer her!

Bruk din e-ID!

Autoriser handlingen!



Identitet

Identitet er opplysninger som en person har om seg selv.

De kan være opplysninger om:

- Personalialia
- Relasjoner
- Oppfatning
- Tilknytting
- Avhengig av sammenheng, dvs. hva du vil legge vekt på i en bestemt situasjon.



E-identitet 1

- Elektronisk representasjon av en person i en gitt sammenheng.
- E-identiteter brukes til ulike formål.

Heykontrast AA | Bokmål Nynorsk English Sámegiella

Innlogging til Samordna opptak

Velg en elektronisk ID for å identifisere deg: [Slik skaffer du elektronisk ID](#)

MinID VELG Bruk ditt personlige passord og kode fra SMS eller kodebrev.	Buypass VELG Bruk smartkort og kortleser fra Buypass.	Commfides VELG Bruk Commfides USB-pinne.
----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------	---------------------------------------------------------------

Hjelp til innlogging: [Kontaktskjema](#) | Tlf: 800 30 300 | [Vanlige spørsmål](#) | [Om bruken av elektronisk ID](#)

Driftet av Direktoratet for forvaltning og IKT (Difø)

Logg på Google

E-post

Passord

Logg på Forbli pålogget

[Får du ikke tilgang til kontoen?](#)



E-identitet 2

Dine forskjellige e-identiteter kan være:

- Din e-postadresse for å bruke Gmail.
- Ditt Skype-navn for å bruke Skype.
- Ditt personnummer for å bruke tjenester fra banker og myndigheter.



MinID



«Myke og harde» e-identiteter 1

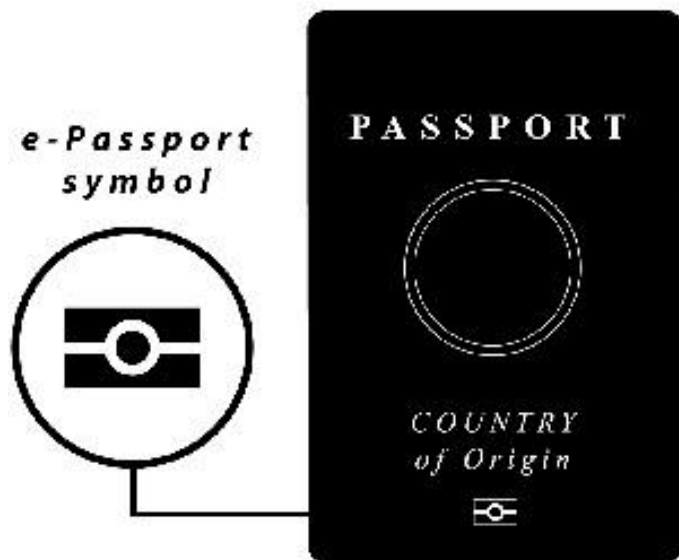
Mange e-identiteter er tilknyttet til «myke» identiteter:

- e-post-adresser
- brukerpseudonymer som for det meste er opparbeidet/skapt av deg selv.



«Myke og harde» e-identiteter 2

E-identiteter kan være tilknyttet til en «offisiell» identitet, for eksempel et pass eller et personnummer og være utstedt av en myndighet.



MinID

bankID™



Autentisering 1

Autentisering er prosessen å bevise man eier den e-identiteten man påstår å eie.

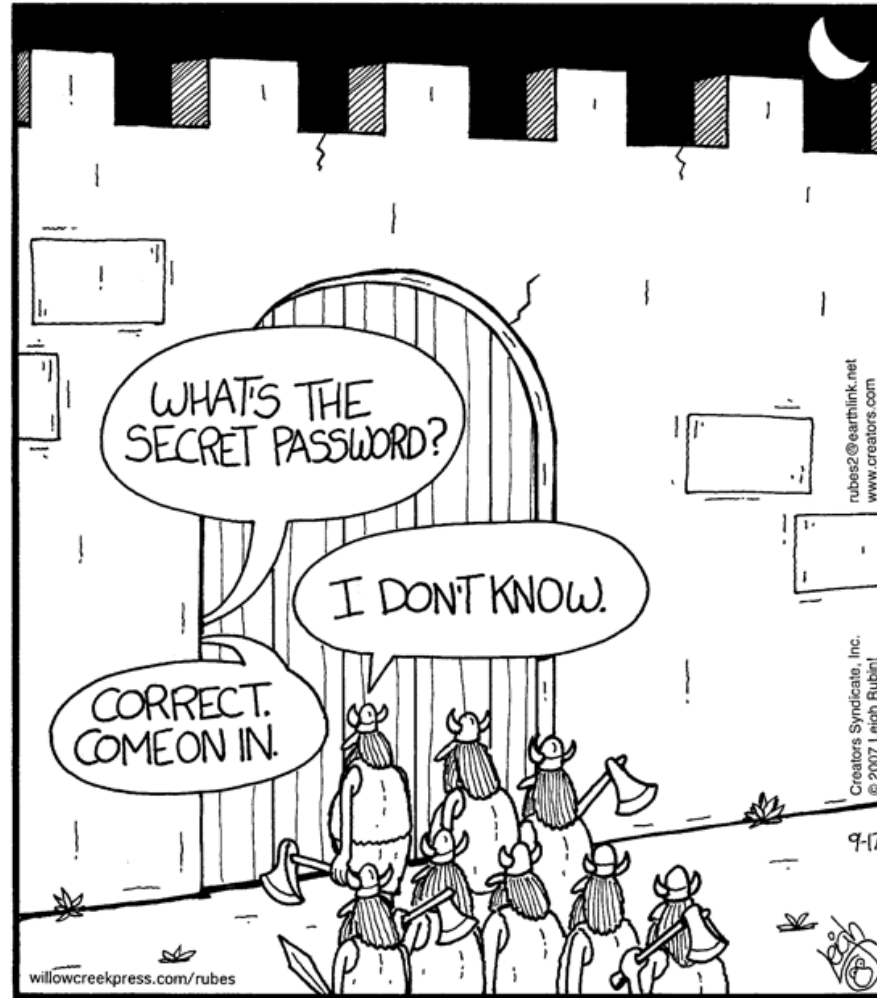
«Er det virkelig deg? Bevis det!»

Høyere grad av sikkerhet oppnås ved bruk av flere faktorer, f.eks.:

- Taste inn et hemmelig passord (noe du vet).
- Bruke nettbankens kodebrikke (noe du har).
- Skanne fingeravtrykk (noe du er).



Autentisering 2

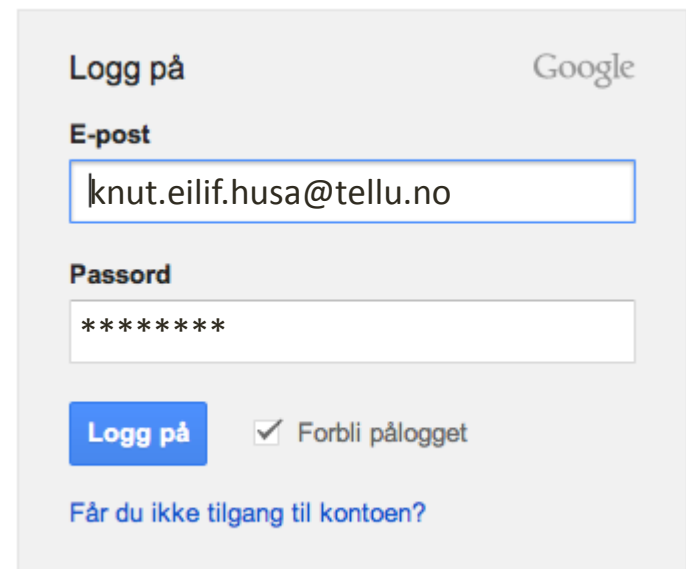


Why great care and consideration should be taken when selecting the proper password



Logge på = Identifisere + autentisere

- Først identifiserer du deg ved å legge fram e-identiteten din.
- Så autentiserer du deg ved f.eks. å taste inn ditt passord.
- Da er det bevist at du er den rettmessige eieren av den påståtte e-identiteten.



The image shows a screenshot of a Google login interface. At the top left, it says "Logg på" and at the top right, "Google". Below this, there is a section for "E-post" with a text input field containing the email address "knut.eilif.husa@tellu.no". Underneath is a "Passord" section with a text input field filled with asterisks "*****". To the left of the password field is a blue button labeled "Logg på". To the right of the password field is a checked checkbox labeled "Forbli pålogget". At the bottom, there is a link that says "Får du ikke tilgang til kontoen?".



Autorisering 1

- Autorisering er prosessen med å beslutte å gi en person, en datamaskin eller et program tillatelse til å bruke bestemte ressurser eller utføre bestemte handlinger.
- Eksempel: nettbanken. Banken kan autorisere deg å bruke bankens ressurser, og at du har lov til å gjennomføre transaksjoner.



“Wait a second, this cat wasn’t stolen. Who authorized the high-speed chase?”



Autorisering 2

- Digital signatur er en autoriseringsteknologi.
- Din e-identitet kan brukes for å lage en digital signatur.
- En digital signatur kan autorisere en handling slik at du ikke senere kan nekte for at du har samtykket.



LET'S PUT A SEAL ON THE DEAL



II Tilgjengelighets- utfordringer i eID

Kristin Skeide Fuglerud (Norsk Regnesentral)

E-post: kristin.skeide.fuglerud@nr.no



Utfordringer – basert på empiri

- Observasjoner i ulike prosjekter
 - Altinn – 1/3 av henvendelser til support
 - MinID – største utfordring ved e-valg
- Identitetshåndtering i hverdagsteknologi
 - Automater (Synshemmedes IKT-barrierer)
 - Nettbank (uu-autentisering)
 - Sosiale medier (Nettborger)
 - Bruksvilkår i private og offentlige tjenester



Automater



Nettbank




Registrering

Security Check

Enter **both** words below, separated by a **space**.

Can't read this? Try another.

Try an audio captcha



Text in the box:

[◀ Back](#)



Bruksvilkår

Bruksvilkår

Vilkår for å ta i bruk Fraktguiden fra Bring

1. Generell informasjon

Endringer i disse vilkårene kommuniseres via e-post til registrerte kontaktpersoner av Fraktguiden og det vil også bli publisert på fraktguide.bring.no. Fortsett bruk av tjenesten med kundens identifikasjonsstreng etter fire uker bekrefter at de nye, endrede avtalevilkår er trådt i kraft og akseptert.

2. Hva er Fraktguiden?

Tjenesten Fraktguide er laget for å gi nettbutikkens kunde informasjon om aktuelle leveringsalternativer, med riktig pris, leveringstidspunkt og transporttid. Dessuten inneholder den ulike hjelpemidler for å presentere leveringsalternativene korrekt og oppdatert.

3. Hva tilbyr Fraktguiden?

Prisen som oppgis er Brings listepriis basert på opplysninger som er gitt i spørringen.. Nettbutikken kan velge å overstyre denne prisen før den vises i nettbutikken. Fakturering til nettbutikken vil skje på vanlig måte, basert på inngått avtale og reell mål og vekt på pakken som sendes.

Leveringstid oppgis enten i antall arbeidsdager etter innleveringsdagen, eller som en konkret leveringsdato. Det siste betinger at nettbutikken kan legge ved korrekt informasjon om når bestillingen overleveres Bring. Beregnet leveringsdato tar hensyn til kalenderen (dvs. korrigerer for dager som ikke er arbeidsdager).

Tjenesten leverer også dekningsområdene for de ulike produktene. Noen av produktene kan ikke leveres overalt i landet, og det tar tjenesten hensyn til. Videre tilbys ytterligere informasjon og tjenester som kan benyttes for å gi mer korrekt og nyttig informasjon til mottaker.

4. Hvem kan benytte Fraktguiden?

Fraktguiden kan benyttes av alle som trenger prisinformasjon, dekningsområde eller transporttid for ulike fraktalternativ levert av Bring. Hovedsakelig er tjenestene utformet etter behovet til nettbutikker som ønsker å gi sine kunder mer oppdatert og nøyaktig informasjon. Andre interessenter kan også fritt benytte tjenestene hvis de også har behov denne informasjonen.

5. Hvordan skal Fraktguiden brukes?

Fraktguiden er ment for å gi korrekt informasjon, og modifiseres noe av innholdet er det viktig at det kommer klart frem hva som er gitt av Bring og hva som er gitt av brukeren. Innhold som modifiseres må ikke oppfattes som levert av Bring hvis det gir et feilaktig bilde av virkeligheten.

Det er ikke lov å bruke innholdet fra våre tjenester på nettsider som bryter norsk lov. Siden Posten Norge AS er en rasismefri sone er det ikke lov å bruke innholdet fra våre tjenester på nettsider som yrter rasistiske holdninger.

6. Hva bør aktive brukere gjøre?

Informasjon om endringer i tjenesten vil legges ut for påloggede brukere på <http://fraktguide.bring.no>. Ved viktige endringer vil det bli sendt varsel til registrert kontaktperson.

Du som bruker plikter å vedlikeholde kontaklinformasjonen. Dersom e-post til kontaktperson ikke blir besvart kan man risikere at brukerkonto blir slettet.

Bring vil jobbe aktivt for å videreutvikle løsningen. Vårt mål er at den skal være bakoverkompatibel. Det vil likevel kunne oppstå en situasjon der brukerne må flytte over til en nyere versjon av tjenesten. Dersom dette skulle bli nødvendig, vil brukere få tre måneders frist til å gå over til ny løsning (gammel og ny løsning vil i en periode være tilgjengelig samtidig).

Bruk av tjenesten vil bli logget av Bring. Data om bruk vil holdes internt i Bring og vil ikke deles med noen tredjepart.

7. Hvordan benytte Fraktguiden?

Bruk av tjenesten er gratis. Dette forutsetter at nettbutikken ikke trenger omfattende support for å komme i gang. Det er utarbeidet en skriftlig veiledning for oppstart. Evt. bistand fra Bring utover dette kan avtales særskilt.

Løsningen vil bli videreutviklet. Den er grundig testet, men dersom brukerne skulle finne feil bes de om å gi tilbakemelding.

8. Hvordan skal innholdet merkes?

Hvis våre retningslinjer følges kan innholdet fritt videreformidles og videreutvikles. Det er da viktig å merke innholdet fra tjenestene slik at det kommer fram at det er levert fra Posten Norge AS. Dette skal merkes med "Data er levert av Posten Norge AS".

9. Hva skjer ved feil bruk?

Dersom du bruker data fra fraktguide.bring.no på nettstedet med svært stor trafikk, eller på andre måter som gjør at våre servere kan bli overbelastet, bes du ta kontakt med Bring slik at vi kan finne en god løsning for begge parter.

Hvis innholdet fra våre tjenester misbrukes på en eller annen måte kan brukeren bli forvist fra ytterligere bruk, og i ytterste konsekvens bli stilt erstatningsansvarlig.

Mer informasjon om Bring sine API: developer.bring.com



Kategorier av utfordringer

- For store kognitive krav
- Mangelfull forklaring/tilbakemelding
- Rekkefølge
- Mange begreper
- Fysiske og tekniske barrierer



For store kognitive krav

- Totalmengden av e-identiteter og autentisering (f.eks. bruker/kort vs. passord/pin)
- Kombinasjoner
- Passordkrav
- Tvinges til å bytte autentisering
- Lange, vanskelige bruksvilkår



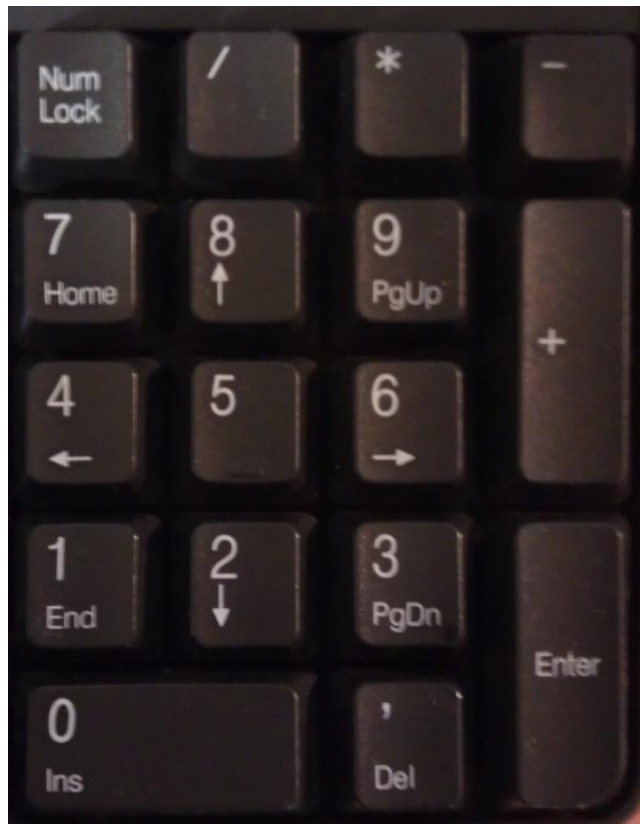
Mangelfull forklaring / tilbakemelding

- Tjenester låser seg uten tilbakemelding.
- Kun skriftlig forklaring
 - Komplisert språk eller engelsk
 - Manglende bruk av illustrasjoner (multimedia)
- Forklaring og input på forskjellig sted => må huske forklaringen.



Rekkefølge 1

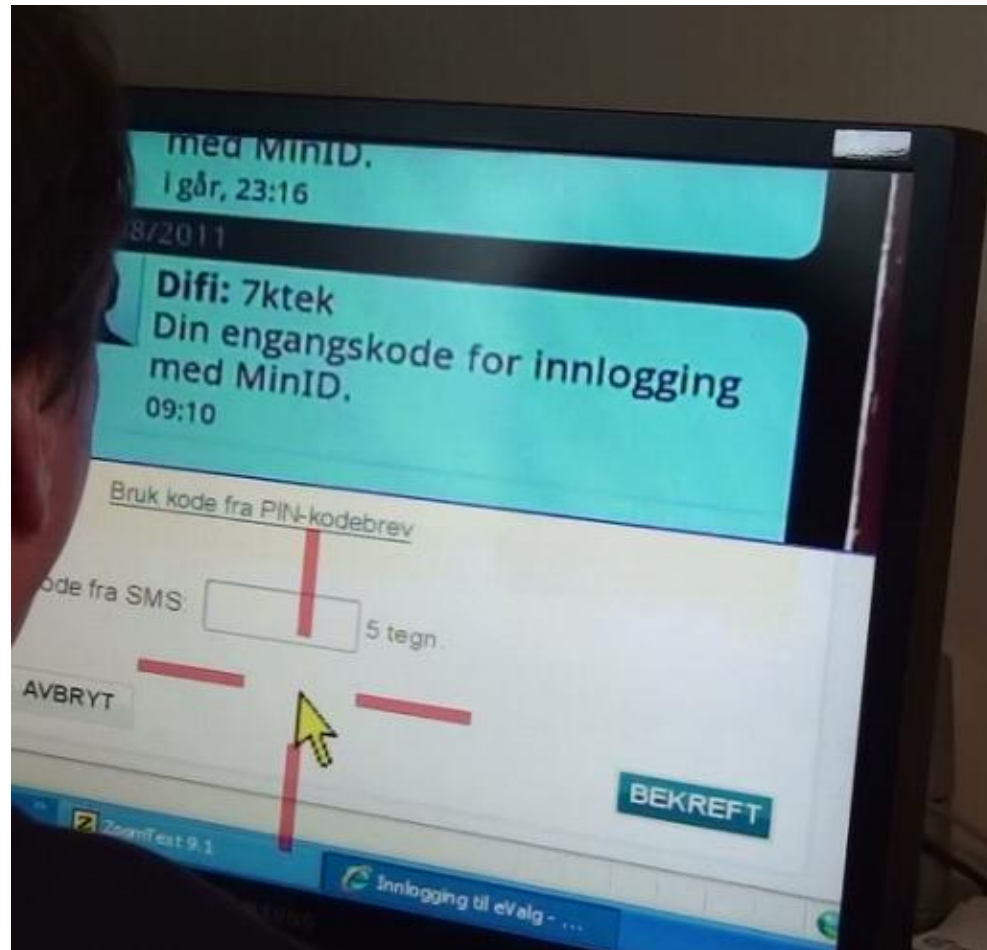
Rekkefølge på talltastatur:



Rekkefølge 2

Rekkefølge og kombinasjon av

- inputfelt på PC
- passord på e-post
- kode på mobil
- kodebrikke/ kodebrev osv.



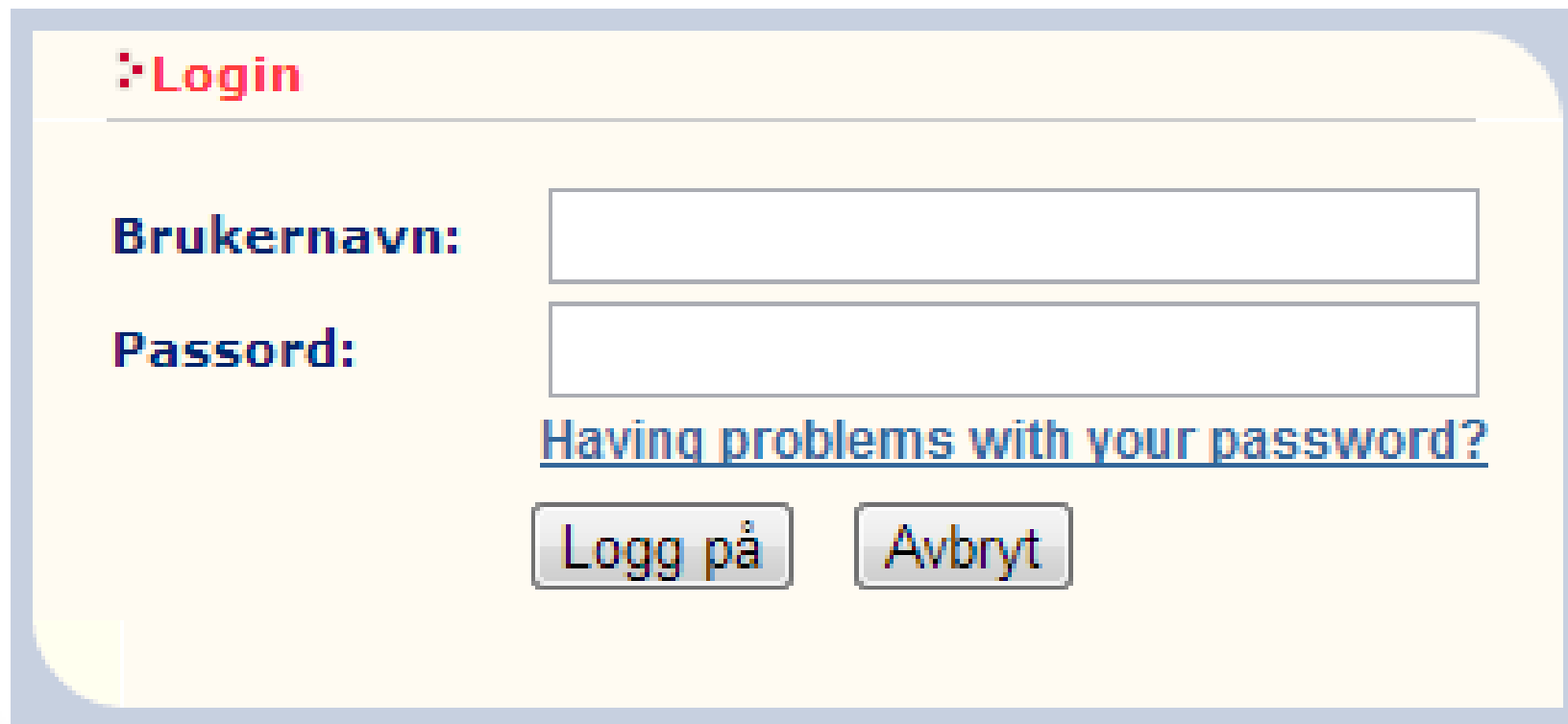
Mange begreper 1

- Fødselsnummer / personnummer – hva er hva?
 - 5, 6 eller 11 siffer?
- Passord
 - Forhåndsdefinert eller egendefinert passord
 - Engangspassord
- PIN
 - Koder fra pinkodebrev
 - Fast kode / engangskode



Mange begreper 2

Ofte blanding av norsk og engelsk:



The image shows a login form with a light yellow background and a blue border. At the top left, the word "Login" is written in red. Below it, there are two input fields: "Brukernavn:" (Norwegian for "Username") and "Passord:" (Norwegian for "Password"). Below the password field, there is a blue underlined link that says "Having problems with your password?". At the bottom, there are two buttons: "Logg på" (Norwegian for "Log in") and "Avbryt" (Norwegian for "Cancel").

Login

Brukernavn:

Passord:

[Having problems with your password?](#)



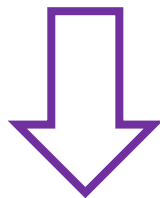
Fysiske og tekniske barrierer

- For liten tekst / dårlige kontraster
- Manglende kompatibilitet med hjelpemidler
- Trykkfølsom skjerm
- Fysisk plassering



Barrierene fører til risikoadferd

- Bruker samme passord alle steder
- Bruker dårlige passord/koder
- Skriver ned passord/pin
- Oppgir passord til andre



- Behov for mer brukervennlige og tilgjengelige løsninger



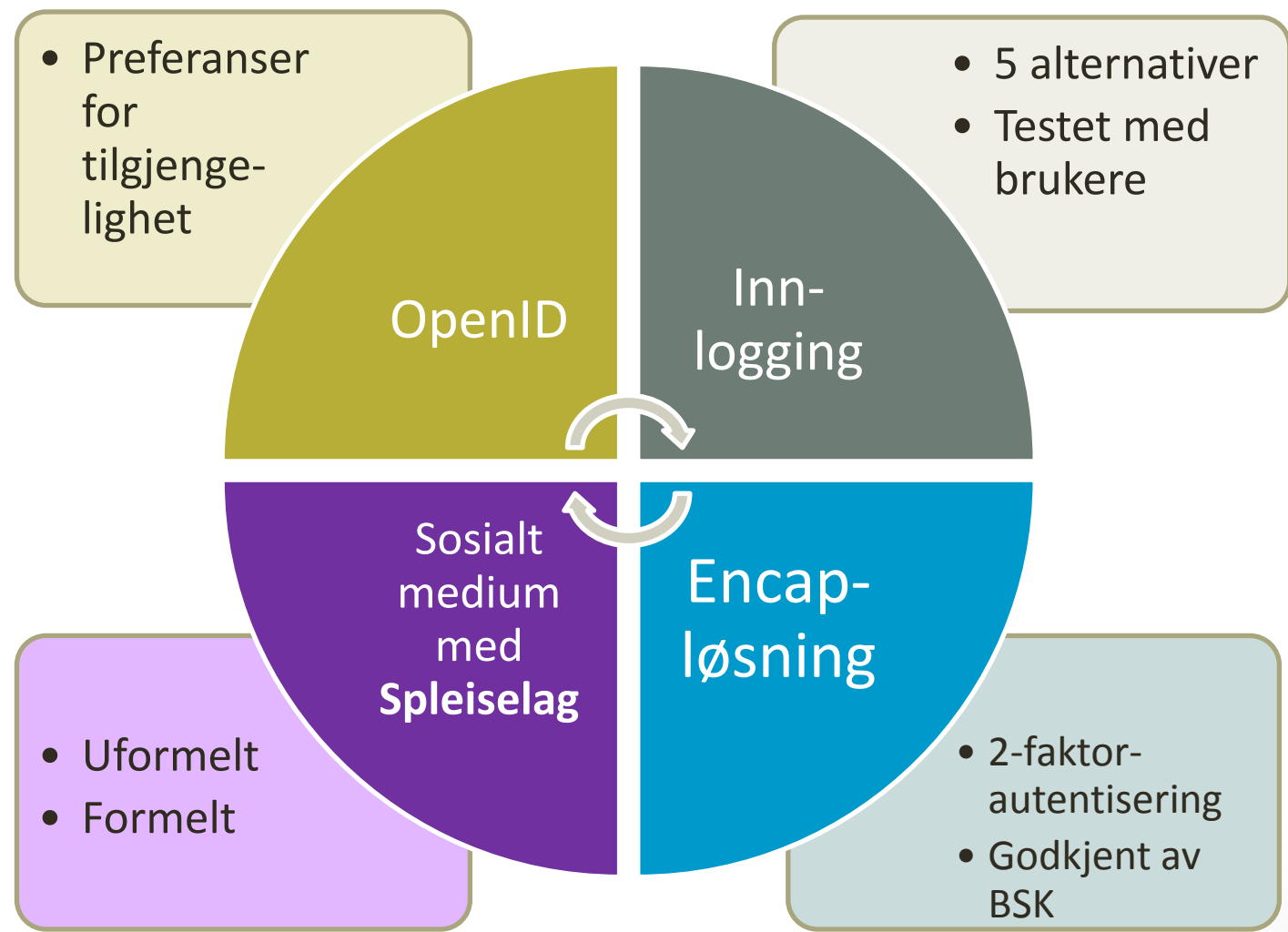
III Alternative eksperimentelle løsninger

Ivar Solheim (Norsk Regnesentral)

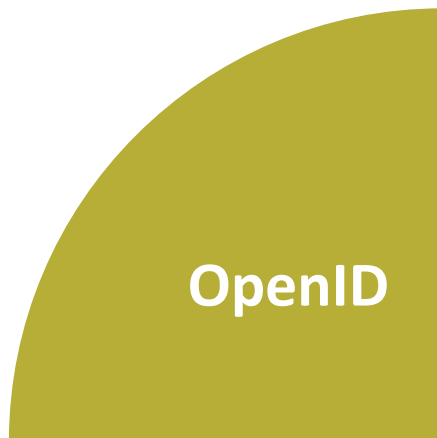
E-post: ivar.solheim@nr.no



e-Me-prototyp



eID med brukerprofil



- Brukerprofil på OpenID.
- Mange tilbydere, én autentisering.
- e-Me:
Innloggingsmekanismer + kontrast

Vanlig kontrast

Høy kontrast



Tilgjengelig innlogging



- Ulike innloggingsmetoder /autentiseringsmekanismer:
 - PIN-kode
 - Bilder
 - Lyder
 - Spørsmål
 - Mønster
- Brukertesting (eldre, studenter, dyslektikere)
- Sikkerhet og personvern varierer
- Laget selvinstruerende test



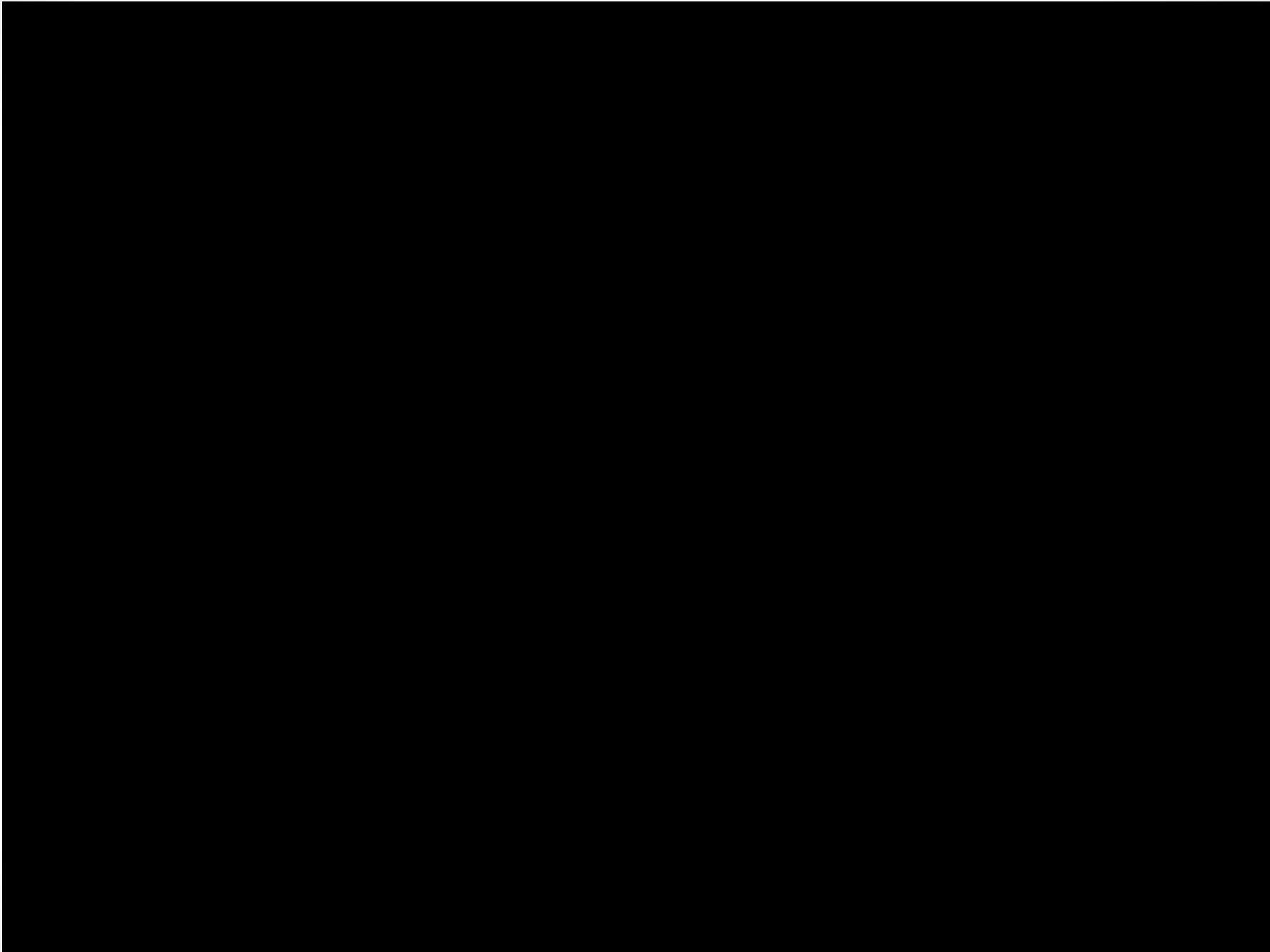
Problemstillinger

- Kan innlogging gjøres enklere og mer tilgjengelig uten at det går utover sikkerheten?
- Kan bruk av lyd og bilde bidra til forenkling og bedre tilgjengelighet?
- Er kombinasjoner av lyd, bilde, tekst bra for brukeren? Hva er brukeropplevelsen?
- Tilgjengelige metoder for synshemmede.
- Fordeler og ulemper ved ulike metoder fra et brukerperspektiv.

Nå skal vi gå gjennom de ulike metodene.

Først passord med tall og bokstaver:



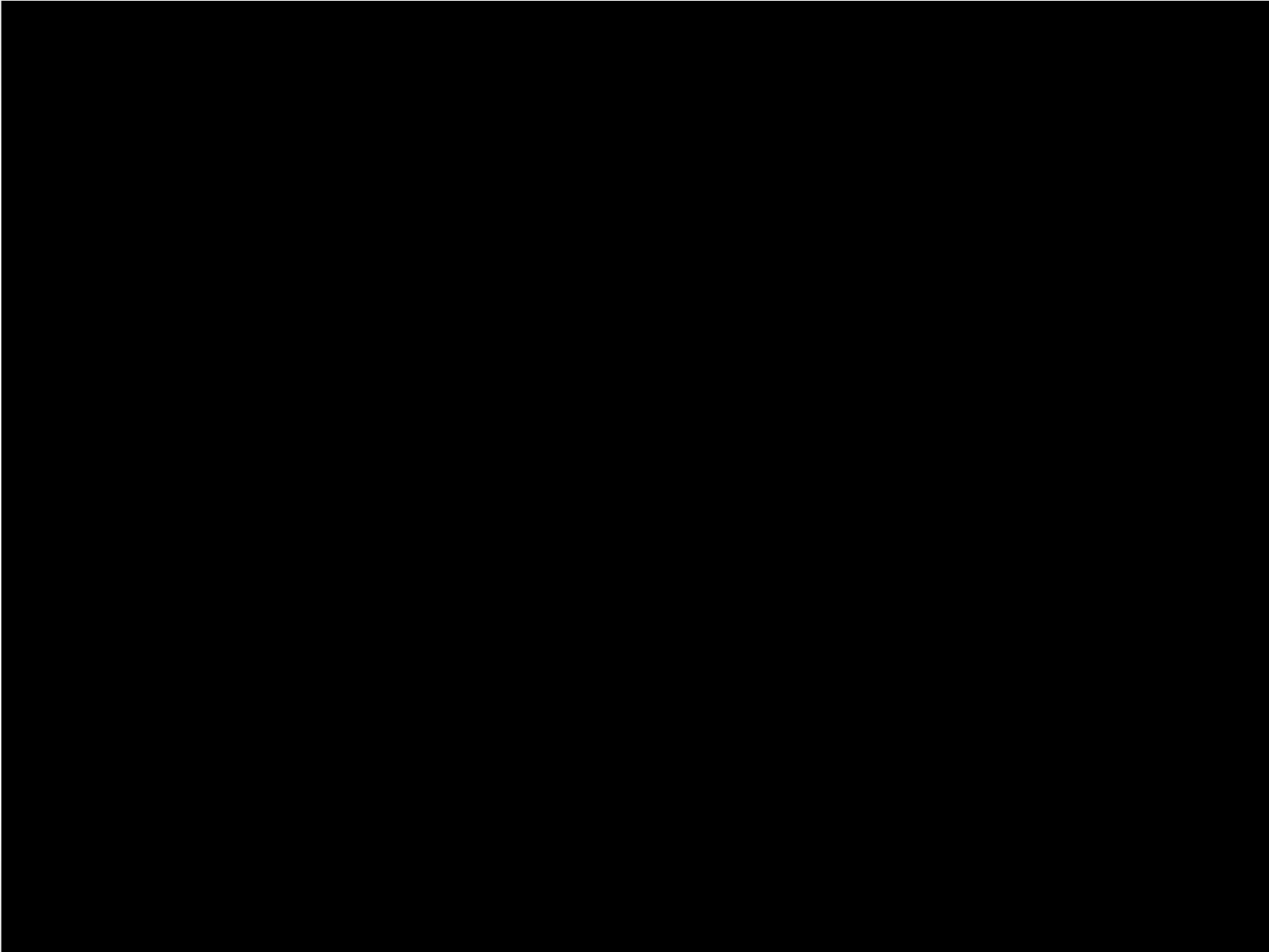


Passord

- Best likt, ved siden av spørsmål.
- Brukt før, er komfortabel med den
- Føler den er sikker.
- Usikkerhet om hvor bra det er og hvorfor:
«*Passord må være veldig bra, siden det er så utbredt*» (sitat fra utprøvingen).

Så skal vi se på en annen metode: Bilder:





Bilder

- Potensiell gevinst: valgte bilder kan være lettere å huske enn f.eks. passord. Slipper skriving.
- Mulig gevinst for dyslektikere.
- «Bilder sier mer enn 1000 ord» – og det er kanskje noe av problemet...
- Bilder kan være mer komplekse enn man tror.
- Viktig å begrense antall bilder.
- Begrense antall bilder pr. rad.
- Sikkerhet og personvern: Passer dårlig hvis andre er i nærheten – kan se bildene.



Lyder

- Er egentlig både lyd og bilde.
- Mye inntrykk å holde styr på.
- Kombinasjon av lyd og bilde er krevende.
- Passer dårlig hvis andre er i nærheten.
- Begrense antall lyder så mye som mulig.
- Valg av lyder viktig.
- Vurderes svakt i brukertest.
- Så skal vi se på mønster:



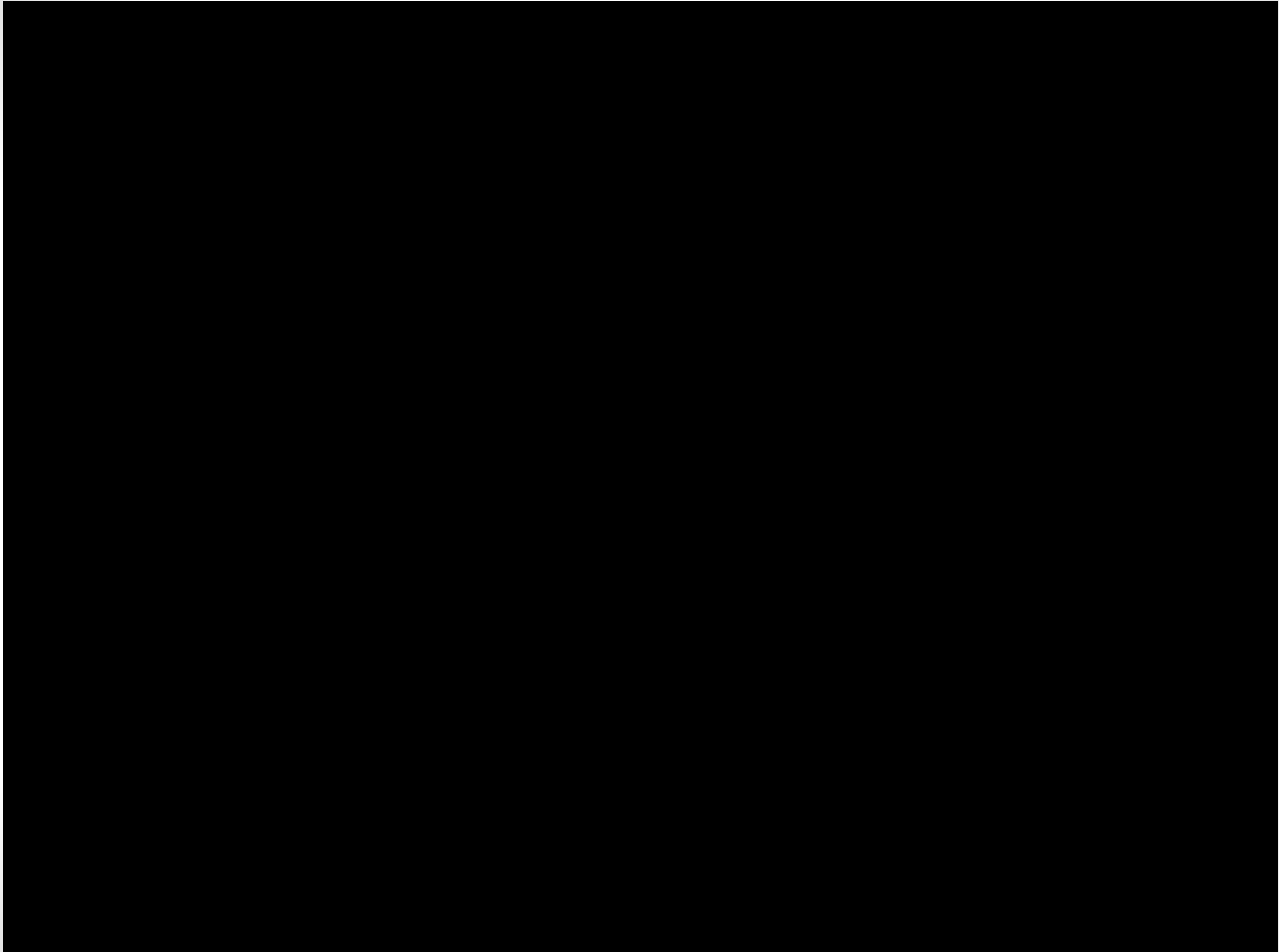


Mønster

- Enkel å bruke for de fleste, intuitiv.
- Ukjent metode, ikke like trygg på denne som noen andre, f.eks. passord og spørsmål.
- Blir gjennomført raskest av de fleste.
- Lett å lage «for enkle» mønster.
- Føler seg ikke trygg på at den er sikker nok.

Så til slutt, spørsmål:





Spørsmål

- Best likt, ved siden av passord.
- Paradoks: også den som tok mest tid for de fleste, mye inntasting.
- Gjenkjennelse, følelse av trygghet, har brukt metoden før.
- Oppfattes som sikker: «Ingen kan vite navnet på mitt første kjæledyr».



Noen foreløpige konklusjoner

- Klart behov for mer tilgjengelige påloggingsmetoder.
- Alternative metoder som bilde, lyd og mønster er interessante, men også krevende og uvant for mange
- Brukere: Følelse av trygghet og gjenkjennelse viktigere enn tidsbruk, brukervennlighet og mye inntasting.
- Begrense valgmuligheter ved bruk av bilder og lyd viktig.
- Sikkerhet oppfattes/vurderes subjektivt og intuitivt.
- Sikkerhetsnivå derfor vanskelig å vurdere for brukere, må ikke overlates til brukerne selv.



Autentisering på mobil

Encap- løsning



- Når penger er med i bildet...
- 2-faktorer: Noe du vet (PIN) og noe du har (mobil).
- Sikker: Brukes av Storebrand bank.
- Hvordan fungerer den?

<http://encapsecurity.com/wordpress/wp-content/uploads/2011/11/Encap-Technical-Overview-Paper-FINAL.pdf>



Spleiselaget

Sosialt medium med Spleiselag

- Formelle transaksjoner i en uformell kontekst.
- Sosialt medium med uformell vennskap og formelle transaksjoner.
- Organisere betalinger når f.eks. én legger ut for andre:
 - Foreldrebetaling
 - Idrettslag
 - Vennegjeng



Steg 1 av 2: Registrer kravdetaljer

Kravet

Alle felt er obligatoriske.

Melding

Beskriv ditt krav.

F.eks. vi kjørte trikk sammen i går, og jeg la ut billetten for deg.

Personer og delbeløp

Legg til personer som skylder deg penger fra vennelisten din. Alle beløp er i kroner.


Nr.	Navn	Delbeløp	
1	Ivar	20	 Slett
2	Riitta	50	 Slett
Sum		70	

 Legg til

Betalinger

Velg hvor pengene skal innbetales.

- Lommebok (200,- kroner disponibelt)
- Bankkonto

 Fortsett

 Avbryt



Oversikt for Spleiselag-tjenesten

Lommebok: 200,- kroner disponibelt

Her kan du:

- Gå til [betalingsarkiv](#)
- Se og endre dine [innstillinger](#) for tjenesten
- Les [bruksvilkårene](#)



Andre krever av deg

Du har ingen betalingskrav rettet mot deg.




Du krever av andre

Her er oversikten over det andre skal betale til deg, ett krav per linje. Det er tatt med betalinger som delvis er betalt.

Gjenstående betalinger	Samlet beløp	Dato
2 (av 2)	50,- kroner	31. oktober 2012



 Nytt spleiselag



IV Rettslige utfordringer i eID

Maryke Silalahi Nuth (Institutt for privatrett, Senter for rettsinformatikk)

E-post: m.s.nuth@jus.uio.no



Utfordringer

- Personvern og personopplysninger
- Informasjonssikkerhet
- Tilgjengelighet
- Nærmere om bruksvilkår



Personvern og personopplysninger 1

Hovedregel:

- Den behandlingsansvarlige må ha rettslig grunnlag for behandlingen: samtykke eller lovhjemmel.
- Samtykke må være uttrykkelig, informert og frivillig.
- Den registrerte skal ha kontroll på egne opplysninger og hva de brukes til.



Personvern og personopplysninger 2

Rettslige krav:

- Opplysningene skal ha tilfredsstillende kvalitet
- Opplysningene kan ikke brukes til andre formål uten nytt samtykke
- Opplysningene skal ikke lagres lenger enn det som er nødvendig for behandlingen



Personvern og personopplysninger 3

Kontroll på opplysningene:

- Hvem har kontroll?
 - Grunleggende prinsipp i personvernretten
- Den registrertes rettigheter for eks. rett til innsyn og informasjon
- Integreerte løsninger



Informasjonssikkerhet

Rettslige krav

- Tilfredsstillende konfidensialitet
- Tilfredsstillende integritet
- Tilfredsstillende tilgjengelighet

Hva er god nok sikkerhet?

- Varierende sikkerhetstiltak i de ulike IKT-løsningene
- Databehandleravtaler



Tilgjengelighet 1

- Rettslige krav (Diskriminerings- og tilgjengelighetsloven):
 - Like muligheter og rettigheter til samfunnsdeltakelse for alle.
 - Samfunnsskapte barrierer må fjernes.
 - Plikt til generell tilrettelegging (universell utforming).
- Universell utforming
 - Felles tilnærming i motsetning til særløsninger
 - Inkluderende IKT-løsning



Tilgjengelighet 2

- Hva må til for at en IKT-løsning skal være inkluderende?
 - Brukervennlighet
 - Flere valgmuligheter og funksjonaliteter
 - Hjelpemidler for informasjonstilgang og dialog
 - *Hele* prosessen bør være inkluderende og også ivareta hensynet til brukermedvirkning



Nærmere om bruksvilkår

Rettslige krav:

- Opplysningsplikt før avtaleinngåelsen
- Vilkår må presenteres på en tydelig nok og forståelig måte
 - Brukergrensesnitt og tilgjengelighet
 - Plassering
- Vilkår må være rimelige
- Samtykke?



V e-Me tutorial

Riitta Hellman (Karde AS)

E-post: rh@karde.no



Hva kommer og når?

- Fagstoff
 - Resultater fra e-Me-prosjektet
 - Resultat fra spørreundersøkelsen nov. 2012
 - Papers og foredrag
 - Kilder
 - Demoer
-
- I årsskiftet 2012-13
 - Legges ut på www.iktforalle.no



Spørsmål?
Kommentarer?

