

Høringsuttalelse om "Elektronisk stemmegivning - utfordringer og muligheter"

fra Eirik Maus og Ola Thoresen

Vi uttaler oss med dette som interesserte privatpersoner, uten å representere noen gruppe, organisasjon eller liknende.

Om rapportens temaer og innfallsvinkel

Rapporten, og utvalgets mandat, fokuserer i all hovedsak på elektronisk avleggelse av stemmen fra velgerens side. Dette virker ensidig, så lenge som et valg består av langt flere elementer. Dessuten går det klart frem av rapporten at det fra et effektiviseringsøyemed er lite å spare på dette. Det kan virke som kostnadene i forbindelse med registrering av stemmene heller kommer til å øke. I forhold til optelling av stemmene og utregning av resultatet er det jo en klar fordel om man slipper å gjøre dette manuelt, men det uttales ikke klart i rapporten. Det kan virke som det er et u-uttalt premiss for utvalgets arbeid at elektronisk avgivning av stemmer er en forutsetning for effektivisering av valgprossessen, noe vi mener er en høyst tvilsom påstand.

Forøvrig virker det som konklusjonene om hvilken retning man vil gå i har kommet før diskusjonen om hvilke kvaliteter ved stemmegivning som skal tas vare på. Etterprøvbarehet for velgerne er for eksempel tatt temmelig lett på.

Potensialet for effektivisering

Fra et overordnet perspektiv kan elektronikk og datautstyr utføre ting som kan deles i 5 kategorier. All bruk av IKT er basert på å kombinere funksjonalitet i disse fem kategoriene. Elektronikk og datautstyr kan:

1. Fange inn hendelser og gi det en digital representasjon egnet for videre, lagring, transport, bearbeiding og gjengivelse. Dette kan være forskjellige slags fenomener som skriving av tekst, at brukeren foretar et valg mellom presenterte alternativer, innfangning av fotografiske avtrykk, digitalisering av lyd osv. Dette forutsetter at datamaskinen er tilknyttet ulike former for sensorer, som f.eks. tastatur, mus, mikrofon, kamera.
2. Lagre den digitale representasjonen (av tekst, valg, bilder osv) for senere bruk. Dette viser seg som regel å være svært plasseffektivt sammenliknet med lagring av ikke-digitale gjengivelser av samme fenomen. Videre lettes gjenfinning ved at det kan sorteres på mange kriterier samtidig, og man kan utnytte elektronisk søking i materialet.
3. Lage nye digitalt representerte data ved av bearbeiding av eksisterende data fra en eller flere kilder. Dette kan være å lage oppsummeringer av hvor mange brukere som har valgt de ulike presenterte alternativene, lage ny versjon av en tekst hvor ord som ikke står i en ordliste er uthevet med rød farge, lage et nytt bilde hvor fargen i de ulike bildepunktene er korrigeret for dårlige lysforhold og kontrast i det originale bildet, og egentlig hva som helst annet hvor det finnes en fremgangsmåte for å produsere ønsket resultat fra de ulike data man allerede har.
4. Overføre en kopi av den digitale representasjonen av noe / informasjonen fra ett sted til et annet.
5. Gjengi data overfor brukere f.eks. i form av fargede punkter formet som bokstaver og valgalternativer på en skjerm, lyd i høyttalere eller annet.

Innsparingspotensialet ved bruk av IKT i alle sammenhenger, ikke bare valg, ligger der hvor man har

manuelle, arbeidskrevende operasjoner som kan puttes inn i en eller flere av kategoriene over. Konkret i forhold til valg er det tre ting som peker seg ut som klare kandidater for innsparing:

- a. Overføring og presentasjon av valgmulighetene til velgeren.
- b. Innfanging av velgerens valg.
- c. Opptelling av velgerens valg og utregning av resultatet.

De endelige valgmulighetene presenteres i dag overfor velgeren i form av papirlister som trykkes opp og distribueres rundt i et et antall som er langt større enn antall velgere. Innfanging av velgerens valg foretas ved at velgeren velger en av listene og eventuelt foretar rettelser. Opptelling foregår til slutt ved å telle de valgte listene.

Rapporten fokuserer i all hovedsak på problemstillinger knyttet til punkt a og b, men praktisk talt ikke til forhold rundt punkt c. Om dette er til tross for eller på grunn av at ting rundt elektronisk innfanging og lagring av stemmer er langt mer kontroversielt enn elektronisk opptelling går ikke fram. Det kan virke som om det er et underforstått premiss ved rapporten og/eller utvalgets mandat at elektronisk avstemning (innfanging av velgerens valg) er en forutsetning for elektronisk opptelling. Dette er ikke tilfelle. Det er fullt mulig å utforme listene slik at de kan leses maskinelt med svært liten grad av menneskelig "assistanse". Straks de er lest inn og digitalisert, vil opptellingen og utregning av mandater kunne gå på sekunder.

Potensialet for tilgjengeliggjøring

Rapporten tar for en stor del for seg problemstillinger knyttet til avstemning med elektronisk utstyr, og kommer inn på muligheter for avstemning over internett eller gjennom andre kanaler. Elektronisk avgivelse av stemme er i seg selv neppe kostnadsbesparende. I stedet kan det benyttes til å gjøre stemmeavleggelse (eller forhåndsstemming) tilgjengelig flere steder enn nå, blant annet hjemme på folks egne datamaskiner, og med åpningstid hele døgnet.

Rapporten nevner knapt mulighetene for å utnytte teknologien til å tilgjengeliggjøre avstemning på andre måter. Vi vil trekke frem at elektronisk stemmegivning åpner for at alternativene kan presenteres overfor velgeren på flere språk. Man kan også (ved hjelp av alminnelige høretelefoner for å sikre hemmelig valg) utnytte opplesing av alternativene, sånn at svaksynte kan delta på like vilkår, og med mindre grad av assistanse fra andre enn de trenger i dag.

Videre vil man også kunne utnytte elektronisk stemmeavlegging til å sikre at stemmen er konsistent og gyldig før den lar seg registrere. Dette kan også betraktes som en form for tilgjengeliggjøring overfor en velger som ellers ville fått sin stemme forkastet.

Vi mener det må vises litt varsomhet i hvilke digitale kanaler og kommunikasjonsformer man velger å benytte til så alvorlige saker som valg. Alle kanaler har sitt eget innhold og sin egen form. En del av disse har en egen kultur for avstemninger av typen "trenger uføretrygdede puter under armene eller et spark bak?" og "er sennep eller ketsjup viktigst på pølsa?". Valg bør foregå i en ramme av seriøsitet som understreker alvorret i handlingen.

Hemmelig valg

Vi vil rose utvalget for en del tillitvekkende forslag når det gjelder hemmelige valg. Denne delen virker for det meste godt gjennomtenkt, og tar opp i seg en del viktige elementer. Vi deler utvalgets syn på at å tillate valg i ukontrollerte omgivelser vil innebære kompromisser mot prinsippet om hemmelig valg. Vi støtter ideen om at valg fra ukontrollerte omgivelser ikke skal tillates siste dag av valget, slik at den stemmeberettigede har mulighet til å avlegge en stemme under kontrollert hemmelige forhold på valgtinget. Det ville i denne sammenheng klart være en fordel om velgeren kunne fått en tilbakemelding dersom en stemme er avlagt i hennes navn, slik at eventuelle feil eller innbrudd kan korrigeres ved at velgeren stemmer på valgdagen.

Som utvalget påpeker krever det å bevare en slik mulighet til om-stemmeing etter forhåndsstemming at en forbindelse mellom velgeren og den avlagte stemmen beholdes helt til avstemningen er avsluttet. Det arbeidet og de forslagene som er presentert på dette området virker meget godt gjennomtenkt.

Vi vil likevel påpeke viktigheten av at elektroniske valg alltid vil være et kompromiss mellom full hemmeligholdelse og etterprøvbarhet. Prinsippet om at man skal kunne kontrollere og verifisere valgresultatet i etterkant av valget må alltid være med, siden dette er en kvalitet ved valg som må sies like viktig å beholde som hemmelig stemmegivning.

Det forundrer oss også at rapporten har såpass få betenkeligheter med å foreslå valg fra usikrede omgivelser (se eget avsnitt om dette), når dette så åpenbart vil stå i sterk motsetning til hemmelige valg.

Sikkerhet, åpenhet, tillit og etterprøvbarhet

I rapporten trekkes den konklusjonen at man av sikkerhetshensyn og kvalitetshensyn ikke kan bruke åpen kildekode. Sikkerhet skal i stor grad ivaretas ved "security through obscurity". Samtidig skal store deler av programsystemet distribueres rundt i landet på et tusentalls CD-ROMer, et antall som er stort nok til at man må regne med at kopier kommer på avveie og blir analysert av interesserte. Vi mener kombinasjonen av sikkerhet gjennom uforståelighet, samtidig som man distribuerer "hemmeligheten" i tusentalls kopier, er dømt til å mislykkes. Den beste måten å da sikre at flest mulig feil og sikkerhetsproblemer knyttet til valgsystemet blir oppdaget før de kan bli utnyttet er at koden i utgangspunktet er åpen og tilgjengelig for alle.

Vi har i et eget avsnitt lenger ned forsøkt å oppklare noen åpenbare misforståelser når det gjelder begrepet "åpen kildekode".

I forhold til åpenhet og tillit er det viktig å påpeke det følgende:

Rapporten sier at elektronisk avstemning og lagring av stemmene vil redusere åpenheten i valgprosedyren og gjøre denne utilgjengelig for folk flest. Dette er vi enig i. Videre påpeker rapporten at dette vil gå i retning av ekspertvelde, hvor bare noen få eksperter må gå god for at prosessen foregår korrekt. Som mekanisme for å likevel beholde tillit, foreslår rapporten et vell av sertifiseringsordninger, meta-sertifisering av sertifiseringsorganene og så videre. Dette utgjør et sett av tiltak som helt sikkert vil redusere antallet aktuelle eksperter til knapt en håndfull i Norge. Utvelgelsen (sertifiseringen) av disse ekspertene skal selv foretas av hva man må kunne omtale som et ekspertvelde, og dermed kunne forsterke problemet. Vi tror ikke manglende tillit til ekspertvelde skyldes manglende tillit til ekspertenes kompetanse, men heller redsel for at ekspertene skal bli en liten klikk med en intern og, for utenforstående, ikke-tilgjengelig agenda. Den foreslåtte medisinen blir dermed "mer av det som er problemet".

I det hele tatt mener vi utvalget er helt på feil spor når det gjelder forholdet mellom ekspertvelde, tillit og åpenhet. Det er riktig at det å sette seg inn i hvordan et program fungerer er noe som krever spesiell kompetanse. Samtidig er ikke denne kompetansen mer spesiell enn at tusentalls mennesker over hele landet besitter den. Tross alt er det klart lettere å lese programkode enn å lage den. Selv om ikke alle kan forstå programkoden og hvordan programmet fungerer, vil vi tro det er overkommelig for de fleste grupperinger å finne noen de kan stole på som kan forstå store deler av den.

Sertifiseringordninger kan sikkert forhindre at helt inkompetente leverandører vil være i stand til å vinne en anbudskonkurranse om å levere systemet. Det er uansett lite trolig at slike ville komme seg gjennom en prekvalifisering eller tilsvarende, og enda mindre at de ville blitt valgt som leverandører. Når man tar i betraktning hvor mange sikkerhetsproblemer det er med produkter leverert av verdens ledende software-leverandører, med enormt dyktige fagfolk, er det likevel tvilsomt om en slik utsiling av inkompetente er tilstrekkelig til å sikre at det ikke blir problemer med systemet. På mange måter fremstår dette som en større mengde sermonier hvis funksjon i like stor grad blir å holde oppdragsgiver og prosjektorganisasjon fri for skyld, om noe mot formodning skulle gå galt, som å sikre at systemet fungerer korrekt og ikke kan manipuleres.

I det hele tatt har utvalget fokusert mer på sikre tilliten til "ekspertveldet" enn å vurdere tiltak som kan motvirke graden av ekspertvelde og sikre at velgerne selv kan forsikre seg om at valget foregår korrekt og er tillitverdig. Dette synes vi er en overraskende feilvurdering.

Vi mener en forutsetning for tillit til systemet er at det er åpent og etterprøvbart for allmenheten og/eller eksperter publikum selv velger. Etterprøvbarhet må være et siktemål både for funksjonaliteten som helhet, for resultatet og for den enkelte velger.

- Alle må kunne forsikre seg om at sin egen stemme er registrert korrekt, og at velgeren får lov til å gå tilbake og registrere prefereransene på nytt, helt til velgeren har fått produsert en stemme som inneholder det velgeren ønsker å stemme på.
- Denne stemmen må være lagret, eventuelt i en kopi, i en form som også er leselig for velgeren, på et ikkemodifiserbart medium.
- Alle avgitte stemmer må lagres på en menneskeleselig og ikke-modifiserbar form, som er egnet for etterprøving og om-telling, helt til alle er enige om resultatet og kvaliteten på valget.
- Det må være mulig for alle å forsikre seg om at behandlingen og opptellingen av stemmene foregår på en måte som er rettferdig og korrekt.
- Åpenhet om systemets funksjon og virkemåte bør være et høyt prioritert mål, og bør være en del av prosjektet helt fra starten sånn at svakheter kan komme på bordet tidsnok til å bli reparert. Alternativet med hemmelighold og sertifisering må ses på som en siste utvei, og må bare benyttes dersom det av andre grunner blir helt umulig å åpne for innsyn i de sentrale deler av systemet.

Kontrollerte eller ukontrollerte omgivelser

Rapporten foreslår at man bør starte forsøk med valg fra ukontrollerte omgivelser (f.eks over internett, via SMS osv).

Selv om sikkerheten ved autentisering av den som avgir stemme og for at de avgitte stemmene kommer med i valget er på plass er det likevel tre viktige grunner til at vi på det sterkeste vil fraråde dette.

- **Etterprøvbarhet.**

Som nevnt tidligere er et vesentlig element i valgprosessen at man i etterkant kan etterprøve resultatet. For at dette skal være mulig er man avhengig av at en form for kvittering for de avgitte stemmene oppbevares på et format som er menneskelig lesbart og ikkemodifiserbart (f.eks papir). Dersom det avgis stemmer fra ukontrollerte omgivelser vil det ikke være praktisk mulig å etterprøve resultatet, da det ikke vil eksistere noen form for bekreftelser på at de stemmene som er avgitt også har blitt talt.

- **Sikkerhet for hemmelige valg**

Kun ved at valget foregår i kontrollerte omgivelser kan man garantere at ikke den som stemmer er utsatt for utilbørlig press, og at det ikke foregår kjøp og salg av stemmer.

- **Tillit til valgsystemet**

Politiske valg er, og skal være, en prosess med en stor grad av tillit rundt seg. Selv om man har et mål om størst mulig valgdeltakelse må ikke det gå på bekostning av tilliten til valgene og det politiske systemet generelt. Vi ønsker ikke at valgene degenereres til avstemninger av typen "er det best med leverpostei eller makrell i tomat på brødiskiva", som i dag er det som kjennetegner f.eks de fleste avstemninger på SMS.

Så lenge disse elementene er umulig å ivareta utenfor kontrollerte omgivelser kan vi ikke se at det vil være mulig å gjennomføre valg fra ukontrollerte omgivelser. En mulig økt valgdeltakelse av ukjent størrelse kan ikke rettferdiggjøre at så viktige prinsipper for demokratiske valg settes til side.

Rettelse av feil om teknologi og gjennomførbarhet

Flere påstander i rapporten om teknologi og "tilstøtende temaer" er feil i en så graverende grad at det ikke kan stå uimotsagt.

Rapportens omtale av åpen kildekode er vanskelig å relatere til virkeligheten. Utvalget omtaler dette som nærmest anarkistiske fritidsprosjekter der vilkårlige personer herfra og derfra limer inn kode i ny og ne uten verken planer eller tidsfrister. Dette er svært langt fra sannheten for de fleste prosjekter. Det finnes mange ulike oppfatninger av hva åpen kildekode er og skal være. Felles for alle er at brukerne av programmet i tillegg til å ha tilgang til de binære maskin-kjørbare komponentene også har tilgang til den tekstlige kildekoden som disse har blitt generert fra.

Selv om man tillater andre å både lese og bruke den kildekoden man selv utvikler, er dette på ingen måte uforenelig med å ha ansatte utviklere som jobber på heltid med fastsatte kvalitetsrutiner, tidsfrister for utgivelser og funksjonalitet. Tvert imot er det ofte nødvendig å ha ekstra strenge slike rutiner hvis ikke alle bidragsyterne er samlokalisert og kan kommunisere uformelt med hverandre. Det er jo heller ikke sånn at "lokale" endringer i et program automatisk og ukritisk får bli en del av det offisielle programmet. Mange prosjekter har svært strenge krav til koden de integrerer i den offisielle versjonen av programmet. De drar likevel nytte av at andre kommer med forslag, eksempler, ideer til løsninger osv. som kanskje gjør utviklerne oppmerksomme på problemer og utfordringer de ellers ville oversett, selv om de ikke nødvendigvis velger å løse det på den måten som den "utenforstående" har foreslått.

Det pågår mange store prosjekter innen blant annet finans og telekom i Norge basert på rammeverk fra åpen-kildekode-prosjekter, så der er det hvertfall ingen som mener det er mer risikabelt å basere seg på slike enn de lukkede. Mange av de mer populære rammeverkene er også utviklet av kommersielle firmaer med faste (og offentlige) planer for utgivelser. Det er ingen grunn til at det skulle være noen motestning mellom å la brukerne se kildekoden og det å ha faste planer for utgivelser.

Å tro at "security through obscurity" vil være sikrere enn å tillate alle kompetente personer å gå gjennom koden har blitt tilbakevist mange ganger. Det siste eksempelet fra Nederland, der en gruppe som kaller seg "Vi stoler ikke på stemmemaskiner" ("Wij vertrouwen stemcomputers niet") analyserte de maskinene som planlegges brukt i det nederlandske valget denne høsten, og fant flere store sikkerhetsproblemer knyttet til disse i løpet av bare ca en måned

Det vil alltid være muligheter for at ondsinnede personer klarer å skaffe seg tilgang til systemer de ønsker å skaffe seg tilgang til. Nettopp derfor er det viktig at flest mulig med gode hensikter også har disse tilgangene. Dermed er sjansen for at feil oppdages og kan rettes **før** de blir utnyttet er størst mulig.

Man må huske på at det store flertallet av programmerere og dataeksperter er lovlidige og fornuftige personer, og at både muligheten til å hjelpe samfunnet, samt det å få "æren" for å ha oppdaget og publisert (og eventuelt rettet) en sikkerhetsfeil i et sånt system vil være en pådriver for at svært mange vil ønske å bidra med en gjennomgang av koden.

De problemene som på denne måten oppdages og publiseres av vennligsinnede vil uansett bli funnet av mindre vennligsinnede, som ikke har noen skrupler med å bryte både lover og låser for å skaffe seg tilgang og kontroll over såpass viktige elementer i et demokrati som gjennomføringen av et valg.

Forøvrig er veldig mange produkter brukt i sikkerhetsøyemed, sånn som webtjenere, brannmurer, krypteringsbiblioteker m.v. basert på åpen kildekode.

Vi er også kjent med at NUUG/EFN har korrigert en del feiloppfatninger om brannmurer i sin uttalelse,

som er verdt å ta med seg.

Forslag til veien mot elektroniske valg i Norge

1. Arbeidet med å utvikle og teste "stemmemaskiner" settes i gang.

- Prosjektene som utvikler dette må åpne for innsyn i all kildekoden som utvikles i prosjektet, sånn at alle kan etterprøve og kontrollere måten resultatene fremkommer på.
- Stemmemaskinene må selvsagt tilpasses norske forhold, og ivareta alle valg-funksjonene vi har i dag, som kummuleringer, strykninger osv
- De må også produsere "kvitteringer" til velgerne som beviser at stemmen er regisert på den måten velgeren ønsket å stemme. Disse kvitteringene må oppbevares på tilsvarende måte som dagens stemmesedler, så de kan brukes som bekreftelse og etterprøving dersom det blir tvil om valgresultatet i etterkant.
- Det er ikke sikkert man behøver å "finne opp hjulet på nytt". En fordel ved bruk av åpen kildekode er at man i svært stor grad kan basere seg på allerede eksisterende systemer, og så eventuelt gjøre egne tilpasninger av disse. Se referansene for eksempel på eksisterende åpne prosjekter for elektroniske valg
- I første omgang gjøres det forsøk med elektroniske stemmemaskiner i enkelte valgkretser både for å teste ut teknologien, og for å få erfaringer med hvordan publikum reagerer og hva slags konsekvenser det får både for valgdeltakelse og for effektivisering av gjennomføringen av valget. Man kan med hell forsøke ut forskjellige typer elektroniske stemmeinnsamlinger samtidig i forskjellige valgkretser for å skaffe seg erfaring med fordeler og ulemper ved flere systemer i løpet av samme valg.

2. Det innføres "elektronisk manntall"

- For forhåndsstemmer, stemmer fra utlandet osv. behøver ikke dette være noe annet enn at det genereres en strekkode ell. som identifiserer den som har stemt, så denne informasjonen kan leses elektronisk på valgdagen. Stemmene deres sendes så inn til valgstyret på samme måte som i dag.
- I stemmelokalene registreres det elektronisk når folk kommer for å stemme.
- Dette kan ha flere fordelaktige bieffekter, som at hvis folk kommer til valglokalet og tidligere har forhåndsstemt, så kan de få beskjed om dette, og på den måten tilleggsverifisere at de vil stemme på nytt, evt. bare for å kontrollere at forhåndsstemmen deres er registrert osv.

3. Når punkt 1 er testet i en del valgkretser og man har kommet fram til en best mulig teknisk løsning, og punkt 2 er innført er det en smal sak å innføre stemmemaskiner og elektroniske valg over hele landet.

Når vi har kommet så langt vil vi mene at vi har elektroniske valg her i Norge. Som påpekt er det vår mening at valg fra ukontrollerte omgivelser ikke kan gjennomføres på en tilfredsstillende måte, derfor ønsker vi ikke å gå videre inn på dette.

Noe vi derimot kan se for oss er at vi kan lage stemmemaskinene så enkle og distribuerbare at definisjonen av et "valglokale" i stor grad kan mykes opp. Så lenge en del krav tilfredsstilles kan er det ikke noe problem å se for seg ambulerende "valglokaler" som drar hjem til folk som ikke har mulighet til å komme til et valglokale. Det kan også organiseres valglokaler på mindre steder og på måter vi i

dag ikke kan forestille oss. Det er ikke noe ønske fra vår side at man skal gjøre det mer vanskelig og tungvint enn nødvendig å få avgitt sin stemme, og at telleprosessen skal ta lengst mulig tid. Men samtidig mener vi at man ikke bør se seg blind på ideen om det er valglokalenes utilgjengelighet som fører til lavere valgdeltakelse, og at bare alle får stemme fra sofaen ved så sende kodeord "valg" til 1814, så blir alt så meget bedre.

Referanser

1. Open Voting Consortium - <http://www.openvotingconsortium.org/>
2. Wikipedia om Elektroniske Valg - http://en.wikipedia.org/wiki/Electronic_voting
3. Voluntary Voting System Guidelines - http://www.eac.gov/vvsg_intro.htm
4. "Wij vertrouwen stemcomputers niet" - <http://www.wijvertrouwenstemcomputersniet.nl/English>
5. Rapporten fra denne nederlandske gruppa, på engelsk - <http://www.wijvertrouwenstemcomputersniet.nl.nyud.net:8080/images/9/91/Es3b-en.pdf>