Utgitt av:
Kommunal- og regionaldepartementet

Offentlige institusjoner kan bestille flere eksemplarer av denne publikasjonen fra:
Departementenes servicesenter
Kopi- og distribusjonsservice
www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefaks: 22 24 27 86

Oppgi publikasjonskode: H-2185
Omslagsillustrasjon: Sissel Sandve
Trykk: Nr1Arktrykk 01/2006 – opplag 800

Rapport

Elektronisk stemmegivning – utfordringer og muligheter

KOMMUNAL- OG REGIONALDEPARTEMENTET

Rapport

Elektronisk stemmegivning – utfordringer og muligheter

KOMMUNAL- OG REGIONALDEPARTEMENTET

Forord

Arbeidsgruppen ble oppnevnt av Kommunal- og regionaldepartementet 26. mai 2004, og fikk i oppdrag å ta stilling til om og eventuelt hvordan det bør innføres elektronisk stemmegivning her i landet.

Gruppen har vært organisert i fire undergrupper med utgangspunkt i medlemmenes kompetanse; en teknisk gruppe, en økonomisk-administrativ gruppe, en demokratigruppe og en jussgruppe. Gruppen har hatt 11 fellesmøter. Undergruppene hatt egne møter i tillegg til fellesmøtene. Selv om undergruppene har hatt ansvaret for hvert sitt kapittel, har hele gruppen vært med på å diskutere og bestemme innholdet i rapporten.

Medlemmer av arbeidsgruppen har vært på studieturer til England, Sveits, USA og Estland. Disse turene er beskrevet nærmere i kapittel 4 og i vedlegg C. Gruppen har i tillegg hatt møter med sentrale aktører og miljøer i forbindelse med diskusjoner av blant annet datasikkerhet, sertifisering og kontroll.

Arbeidsgruppen vil få takke alle de enkeltpersoner og institusjoner som har kommet med verdifulle innspill i løpet av mandatperioden.

Februar 2006

Innhold

1 Mandat og sammensetning

Arbeidsgruppen ble oppnevnt av Kommunal- og regionaldepartementet 26.05.04, og fikk i oppdrag å utrede bruk av elektroniske medier når stemme avgis ved valg til storting, fylkesting og kommunestyrer.

1.1 Medlemmer

1. Bernt Aardal – leder, Institutt for samfunnsforskning
2. Asbjørn Ausland – Oslo kommune
3. Cort A. Dreyer – Nærings- og handelsdepartementet
4. Are Vegard Haug – UiO, Jur.fak., avd. for forvaltningsinformatikk
5. Einar Nødtvedt – Senit Rådgivning AS
6. Kristian Pinaas – Intentor Solutions AS
7. Bjørn Erik Rasch – UiO, Institutt for statsvitenskap
8. Marianne Riise – Kommunal- og regionaldepartementet
9. Gerhard Skagestein – UiO, Institutt for informatikk
10. Kristin Thorud Skorpen – Drammen kommune
11. Kari Aarnes – Trondheim kommune

Rune Karlsen – sekretær, Institutt for samfunnsforskning
Guro Stavn – sekretær, Institutt for samfunnsforskning

1.2 Mandat

Følgende er arbeidsgruppens mandat:
”Arbeidsgruppen skal på prinsipielt grunnlag vurdere og ta stilling til *om og ev. hvordan* det bør innføres muligheter for elektronisk stemmegivning her i landet. Videre skal gruppen vurdere og foreslå hvilke regler og krav som bør stilles til systemer for elektronisk stemmegivning. (For å lette henvisningene til de ulike punktene i mandatet, har arbeidsgruppen valgt å nummerere de enkelte punktene).
Til dette inngår følgende elementer:

1. vurdere betydningen av innføring av et elektronisk system i et demokratisk perspektiv, herunder legitimitet og valgdeltagelse
2. gi en oversikt/utredning av ulike måter/system å avgi stemme elektronisk gjennom ulike typer kanaler (Internett, pekeskjerm, SMS, digital-tv m.m.)
3. peke på fordeler og ulemper ved de ulike systemene/kanalene
4. gi en vurdering av disse ut fra brukervennlighet og sikkerhet
5. drøfte og vurdere om det bør tillates elektronisk stemmegivning ved hjelp av Internett-teknologi, både i og utenfor valglokalene
6. vurdere løsninger for identifisering av velger i forbindelse med elektronisk stemmegivning (smartkort, id-kort e.l.)
7. problemstillingen ”utilbørlig påvirkning” i forbindelse med stemmegivning utenfor valglokalet må vurderes særskilt, jf. også diskusjonen poststemmer
8. vurdere problematikken kjøp/salg av stemmer eller identitet i forbindelse med stemmegivning utenfor valglokalet

9. vurdere om det bør innføres verifikasjonsløsninger i systemene, og i tilfelle komme med forslag til hvordan slike løsninger kan legges opp
10. vurdere problematikken åpen kildekode
11. vurdere ev. bruk av et landsdekkende elektronisk manntall, betydningen i forhold til et system der stemmer avgis elektronisk
12. vurdere fordeler og ulemper ved elektronisk stemmegivning vs ordinær stemmegivning
13. vurdere kostnadselementer ved elektronisk stemmegivning i større skala, på kort og lang sikt, herunder hvilke innsparingspotensial som finnes på kort og lang sikt
14. vurdere betydningen av en overgang fra lekmannskontroll til profesjonalisering; blant annet betydningen for valgsystemet mht kontroll, administrasjon av valg, kompetanse
15. vurdere ansvarsforholdene ved elektroniske valg, lokalt og nasjonalt
16. vurdere hvordan godkjenning av elektroniske system bør foregå
17. sammenstille forskning/utredninger på området
18. redegjøre for internasjonale erfaringer med ulike typer system for stemmegivning.

Det pågår i regi av Europarådet et arbeid med utvikling av et *felles juridisk og teknisk rammeverk* (inkl. datateknisk standardspråk EML) *for e-voting*, hvor Norge deltar. Europarådets rekommandasjon ventes å bli behandlet innen utgangen av 2004. Arbeidsgruppen skal vurdere hva rekommandasjonens bestemmelser betyr for Norge i praksis.

Utover de spesifikke spørsmål nevnt i mandatet, står gruppen fritt til å ta opp andre spørsmål knyttet til bruk av elektroniske medier ved stemmegivning.

Arbeidsgruppens vurderinger skal munne ut i en rapport som skal legges frem for departementet innen 31. desember 2005.”

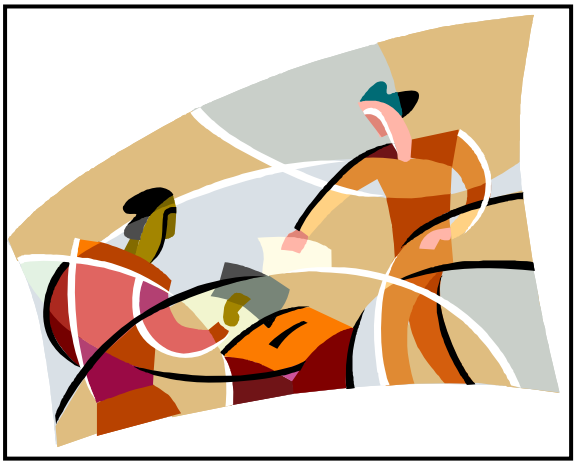
2 Arbeidsgruppens anbefalinger

2.1 Innledning

I denne rapporten diskuterer arbeidsgruppen om det bør innføres elektronisk stemmegivning her i landet, og eventuelt hvordan dette bør gjennomføres. Spørsmålet er vurdert ut fra demokratiske, juridiske, tekniske og økonomisk-administrative hensyn. Diskusjonen er strukturert i forhold til tre sentrale dimensjoner for hvordan velgerne avgir stemme:

1. Et viktig skille går mellom tradisjonell papirstemmegivning og elektronisk stemmegivning.
2. Et annet skille går mellom stemmegivning i valglokaler under kontroll av valgfunksjonærer (såkalte *kontrollerte* omgivelser) og stemmegivning utenfor valglokalene (såkalte *ukontrollerte* omgivelser).
3. Et tredje skille har å gjøre med tidspunktet for stemmegivningen, der vi skiller mellom forhåndsstemmegivning før valgtinget (i rapporten kalt *fase 1*) eller på valgtinget (i rapporten kalt *fase 2*). En nærmere oversikt over kombinasjoner av de tre dimensjonene vises i tabell 3.1 og 3.2 i kapittel 3.

Det overordnede mål for arbeidsgruppens anbefalinger er å gjøre det enklere og mindre kostnadskrevende for velgeren å utøve sine demokratiske rettigheter. Et middel for å oppnå dette er å tilby elektronisk stemmegivning i ukontrollerte omgivelser for alle velgere. I tillegg til økt tilgjengelighet vil elektronisk stemmegivning på sikt bidra til reduserte kostnader i forbindelse med valgavviklingen, og raskere og mer nøyaktig opptelling av stemmene. Det kan innvendes at denne form for stemmegivning vil svekke det preg av høytidelighet som kjennetegner valghandlingen i et tradisjonelt valglokale. I den forbindelse vil arbeidsgruppen understreke at elektronisk stemmegivning kun anbefales som et *supplement* til den tradisjonelle måten å avgi stemme på, og at stemmegivning i valglokale vil bestå i overskuelig fremtid. Dette innebærer at velgere som ikke føler seg trygge på teknologien, fortsatt vil kunne stemme på tradisjonell måte. Det kan i den forbindelse nevnes at den utstrakte bruken av forhåndsstemmegivning i de senere årene allerede har bidratt til å endre den tradisjonelle måten å avgi stemme på.[1] Men uansett hvilken måte valget gjennomføres på, er det en avgjørende forutsetning at velgerne har tillit til systemet og prosessen.



Hvis man skal tillate stemmegivning i ukontrollerte omgivelser – uansett om stemmen avgis elektronisk eller manuelt (for eksempel pr. brev) – har man ikke lenger en garanti for at kravet om hemmelig stemmegivning blir ivaretatt på en tilfredsstillende måte. Det åpnes både for utilbørlig påvirkning av velgeren (for eksempel *family voting*) og kjøp og salg av stemmer. Ved å tillate velgeren å stemme flere ganger i forhåndsstemmeperioden, og mulighet

[1] Ved de tre siste stortingsvalgene er rundt 20 prosent av stemmene avgitt på forhånd. Se figur 5.1 i kapittel 5.

til å stemme på nytt i kontrollerte omgivelser på valgtinget, reduseres denne faren betydelig selv om den ikke forsvinner helt.

I det følgende skal vi kort oppsummere noen hovedpunkter i arbeidsgruppens anbefalinger.

2.2 Demokratiske prinsipper og legitimitet (se kapittel 5)

Prinsippet om hemmelige valg er særlig vanskelig å ivareta i forbindelse med stemmegivning – elektronisk eller pr. brev – utenfor valglokalene. Det å tillate elektronisk stemmegivning i ukontrollerte omgivelser på valgdagen (fase 2), kommer klart i strid med prinsippet om å gi alle velgere mulighet for hemmelig stemmegivning. Arbeidsgruppen legger derfor følgende premisser til grunn for tilfredsstillende tekniske løsninger: 1) Valg skal fortsatt gjennomføres i to faser, med en periode for forhåndsstemmegivning og et valgting, 2) Elektronisk stemmegivning i ukontrollerte omgivelser er kun aktuelt i perioden for forhåndsstemmegivning.

Velgere kan selvsagt være utsatt for utilbørlig påvirkning også om stemmegivningen foregår i ukontrollerte omgivelser i fase 1. Likedan utgjør kjøp og salg av stemmer et mulig faremoment. For å møte problemer av denne typen, foreslås et system med en *angremulighet* for velgere som stemmer elektronisk i fase 1. Samtidig opprettholdes tradisjonelle valglokaler, dvs. steder hvor velgere garantert kan avgi en hemmelig stemme selv om de har stemt elektronisk én eller flere ganger tidligere. I fase 2 kan det som i dag stemmes bare én gang og da kun med papirstemmesedler. Velgere som har stemt *elektronisk* i fase 1, kan avgi (ny) stemme i godkjent valglokale – enten i fase 1 eller fase 2. Sist avgitte stemme er alltid tellende.

Gitt det opplegget som skisseres ovenfor, er det grunn til å tro at alle velgere har god mulighet til å avgi stemme usett og upåvirket – selv om det tillates å stemme elektronisk i ukontrollerte omgivelser. Likedan sikrer en seg mot kjøp og salg av stemmer, fordi en potensiell kjøper aldri kan være sikker på at en kjøpt, elektronisk stemme faktisk blir tellende.

2.3 Juridiske hensyn (se kapittel 6)

I rapporten gis det en vurdering av både nasjonal og internasjonal lovgivning som har betydning for elektronisk stemmegivning, og hvilke krav som må settes til et regelverk for slik stemmegivning. Særlig viktig er Europarådets anbefaling (rekommandasjon) om standarder for elektronisk stemmegivning. Etter dagens lovgivning er elektronisk stemmegivning ikke tillatt. Valgloven og forskrift til denne er basert på at velgerne skal benytte papirstemmesedler ved avgivelse av stemme. Dersom det innføres muligheter til å stemme elektronisk, må valglovgivningen derfor endres. Inntil slik endring eventuelt finner sted, vil det imidlertid være anledning til å gjennomføre forsøk der det utformes midlertidige regler for spesifikke forsøk i forskrift.

Selv om demokratiske krav til hemmelig stemmegivning i prinsippet ikke uten videre er forenlig med elektronisk stemmegivning, er det juridisk delte meninger om hvor langt kravet strekker seg i forhold til Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 3. Venezia-kommisjonen legger til grunn at elektronisk stemmegivning lar seg forene med EMK så fremt det tas visse forhåndsregler. I siste instans vil spørsmålet måtte løses rettslig,

nasjonalt eller internasjonalt. Siden rettsstillingen synes å være såpass uklar, vil domstolene i en eventuell rettssak måtte legge stor vekt på praksis.

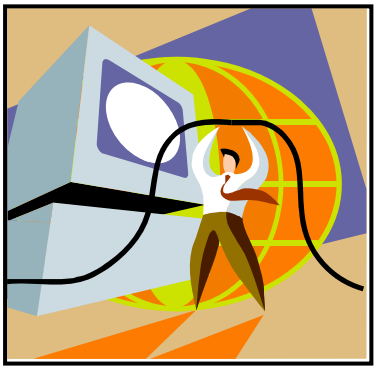
2.4 Økonomisk-administrative hensyn (se kapittel 7)

I dag brukes det store ressurser på å gjennomføre valg i Norge. Fra kommunenes side må det være en forutsetning at bruk av moderne teknologi reduserer ressursbehovet og ikke øker det. Elektronisk stemmegivning vil ha en rekke administrative fordeler både ved at presisjonen på valgoppgjøret bedres og at de endelige resultatene vil foreligge raskere. Elektronisk stemmegivning vil også bidra til å redusere en rekke manuelle prosedyrer og kontrollrutiner som i dag er ressurskrevende. Elektronisk stemmegivning i *kontrollerte omgivelser* vil imidlertid utløse nye kostnader i form av investeringer i nytt datautstyr, riggkostnader samt behov for flere avlukker, eventuelt lokaler med større bemanning enn ved tradisjonelle valg.

Det er først ved elektronisk stemmegivning i *ukontrollerte omgivelser* at arbeidsgruppen mener man på sikt kan forvente å oppnå økonomiske besparelser. Forsøksvirksomheten vil imidlertid innebære at man både kompliserer den administrative gjennomføringen og øker ressursbruken fordi man må tilby elektroniske løsninger i tillegg til ordinær valggjennomføring. Arbeidsgruppen anbefaler derfor at forsøksvirksomheten ikke bare må styres fra sentralt hold, men at den også forutsetter statlig finansiering.

2.5 Teknologiske utfordringer og mulige løsninger (se kapittel 8)

Teknologisk er det to hovedutfordringer i forbindelse med elektronisk stemmegivning i ukontrollerte omgivelser: dels å vite hvem velgeren er (identifisering og autentisering), og dels å kunne registrere, overføre og telle velgerens stemme på en hundre prosent sikker måte. Identifikasjon og autentisering av velgeren kan gjøres enten ved hjelp av noe velgeren *har* (for eksempel et smartkort), noe velgeren *vet* (for eksempel en PIN-kode), eller noe velgeren *er* (dvs. en fysisk egenskap ved velgeren som kan avleses, som fingeravtrykk eller retinamønster). Arbeidsgruppen mener at man bør unngå å innføre egne identifikasjonsmekanismer for elektroniske valg. I dagens situasjon er det PKI-løsningen som er planlagt brukt i elektronisk kommunikasjon med offentlig sektor, som er den mest aktuelle løsningen, og da på sikkerhetsnivå "Person-høyt".



Når det gjelder registrering og overføring av velgerens stemme, mener arbeidsgruppen at dagens teknologi brukt i ukontrollerte omgivelser ikke gir tilstrekkelig sikkerhet. Det er imidlertid grunn til å tro at sikrere løsninger vil komme på markedet etter hvert.

Arbeidsgruppen foreslår at elektroniske stemmer avgitt i ukontrollerte omgivelser skal kunne trekkes tilbake, enten gjennom en ny elektronisk stemme eller ved stemmegivning på selve valgtinget. For å oppnå dette, må hver enkelt elektronisk stemme være koblet til velgerens identitet helt fram til stemmen ikke lenger kan kalles tilbake, men selve stemmen må i hele denne perioden være forseglet (i praksis kan dette gjøres ved hjelp av kryptering). Dette setter spesielle krav til rutinene rundt behandling av elektroniske stemmer. Dette utdypes nærmere i kapittel 8.

2.6 Kontroll og godkjenning (se kapittel 9)

For å kunne sikre at de tekniske løsningene i et system for elektronisk stemmegivning er trygge, og at velgerne har tillit til systemet, anbefaler arbeidsgruppen at en uavhengig instans, utpekt av valgmyndighetene, skal kontrollere at systemene er i orden og at de nødvendige forholdsregler med hensyn til sikkerhet er tatt hos leverandørene. Dette innebærer konkret at det bør gjennomføres en forhåndsgodkjenning (sertifisering) av *personell og virksomheter* som på vegne av valgmyndighetene skal godkjenne leverandører og tekniske løsninger for elektroniske valg (akkrediterte sertifiseringsorgan eller evalueringsfirmaer). Det bør videre gjennomføres en forhåndsgodkjenning av *prosedyrer og rutiner* som leverandører av elektroniske valgløsninger skal følge for å sikre valgløsningene. Ansvarlig for å godkjenne leverandørene er akkrediterte sertifiseringsorganer. Valgmyndighetene skal *kun* anvende leverandører som er godkjent/sertifisert på de kritiske delene av løsningen for elektroniske valg. Det bør også gjennomføres en forhåndsgodkjenning (sertifisering) av *teknisk utstyr og teknisk løsning*. Utstyr som mangler godkjenning/sertifisering bør som hovedregel ikke anvendes i valgløsningen. På kritiske deler av løsningen *skal* sertifisering foreligge.

Den anbefalte løsningen vil medføre en delvis overgang fra lekmannskontroll til profesjonell kontroll. Den vil slik sett få betydning for hele valgsystemet, både med hensyn til kontrollfunksjonen, administrasjon av valg og kompetanse. En forutsetning for den anbefalte løsningen er at det utferdiges en kravspesifikasjon for elektroniske valg i Norge. Inntil det eventuelt foreligger en *de facto* standard for elektroniske valg eller lov og forskrift, skal kravspesifikasjonen bygge på de juridiske, operasjonelle og tekniske krav som fremsettes i Europarådets rekommandasjon, inkludert de endringer som er skissert i kapittel 8.

Arbeidsgruppen legger imidlertid til grunn at dagens kontroll- og godkjenningsrutiner stort sett bør ligge fast i forsøksperioden. Utviklingen av nye løsninger for kontroll og godkjenning bør derimot inngå som en viktig oppgave for den anbefalte prosjektgruppen, jf. kapittel 10. Som en midlertidig løsning bør denne prosjektgruppen ha godkjenningsansvar for den tekniske løsningen.

2.7 Langsiktig mål og offensiv satsing

Hvis man åpner opp for elektronisk stemmegivning i ukontrollerte omgivelser, er det en ufravikelig forutsetning at det legges til grunn strenge krav til sikkerhet, og at det skjer på en måte som ikke svekker velgernes tillit til systemet. Med dagens teknologi er det ikke mulig å garantere en slik sikkerhet. Arbeidsgruppen vil derfor ikke anbefale elektronisk stemmegivning i ukontrollerte omgivelser i fullskala nå. Det dreier seg derfor om en langsiktig målsetning.

Det kan likevel tenkes at det vil oppstå et betydelig press i retning av å innføre elektronisk stemmegivning i ukontrollerte omgivelser på et senere tidspunkt. Et slikt press kan for eksempel komme som følge av den generelle samfunnsutvikling der IKT tas i bruk på stadig flere områder, fordi elektronisk stemmegivning innføres i andre land eller at det kommer krav om elektronisk stemmegivning som følge av dramatisk fall i valgdeltakelsen. Arbeidsgruppen ser det som svært viktig at elektronisk stemmegivning i ukontrollerte omgivelser *ikke* blir innført uten forutgående utprøving, og vil derfor sterkt understreke behovet for en offensiv satsing fra myndighetenes side. Det bør så snart som mulig settes i gang planmessige forsøk og systematisk evaluering. Formålet med forsøkene er tosidig: dels en utprøving av tekniske løsninger, og dels en bygging av tillit til elektronisk stemmegivning blant velgerne.

2.8 Trinnvis innføring (se kapittel 10)

Arbeidsgruppen foreslår en trinnvis prosess bygd på systematiske forsøk med elektronisk stemmegivning. Forsøkene behøver imidlertid ikke gjennomføres i tilknytning til ordinære valg. En del forsøk kan gjøres som kontrollerte eksperimenter der spesielle grupper av velgere deltar. Det gjelder for eksempel utprøving av brukergrensesnitt. Andre former for avstemninger som lokale folkeavstemninger kan også være hensiktsmessige å bruke i forsøksvirksomheten. Valg av arena for forsøkene bør først og fremst være bestemt av hensynet til håndterbarhet og effektiviseringsgevinst. Når det gjelder forsøk som er knyttet opp mot valg, bør de gjennomføres i tre trinn:

2.8.1 Trinn 1

I første trinn foreslås elektronisk stemmegivning i kontrollerte omgivelser med sikret nett og datamaskiner med sikkerhetslogg. Det vil si at velgeren stemmer ved hjelp av en datamaskin i et godkjent valglokale under oppsyn av offentlige valgfunksjonærer. Sikkerhetsloggen sørger for at stemmen ikke går tapt ved et eventuelt systemsammenbrudd. I den grad man kan sikre datamaskinen hos velgeren (for eksempel ved hjelp av egen CD-rom for oppstart av maskinen), kan forsøket også omfatte stemmegivning i ukontrollerte omgivelser. I det sistnevnte tilfellet anbefaler arbeidsgruppen at forsøket avgrenses til ikke-bindende valg, for eksempel rådgivende, lokale folkeavstemninger. Formålet med forsøkene vil være å prøve ut brukergrensesnitt, tekniske løsninger samt velgernes tiltro til de valgte løsningene.

2.8.2 Trinn 2

Etter en systematisk evaluering av erfaringene i trinn 1, vil det være naturlig å gå videre til trinn 2 der arbeidsgruppen anbefaler at man gjør forsøk med elektronisk stemmegivning i ukontrollerte omgivelser i mindre skala for spesielle grupper (for eksempel utenlandsboende, funksjonshemmede eller enkeltkommuner). I dette trinnet kan forsøkene med kontrollert datamaskin i ukontrollerte omgivelser også omfatte bindende valg. For ukontrollert datamaskin i ukontrollerte omgivelser anbefaler arbeidsgruppen forsøk i forbindelse med ikke-bindende valg (se for øvrig kapittel 10).

2.8.3 Trinn 3

Gitt at erfaringene fra trinn 2 tilsier at man går videre, vil det være naturlig med en gradvis utvidelse av forsøkene med stemmegivning i ukontrollerte omgivelser med ukontrollert datamaskin også for bindende valg, slik at forsøkene omfatter stadig større velgergrupper.

2.9 Sentralt ansvar og godkjenningsordninger

Før man setter i gang forsøk med elektronisk stemmegivning, bør det etableres en egen prosjektgruppe som har et overordnet ansvar for planlegging, gjennomføring og evaluering av forsøksvirksomheten. I tillegg må det etableres et sentralt godkjenningsregime for kravspesifikasjoner, inkludert overvåking, kontroll og gjennomføring. Det gjelder godkjenning av virksomheter som skal gjennomføre sertifisering, godkjenning av prosedyrer og rutiner hos leverandørene og godkjenning av teknisk utstyr og løsninger.

I den grad man velger å innføre elektronisk stemmegivning som en ordinær del av valget, vil arbeidsgruppen peke på at en del av prosjektgruppens oppgaver vil ha en langsiktig og til dels varig karakter. Dette aktualiserer spørsmålet om man bør opprette en sentral valgkommisjon som kan tilføres også andre oppgaver knyttet til planlegging og gjennomføring av valg. Dette

er imidlertid et spørsmål som bør vurderes i sammenheng med de erfaringer som gjøres i forbindelse med prosjektgruppens arbeid.

3 Valg - en sammensatt prosess

3.1 Innledning

I dette kapitlet skal vi sette spørsmålet om elektronisk stemmegivning inn i en større sammenheng, og ikke minst vise at planlegging og gjennomføring av valg er en omfattende og sammensatt prosess. Videre plasserer vi diskusjonen om elektronisk stemmegivning inn i en ramme av tre overordnede dimensjoner, og diskuterer fordeler og ulemper ved ulike typer elektronisk stemmegivning.

Frie, rettferdige og hemmelige valg er en nødvendig forutsetning for et demokratisk politisk system. Men det er ikke en tilstrekkelig forutsetning. Vi finner mange eksempler på at ikke-demokratiske regimer avholder valg for å styrke sitt omdømme både i egen befolkning og i den internasjonale opinion.[2] Dette illustrerer imidlertid den store betydning demokratiske valg har for borgernes oppslutning om sine politiske ledere og deres tiltro til det politiske systemet.

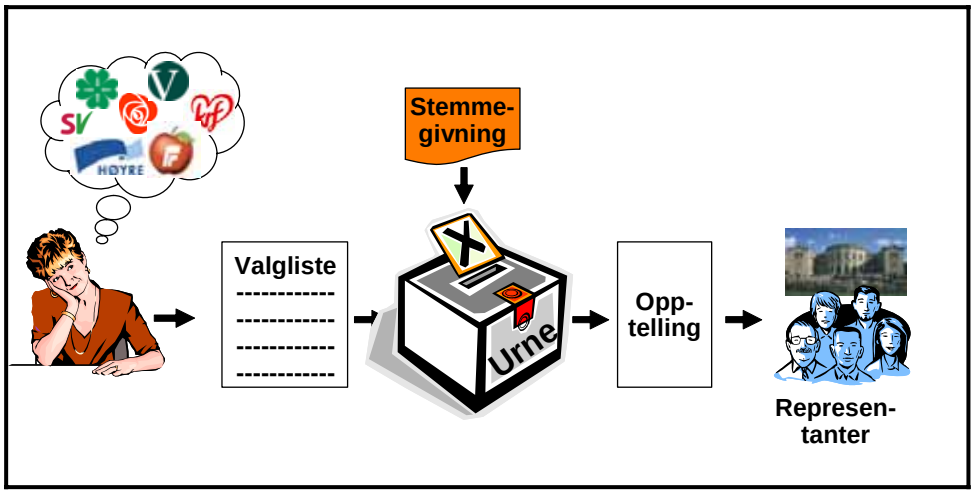
Politiske valg avholdes på ulike geografiske nivåer. I Norge har vi fire typer valg: stortingsvalg, kommunestyrevalg, fylkestingsvalg og sametingsvalg. Valg kjennetegnes ved at de er strengt lovregulert. Det gjelder både hvem som kan avgi stemme, hvem som kan velges, hvordan avstemningen foregår, hvordan valgkretsene er inndelt, hvor mange representanter som velges og hvordan fordelingen av representanter skjer i forhold til de avgitte stemmene. Prinsippet om "én velger - én stemme" regnes som grunnleggende, mens tilleggskravet om "én verdi" – dvs. at stemmene skal telle like mye – ikke alltid realiseres i samme grad. Det sistnevnte kan blant annet skje ved at fordelingen av mandater ikke er proporsjonal med antall innbyggere i valgkretsen (Aardal 1997). Dette er som kjent tilfelle i Norge. Når det gjelder sametingsvalget, er det spesielle regler både for manntall, valggjennomføring og opptelling, nedfelt i en egen forskrift. Mange av de problemstillinger vi berører i denne rapporten er imidlertid relevante for alle typer valg.

3.2 Faser i valgprosessen

Som velger tenker man kanskje på valg først og fremst som det som skjer i valglokalet, men valg består egentlig av mange ulike elementer som er lenket sammen i en kjede. Svært forenklet kan man dele valgprosessen i tre: 1) det som skjer *før* valget (forberedelse), 2) det som skjer *under* valget (stemmegivning), og 3) det som skjer *etter* valget (opptelling, kontroll og rapportering).

Innenfor alle de tre hovedfasene består imidlertid prosessen av flere ledd. Uten å gå alt for detaljert til verks kan følgende punkter gi et visst inntrykk av hvor sammensatt prosessen er:

[2] Selv om valg som avholdes av ikke-demokratiske regimer kan være hemmelige, bryter de alltid med kravet om å være frie og rettferdige.



Figur 3.1: Faser i valgprosessen

3.2.1 Oppretting og vedlikehold av manntall

I Norge er alle stemmeberettigede innført i manntallet i den kommunen de er bosatt i pr. 31. mai i valgåret.[3] Det er kommunene som eier manntallet og som henter opplysningene fra folkeregisteret. Kommunene kan be et datafirma om å utarbeide et elektronisk manntall til bruk i forhåndsstemmeperioden. Norske statsborgere som har vært bosatt i utlandet i mer enn 10 år, må søke om innføring i manntallet for å kunne stemme ved valget. Manntallet kan, på grunnlag av forhold angitt i valgforskriften, endres helt frem til valgtinget. Oppføring i manntallet gir velgeren rett til å avgi stemme i forbindelse med forhåndsstemmegivning eller stemmegivning på valgtinget. Elektronisk oppdatering gir grunnlag for det papirmanntallet som benyttes på valgtinget, der alle som har avgitt forhåndsstemme er krysset av. Denne manntallskopien lages ferdig etter at forhåndsstemmegivningen er avsluttet.

3.2.2 Kontroll av listeforslag mot manntall og folkeregister

Manntallet og folkeregisteret benyttes også i forbindelse med valgstyrenes godkjenning av partienes listeforslag. Listeforslag fra partier og grupper som ønsker å stille til valg, skal innleveres til valgmyndighetene som tar stilling til om forslagene kan godkjennes etter kravene i valglovens kapittel 6. Blant annet må kandidatene være valgbare og listeforslagene være underskrevet forskriftsmessig. Antall underskrifter er knyttet til om listeforslaget utgår fra et registrert politisk parti med en viss valgoppslutning, eller om det utgår fra andre grupper/partier. I førstnevnte tilfelle skal listeforslaget underskrives av to personer, mens det i sistnevnte må være underskrevet av 500 personer ved fylkestings- og stortingsvalg eller 2 prosent av de stemmeberettigede i kommunen ved kommunestyrevalg.

Registrerte politiske partier har anledning til å sende inn elektroniske underskrifter, dersom forholdene er lagt til rette for digital kommunikasjon med kommunen/fylkeskommunen. Underskrifter som samles inn fra grupper/partier uten en viss valgoppslutning, skal være på papir, jf. valgforskriften § 13. Det vil derfor ikke være anledning til innsamling av underskrifter elektronisk for disse gruppene. Forskriften fastsetter også at disse underskriftene er underlagt taushetsplikt og ikke skal offentliggjøres. At man har skrevet under på et listeforslag vil være opplysninger om "noens personlige forhold" og således underlagt taushetsplikt, jf. forvaltningsloven § 13 (1). Valgmyndighetene benytter folkeregisteret og valgmanntallet for å kontrollere og godkjenne listeforslagene. Alle godkjente listeforslag trykkes som stemmesedler ved det aktuelle valget.

[3] Ved det første sametingsvalget man deltar i må velgeren selv registrere seg i samemanntallet.

3.2.3 Tilrettelegging av valglokaler, opplæring av valgfunksjonærer

En del av valgforberedelsene som er lite synlig for den enkelte velger, er den praktiske tilrettelegging i form av stemmelokaler både for forhåndsstemmegivning og for valgtingsstemmegivning, rekruttering og opplæring av valgfunksjonærer m.m. Dette er imidlertid forhold som trekker store ressurser både personellmessig og økonomisk.

3.2.4 Identifisering av velgeren og avkryssing i manntallet

Den norske valgloven gir anledning til å avgi stemme før valgdagen, såkalt forhåndstemmegivning. Under perioden for forhåndsstemmegivning mottar kommunene stemmer fra flere kanaler. Kommunene etablerer faste mottakssteder for forhåndsstemmer, det organiseres mottak av forhåndsstemmer på helse- og sosialinstitusjoner og det tilrettelegges for såkalt ambulerende stemmegivning (velgere som ikke kan avgi stemme i et etablert mottakssted, kan søke om å få avgi stemme der de oppholder seg). I noen kommuner etableres det faste mottakssteder for forhåndsstemmer også ved andre typer institusjoner, som for eksempel videregående skoler, høgskoler og universitet. Kommunene mottar også forhåndsstemmer via postsendinger fra andre kommuner i tillegg til at det mottas stemmer avgitt utenriks, på Svalbard og Jan Mayen. Utenriks er det i særskilte tilfeller også mulig å avgi brevstemme. Etter hvert som stemmegivningene kommer inn til valgstyret foretas det fortløpende godkjenning og avkryssing i manntallet. På valgtinget er det kun mulig å avgi stemme i den kommunen man er manntallsført. Det er imidlertid tillatt å avgi stemme i en annet valgkrets i kommunen enn der man er manntallsført, såkalt fremmedstemme. Denne fleksibiliteten stiller spesielle krav til rutinene for manntallsavkryssing. Manntallet benyttes til avkryssing både ved forhåndsstemmegivning og ved stemmegivning på valgtinget. Til valgtinget produseres det en egen papirkopi til hver enkelt valgkrets som kun inneholder navn og fødselsdato på de som er stemmeberettigede i valgkretsen.

Stemmemottaker kan kreve at velgeren identifiserer seg før stemme avgis. Velgeren blir krysset av i manntallet idet stemmegivningen godkjennes. Avkryssingen i manntallet skal sikre at vedkommende velger ikke får godkjent flere stemmegivninger. Velgere som har forhåndsstemt, kan i følge gjeldende valglov ikke stemme på nytt på valgtinget. Stemmer fra velgere som på valgtinget ønsker å avgi fremmedstemme må behandles spesielt. Velgeren legger stemmeseddelen i en stemmeseddelkonvolutt, som igjen legges i et omslag der velgerens navn skrives på. Manntallskopien der velgeren står oppført befinner seg på et annet sted, og for å unngå at velgeren stemmer mer enn én gang holdes derfor fremmedstemmene atskilt. Etter at valglokalene er lukket, kontrolleres fremmedstemmene mot valgdagsmanntallet i velgerens krets. Først når det er konstatert at det ikke er krysset her, godkjennes stemmegivningen.

3.2.5 Stemmegivning

Som nevnt kan velgeren avgi forhåndsstemme både i egen og andre kommuner. Etter gjeldende lov er det ikke tillatt å stemme om igjen, med mindre det avdekkes formelle feil ved stemmegivningen. Ved forhåndsstemmegivning blir stemmeseddelen lagt i en stemmeseddelkonvolutt. Denne legges i en omslagskonvolutt sammen med valgkortet. Forhåndsstemmene åpnes og telles på valgdagen før valglokalene lukkes. Ved stemmegivning på valgtinget legges stemmeseddelen direkte i valgurnen uten konvolutt, med mindre velgeren avgir stemme i en annen valgkrets i kommunen enn der vedkommende er manntallsført.

3.2.6 Oppbevaring og transport av stemmene

Både for forhåndsstemmer og valgtingsstemmer vil det være behov for å oppbevare stemmene helt til de transporteres til opptellingslokalet. Varigheten av oppbevaringen og formene for transport varierer, men må uansett skje på en trygg og sikker måte. Regler om dette er gitt i valgforskriften §§ 33 og 34.

3.2.7 Opptelling og kontroll

Valgoppgjøret kan grovt sett deles i tre deler: opptelling (foreløpig og endelig), mandatberegning og kandidatkåring. De fleste kommuner foretar i dag foreløpig opptelling av valgtingsstemmer i valglokalet umiddelbart etter at lokalet er stengt. Foreløpig opptelling av forhåndsstemmer skal administreres av valgstyret. Endelig opptelling av både forhånds- og valgtingsstemmer gjøres vanligvis sentralt, og skal foregå under tilsyn av valgstyret. Ved kommunestyrevalg foretas mandatberegning og kandidatkåring av valgstyret. Godkjenning av valget skjer i kommunestyret. Ved fylkestingsvalg og stortingsvalg samles stemmesedlene fra kommunene på fylkesnivå hos fylkesvalgstyret for kontroll og ny opptelling. Fylkesvalgstyret foretar dessuten mandatberegning og kandidatkåring til fylkestingsvalget. Godkjenning av valget skjer i fylkestinget. Fylkesvalgstyret foretar også mandatberegning og kåring av distriktsmandatene ved stortingsvalg. Utjevningsmandatene kåres av riksvalgstyret. Godkjenning av valget skjer i Stortinget. Valgoppgjøret med endelig opptelling, beregning av mandatfordeling og kandidatkåring er i mange kommuner automatisert gjennom bruk av optiske tellesystemer og terminalbasert registrering.

3.2.8 Rapportering av valgresultatet

Det siste leddet av valgprosessen er rapportering av valgresultatet i form av statistiske oversikter over stemmetall, mandatfordeling, valgte kandidater med vararepresentanter, valgdeltakelse og så videre.

Går vi tilbake til den enkle tredelingen vi gjorde innledningsvis, hører punktene 1-3 til førvalgsfasen, punktene 4-5 til valgfasen og punktene 6-8 til ettervalgsfasen. Men som vi har sett går de ulike elementene ofte over i hverandre.

3.3 Informasjons- og teknologisamfunnet

Tradisjonelt har gjennomføring av valg vært en manuell og arbeidsintensiv prosess. I de senere år er imidlertid optiske lesere og dataterminaler i økende grad tatt i bruk i forbindelse med opptelling og registrering av stemmene. Informasjons- og kommunikasjonsteknologi (IKT) er også tatt i bruk både i forbindelse med manntallet, beregning av mandatfordelinger og valgrapporter (møtebøker). Til nå har teknologien hovedsakelig blitt brukt av de som administrerer valget, ikke av velgerne selv. Det å bruke IKT til administrativ forenkling og økonomisk effektivisering er i stor grad ukontroversielt og vil fortsette i tiden framover, selv om det kan innebære sikkerhetsmessige utfordringer som kan tilsi større grad av sentral kontroll og godkjenning av maskin- og programvare enn hva som har vært tilfellet til nå. Dette spørsmålet bør vurderes nærmere av den foreslåtte prosjektgruppen.

Den stadig økende bruk av IKT er en viktig del av samfunnets generelle modernisering. På alle områder i samfunnet øker tilgangen til og bruken av IKT. Ifølge TNS Gallups Intertrack-undersøkelse er det pr. august 2005 over 3 millioner nordmenn over 12 år som har tilgang til Internett, mens over 2 millioner bruker nettet daglig. Andelen som bruker Internett jevnlig er

dessuten økende over tid. For mange nordmenn er det blitt selvsagt å bruke Internett til å betale regninger, sende søknader til offentlige myndigheter, levere selvangivelse og foreta innkjøp. I løpet av relativt kort tid skjer det en tilvenningsprosess der den enkelte borger venner seg til (og dels blir tvunget til) å bruke Internett som informasjonskilde og kommunikasjonskanal både i forhold til familie, venner, jobb og omverdenen ellers. I sin tur vil dette kunne utløse krav om at private og offentlige tjenester skal være tilgjengelig på en enkel og direkte måte gjennom nettet.

3.4 Elektronisk stemmegivning

Ville det ikke være naturlig at vi også kunne avgi stemme fra datamaskinen hjemme eller på jobb? Valg er egentlig ganske enkelt når man først har bestemt seg for hvilket parti eller hvilken kandidat man vil stemme på. Ved stortingsvalg gjelder det først og fremst å velge en liste og så levere den på riktig sted. Ved lokalvalg er det noen flere valgmuligheter, blant annet kan velgerne gi personstemmer til kandidatene. På en datamaskin vil prosessen bestå i hake av på en liste, eventuelt markere endringer for en eller flere kandidater og så trykke på send-knappen. Dette kan man dessuten gjøre uansett hvor i landet – eller verden for øvrig – man befinner deg. Tilgjengeligheten for studenter som bor hjemmefra, uføre som har vanskelig for å bevege seg eller har dårlig syn, nordmenn som bor i utlandet eller folk på reise vil øke dramatisk. Tilgjengelighet er for øvrig et viktig demokratisk hensyn. Det er ikke for ingenting at vi snakker om stemme*berettigede*. Det er faktisk en demokratisk rett å kunne avgi stemme ved valg. I en tid da valgdeltakelsen har en fallende tendens i mange land kan valg via Internett bidra til å styrke deltakelsen, særlig i velgergrupper som tradisjonelt er lite flinke til å benytte stemmeretten – som ungdom. Opptellingen av stemmene og mandatberegninger vil dessuten kunne skje raskt og nøyaktig. Gitt at datamaskinene er programmert på riktig måte vil mulighetene for manuelle feil i opptellingen nærmest forsvinne. Kostnadene ved gjennomføring av valg – både i form av personell og andre utgifter – vil også kunne reduseres.

Men er det så enkelt? Sammenligningen med banktransaksjoner er besnærende, men halter på flere punkter. Når vi betaler regninger på nettet, kan både avsender og mottaker i ettertid kontrollere at overføringen er riktig utført ved å sjekke kontoutskrifter og betalingsmeldinger. I valgsystemer gjør kravet til hemmelig stemmegivning en slik kontroll og bekreftelse umulig. Et valgsystem må utformes slik at det ikke kan reises noen tvil om at hver enkelt velgers stemme blir registrert, talt opp og bidrar til det endelige valgresultatet på korrekt måte, samtidig som det ikke skal være mulig å koble velgerens identitet til innholdet av stemmen. Et elektronisk valgsystem vil imidlertid være teknisk mer komplisert enn et tradisjonelt system med papirstemmesedler der det er mulig for lekfolk å forstå og kontrollere det som foregår. Med et elektronisk valgsystem er det bare eksperter som har forutsetninger for å forstå alt som skjer inne i datamaskinene og i datanettet. Lekmannskontrollen må med andre ord erstattes av tillit til ekspertene – både de som har utformet og laget systemet, sertifisert og kontrollert at det fungerer korrekt.

Samtidig er det viktig å huske på at et manuelt, papirbasert valgsystem heller ikke er feilfritt. Det ser vi ikke minst av klager på valggjennomføringen fra enkeltvelgeres side (se nærmere om dette i kapittel 5 og Vedlegg D). Menneskelige feil som følge av manglende opplæring, svikt i rutiner eller juks kan føre til at stemmer forsvinner, ikke blir talt opp eller blir røpet. Selv om vi vet at feil forekommer, har norske velgere likevel stor tillit til at valggjennomføringen har gått riktig for seg og at valgresultatet er korrekt. I et elektronisk

system kan imidlertid utilsiktede eller tilsiktede feil i maskin- og programvare påvirke valgresultatet i en mye større skala. Maskinene kan bryte sammen på grunn av strømbrudd eller andre grunner slik at avgitte stemmer forsvinner, den eller de maskinene som tar i mot stemmene kan blokkeres ved at noen bombarderer dem med andre oppgaver, noen kan fange opp stemmen mens den er underveis i nettverket og endre den, nettverket kan være avlyttet eller det kan være virus eller trojanske hester på avsendermaskinen (se nærmere om sikkerhetsutfordringer i vedlegg B, og ordliste i Vedlegg E).

En viktig forskjell mellom manuelle og elektroniske valg er at det i det førstnevnte tilfellet trengs mange personer spredt på flere valglokaler for å gjøre stor skade, mens det i det sistnevnte tilfellet bare trengs én person. Vel så problematisk er det at det ikke er så lett å avdekke om det faktisk har forekommet tilsiktede eller utilsiktede uregelmessigheter i bruken av systemet. Selv om det ikke har skjedd noe galt, kan en *påstand* om at det elektroniske systemet er feil være nok til å undergrave tilliten til både resultatet og valgprosessen. Selv om en kan sette inn mottiltak, er det umulig å oppnå absolutt sikkerhet. Samtidig er tillit til systemet og prosessene helt avgjørende. Selv om det blir gjort feil med manuelle systemer, har velgerne stor tiltro til at ingen jukser. Denne tilliten er det viktig å ta vare på også når man tar i bruk moderne teknologi – uansett om det gjelder valgadministrasjon eller selve valghandlingen.[4]

Et annet forhold det er viktig å være oppmerksom på, er ulikhet i tilgang til og bruk av informasjons- og kommunikasjonsteknologi, såkalte digitale skiller (jf. Norris 2001, Van Dijk 2005, Rønning m.fl. 2005). Denne type ulikhet gjelder ikke bare tilgang til teknologien, men også kunnskap og trygghet knyttet til bruk. Selv om stadig flere får tilgang til Internett, er det fortsatt store skjevheter med hensyn til hvilke grupper som behersker den nye teknologien. Unge menn med høy utdanning er blant dem som bruker nettet mest, og som har mest tillit til eget kunnskapsnivå. Tilgang og bruk av nettet har også sterk sammenheng med inntekt. Undersøkelser fra Norge viser at personer med høy utdanning og høy inntekt i større grad enn andre ønsker å stemme via Internett (Karlsen, Aardal og Christensen 2005). Forsøk med stemmegivning over Internett i Sveits viser lignende forskjeller (Cristin og Trechsel 2004). Det er derfor mulig at stemmegivning via Internett kan bidra til at ressurssterke grupper deltar i enda større grad enn før, slik at forskjellene mellom ressurssterke og ressurssvake velgere øker. På den annen side kan man ikke utelukke at Internettstemmegivning virker utjevnende på valgdeltakelsen mellom unge og eldre velgere.

3.5 Sentrale valgdimensjoner

I denne rapporten skal vi se nærmere på ulike sider ved elektronisk stemmegivning. Som et hjelpemiddel i den videre diskusjon skal vi først presentere en inndeling av valghandlingen langs tre dimensjoner. For det første går det et skille mellom tradisjonelle, papirbaserte valgsystemer på den ene side og elektroniske systemer på den andre. Et elektronisk valgsystem behøver ikke nødvendigvis bety stemmegivning via Internett. Det kan også være ulike former for valgomat eller kioskløsninger der man avgir stemme ved hjelp av en minibanklignende terminal i valglokalet. I Norge prøvde man ut en slik løsning i tre kommuner – Oppdal, Larvik og Bykle - ved kommunevalget i 2003, og ved lokalstyrevalget i

[4] Selv i etablerte demokratier som for eksempel USA kan tilliten til måten valg gjennomføres på være nokså tynnslitt (Fund 2004).

Longyearbyen samme år.[5] Den andre viktige dimensjonen gjelder spørsmålet om hvor stemmegivningen finner sted, enten i valglokalet under oppsyn av offentlig utpekte valgfunksjonærer eller et sted der ingen kan føre kontroll med hvordan avstemningen skjer – enten det nå er hjemme eller på jobb. I det første tilfellet kan man si at stemmegivningen foregår i *kontrollerte* omgivelser, mens den i det sistnevnte tilfellet skjer i *ukontrollerte* omgivelser. Grunnen til at valg gjennomføres under offentlig oppsyn, er kravet om hemmelig valg og at stemmegivningen skal skje uten utilbørlig påvirkning av andre i valgøyeblikket. Slik påvirkning kan for eksempel skje ved at et familiemedlem pålegger et annet å stemme på en bestemt måte (såkalt *family voting*), eller at noen er villige til å kjøpe og selge stemmer.

La oss først koble sammen de to nevnte dimensjonene. Vi får da en inndeling som vist i tabell 3.1.

Tabell 3.1: Stemmegivning etter medium og omgivelser

	Kontrollerte omgivelser	**Ukontrollerte omgivelser**
Papir	**1.** Tradisjonell papirstemmeseddel i valglokalet	**3.** Stemmegivning på papir utenfor valglokalet (brevstemme)
Elektronisk	**2.** Elektronisk utstyr i valglokalet (datamaskin med pekeskjerm, mus eller tastatur)	**4.** Elektronisk stemmegivning utenfor valglokalet (Internett, SMS, o.l.)

Kilde: (Karlsen et al. 2005)

I celle 1 finner vi den tradisjonelle måten å avgi stemme på. I celle 2 finner vi det forsøket man gjorde med elektroniske terminaler (valgomater) ved kommunestyrevalget i 2003. I celle 3 finner vi stemmegivning på papir utenfor valglokalet. I Norge gis det adgang til brevstemmegivning, men da kun som et unntakstilfelle for nordmenn bosatt i utlandet.[6] Grunnen til unntaksbestemmelsen er at det gjøres en avveining mellom velgerens rett til å delta i valget og hensynet til hemmelighold av stemmen.[7] I noen land, som for eksempel England, er dette en utbredt form for stemmegivning. Fra og med 2006 innføres brevstemmegivning for utenlandsboende som en permanent ordning i Sverige.[8] Det er viktig å merke seg at stemmegivning pr. brev skjer i ukontrollerte omgivelser, uten oppsyn av en offentlig valgfunksjonær. Det er likevel i celle 4 vi finner det mest kontroversielle alternativet, nemlig at stemmegivningen skjer elektronisk utenfor valglokalet via Internett, SMS eller lignende.

[5] Se Christensen et al. (2004). Se også kapittel 4.
[6] I Valglovens paragraf 8-2, tredje ledd heter det at: ” Dersom en velger som oppholder seg utenfor riket ikke har mulighet til å oppsøke en stemmemottaker, kan vedkommende avgi stemme ved brevpost uten at en stemmemottaker er til stede ved stemmegivningen.”
[7] Brevstemmegivning er altså noe annet enn det å kunne forhåndsstemme på postkontoret slik man kan i enkelte land.
[8] I Sverige understrekes det også at det har skjedd en avveining mellom velgernes rett til å bruke stemmeretten sin på den ene side og kravet om hemmelighold av stemmegivningen på den andre (SOU 2004:111).

I tillegg til spørsmålet om papir eller elektronikk og kontroll eller ikke kontroll, er det enda en dimensjon som kan ha betydning for diskusjonen om elektronisk valg. Det gjelder spørsmålet om *når* valghandlingen finner sted. Som vi skal se senere i rapporten kan bruken av elektronisk stemmegivning fortone seg annerledes hvis det skjer i forbindelse med forhåndsstemmegivning enn om den skjer på selve valgtinget. I denne rapporten vil vi gjennomgående omtale forhåndsstemmegivning som *fase 1*, og stemmegivning på valgtinget som *fase 2*.

Hovedalternativene i tabell 3.2 er de samme som i tabell 3.1, men i tillegg skiller vi mellom tidspunktet for stemmegivningen, enten før valget eller på valgtinget. Som diskusjonen i kapittel 5 viser, er muligheten til å stemme om igjen viktig for å hindre utilbørlig påvirkning og kjøp og salg av stemmer. Det å stemme elektronisk i ukontrollerte omgivelser på valgtinget, samtidig som man skal kunne stemme om igjen på det samme valgtinget, vil imidlertid medføre store tekniske og administrative problemer. Derfor faller alternativet i celle 8 bort.

Tabell 3.2: Stemmegivning etter medium, omgivelser og tidspunkt

	Kontrollerte omgivelser (i valglokalet)		**Ukontrollerte omgivelser (utenfor valglokalet)**	
	Papir stemme	Elektronisk stemme	Papir stemme	Elektronisk stemme
Fase 1 Før valgtinget	**1.** Tradisjonell papirstemme i valglokalet	**2.** Elektronisk utstyr i valglokalet (datamaskin med pekeskjerm, mus eller tastatur)	**3.** Stemmegivning på papir utenfor valglokalet (brevstemme)	**4.** Elektronisk stemmegivning utenfor valglokalet (Internett, SMS, o.l.)
Fase 2 Valgtinget	**5.** Tradisjonell papirstemme i valglokalet	**6.** Elektronisk utstyr i valglokalet (datamaskin med pekeskjerm, mus eller tastatur)	**7.** Stemmegivning på papir utenfor valglokalet (brevstemme)	**8.** Elektronisk stemmegivning utenfor valglokalet (Internett, SMS o.l.)

Den videre diskusjon vil fokusere på de cellene som ikke er skyggelagt, dvs. celle 2, 4 og 6. Dette følger av arbeidsgruppens mandat. Det er imidlertid viktig å være klar over at mange av de motforestillingene som kan reises mot elektronisk stemmegivning ikke primært gjelder bruken av elektroniske medier, men at stemmegivningen skjer i *ukontrollerte omgivelser*. Det kan argumenteres for at hvis man først skal tillate stemmegivning i ukontrollerte omgivelser, er det bedre å bruke elektroniske enn papirbaserte løsninger. Elektroniske løsninger gir mulighet for en mye sikrere identifikasjon og autentisering av velgeren, og muligheten for å stemme om igjen forhindrer i utstrakt grad mulige problemer i form av utilbørlig påvirkning og kjøp og salg av stemmer

Når vi senere i denne rapporten skal diskutere ulike alternativer for å kunne avgi stemme, vil klassifikasjonene i tabell 3.2 være et viktig referansepunkt.

3.6 Internasjonale erfaringer med elektronisk stemmegivning

Diskusjonen om elektronisk stemmegivning er langt fra noe særnorsk fenomen. I en lang rekke land prøver man ut ulike typer teknologi i tilknytning til valg og stemmegivning. Mange har i den forbindelse følt behov for en samordning av retningslinjer og praksis på tvers av landegrensene. Europarådet har i flere år arbeidet med spørsmålet om demokratiets virkemåte i prosjektet **"**Making democratic institutions work." Som en del av dette prosjektet vedtok Ministerkomiteen i Europarådet 30. september 2004 en egen anbefaling (rekommandasjon) med sikte på juridiske, operasjonelle og tekniske standarder for elektronisk stemmegivning.[9] I sluttdokumentet fra demokratiprosjektet oppfordrer Europarådet til at det innføres stemmegivning utenfor valglokalene, enten pr. brev eller elektronisk.[10] Men inntil elektronisk stemmegivning er alminnelig akseptert, anbefales dette kun som et supplement til ordinær stemmegivning. Generelt anbefales at brevstemmegivning introduseres før elektronisk stemmegivning, og at stemmegivning over en periode gjøres tilgjengelig både i og utenfor valglokalene.

Tanken om å tillate stemmegivning i ukontrollerte omgivelser er med andre ord ikke ukjent i toneangivende, internasjonale kretser. Men før vi går dypere inn i denne diskusjonen, skal vi redegjøre for erfaringer som er gjort i andre land i forbindelse med forsøk med ulike former for elektronisk stemmegivning. Dette er tema for neste kapittel.

[9] Europarådets anbefaling er et juridisk instrument som må vedtas enstemmig av medlemsstatene, men er ikke folkerettslig bindende. Dens standarder kan ikke gjøres juridisk bindende med mindre bestemmelsene tas inn i norsk lov eller forskrift.
[10] *Green Paper: The Future of Democracy in Europe.*

4 Elektronisk stemmegivning – norske og internasjonale erfaringer

4.1 Innledning

I dette kapitelet skal vi gjøre rede for norske og internasjonale erfaringer med og debatter angående elektronisk stemmegivning. Grovt sett er det tre ulike måter å forholde seg til elektronisk stemmegivning på. For det første er det de som ikke ønsker å ta i bruk elektronisk stemmegivning i det hele tatt. For det andre er det de som bare tar i bruk elektronisk stemmegivning i valglokalet. For det tredje er det de som (også) tar i bruk stemmegivning over Internett i ukontrollerte omgivelser. Elektronisk stemmegivning i stemmelokalet er gjennomført i stort omfang i land som USA, Belgia, Nederland, Brasil og India. Internettstemmegivning er mindre utbredt og møtt med mye skepsis. Stemmegivning via Internett i ukontrollerte omgivelser er likevel prøvd ut i lokalvalg i Storbritannia i 2002 og 2003 og Estland i 2005, og ved nasjonale folkeavstemninger i Sveits.

Det er altså stor variasjon fra land til land i synet på elektronisk stemmegivning. Dette må ses i sammenheng med ulik politisk tradisjon og politiske utviklingstrekk. I land med høy valgdeltakelse og der valg nyter stor legitimitet i befolkningen, som i Norden, har interessen for å innføre elektronisk stemmegivning vært liten. I land med lavere valgdeltakelse, som i Storbritannia, er interessen større. Hyppige valg, som vi ser i Sveits, og kompliserte valg, som i Belgia og Nederland, bidrar også til å øke interessen for elektronisk stemmegivning.

Det eksisterer etter hvert mye litteratur om elektroniske valg, både i form av rapporter, bøker og vitenskapelige artikler. Denne litteraturen var utgangspunktet for gruppens arbeid og dannet bakgrunn for arbeidsgruppens studieturer til USA, Storbritannia, Genève og Estland. Studieturene har på den måten utdypet og supplert det skriftlige materialet. Dette kapitlet bygger på studieturene og relevant litteratur om elektronisk stemmegivning. Følgende punkter fra mandatet blir tatt opp i kapitlet:

- Sammenstille forskning/utredninger på området (pkt. 17).
- Redegjøre for internasjonale erfaringer med ulike typer system for stemmegivning (pkt. 18).

Vi begynner med å se på hva våre nordiske naboland mener om elektronisk stemmegivning. I den forbindelse skal vi også se på norske erfaringer. Deretter skal vi se nærmere på Storbritannia hvor forsøk med e-stemmegivning er del av en større moderniseringsprosess. Så tar vi for oss erfaringer fra og debatten i USA. Her er e-stemmegivning i valglokalet utbredt, mens det er stor skepsis til Internett-valg. Både Sveits og Estland har gjennomført forsøk med Internett-stemmegivning som en del av offisielle valg, og vi skal se nærmere på disse forsøkene før vi tar for oss erfaringer med elektronisk stemmegivning andre steder.

4.2 Norden

Interessen for å innføre elektronisk stemmegivning har, som nevnt, vært relativt liten i Norden. Dette gjelder spesielt Sverige. Elektronisk stemmegivning er riktignok drøftet i

mange offentlige dokumenter, men konklusjonen har vært at elektronisk stemmegivning ikke skal tas i bruk ved politiske valg (Olsson 2001, Ju2002E, SOU 2004: 111). I Sverige er det stor tillit til valgene i befolkningen samtidig som valgdeltakelsen er svært høy. Frykten for at e-stemmegivning skal ødelegge noe som fungerer godt er derfor stor. Komiteen som ble nedsatt for å vurdere valgloven i Sverige anbefaler i sin sluttrapport at elektronisk stemmegivning ikke blir tatt i bruk ved offisielle politiske valg på det nåværende tidspunkt. De peker spesielt på problemer knyttet til hemmelige valg, valgfusk og utilbørlig påvirkning, samt sikkerhetsproblemer knyttet til teknologien (SOU 2004: 111 s 175-185).

Danmark er heller ikke i front når det gjelder elektronisk stemmegivning. Selv om elektroniske løsninger har blitt prøvd ut i enkelte lokale folkeavstemninger, har det ikke vært noe initiativ angående elektronisk stemmegivning fra myndighetenes side.

I Finnland er holdningene til elektronisk stemmegivning mer positive enn i Sverige og Danmark, og en arbeidsgruppe har høsten 2005 anbefalt en gradvis innføring av elektronisk stemmegivning i kontrollerte omgivelser. Det skal gjennomføres et pilotprosjekt med e-stemmegivning i tre kommuner i forbindelse med riksdagsvalget i 2007. Arbeidsgruppen begrunner innføring av elektronisk stemmegivning med å "påskynde röstningsförfaranden" for velgerne, redusere administrasjonsarbeidet og spare kostnader. E-stemmegivning er en del av et større reformprosjekt av valgdatasystemet ved Justitieministeriet[11].

I Norge er det også gjennomført fire forsøk med elektronisk stemmegivning i valglokalet i forbindelse med valgene i 2003. Nedenfor ser vi nærmere på erfaringene fra disse.

4.2.1 Norske erfaringer

Forsøkene i Oppdal, Bykle, og Larvik ble gjennomført i forbindelse med det ordinære kommunevalget 15. september 2003, mens forsøket i Longyearbyen ble gjennomført i forbindelse med lokalstyrevalget 26. og 27. oktober 2003. Den tekniske løsningen var lik alle fire steder og ble levert av IKT-firmaet ErgoEphorma. Løsningen gikk ut på å gi velgere muligheten til å avgi stemme via et elektronisk medium, istedenfor med vanlig stemmeseddel. Stemmegivningen foregikk i valglokalet, på såkalte "valgomater" eller elektroniske valgurner. Den elektroniske valgurnen var utformet som en vanlig datamaskin med pekeskjerm, utseendemessig så den ut som en minibankterminal. Den elektroniske stemmegivningen var en del av det ordinære kommunestyre- og fylkestingsvalget.

Forsøket i Oppdal var mest omfattende. Her var det nesten 5000 stemmeberettigede, og det var mulig å stemme elektronisk i alle sju valgkretsene i kommunen. Bykle er en liten kommune med i underkant av 700 stemmeberettigede. Her var det mulig å stemme elektronisk i begge kretsene i kommunen. Larvik er en stor kommune med nesten 32 000 stemmeberettigede, men her var det på valgdagen bare mulig å stemme elektronisk ved Østre Halsen stemmekrets. Dette er riktignok en relativt stor krets med i underkant av fire tusen stemmeberettiggede. I kretsene i Oppdal, Bykle og Larvik var det bare plassert ut en valgomat i hvert stemmelokale. Ved valget til Longyearbyen lokalstyre var det rundt 1300 stemmeberettigede. Her var det bare ett stemmelokale hvor det var to valgomater. I Longyearbyen var det også mulig å stemme på den vanlige måten, men bare velgere som ba spesielt om det, ble tilbudt denne muligheten. Her var elektronisk stemmegivning det vanlige.

[11] http://www.vaalit.fi/21331.htm

Valghandlingen ble utført på følgende måte: Etter å ha identifisert seg gjennom å sette et smartkort inn i kortleseren, kunne man avgi sin stemme. I det første skjermbildet valgte man mellom kommunestyrevalget og fylkestingsvalget.[12] Deretter pekte man på det partiet man ønsket å stemme på. Man kunne så avgi personstemme ved å peke på navnet til en eller flere kandidater. Det ble da satt et kryss i boksen ved siden av navnet. Samme framgangsmåte gjaldt for fylkestingsvalget. Ved kommunestyrevalg kunne man i tilegg gi tilleggsstemme til kandidater som stod på andre valglister, såkalte slengere. Dette gjorde en enten ved å gå inn på en alfabetisk liste over kandidatene eller ved å søke i de ulike partienes lister. Det var også mulig å stemme blankt ved begge valg, samtidig som en kunne velge å stemme bare ved ett av valgene. Kravet om at velgerne skulle ha det samme handlingsrommet med hensyn til å rette på stemmeseddelen som ved den tradisjonelle papirløsningen ble med andre ord ivaretatt.

I Longyearbyen stemte 91 prosent elektronisk. I Bykle benyttet 53 prosent av velgerne seg av denne muligheten. 34 prosent stemte elektronisk i Oppdal. I Østre Halsen stemmekrets valgte 18 prosent å avgi elektronisk stemme.[13]

Evaluering av forsøket var først og fremst en evaluering av brukervennligheten og den generelle gjennomføringen, der spesielt velgernes reaksjon stod i sentrum. Den tekniske løsningen var ikke gjenstand for evaluering.

Ønsket om å prøve noe nytt var den vanligste grunnen til at folk stemte elektronisk, et ønske om å delta i et forsøk som de fant nytt og spennende. Velgere som ikke stemte elektronisk delte seg inn i fire nesten like store grupper. En fjerdedel var motstandere av elektronisk stemmegivning, en fjerdedel hadde ikke tid, en fjerdedel var redd det var vanskelig, og en fjerdedel oppgav andre svar (”manglende informasjon”, ”kan ikke data” var typiske svar).

Materialet viser at velgere i forsøkskommune er svært positive til bruk av IKT i forbindelse med valg. E-velgere er selvsagt mer positive enn velgere som stemte på den vanlige måten. De som stemte på den vanlige måten fordi de hadde dårlig tid, ligner mest på e-velgerne, og er nesten like positive til bruk av IKT. Også de som var redde for at det var vanskelig å stemme elektronisk, var positive til bruk av IKT. Det var først og fremst gruppen som sa de var motstandere av elektronisk stemmegivning, som var negative til e-valg – naturlig nok.

Sju av ti velgere som stemte elektronisk, kunne tenke seg å stemme via Internett om dette hadde vært mulig. Over halvparten av dem som ikke stemte elektronisk, kunne også tenke seg å stemme via Internett.

Nesten av ni av ti velgere som var med på forsøket, mente at det var svært lett å stemme elektronisk, og like mange kan tenke seg å stemme elektronisk også i fremtiden.

4.2.2 Ønsker nordmenn å stemme via Internett?

I forbindelse med lokalvalgsundersøkelsen 2003 ble det stilt spørsmål til norske velgere om de kunne tenke seg å stemme elektronisk via Internett om dette var mulig. Her er det viktig å understreke at velgerne ikke ble presentert for fordeler eller ulemper med Internett-stemmegivning. Alt i alt hevder 6 av 10 at de ønsker å stemme via nettet. Det er imidlertid store forskjeller knyttet til alder, utdanning og inntekt. Mens 8 av 10 under 44 år kan tenke seg å stemme via nettet, gjelder dette for 56 prosent i aldersgruppen 45-66 år, og bare for 18

[12] Se illustrasjon i kapittel 5
[13] Kilde: ErgoEphorma

prosent i aldersgruppen over 67 år. Og mens 3 av 10 med grunnskole som høyeste utdanning ønsker å stemme via nettet, ønsker 74 prosent med universitets- eller høyskoleutdanning Internett-valg. Blant gruppen som har lavest inntekt hevder halvparten at de ønsker Internett-valg, mens 3 av 4 i gruppen med høyest inntekt vil stemme via nettet (Karlsen, Aardal og Christensen 2005).

4.3 Storbritannia

I Storbritannia er man i gang med en omfattende modernisering av hele valgprosessen. I denne moderniseringsprosessen spiller elektronisk stemmegivning en sentral rolle, og det er først og fremst interesse for e-stemmegivning fra andre steder enn i valglokalet. Bakgrunnen er en svært lav og synkende deltakelse i valg. I perioden 1990-99 lå valgdeltakelsen i snitt på 36 prosent, mens den i 2000 var like i overkant av 30 prosent. Storbritannia har gjennomført forsøk med elektronisk stemmegivning både ved lokalvalget i 2002 og i 2003. I 2002 gjennomførte 9, og i 2003 gjennomførte 20 lokale myndigheter forsøk med elektronisk stemmegivning. Regjeringens budsjett for satsningen er 30 millioner pund over en periode på tre år (The Electoral Commission 2003). Bare i 2003 ble det brukt 18.5 millioner pund. Forsøkene inkluderte flere ulike teknologileverandører.

Utgangspunket for den britiske valgkommisjonen er at sikkerheten ved elektroniske løsninger skal være minst like god som ved mer tradisjonelle metoder. Forsøkene skulle bidra til å forenkle stemmegivning gjennom å gjøre det så bekvemt som overhodet mulig for innbyggerne å få benyttet stemmeretten. Et hovedsatsningsområde var Internett-valg, og denne løsningen ble benyttet i 14 av forsøkene. Tre forsøk var innrettet mot bruk av elektroniske kiosker i valglokalene, mens tre benyttet ny teknologi ved opptellingen av stemmene. For første gang ble det mulig å stemme ved hjelp av interaktivt digitalt TV. Totalt benyttet i overkant av 160 000 velgere seg av et eller annet elektronisk medium. Nedenfor følger en kort gjennomgang av de tekniske løsninger som ble prøvd ut, og måten de ble gjennomført på.

4.3.1 Internett-valg

Internettløsningen bestod i at velgeren koplet seg opp mot stemmemottakers nettadresse, altså valgtjeneren. Dette kunne gjøres fra hvilken som helst datamaskin med Internett-oppkobling. Adressen til valgtjeneren fant velgeren enten sammen med valgkortet eller via kommunens nettside. Pålogging ble utført ved at velgeren skrev inn sitt passord, som han/hun hadde mottatt sammen med valgkortet (enten en PIN-kode eller et passord). Neste skritt var å velge kandidat, noe som kunne gjøres enten ved å klikke på selve stemmeseddelen eller ved å skrive inn en kandidatkode (vedlagt det tilsendte materialet). Velgerne kunne også stemme blankt. Systemet viste til slutt den kandidaten(e) som var merket av, og velgeren ble bedt om å bekrefte sin stemme. Det hele ble avsluttet ved at systemet ga velgeren en kvittering på at stemmen var mottatt. I evalueringsrapporten peker valgkommisjonen på at ordningen med PIN koder skapte forvirring. De ulike teknologileverandørene benyttet seg av ulike metoder for å identifisere velgerne, samtidig som ulike kodevarianter ble benyttet i ett og samme valg avhengig av hvilket medium velgeren ønsket å stemme på. PIN-kodene ble i tillegg sendt i samme forsendelse som valgkortet, og ikke i to forsendelser som er vanlig når for eksempel nye bankkort utstedes. Valgkommisjonen peker også på at informasjon om koblingen mellom PIN-koder og velgernes identitet kun bør tilflyte valgadministrasjonen, og ikke teknologi-leverandørene. Kitcat (2003) som er kritisk til forsøket, viser til at sikkerhetsanalysene både under og etter selve stemmegivningen var mangelfulle.

4.3.2 Telefon

Her ringte velgeren et gratis telefonnummer (stemmemottaker) der han/hun ble møtt av en automatisk telefonsvarer. Første skritt var å logge på ved å taste inn en kode, for deretter å taste inn kandidatkoden (eller kodene). Systemet leste så opp de kandidatene som velgeren hadde stemt på, og ba om en bekreftelse. Velgeren kunne enten bekrefte eller gå tilbake og endre sitt valg. Når velgeren endelig bekreftet sitt valg, ble det lest opp en kvittering på at stemmen var mottatt. Valgkommisjonen er skeptisk til å videreføre telefonvarianten. Den var i liten grad tilgjengelig for handikappede, samtidig som velgerne ble forvirret ved at de måtte taste inn relativt lange koder. I flere pilotforsøk måtte velgeren taste tallkodene inn samtidig som han/hun leste av kandidatkodene på selve valgkortet.

4.3.3 SMS

Tekstmeldingsløsningen var, i motsetning til de foregående, ikke interaktiv. Oppringingen ble videre belastet velgerens egen telefonregning, ikke stemmemottakers. Stemmegivningen ble utført i en og samme tekstmelding, og en godkjent stemme (melding) måtte inneholde velgernes kode, kretskode, samt koden til den kandidaten velgeren ønsket å stemme på. Inneholdt meldingen en gyldig stemme fikk velgeren en bekreftelse på at stemmen var mottatt. Kvitteringen identifiserte ikke hvem en hadde stemt på. Feilmelding innebar at stemmen ikke var gyldig. Valgkommisjonen er kritisk til videreføring også her. Løsningen er lite tilgjengelig for handikappede, og anses også å trivialisere valghandlingen.

4.3.4 Digitalt TV og pekeskjermer

Stemmegivning via digitalt TV fulgte tilnærmet samme prosedyre som Internett-løsningen. Den eneste forskjell bestod i at en annen metode ble benyttet for å logge på selve valgtjenesten (stemmemottaker). Dette ble gjort gjennom å navigere på TV-apparatets menysystem, men når velgerne først hadde entret selve stemmetjenesten var prosessen den samme. Det ble også plassert ut flere elektroniske kiosker, og de fleste av disse var utstyrt med pekeskjerm. I fire kommuner var kiosker den eneste muligheten en velger hadde til å få stemt på selve valgdagen, mens fem kommuner hadde elektroniske kiosker plassert som et supplement til valglokalene på offentlige knutepunkter som biblioteker og supermarkeder. En kommune brukte kioskløsningen parallelt med tradisjonell papirstemmegivning i selve valglokalet. I Sheffield ble det forsøkt en ordning med smartkort for å forenkle registrerings-prosessen (man kunne også stemme uten), og kortet ble sendt via posten på forhånd. I Chester og Epping ble smartkort først utlevert sammen med registreringen. I samtlige tilfeller var smartkortet programmert med en stemmeseddel.

4.3.5 Valgkommisjonens generelle vurdering av forsøkene

Kommisjonen viser til at regjeringen hadde ansvaret for å skrive kontrakter med leverandørene av løsningene for elektronisk stemmegivning. I den forbindelse var det utarbeidet en kravspesifikasjonsliste med 61 separate krav. Kravene dekket et bredt spekter, og omfattet alt fra funksjonalitet, sikkerhet og administrasjon til evaluering. Når det gjelder selve gjennomføringen, har valgkommisjonen flere kritiske merknader.

Kommisjonen er kritisk til at ingen enkeltorganisasjon hadde ansvaret for å integrere elektronisk stemmegivnings-løsningene i de lokale IKT systemene. Dette medførte at sikkerheten ikke ble tilstrekkelig ivaretatt. Det var ikke etablert klare rutiner for å løse opp i

eventuelle uklarheter som måtte oppstå. Konkurrerende leverandører måtte samarbeide på relativt kort varsel uten at dette var varslet på forhånd eller kontraktfestet. Dette bidro til at det ble vanskelig å få gjennomført tilstrekkelige sikkerhetsanalyser både under selve gjennomføringen av valget og i etterkant.

Kommisjonen slår videre fast at de lokale valgstyrene ikke tok tilstrekkelig hensyn til at ny teknologi skulle tas i bruk. Mye av ansvaret ble delegert til teknologileverandørene, noe som valgkommisjonen er svært kritisk til. Særlig gjaldt dette opptellingsprosedyrene, der data blant annet ble transportert manuelt via e-post og så importert i applikasjoner som i Word eller Excel for å beregne resultatene.

Kommisjonen konkluderer med at fremtidige løsninger for Internett-valg må ta hensyn til lokale IKT-systemer, samtidig som det må satses ressurser på å bygge opp teknologikompetansen internt i den lokale valgadministrasjonen. Dette er forutsetninger som må komme på plass for at et Internett-valg skal kunne gjennomføres sikkert og korrekt.

Kommisjonen har også innvendinger mot kvalitetssikringen av den teknologiske infrastrukturen. Verifisering er nøkkelbegrepet her. Det pekes på at det bør gjennomføres en uavhengig verifisering/kontroll av teknologien for at elektroniske valgløsninger skal ha legitimitet. Konkret betyr dette at det må legges til rette for at uavhengige aktører kan kontrollere resultatene, samt at teknologileverandørene stiller sine systemer åpne for innsyn og kontroll.

Når det gjelder brukervennlighet, foreslår kommisjonen at brukergrensesnittet for elektronisk stemmegivning standardiseres. Det betyr ikke at samme leverandør skal benyttes, men at de leverandører som skal levere utstyr, har et standardisert grensesnitt som velgerne kan kjenne igjen fra valgkrets til valgkrets.

Kommisjonen er også opptatt av kostnadsaspektet. Ett sentralt argument for å bruke ny teknologi i valgsammenheng er gjerne at det kan bidra til å redusere utgiftene i forbindelse med gjennomføringen av valg. Det understrekes at elektronisk stemmegivning neppe vil redusere kostnadene så lenge det i tillegg er mulig å stemme på vanlig måte i valglokalene. Dette må veies mot at det å ta i bruk alternative kanaler vil gi velgerne større valgmuligheter. Pratchett (2002), som også er opptatt av kostnadssiden, peker på at reduserte kostnader kan oppnås hvis elektronisk valgutstyr kan brukes til andre formål enn valg. Motargumentet er at det er betydelig lettere å sjekke programvaren i maskiner som kun brukes til valg, enn maskiner med flere bruksområder. Det ser altså ut til å være en balansegang mellom sikkerhet og bruksområder her.

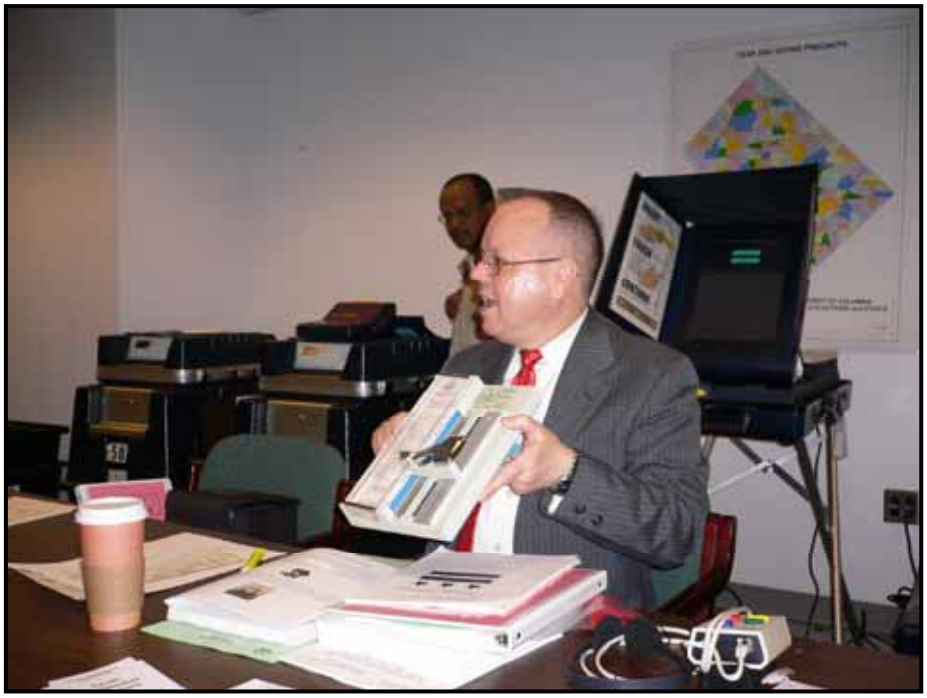
Når det gjelder bruk av elektroniske kiosker, mener kommisjonen at disse bør målrettes i større grad enn i 2003, og begrunner det med at kiosker plassert i valglokalene ikke ser ut til å ha effekt på valgdeltakelsen. Kommisjonen argumenterer derfor for mer desentraliserte løsninger (utenfor valglokalene), og gjerne i kombinasjon med forhåndsstemmegivningen.

Hva så med målsetningen om å ha en ferdigutviklet Internett-basert valgløsning på plass innen 2006? Kommisjonen er skeptisk til dette, og mener en i så fall har en lang vei å gå: "pilots should have more demonstrable and rigorous security with formalised accreditation; more mature processes are needed with greater control exercised by local authorities" (Electoral Commission 2003: 81).

4.3.6 Storbritannia avlyser videre forsøk med elektronisk stemmegivning

Høsten 2005 kunngjorde myndighetene at de avlyser forsøkene som var planlagt i forbindelse med lokalvalgene i 2006. Avlysningen begrunnes med at tidspunktet ikke er riktig for elektronisk stemmegivning.[14]

4.4 USA



← Bill O'Field fra DC Board of Elections and Ethics i Washington DC demonstrerer utstyr til bruk ved stemmegivning.

I USA er det etter hvert blitt vanlig med elektronisk stemmegivning i valglokalet, og ved presidentvalget i 2004 ble det avgitt rundt 40 millioner elektroniske stemmer. Stemmegivning via Internett er det, som vi skal se, imidlertid stor skepsis til.

Det er lite nasjonal lovgivning knyttet til valg i USA. Lovgivning og gjennomføring står hver enkelt stat for. Dette betyr i noen grad at ulike valgregler gjør seg gjeldende fra delstat til delstat, og til dels fra fylke (county) til fylke. Den enkelte stat bestemmer selv om de skal benytte e-stemmesystem og/eller papirstemmesedler. I kjølvannet av valget i 2000 og problemene med de mekaniske hullkortmaskinene, ble Help America Vote Act (HAVA) vedtatt. The U.S. Election Assistance Commission (EAC) ble ved denne loven etablert som "a national clearinghouse and resource for information and review of procedures with respect to the administration of Federal elections." EAC fikk i oppgave å lage tekniske retningslinjer for administrasjon av riksvalg, prosedyrer for e-stemmesystem, og utvikle et nasjonalt program for testing og sertifisering av e-stemmesystem.[15]

USA er langt fremme i utviklingen når det gjelder elektronisk stemmegivning i valglokalet. Debatten her skiller seg imidlertid fra den europeiske debatten fordi den er mer kritisk til

[14] "The Government believes that the time is not yet right to take forward the piloting of e-voting" het det i følge the Independent (6. september) i en uttalelse fra The Department of Constitutional Affairs.
[15] Se 2005 Voluntary Voting System Guidelines
http://guidelines.kennesaw.edu/vvsg/docs/Volume1Section1.pdf, og omtalen av NIST i Vedlegg C

sikkerheten på Internett. Flere IT-eksperter har også engasjert seg i debatten som motstandere av elektronisk stemmegivning, spesielt bør Rebecca Mercuri[16] og Aviel D. Rubin[17] nevnes.[18]

Pekeskjerm → som brukes til elektronisk stemmegivning i Washington DC.

Debatter angående valgreformer i USA er skarpt polarisert mellom demokrater og republikanere. Demokratene er overveiende mest opptatt av flest mulig velgere skal registrere seg og bruke stemmeretten, mens republikanerne synes å være mer opptatt av integriteten i registreringsarbeidet og valggjennomføringen.

Før valget i 2004 ble det utarbeidet en løsning for stemmegivning over Internett kalt SERVE. Dette er en ordning som først og fremst var beregnet på militærpersonell stasjonert i utlandet. Løsningen ble evaluert av en ekspertgruppe høsten 2003. Fire av ekspertgruppens medlemmer publiserte en egen evalueringsrapport (Jefferson, Simons, Rubin og Wagner 2004)[19] der de konkluderte med at den utviklede løsning ikke kunne anbefales. Mindretallsrapporten trekker frem angrep rettet mot velgerens datamaskin, sårbarheten i Internett og bruken av spesialutviklet, leverandørkontrollert programvare på tjenerne som de største truslene:

> *"The vulnerabilities we describe cannot be fixed by design changes or bug fixes to SERVE. These vulnerabilities are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today. They cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough. It is quite possible that they will not be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet." (Jefferson, Simons, Rubin og Wagner 2004)*

[16] Mercuris hjemmeside http://www.notablesoftware.com/evote.html om elektroniske valg har mye relevant informasjon og litteratur.
[17] Arbeidsgruppen møtte Rubin under studieturen til USA. Et kort referat fra møtet er lagt ved rapporten i Vedlegg C.
[18] Se Vedlegg C for et større innblikk i denne debatten gjennom referater fra møter arbeidsgruppen hadde med ulike amerikanske aktører.
[19] http://www.servesecurityreport.org

4.5 Estland

I Estland ble ideen om elektronisk stemmegivning lansert første gang i 2001, og målet har hele tiden vært stemmegivning via Internett i ukontrollerte omgivelser (Dreschler og Madise 2004). Selv om planen til å begynne med var å gjennomføre Internett-stemmegivning allerede i 2002, drøyde det til lokalvalgene i 2005 før stemmegivning via Internett ble gjennomført.[20]

Målet med stemmegivning via Internett er for det første å øke valgdeltakelsen, både gjennom å "beholde" velgere og øke interessen hos unge. For det andre er det å tilpasse stemmegivning til et moderne IKT-samfunn og gjøre det mer bekvemt å avgi stemme.

Det elektroniske stemmegivningssystemet utnytter det personlige ID-kortet som alle innbyggere i Estland skal ha. Dette er et smartkort med alle de nødvendige nøkler og PIN-koder. Kortet er tenkt brukt for alle transaksjoner der det er nødvendig med sikker brukeridentifisering og juridisk bindende digitale signaturer, herunder ved elektronisk stemmegivning.

Det estiske opplegget for elektronisk stemmegivning er av spesiell interesse for oss fordi det har mange likhetstrekk med hvordan arbeidsgruppen mener elektroniske valg kan gjennomføres i Norge. Ved valgene i 2005 foregikk stemmegivning via Internett bare i forhåndsstemmeperioden. Selv om forhåndsstemmeperioden varte i 9 dager fra 13. til 4. dag før valgdagen, var det bare mulig å stemme på nettet i tre av dem, fra 6. til 4. dag før valgdagen. For å forhindre kjøp og salg av stemmer og utilbørlig påvirking var det mulig å avgi elektronisk stemme flere ganger, men den sist avlagte stemmen var den som gjaldt. Opprinnelig var tanken at velgere som hadde stemt på nettet også skulle kunne avgi stemme på valgdagen, på samme måte som arbeidsgruppen foreslår for norske valg. Denne muligheten ble imidlertid fjernet med den begrunnelse å likestille alle former for forhåndsstemmegivning.

Selve stemmegivningen foregikk på nettstedet www.valimised.ee. De mest populære stedene å stemme var hjemme, banker, stats- og kommunale kontorer og telekommunikasjons-kontorer. For å kunne stemme hjemmefra, måtte velgeren ha en Internett-tilknyttet personlig datamaskin med smartkortleser.

For å forhindre at innholdet av velgerens stemme kunne knyttes til velgeren, ble det brukt et dobbelkonvoluttsystem basert på asymmetrisk kryptering, tilsvarende det systemet som arbeidsgruppen foreslår i kapittel 8. Anonymisering og dekryptering av stemmene ved hjelp av valgets strengt hemmeligholdte private nøkkel ble utført i høytidelige rammer i den estiske parlamentsbygningen helt på slutten av selve valgdagen.

Ni tusen velgere stemte via nettet. På de tre dagene for e-stemmegivning var stemmetallene henholdsvis 3683, 2967 og 3031. Dette var i underkant av 8 prosent av alle forhåndsstemmene som kom inn, og 1,8 prosent av alle avlagte stemmer.

[20] Gjennomgangen av valget i Estland bygger i stor grad på foredrag av Maaten http://www.vvk.ee/english/epp.ppt og Madise http://www.vvk.ee/english/ylle.ppt

Selve programvaren for stemmegivningen er laget av et estisk firma, Cybernetica AS. Firmaet er sprunget ut av Estlands satsing på å bygge opp kompetanse på datasikkerhet. Det er lagt vekt på å lage programvaren så enkel at det er mulig å verifisere at den ikke inneholder sikkerhetshull. En gruppe estiske sikkerhetseksperter har foretatt en sikkerhetsanalyse[21] av spesifikasjonene for systemet og selve programvaren. En forskjell mellom estiske og norske valgprosedyrer er at stemmesedlene er betydelig enklere, og at det ikke er mulig å foreta endringer. Dette gjør det mulig å gjøre visse forenklinger i de elektroniske løsningene.

Politisk sett er det flertall for elektroniske valg i ukontrollerte omgivelser i Estland, men to politiske partier er motstandere av slike løsninger. Innvendingene går først og fremst på at valgprosessen ikke lenger lar seg observere, på faren for kjøp og salg av stemmer og på mulighetene for utilbørlig påvirkning. Mulige sikkerhetsmessige problemer med teknologien blir kun nevnt som et tilleggsmoment[22]. Undersøkelser viser imidlertid at det blant velgere som sogner til disse to partiene er nesten like mange tilhengere av elektroniske valg som blant velgerne generelt[23].

4.6 Sveits

I Sveits gjennomføres det mellom fire og seks valg i året. Dette gjør at det er mer å tjene på å innføre elektronisk stemmegivning her enn i de fleste andre land. Landet er også langt fremme i utviklingen når det gjelder elektronisk stemmegivning. Antageligvis som en følge av hyppige valg slet landet lenge med lav valgdeltakelse, noe som førte til at 25 av 26 kantoner innførte brevstemmegivning for rundt ti år siden. For å opprettholde den positive erfaringen med brevstemmegivning, valgte myndighetene å videreutvikle løsningen til også å omfatte muligheten til å stemme via nettet. For å kartlegge potensialet for elektronisk stemmegivning ble det dessuten gjennomført flere empiriske studier. Undersøkelsene viste at Internett-avstemming hadde betydelig støtte i befolkningen. I følge et representativt utvalg ønsket 66 % av innbyggerne muligheter til å stemme via Internett. Også de fleste politiske partiene og administrativt ansatte var for elektronisk stemmegivning (Geser 2004:80). I 1999 opprettet sentrale myndigheter derfor et prosjekt for elektronisk stemmegivning der alle kantoner ble invitert til å delta. Tre ble valgt ut: Genève, Zürich og Neuchatel. Om lag 80 % av kostnadene ble finansiert av sentrale myndigheter.

Genève kom først i gang med forsøkene, blant annet fordi kantonen allerede hadde et elektronisk velgerregister, valgloven åpnet for forsøk og de hadde erfaring med poststemmegivning. Dessuten var det stor støtte i folket, hos politikerne og i administrasjonen. Totalt er e-valgløsningen tatt i bruk ved syv anledninger, de to siste gangene også på nasjonalt nivå. Det er bare folkeavstemninger som er prøvd ut; det er ikke gjort forsøk i forbindelse med valg til representative organer.

Europarådets anbefaling er ikke lagt til grunn for utviklingen av systemet, men det hevdes at dagens løsning tilfredsstiller hovedprinsippene i anbefalingen. Systemet baserer seg ikke på EML-standarden.[24]

---

[21] Se dokumentasjonen av systemet og sikkerhetsanalysen (på estisk) på http://www.vvk.ee/elektr/
[22] Se "Position of the Estonian People's Union Faction of the Riigikogu on the use of the Internet voting outside the polling station", datert 15.10.2005
[23] Ülle Madise: http://www.vvk.ee/english/ylle.ppt
[24] Se avsnitt 8.7.3 for en gjennomgang av EML-standarden

Genève mottok rundt 10 tilbud på gjennomføringen. Løsningen fra Hewlett Packhard og Wisekey ble valgt. Fra en opprinnelig spesifikasjon som krevde distribusjon av CD-ROM til alle velgere endte man med en løsning basert på 3 separate nøkler, en for pålogging, en for kvittering fra tjener, og en for autorisering av stemmen.

I forhåndsstemmeperioden, som varer i tre uker fram til valgdagen, kan man stemme per post eller via Internett. Ønsker man å stemme på valgdagen må, man møte opp i et valglokale.

Valget 28. november 2005 var en føderal folkeavstemning, og valgdeltakelsen i Genève var på 41 prosent. Alle velgerne i fire kommuner hadde muligheten til å stemme via Internett, og 23 prosent av dem som stemte benyttet seg av denne muligheten. Dette er ca den samme andelen som i de seks først valgene det var mulig å stemme via nettet. Andelen unge velgere som stemmer via nettet, er høyere enn andelen eldre. Velgere med høy utdanning stemmer også hyppigere på nettet enn velgere med lav utdanning (Cristin og Trechsel 2004).

4.7 Andre erfaringer med e-stemmegivning i kontrollerte omgivelser

4.7.1 Nederland og Belgia

Nederland har brukt elektroniske stemmegivningsmaskiner i valglokalene siden slutten av 1990-årene. I følge observatører var det ved innføringen lite oppmerksomhet knyttet til sikkerhet og spørsmål av typen hvordan man egentlig kom fram til valgresultatet.[25] Bruker-vennligheten, spesielt for eldre, stod i sentrum for debatten. I forbindelse med valget til Europaparlamentet i 2005 var det mulig for velgere bosatt i utlandet å stemme via Internett eller via telefon.

I Belgia ble elektronisk stemmegivning i valglokalet introdusert så tidlig som i 1991, mest på grunn av et komplisert valgsystem med tidkrevende manuelle kontroller og telleprosedyrer.[26] Det juridiske rammeverket kom på plass i 1994, og e-stemmegivning ble brukt i stor utstrekning ved valgene i 1999, 2000, 2003 og 2004. I 2003 stemte 44 prosent av velgerne (3.2 millioner velgere) elektronisk.[27] Stemmegivningsmaskinen, eller valgomaten, består av en personlig datamaskin med skjerm, en optisk penn og en magnetkortleser. Valgurnen er en personlig datamaskin med to magnetkortlesere: en for å sjekke magnetkortet, og en for å registrere stemmer.

4.7.2 India og Brasil

Brasil og India har i henholdsvis 2000 og 2003 også gjennomført fullstendige elektroniske valg i kontrollerte omgivelser. Bakgrunnen her var ønsket om å gjøre valgene mer tilgjengelige for de deler av befolkningen som ikke kan lese eller skrive. India har også en historie med mye bråk og uro knyttet til stemmegivning, og svært omfattende valgsabotasje.

Rundt 370 millioner indiske velgere, av totalt mulige 675 millioner, stemte elektronisk i et hel-elektronisk parlamentsvalg i 2004. Opplegget besto av en million e-stemmegivnings-

[25] http://www.cs.ru.nl/sos/research/society/voting/index.html
[26] Belgia har obligatorisk stemmegivning, og opp mot fem valg skal gjennomføres samtidig på tre ulike språk. Velgere har anledning til å personstemme, og det kan være opp mot 87 kandidater per liste
[27] se http://www.steria.com

maskiner fordelt på landets 800 000 stemmelokaler. Selve maskinen er på størrelse med en koffert og består av to deler. ”Kontroll-delen” ble administrert av en valgmedarbeider, mens ”stemmegivnings-delen” ble plassert i stemmebåsen. Velgeren trykket på knappen ved siden av kandidaten hun ønsket å stemme på. I tillegg til navnet hadde også kandidatene et symbol knyttet til seg.

Innkjøp av 800 000 maskiner krevde en investering på rundt 200 millioner amerikanske dollar. Men myndighetene vil spare opp mot 10 000 tonn med stemmesedler i hvert nasjonale valg framover.

For å minimere risikoen for virusangrep og hacking var ikke maskinene tilknyttet noe nettverk. Selv om valget ble betegnet som en suksess av myndighetene, ble det likevel reist en del kritiske spørsmål. Maskinene ga ingen papirkvitteringer, og resultatet maskinene kommer fram til kunne dermed ikke etterprøves. Det faktum at kildekoden ikke var åpen, ble også kritisert.[28]

Brasil gjennomførte elektronisk stemmegivning første gang ved lokalvalget i 1996. Men den gangen var det bare de store byene som stemte elektronisk. Bruken av elektronisk stemmegivning ble utvidet i 1998, og ved valgene i 2000 og 2002 ble mer enn 400 000 elektroniske stemmegivningsmaskiner tatt i bruk.

4.7.3 Irland

I Irland hadde de planene klare for gjennomføring av elektronisk stemmegivning med pekeskjermer ved lokalvalget og valget til Europaparlamentet i juni 2004. Ved valget i 2002 ble det gjennomført forsøk i 3 av 42 valgkretser, og det ble avgitt 138 011 elektroniske stemmer (Laver 2004).

Kommisjonen som fikk i oppdrag å evaluere den valgte løsningen, anbefalte imidlertid å ikke ta den i bruk, og alle planer om elektronisk stemmegivning ble stoppet inntil videre. Kommisjonens konklusjon var ikke basert på funn som tydet på at systemet ikke ville fungere. Argumentet var at gruppen ikke var overbevist om at løsningen ville fungere.[29]

Det ser imidlertid ut til at irske myndigheter ikke har lagt elektronisk stemmegivning helt på is. I løpet av 2005 er det blitt tatt initiativ til en risiko- og sikkerhetsanalyse av e-valg systemet. Det er imidlertid usikkert om dette innebærer at det neste irske valg blir elektronisk.

4.7.4 Noen mindre forsøk[30]

I Frankrike gjennomførte kommunen Brest elektronisk stemmegivning i forbindelse med lokalvalget 21. og 28. mars 2004. Løsningen ble levert av det nederlandske firmaet Nedap, og ga velgerne muligheten til å avgi stemme via en elektronisk valgurne i stemmelokalet. Fem andre kommuner gjennomførte også forsøk, men disse var ikke del av det offisielle valget. I forbindelse med valget til Europaparlamentet 13. juni gjennomførte 18 franske kommuner forsøk med elektronisk valg, men alle forsøkene var heller ikke denne gangen del av det offisielle valget. Også disse forsøkene gikk ut på at velgerne skulle stemme elektronisk inne i valglokalet. Tre ulike løsninger ble prøvd ut.[31] Elektronisk stemmegivning har i prinsippet

[28] http://europa.eu.int/ida/en/document/2551/358
[29] Se kommisjonens rapport: http://www.cev.ie/index.htm
[30] Dette avsnittet bygger i stor grad på nettsiden http://focus.at.org/e-voting/countries
[31] Dette var Nedap 2.07, Ivotronic og Point&Vote (Indra)

vært lovlig i Frankrike siden 1969, men ble aktualisert gjennom en "decree" fra myndighetene 18. mars 2004, som autoriserte 33 kommuner til å drive forsøk.[32] Ved folkeavstemningen om EUs grunnlov 29. mai 2005 ble det brukt stemmemaskiner i 60 kommuner. I noen av kommunene var stemmegivningen juridisk bindende. ¾ av kommunene brukte stemmemaskinen NedDap Powervote. En kommune testet stemmemaskiner der velgeren identifiserte seg med smartkort.

Spania gjennomførte forsøk i liten skala både i 2003 og 2004, og gjennomførte et større pilotprosjekt i forbindelse med folkeavstemningen om EUs grunnlov i februar 2005. Fra 1. til 18. februar kunne potensielt to millioner velgere fra 52 testkommuner delta i forsøket. Avstemmingen var ikke juridisk bindende. Stemmegivningen kunne foregå fra enhver datamaskin med Internett-tilgang, og velgeren identifiserte seg med smartkort og PIN-kode. I overkant av 10 000 stemmeberettigede deltok i forsøket.[33] Forsøkene i 2004 ble gjennomført i forbindelse med parlamentsvalget 14. mars, men var ikke del av det offisielle valget.[34] Løsningene gikk ut på at velgere enten kunne stemme via SMS eller personlig datamaskin med en Internett-løsning. Disse datamaskinene sto i valglokalene. Løsningene ble levert av firmaet Indra som benyttet muligheten til å vise fram forsøkene til inviterte gjester fra 27 europeiske og latinamerikanske land. Indra leverte også løsningen til piloten i februar 2005.

Over 9000 velgere deltok i et forsøk med elektronisk stemmegivning i Portugal i forbindelse med valget til Europaparlamentet 13. juni 2004.[35] Forsøket ble gjennomført i ni kommuner valgt ut etter geografi, størrelse og politiske preferanser, men var ikke en del av det offisielle valget. Deltakerne ble bedt om å delta i forsøket etter at de hadde avgitt stemme ved valget. Til sammen 9 300 av 50 562 velgere takket ja. Tre ulike løsninger ble prøvd ut: "Pekeskjerm", "lyspenn" og "elektroniske kort". Evalueringen slår fast at 93 prosent av deltakerne foretrakk en av disse formene for stemmegivning framfor den tradisjonelle metoden. Her må selvsagt selvseleksjon tas med i betraktningen.

Romania gjennomførte 18. og 19. oktober 2003 et forsøk som gikk ut på å tilby militærpersonell stasjonert i utlandet muligheten til å stemme via nettet. Forsøket ble gjennomført i forbindelse med en folkeavstemning om endring av Romanias grunnlov. 97 prosent av 1 600 potensielle velgere deltok i forsøket som blir betegnet som en suksess.

Venezuela gjennomførte elektronisk stemmegivning i valglokalet i forbindelse med folkeavstemningen om Hugo Chàvez skulle fortsette som president. Som kjent ble resultatet at presidenten ble sittende, og opposisjonen hevdet at det foregikk storstilt valgsvindel. De påstod også at tilbudet fra de internasjonale valgobservatørene om en revisjon av resultatet ikke ville føre fram fordi stemmegivningen hadde foregått elektronisk. Valget ble gjennomført ved hjelp av et konsortium – SBC – bestående av tre firmaer. Mer enn 14 000 personer ble mobilisert og trent opp av SBC for å gjennomføre valget, og løsningen kostet myndighetene rundt 22 millioner euro. SBC hevder imidlertid at Venezuela kan spare ca 25-30 millioner euro per valg i tiden framover.

[32] se http://europa.eu.int/ida/en/document/2635/358 og http://europa.eu.int/ida/en/document/2314/358
[33] se http://europa.eu.int/idabc/en/document/3923/358
[34] se http://europa.eu.int/ida/en/document/2287/358
[35] se http://europa.eu.int/ida/en/document/2633/358

5 Demokratiske prinsipper og legitimitet

5.1 Innledning

I formålsbestemmelsen til valgloven sies det at loven skal ”legge forholdene til rette slik at borgerne ved frie, direkte og hemmelig valg skal kunne velge sine representanter til Stortinget, fylkesting og kommunestyrer” (§ 1-1). I dette kapitlet skal vi komme nærmere inn på noen av de overordnede prinsippene som ligger til grunn for gjennomføringen av valg. Dette er prinsipper som må imøtekommes for at valg skal kunne betegnes som demokratiske, og bli oppfattet som legitime uttrykk for velgernes ønsker.

I de senere årene har informasjons- og kommunikasjonsteknologi (IKT) åpnet nye muligheter også når det gjelder demokratiske former (McLean 1989; Kersting og Baldersheim 2004). Det som særlig har blitt fremhevet, er hvordan ny teknologi letter tilgangen på informasjon, og gjør det enklere å kommunisere og engasjere seg i demokratiske prosesser. Dette kan på sikt bety en styrking av demokratiske ordninger som vektlegger diskusjon, dialog og deltakelse. Samtidig vil forskjellige former for umiddelbar (”instant”) deltakelse kunne svekke de tradisjonelle kanalene som partier og organisasjoner utgjør (Westholm 2002).

Vi skal i dette kapitlet ikke behandle e-demokrati i hele sin bredde, men konsentrere oss om e-stemmegivning. Følgende punkter i mandatet blir tatt opp:

- Vurdere betydningen av innføring av et elektronisk system i et demokratisk perspektiv, herunder legitimitet og valgdeltakelse (pkt. 1).
- Problemstillingen ”utilbørlig påvirkning” i forbindelse med stemmegivning utenfor valglokalet må vurderes særskilt, jf. også diskusjonen om poststemmer (pkt. 7).
- Vurdere problematikken kjøp/salg av stemmer eller identitet i forbindelse med stemmegivning utenfor valglokalet (pkt. 8)
- Vurdere fordeler og ulemper ved elektronisk stemmegivning vs ordinær stemmegivning (pkt. 12).
- Vurdere betydningen av en overgang fra lekmannskontroll til profesjonalisering, blant annet betydningen for valgsystemet mht kontroll, administrasjon av valg, kompetanse (pkt. 14).
- Sammenstille forskning/utredninger på området (pkt. 17).

Punkt 14 vil bare så vidt bli berørt i dette kapitlet, men behandles mer utførlig i kapittel 6 og 9. Det er lagt vekt på å sammenstille og referere forskningsresultater der det er relevant, ikke minst når det gjelder hva som påvirker deltakelsen ved valg. Det meste av diskusjonen i dette kapitlet er av overordnet karakter. Prinsippene som trekkes frem i avsnitt 5.2 er forankret i normativ demokratiteori, men vi gjenfinner dem også i større eller mindre grad i internasjonale regelverk og anbefalinger på området. I avsnitt 5.3 ser vi nærmere på det å avgi stemme før valgdagen – det vil si i ”fase 1” (forhåndsstemmegivning). Dette fordi det nettopp er i denne fasen, og ikke på selve valgdagen, at elektronisk stemmegivning utenfor godkjent valglokale fremstår som en mulighet som lar seg begrunne normativt eller prinsipielt. Avsnitt 5.4 redegjør for mulige feilkilder ved dagens manuelle valgoppgjør. Dette er det viktig å ha med seg ved vurderingen av fordeler og ulemper ved valg basert på henholdsvis elektronisk og tradisjonell stemmegivning. Konklusjoner trekkes i avsnitt 5.5, og disse utgjør en viktig del av premissgrunnlaget for de tekniske løsningene som behandles i kapittel 8.

5.2 Frie og rettferdige valg

Demokrati betyr folkestyre, men folkestyrets former er mange og forskjelligartede. Det er likevel klart at det er tale om en form for representativt styre: Styrerne pekes ut og opptrer på vegne av de styrte, og skal ivareta deres interesser på en systematisk måte. Det virkemidlet som gjør dette mulig, er gjennomføring av valg til ledende posisjoner. I et demokrati er i alle fall medlemmene av parlamentet − og tilsvarende forsamlinger på regionalt og lokalt nivå − direkte valgt av folket. Mange vil hevde at demokrati fordrer langt mer enn valg. Det pekes på slike ting som høy deltakelse ved valgene og i andre politiske kanaler, samt bredt politisk engasjement og grundige diskusjoner frem mot de vedtakene som fattes mellom valgene. Det er helt klart at dette er nødvendige ingredienser i et levende folkestyre. Samtidig er det liten tvil om at uten valg kan det i alle fall ikke være snakk om demokrati.

Demokratiske valg har to viktige funksjoner. For det første er valg en metode for utvelgelse av det politiske lederskapet. Valgene kan bidra til at de som styrer, blir et rimelig representativt utsnitt av befolkningen når det gjelder verdier, holdninger, meninger og kanskje også viktige bakgrunnskjennetegn. For det andre er valg en metode for ansvarliggjøring og kontroll av det politiske lederskapet i parlament og regjering. I et demokrati kan velgerne ”avsette” makthaverne, og peke ut nye. Folkets representanter må søke å ivareta velgernes interesser for å få fornyet tillit ved neste valg. Valgene kan dermed bidra til at *styringen* blir representativ, i tillegg til at de gjør *styrerne* representative.

Valg gjennomføres i mange sammenhenger, og ikke alle valg er demokratiske. Vi skal nå redegjøre nærmere for noen av de kravene som må tilgodeses for at valg skal kunne oppnå demokratisk legitimitet. Det finnes mange formuleringer av slike krav i faglitteraturen på området,[36] og ikke minst i retningslinjer og manualer fra forskjellige instanser som arbeider med valg.[37] Selv om valget av betegnelser på de ulike prinsippene kan variere, er det bred enighet om hvilke forhold som er sentrale.

På det generelle plan fremheves det gjerne at valgene skal være ”frie og rettferdige”, et uttrykk som først ble benyttet for å karakterisere valg så sent som midt på 1950-tallet. At valg er frie, innebærer i denne sammenheng først og fremst fravær av tvang og hemmende begrensninger på alle trinn av valgprosessen. I praksis forutsetter det at valget skjer innenfor en ramme der grunnleggende menneskerettigheter blir respektert. Med rettferdige valg siktes det primært til at de gjennomføres på en måte som er preget av upartiskhet, nøytralitet og likhet. Vi vil nå ta opp noen av grunnprinsippene som må ivaretas innenfor en demokratisk ramme av frie og rettferdige valg.

5.2.1 Periodiske valg

I et demokratisk system er representantene valgt for en nærmere angitt periode. I parlamentariske systemer innebærer dette at det er bestemt hvor lenge de folkevalgte maksimalt kan sitte; perioden kan bli ”avbrutt” hvis det utskrives nyvalg. Stadig tilbakevendende valg gjør at partier og representanter er gjort avhengig av fornyet tillit i velgerskaren for å fortsette sitt virke. Dette bidrar til å *ansvarliggjøre* de valgte, og i større

[36] For en oversikt, se Nygård (2003), Choe (1997) eller Elklit og Svensson (1997).
[37] Se neste kapittel. Ikke minst er det slik at de grunnleggende prinsippene vi her har i tankene har blitt diskutert inngående i forbindelse med observasjon av valg, noe som blant annet. reflekteres i dokumenter av typen ”Declaration of Principles for International Election Observation” (FN, 7. juli 2005).

eller mindre grad sikre at de søker å opptre på en måte som samsvarer med interesser og holdninger som gjør seg gjeldende blant velgerne. Hvor klar ansvarliggjøringen vil være i praksis, avhenger blant annet av hvilket valgsystem som benyttes og de politiske partienes struktur og betydning.

I fremtiden kan en tenke seg at IKT gjør det vesentlig enklere enn i dag å gjennomføre valg, både fordi selve stemmehandlingen blir mindre krevende − særlig om den foregår via elektronisk medium utenfor offisielt valglokale − og fordi opptellingen automatiseres. Slike forenklinger kan i sin tur skape et press i retning av å benytte valgmekanismen i langt sterkere grad enn det som er tilfelle i dag. Det kan på den ene siden trekke i retning av hyppigere valg og kortere valgperioder, og det vil selvsagt være delte meninger om den økte "velgerfølsomheten" som dette foranlediger er gunstig eller ikke. På den andre siden kan det trekke i retning av økt bruk av folkeavstemninger. Hvorfor kan ikke folket avgjøre flere saker direkte – eller gi politikerne et (ikke-bindende) råd oftere – hvis det likevel er små kostnader forbundet med å gjøre det? (Morris 1999). Over tid vil en derfor kunne oppleve at den representative karakteren som preger dagens styringssystem endres (jf. Buchstein 1997). Kritikere har i denne sammenheng skissert konturene av et "trykknappdemokrati" eller "øyeblikksdemokrati", med kortsiktighet og politiske ledere med svekket ansvar som ingredienser.

5.2.2 Ulike politiske alternativer

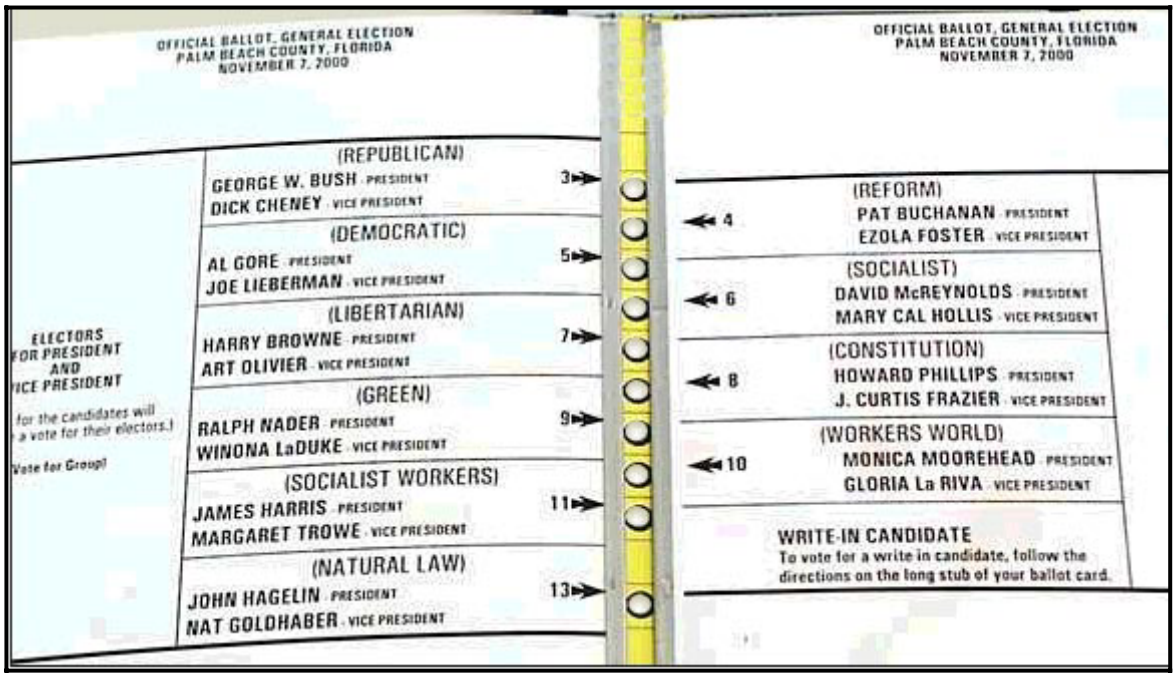
I et demokratisk valg er det konkurranse mellom ulike politiske alternativer. Det må være vid adgang for forskjellige grupperinger − store og små, etablerte eller nye − å stille til valg, og velgerne må ha et reelt valg mellom flere partier, lister eller kandidater. Dette legger klare føringer på tiden før valget, inkludert selve valgkampen. Betingelsene de forskjellige grupperingene møter trenger å være noenlunde likeartede; de bør være preget av nøytralitet i den forstand at ingen favoriseres i urimelig grad. Dessuten må det sikres at velgerne kan opptre fritt og utvungent.

En rettferdig politisk strid på dette området forutsetter i det minste respekt for grunnleggende friheter og rettigheter, så som ytringsfrihet, forsamlingsfrihet og organisasjonsfrihet. Det er nødvendig for å etablere og klarlegge innholdet i politiske alternativer overfor velgerne. Samtidig er det klart at prosedyrene for registrering av partier og nominasjon av lister eller kandidater må være upartiske, og de godkjenningskriteriene som legges til grunn må oppfattes som rimelige.

Ny teknologi har et stort potensial også på dette feltet, ikke minst ved å forenkle registreringsrutiner og gi bedre oversikt. Når det gjelder spørsmålet om stemmegivning, er det en del subtile − av og til vridende − effekter ved tradisjonelle stemmeformer som også kan ha paralleller ved elektronisk stemmegivning. Ikke minst ble det tydeliggjort under det amerikanske presidentvalget høsten 2000 at utformingen av stemmesedlene kan ha stor betydning. "Sommerfuglstemmeseddelen" i Palm Beach County i Florida (se Boks 5.1) kostet antakelig demokraten Al Gore over 2.000 stemmer (demokrater som feilaktig stemte på kandidaten Pat Buchanan), i en situasjon hvor George Bush tok Florida med en offisiell margin på 537 stemmer − og denne staten avgjorde hvem som ville innta Det hvite hus (se f. eks. Wand m.fl. 2001 og New York Times 2001). Nyere forskning har vist at stemmesedlenes utforming så vel som teknologien som benyttes i valglokalet kan ha betydning for hvor mange og hvilke stemmer som avgis og registreres i samsvar med velgerens intensjoner.[38] I en

[38] Se for eksempel Bullock og Hood (2002), Niemi og Herrnson (2003) og Ansolabehere og Stewart (2005).

omfattende undersøkelse av Reynolds og Steenbergen (2005) bekreftes det at stemmesedler med enkelt design fører til at færre stemmer forkastes. Kontrollerte eksperimenter tyder på at velgere flest vil stemme på samme måte uansett design (bruk av symboler, farger, fotografier, og lignende), men utformingen kan likevel systematisk fordreie et ikke ubetydelig antall velgeres stemmegivning − kanskje velgere med hastverk, lav utdanning eller svake leseferdigheter.

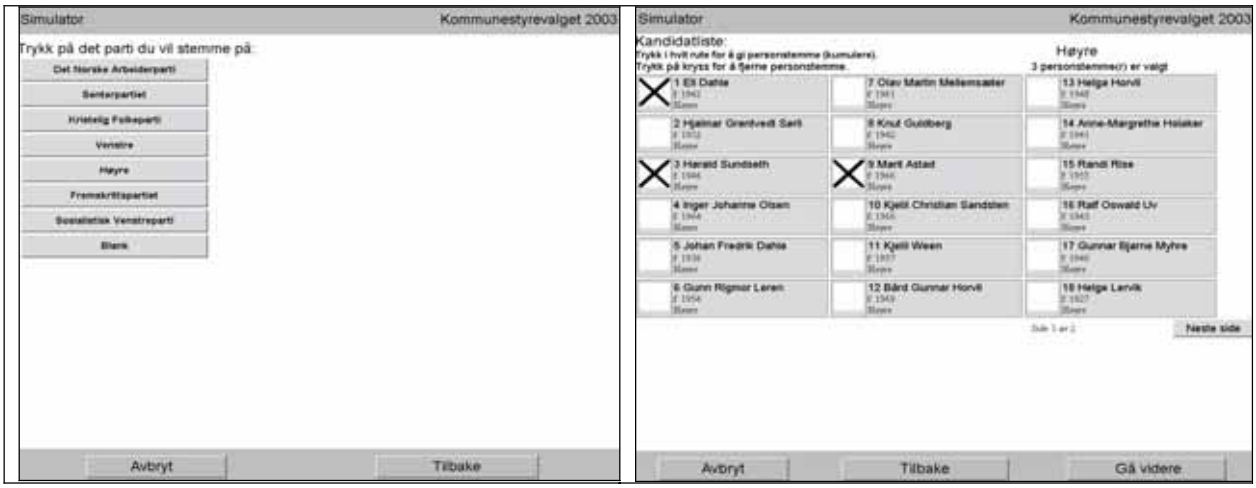


Palm Beach County sto selv ansvarlig for utforming av stemmeseddelen. Den spesielle utformingen med to kolonner med kandidater i stedet for bare én, var motivert ut fra et ønske om å benytte så store skrifttyper som mulig gitt de begrensningene som utstyret i valglokalene ga. Tanken var at dette særlig ville hjelpe eldre velgere, som det er mange av i fylket. Velgeren skulle benytte et "stempel" og hulle ut den lille sirkelen for ønsket kandidat i midtfeltet mellom kandidatnavnene. Det øverste hullet gjelder kandidaten øverst til venstre (George Bush), det nest øverste gjelder kandidaten øverst til høyre (Pat Buchanan), det tredje øverste gjelder den nest øverste kandidaten til venstre (Al Gore), osv. Mange av de som stemplet det nest øverste hullet, hadde til hensikt å avgi stemme på Al Gore. I så fall var det tale om feilstemmegivning. I tillegg var det et uvanlig høyt antall "overvotes" (for mange merkede hull på stemmeseddelen) i Palm Beach County. Disse stemmesedlene ble forkastet, og utformingen av stemmeseddelen kan dermed i realiteten også sies å ha "fratatt" mange velgere stemmeretten.

Figur 5.1: "Sommerfuglstemmeseddelen" (the butterfly ballot) i Palm Beach County, Florida, ved presidentvalget i 2000.

Brukergrensesnittet ved elektronisk stemmegivning kan sammenlignes med designet for papirstemmesedler, og har tilsvarende betydning. Slike ting som brukergrensesnitt, skjermbildenes struktur og forekomst av klikkbar (tilleggs)informasjon blir vesentlig dersom det stemmes på datamaskin – enten den befinner seg i eller utenfor valglokalet. Selv om brukergrensesnittet holdes enkelt, er det uproblematisk å håndtere kompliserte valgordninger med sammensatte rettemuligheter. Det er ikke tilfeldig at flere av de landene som har satset på å utplassere datamaskiner (for eksempel valgomater) i alle valglokaler har relativt kompliserte valgsystemer (Belgia, Nederland, Irland); elektronikken har gitt betydelige gevinster i form av nøyaktighet og hurtighet ved opptellingen.

Det er lett å tenke seg at hvis brukergrensesnittet gjør det enkelt å foreta endringer på stemmeseddelen (som kumuleringer, strykninger og "slengere"), øker også antallet velgere som benytter seg av muligheten. Forsøkene med elektronisk stemmegivning i utvalgte kommuner i 2003 gir imidlertid ikke grunnlag for å trekke entydige konklusjoner på dette punktet.[39] På den annen side kan elektronisk stemmegivning forhindre at stemmesedler forkastes fordi de er rettet feil, simpelthen ved at velgeren får en feilmelding når en feilaktig stemmeseddel forsøkes innlevert. Teknologi kan også bidra til å innsnevre velgerens muligheter. SMS-stemmegivning på dagens mobiltelefoner kan vanskelig bestå av annet enn enkel innsending av en urettet liste- eller partistemme.



Figur 5.2: Eksempel på brukergrensesnitt fra forsøkene med elektronisk stemmegivning i utvalgte kommuner i 2003.

Når det gjelder det å forstå betydningen av brukergrensesnitt nærmere, kan kontrollerte eksperimenter være en metode å vinne viktig erfaring på før bestemte løsninger settes ut i livet. Formålet må være at elektronikken like lite som tradisjonell stemmegivning skal gi mer eller mindre tilsiktede fortrinn for noen av de politiske konkurrentene, eller påvirke valget på andre måter.

5.2.3 Inkluderende valg med alminnelig stemmerett

Allmenn stemmerett er et helt grunnleggende vilkår i demokratisk teori og praksis, og har vært det i alle fall siden første del av 1900-tallet. Stemmeretten kan ikke være forbeholdt et mindretall, men må omfatte hele den voksne befolkning. Det bør heller ikke være slik at faktisk deltakelse ved valgene er sterkt begrenset; de fleste er tilbøyelig til å se lav valgdeltakelse som et problem, selv om det ikke er godt å sette noen entydig nedre grense for hva som er et akseptabelt deltakelsesnivå.

I et demokrati kan det heller ikke være vesentlige forskjeller på stemmeretts- og valgbarhetskriterier, selv om de sistnevnte kan være noe mer restriktive enn de førstnevnte. Tilsvarende skal det mye til for å bli fratatt stemmeretten (jf. Grl. § 53). Valgsystemet må også gi sikkerhet mot at personer uten stemmerett kan få stemmer godkjent.

[39] Se Christensen, Karlsen og Aardal (2004: 39). Erfaringene fra forsøkene er begrensede, i og med at det bare er sett på to forsøkskommuner – Bykle og Oppdal. Når det gjelder forhåndsstemmegivning, var andelen rettelser større for de som stemte elektronisk enn de som stemte på papir. På selve valgtinget var det noen flere rettelser blant de som stemte manuelt i Bykle, mens det ikke var noen forskjell i Oppdal. Konklusjonen blir altså noe blandet.

Uten at valg er inkluderende − både når det gjelder retten til å stemme og å stille til valg − svekkes representativiteten i systemet. Videre er det større sikkerhet for at den folkevalgte forsamlingen opptrer i tråd med velgernes interesser og holdninger hvis alle deler av velgerskaren mobiliseres ved valgene, og at det ikke er systematiske skjevheter i velgerfrafallet. Hvis elektoratet er skjevt i forhold til befolkningen som helhet, kan dette forplante seg videre både til den representative forsamlingen og innholdet i den politikken som føres. Empirisk slår faktorer som alder, utdanning og sosioøkonomisk status mer eller mindre kraftig ut i denne sammenheng.

5.2.4 Nærmere om valgdeltakelsen

Det er mange forhold som påvirker deltakelsen ved valg, noe omfattende forskning har vist. Fire forhold er særlig viktige. For det første spiller selve valgsystemet og tilsvarende institusjonelle mekanismer en rolle. Det er godt dokumentert at valgdeltakelsen har en tendens til å være lavere i land som benytter flertallsvalg enn der forholdstallsvalg råder grunnen (Lijphart 1997). Det norske valgsystemet er som kjent av den sistnevnte typen, der det er et relativt godt samsvar mellom partienes oppslutning blant velgerne og partienes andel av mandatene på Stortinget. For det andre kommer kostnadene − vidt forstått − ved å avgi stemme inn; jo vanskeligere og mer ”kostnadskrevende” det er å avgi stemme, desto lavere valgdeltakelse. Noe som har vist seg å ha stor betydning i denne sammenheng, er om registreringen av velgere i manntallet skjer automatisk (som i Norge) eller om velgeren selv må ta aktive skritt for å bli manntallsført (som i USA og Frankrike). Tungvinte registreringsprosedyrer reduserer deltakelsen. Andre forhold som er knyttet til kostnader er antallet valgdager, om valgdagen er fridag, avstanden til stemmestedet, hvorvidt det er store køer i valglokalet, og lignende. Her er imidlertid effektene mindre klare. Enkelte land har stemmeplikt, og bøtelegger velgere som ikke deltar. Selv et lavt eller symbolsk bøtenivå synes å påvirke deltakelsen. For det tredje spiller mer politiske forhold inn. For eksempel er det slik at valgdeltakelsen øker når det er klare politiske alternativer som står mot hverandre, og det er stor spenning og usikkerhet knyttet til utfallet av valget. For det fjerde har mange undersøkelser vist at kjennetegn ved velgerne selv er av betydning for å forstå deltakelsesmønsteret ved valg. Gjennomgående deltar yngre velgere mindre enn andre. Deltakelsen øker med økt utdanning og økt inntekt.

Mange har pekt på stemmegivning via Internett som en reform som kan øke valgdeltakelsen, og særlig trekke en større andel unge velgere til valgurnen. I og med at erfaringene med elektroniske valg til nå er svært begrenset, er det vanskelig å si om − og ikke minst hvordan − Internett-stemmegivning vil påvirke valgdeltakelsen. Én mulighet er rett og slett at eksisterende skjevheter i deltakelsesmønsteret forsterkes. Fortsatt finnes det markante digitale skillelinjer (jf. Rønning m.fl. 2005), og elektronisk stemmegivning kan bidra til at de grupper som allerede har høyt deltakelsesnivå mobiliseres ytterligere (Norris 2004a, Gibson 2001, Kenski 2005, Alvarez og Nagler 2001). Deltakelsen kan med andre ord øke, men kanskje ikke først og fremst i grupper som er lite aktive i dag.

Brevstemmegivning ligner i noen grad på stemmegivning over Internett. Begge deler representerer en forenkling av det å avgi stemme, og kan tenkes å ha nokså likeartede virkninger. Analyser tyder ikke på at vide muligheter til å stemme hjemmefra per brev har noen helt entydig effekt på deltakelsesnivået. Enkelte steder har valgdeltakelsen gått opp,

mens den andre steder har vært nærmest upåvirket (Qvortrup 2005).[40] Gjennomgående er det imidlertid ikke slik at nye velgergrupper mobiliseres; deltakelsesmønsteret ved brevstemmegivning er ofte ikke vesentlig annerledes enn ved tradisjonell stemmegivning. En rekke studier viser at der økt deltakelse faktisk blir resultatet, er det den mest ressurssterke halvdelen av elektoratet som står for økningen (Magleby 1987, Karp og Banducci 2000, Berinsky m.fl. 2001). I en undersøkelse av brevstemmegivning i Sveits viste det seg at valgdeltakelsen i de aktuelle kantonene gjennomgående ikke ble påvirket (Funk 2004).[41] Norris (2004a) sammenligner valgdeltakelsen i 25 land i 1990-årene, og konkluderer med at muligheter for å stemme per brev ikke har signifikant effekt på deltakelsesnivået. Det eneste av mer voteringsteknisk art som synes å ha en viss positiv betydning, er at valgdagen er en hviledag (i praksis betyr det lørdag eller søndag). Den britiske valgkommisjonen konkluderer imidlertid med at forsøkene med brevstemmegivning i 2002 og 2003 tyder på at denne tilnærmingen er effektiv for å øke valgdeltakelsen (The Electoral Commission 2003). Også Norris (2004b:211) understreker at de britiske forsøkene med brevstemmegivning var en suksess. I valgdistrikter med brevstemmegivning økte valgdeltakelsen i gjennomsnitt fra 34 til 49 prosent.[42]

Det er betydelig usikkerhet knyttet til om elektronisk stemmegivning utenfor valglokalet vil bidra til å øke valgdeltakelsen på en markant og varig måte. Det er usikkert om e-stemmegivning er et virkemiddel som vil få yngre velgere til å delta i langt sterkere grad enn i dag. Selv om det ikke er noen tvil om at elektronisk stemmegivning vil øke tilgjengeligheten og gjøre det lettere å avgi stemme, gir forskningen ikke noe klart grunnlag for å vente vesentlig høyere valgdeltakelse. Økt valgdeltakelse er følgelig heller ikke noe sterkt argument *for* å introdusere elektronisk stemmegivning utenfor valglokalene, fordi det er usikkert om dette faktisk vil bli resultatet.

En bør i denne sammenheng også være oppmerksom på den mulighet at elektronisk stemmegivning utenfor valglokalet i fase 1 (forhåndsstemmegivning) over tid reduserer behovet for valglokaler under selve valgtinget. Hvis dette fører til at det blir færre stemmesteder på valgdagen, er det noen velgere som vil oppleve *redusert* tilgjengelighet som følge av denne utviklingen.

5.2.5 Lik stemmerett

Demokratiske valg bygger på en forutsetning om politisk likhet; demokrati er i bunn og grunn et system for maktspredning. Hver velgers oppfatning er like verdifull; ved valgene skal hver stemme telle tilnærmet likt − og stemmene innenfor én og samme opptellingsenhet skal det i alle fall ikke være forskjell på. Politisk likhet innebærer at det ikke har noen betydning *hvem* en velger er, og stemmene kan følgelig tenkes byttet om velgere imellom i et distrikt uten at det får noen som helst betydning for resultatet. Uttrykket ”tilnærmet likt” er benyttet ovenfor, og det skyldes at det ved en del valg − herunder stortingsvalg − kan ha betydning *hvor* en

[40] Det har vært to grunner til innføring av brevstemmegivning. For det første har det vært et tiltak for å bøte på lav valgdeltakelse. For det andre har begrunnelsen vært å redusere de administrative kostnadene ved å gjennomføre valg.

[41] I samme undersøkelse vises det at det å ta bort stemmeplikten, som flere kantoner har gjort de senere årene, hadde klart negativ betydning for valgdeltakelsen. Dette til tross for at de aktuelle lovbestemmelsene om stemmeplikt i overveiende grad var symbolske, med ubetydelige sanksjoner av brudd på plikten til å stemme (små bøter).

[42] Det totale antall utenlandsstemmer i Sverige økte fra 32 000 i 1998 da det bare var mulig å stemme per brev fra Sveits og Tyskland, til 50 000 i 2003 da det var åpnet for brevstemmegivning for alle svensker bosatt i utlandet (SOU 2004:111).

velger har rett til å stemme.[43] Denne typen forskjeller mellom velgerne krever særskilt begrunnelse, og kan ikke bli særlig markante før de utgjør et demokratisk problem.

Likhetsprinsippet innebærer ellers at de rutinene og den teknologi som benyttes ved valget, sikrer at hver velger bare får avgi én tellende stemme, og det må garanteres at denne faktisk registreres og telles. Systemet må forhindre at en velger avgir flere tellende stemmer, at samme stemme telles flere ganger, at stemmer forsvinner og at stemmer "fordreies" underveis i valgprosessen (slik at registrert stemme ikke er i samsvar med velgerens intensjon og handling). Manuelle valgprosesser er i mange land utviklet og forbedret over svært lang tid, og det benyttes rutiner som i all hovedsak sikrer ivaretakelse av de ovennevnte likhetshensynene. Ny teknologi kan utvilsomt bidra til hurtig å produsere et korrekt resultat av valget, men hele prosessen vil være mindre gjennomsiktig.

5.2.6 Åpenhet og etterprøvbarhet

Åpenhet eller transparens er viktig av flere grunner. Den bidrar til at valggjennomføringen blir forutsigbar, forståelig og mulig å følge for borgerne, og dette gir i sin tur grunnlag for bygging av tillit. Tillit og legitimitet er nært forbundet. Etterprøvbarhet og gode kontrollrutiner må antas å virke på samme måte. Det sørger for ansvarlighet, og er en kilde til at valgresultatene oppfattes som troverdige. Det er tidkrevende og vanskelig å bygge opp tillit, men det er samtidig noe det er lett å ødelegge eller rive ned.

Det at velgere skal kunne ha mulighet til å forstå hvordan valgsystemet virker og valg gjennomføres, legger begrensninger på hvilke ordninger som kan legges til grunn. Det har en verdi i seg selv at de er så enkle som mulig.

Både valgsystemets virkemåte og rutinene for valggjennomføring som foreskrives i lov og forskrifter er det mulig å forstå for de som vil, selv om det utvilsomt kan kreve noe innsats. På dette punktet er det en vesensforskjell mellom et manuelt valgoppgjør og et som hviler på elektroniske løsninger. De tekniske sidene ved elektronisk stemmegivning er det bare et mindre antall eksperter som kan forstå fullt ut; velgerne må ha tillit til at de vurderingene som ekspertene – eller ekspertorganer – gjør er riktige, og at systemene fungerer etter forutsetningene. Merk at tilliten må bygges på et langt svakere grunnlag enn for eksempel elektroniske banktjenester, hvor handlinger er dokumenterte- og etterprøvbare i en helt annen grad en det som er mulig ved valg som jo skal være hemmelige.

Det er avgjørende at et valgoppgjør er sikkert og pålitelig. Oppstår det tvil om et valgresultat er riktig, for eksempel etter at det er fremsatt troverdige påstander om teknisk svikt eller fusk, må det være mulig å verifisere de forholdene striden gjelder, og fastslå entydig om resultatet er riktig eller ikke. I et elektronisk system kommer en vanskelig utenom former for logging/sikkerhetskopiering hvis det skal være mulig å rekonstruere handlinger og hendelser i ettertid med sikte på å avdekke hva som er riktig.

[43] En stemme i Oslo veier for eksempel mindre enn en stemme i Finnmark. I valgordningen som ble tatt i bruk første gang ved stortingsvalget i 2005 er det bygget inn en "arealfaktor"; antall mandater i et fylke bestemmes ut fra en veid sum av folketall og areal (hver innbygger gir 1 poeng og hver kvadratkilometer areal gir 1,8 poeng). Dette bryter med prinsippet om lik stemmerett all den stund folk bor i fylker med forskjellig størrelse. Merk også at fordelingen skjer ut fra antall innbyggere, og ikke antall velgere.

Bruk av IKT ved valg trekker uvilkårlig i retning av større grad av profesjonalisering av valgoppgjøret. Det blir vanskelig å gi lekmenn like stor betydning for kontroll og bygging av tillit som i et manuelt system.

5.2.7 Hemmelig valg

Hemmelige valg er et sentralt prinsipp i alle moderne demokratier, noe som reflekteres i at det er vanlig å gi prinsippet grunnlovsmessig status. Vår egen grunnlov er taus på dette punktet, men det ble i 1814 satt inn en beslektet bestemmelse om at velgere som kjøpte stemmer, eller som solgte sin egen stemme, ville tape stemmeretten (Grl. § 53 d). Bestemmelsen ble tatt ut av Grunnloven i 2003.[44]

Hemmelige valg er nært knyttet til det som tidligere er sagt om politisk likhet og lik stemmerett, og det er hemmeligholdelsen *i seg selv* som er det sentrale. Hemmelighold er et avgjørende virkemiddel for å garantere frie og rettferdige valg. Det er i dag svært få som tar til orde for at åpen stemmegivning bør gjennomføres – eller gjeninnføres – ved parlamentsvalg og tilsvarende (men se Sturgis 2005).

Hemmelig valg ble innført i Norge i 1884. Det var bare et lite konservativt mindretall som stemte mot endringen i Stortinget, og da ut fra den argumentasjon at velgerens frihet ble innsnevret når det ikke lenger ble anledning til åpent å tilkjennegi sin stemmegivning. Norge var i denne sammenheng relativt tidlig ute. Hemmelig valg begynte å spre seg i britiske kolonier på 1850-tallet, og ble kjent som ”den australske stemmemåten” (Newman 2003).

Rent teknisk ble hemmelig stemmegivning i Norge sikret gjennom endringer i valgloven som satte forbud mot stemmesedler med underskrift eller andre personlige påtegnelser, og som bestemte at det skulle være avlukker i valglokalene. Videre ble velgerne pålagt å benytte godkjente konvolutter som ble delt ut i lokalet, og velgeren skulle selv legge konvolutten med stemmeseddel i valgurnen. Velgeren skulle dermed usett kunne velge stemmeseddel og sikre seg at denne stemmeseddelen – uten noen form for kjennemerke – ble blandet med de øvrige stemmesedlene.

Hemmelig valg har to komponenter. For det første må velgeren kunne avgi stemme usett, uforstyrret og i fortrolighet; stemmegivningen er personlig og privat, i motsetning til åpen eller offentlig. For det andre skal alle spor slettes når stemmen er avgitt, slik at det ikke vil være mulig å knytte stemmen til person. Stemmene som telles opp er med andre ord anonyme. De to forholdene som er nevnt har som implikasjon at velgeren *ikke kan bevise* overfor andre hvordan han eller hun har stemt. Dette er det essensielle ved hemmelige valg. Det er selvsagt ingen ting i veien for at en velger ytrer seg om hva en har stemt på, men ingen informasjon om egen stemmegivning vil være etterprøvbar og fullt ut troverdig under et hemmelig valg. Vi merker oss også at det er *myndighetenes ansvar* gjennom betryggende prosedyrer og rutiner å legge til rette for hemmelighold, dette er ikke noe som i utgangspunktet overlates til velgeren selv.

Det er to grunner til at hemmelig valg fremstår som et viktig demokratisk anliggende. For det første hindrer hemmelighold *utilbørlig påvirkning* av velgeren under stemmegivningen. Det

[44] Bestemmelsen ble vurdert som lite aktuell. Følgende ble ellers angitt som grunn til opphevelsen: ”Bestemmelsen innebærer at valgstyret har rett og plikt til å utelukke en som tas i alvorlige valgmisligheter fra valget uten å avvente utfallet av ens straffesak.” Se Innst. S. nr. 209 (2002-03) fra Kontroll- og konstitusjonskomiteen (s. 1).

betyr at en forhindrer at den som påvirkes i realiteten fratas stemmeretten og at den som påvirker får mer enn én stemme. Utilbørlig påvirkning i form av trusler, press og lignende ville med andre ord ha brutt med hensynet til politisk likhet. Mens det i tidligere tider, spesielt før kvinner fikk stemmerett, var frykt for utilbørlig press fra arbeidsgivere, øvrighetspersoner og lokale ledere som betinget hemmelighold, er det i dag uakseptabel påvirkning innenfor rammen av familie og slekt som står i fokus (”family voting”). Hvis alle kan avgi stemme usett og uforstyrret, har et familieoverhode ingen mulighet til å diktere andre familiemedlemmers stemmegivning. Takket være anonymiteten – det at stemmen og velgerens identitet ikke er knyttet sammen – kan ingen i familien kontrollere andres stemmegivning i etterkant.

Den andre grunnen til hemmelige valg er at kjøp og salg av stemmer forhindres. All den stund en velger ikke kan bevise sin stemmegivning, har det heller ingen garantert verdi å kjøpe en stemme – og et ”marked” utvikler seg ikke. Også kjøp og salg av stemmer ville brutt med hensynet til politisk likhet; noen personer ville fått større innflytelse på valgresultatet enn andre, og da ved hjelp av ressurser som i demokratisk sammenheng er helt illegitime (for eksempel penger).

Til tross for det som er sagt, kan ikke hemmelig valg i praksis forstås som et absolutt og ufravikelig krav. På den ene siden er det slik at det kan bli benyttet prosedyrer ved valgene som går på akkord med prinsippet om hemmelighold. Dette gjelder også norske valg. I dag er det slik at velgeren på valgdagen går i stemmeavlukket, velger en stemmeseddel, bretter stemmeseddelen og går frem til valgfunksjonær og valgurne. Stemmen skjules ikke i konvolutt. Velgeren har med andre ord selv ansvar for å skjule stemmen fra valgavlukket til valgurnen. En ting er at velgeren uforvarende kan komme til å vise stemmeseddelen til andre ved å brette den feil vei. Men i teorien er det også mulig at det står noen i valglokalet – det vil si en ”kjøper” – som kan kontrollere hva den enkelte har stemt. Dette er også høyst relevant i forhold til familiestemmegivning. Et familieoverhode vil under uheldige omstendigheter uten særlige problemer kunne kontrollere hva familiemedlemmer stemmer ved å se på stemmeseddelen som er valgt før den puttes i urnen.

Det at mange land godtar brevstemmegivning, er også et eksempel på at hemmelige valg ikke kan ses som et ufravikelig krav. Ved brevstemmegivning er det jo velgeren selv som har ansvaret for å sikre at stemmen avgis uten utilbørlig påvirkning. Og det bygger på tillit at brevstemmene som kommer inn ikke er solgt og kjøpt, men at det er de aktuelle brevvelgernes egen politiske preferanse som kommer til uttrykk i det innsendte materialet.

I norsk sammenheng er brevstemmegivning i dag bare tillatt for velgere som oppholder seg i utlandet, og som ikke har mulighet til å oppsøke en stemmemottaker (for eksempel en norsk ambassade). Det er kun snakk om et lite antall stemmer ved hvert valg. Som det fremgår av neste avsnitt, har imidlertid brevstemmegivning tradisjoner helt tilbake til 1814 i Norge (Grl. § 60). Grunnen til at denne formen for stemmegivning ble fjernet for vel 75 år siden, var frykten for utilbørlig påvirkning og andre former for misbruk.

Hvordan stiller elektronisk stemmegivning utenfor godkjent valglokale seg til prinsippet om hemmelige valg? Når det gjelder det å avgi stemmen *usett* og uten utilbørlig påvirkning, er dette noe velgeren selv i så fall må ivareta. Situasjonen er nøyaktig den samme som for brevstemmegivning. I den grad brevstemmegivning godtas som forenlig med prinsippet om hemmelig valg, må det samme gjelde Internett-stemmegivning og lignende (i ukontrollerte omgivelser).

Et mulig virkemiddel for å bøte på problemet med fare for utilbørlig påvirkning ved stemmegivning utenfor godkjent valglokale, er kun å godta slik stemmegivning i fase 1, og i tillegg åpne for at velgere som benytter seg av muligheten til å stemme i ukontrollerte omgivelser kan "angre" og stemme på nytt – enten i fase 1 eller fase 2. Av praktiske og administrative grunner (se kapittel 7) kan en slik fremgangsmåte ikke anbefales i forbindelse med brevstemmegivning. De praktiske og administrative hensynene er imidlertid ikke like tungtveiende ved elektronisk stemmegivning. Vi kan konkludere med at en ordning med elektronisk stemmegivning i ukontrollerte omgivelser i fase 1, kombinert med en angremulighet (flergangsstemmegivning) for velgere som benytter seg av muligheten, i rimelig grad sikrer at stemme kan avgis usett og uforstyrret – eller uten utilbørlig påvirkning. Gitt dette opplegget med faseinndeling og flergangsstemmegivning, kan en velger ikke bevise hva hun eller han har stemt.

I forhold til det andre aspektet ved hemmelige valg, nemlig det at alle spor tilbake til velgeren slettes når stemmen er avgitt (anonymitet), reiser elektronisk stemmegivning utenfor godkjent valglokale nye utfordringer. Det er her viktig å huske at det ikke er mulig å operere med noen form for kvittering for stemmegivningen, for eksempel for kontrollformål, uten at det oppstår problemer i forhold til ønsket om hemmelig valg.

Sentrale prinsipper for vurdering av om valg er demokratiske.

"Frie og rettferdige valg"

— *Gode muligheter for å ivareta demokratiske rettigheter, spesielt fravær av tvang*

— *Upartisk og nøytral gjennomføring av valget*

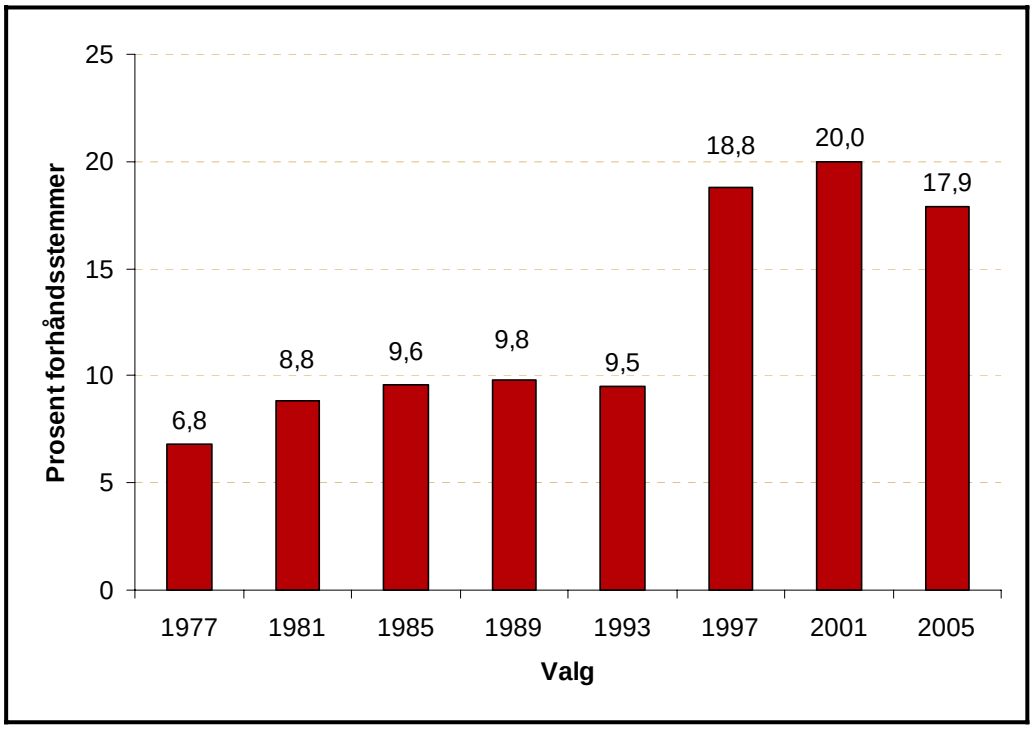
- Direkte valg
  - Velgerne stemmer direkte på kandidater eller lister til den representative forsamlingen (uten mellomledd)
- Periodiske valg
  - Representantene velges for en begrenset periode
- Ulike politiske alternativer
  - Vid adgang til å etablere politiske alternativer
  - Velgerne har reelle valgmuligheter
- Inkluderende valg
  - Alminnelig stemmerett (universalitet)
  - Bred deltakelse
- Likhet
  - Lik stemmerett
- Åpenhet og kontroll
  - Gjennomsiktig, nøytral og kompetent administrasjon
  - Etterprøvbarhet eller sporbarhet
- Hemmelig valg
  - Usett (individuell eller privat stemmegivning)
  - Anonymitet (alle spor slettet når stemmen er avgitt)

5.3 Forhåndsstemmegivning – ”fase 1” og ”fase 2”

De aller fleste av dagens demokratier – opp mot 90 prosent – gjennomfører parlamentsvalg med kun én valgdag. I ytterst få tilfeller foregår valgene over mer enn to dager. Søndag er den ukedagen som benyttes oftest blant landene som konsentrerer valget til én dag, men lørdag og mandag er også ofte brukt. Empiriske analyser tyder på noe høyere valgdeltakelse i de tilfellene valgdagen er hviledag (jf. Franklin 1996).

En grunn til at én valgdag er typisk, er de utfordringene som oppstår når det er behov for å lagre valgmateriell over natten. En annen grunn er de administrative ressursene som kreves for å holde mange stemmesteder åpne over flere dager. Det å holde seg til én valgdag kan sies å balansere hensyn til tilgjengelighet, kostnader og sikkerhet på en rimelig måte.

Noen legger sterk vekt på at valgdagen (eller valgdagene) holdes i hevd som spesielle og litt høytidelige dager. Selve valghandlingen betraktes som en ”borgerplikt”, og den bør – hevdes det – fortrinnsvis foregå i det offentlige rom eller i kontrollerte omgivelser. I dette perspektivet fremstår en ”privatisering” av valghandlingen, ved å tillate stemmegivning hjemmefra, fra arbeidsplasser og lignende, som uheldig. Det vil føye seg inn i rekken av elementer som svekker eller undergraver en levende politisk kultur og en ”borgerånd”.



Figur 5.3: Andel forhåndsstemmer ved stortingsvalg 1977-2005.
Kilde: SSB (www.ssb.no/00/01/10/stortingsvalg).

Samtidig er det klart at valgdagen er under press på en annen måte, og at den lenge har vært det. De aller fleste demokratier har åpnet opp for forhåndsstemmegivning (fase 1) i en kortere eller lengre periode før selve valgtinget (fase 2). Det er også slik at en betydelig andel av stemmene hos oss og i mange andre land avgis på forhånd. Figur 5.3 viser andelen forhåndsstemmer ved stortingsvalgene i perioden 1977-2005. Vi har neppe noen grunn til å regne med at mindre enn en femtedel av stemmene i overskuelig fremtid vil bli avgitt som forhåndsstemmer. I realiteten er det i dag ikke mulig å stramme inn adgangen til

forhåndsstemmegivning uten at det får markante følger for valgdeltakelsen. Hensynet til at alle skal kunne delta ved valget (jr. prinsippet om inkluderende valg) tilsier at dagens valg må gjennomføres i to faser – uansett om selve valgdagen søkes holdt i hevd.

Det er svært lang tradisjon for forhåndsstemmegivning i Norge. Allerede i 1814 åpnet Grunnloven for at velgere som ikke kunne være til stede på valgtinget skulle få anledning til å avgi stemme på forhånd (Grl. § 60). Det var imidlertid tale om *brevstemmegivning*, og denne stemmeformen kunne benyttes ved sykdom, utenlandsopphold og annet gyldig forfall. Stemmeformen ble for eksempel etter hvert viktig for sjøfolk og fiskere som var ute på havet under valget. Rent konkret forpliktet velgeren seg til å stemme selv, og skulle uten innblanding fra andre legge stemmeseddelen i en konvolutt som så ble forseglet. Velgerens signatur skulle bevitnes av en pålitelig person over 21 år, og stemmeseddelkonvolutten sendes inn sammen med en redegjørelse for grunnen til forhåndsstemmegivning. Det er også verd å merke seg at det fantes en angremulighet for alle som stemte per brev: De kunne sende inn ny stemmeseddel (den måtte komme inn før valglokalene stengte), eller de kunne komme på valgdagen hvis det viste seg at dette likevel var mulig (brevstemmen ble da tatt ut før opptelling).

Det var et betydelig innslag av forhåndsstemmegivning ved valgene, men stor variasjon fra valg til valg og ulike landsdeler imellom. Ved stortingsvalget i 1912 var det på landsbasis vel 5 prosent av velgerne som stemte på forhånd i første valgomgang, og nærmere en tredjedel av velgerne i Finnmark som gjorde det samme (Saby 1918: 298).

Fra 1930 endret forhåndsstemmegivningen karakter. Frykten for ”misbruk i form av utilbørlig innvirkning på velgerne fra agitatorers side” (Castberg 1947: 406), gjorde at brevstemmen i all hovedsak ble tatt bort. Fra nå av bestemte valgloven at forhåndsstemme bare kunne avgis ved personlig fremmøte hos en godkjent stemmemottaker.

Selve valgtinget eller fase 2 er kort, mens fase 1 i prinsippet kan strekke seg over uker eller måneder. I norsk sammenheng har det hele tiden vært lagt vekt på at velgeren skal kunne kjenne til den politiske situasjonen ved valget, og det taler for at perioden for forhåndsstemmegivning begrenses i tid. De som stemmer på valgtinget vil likevel ha tilgang på mer informasjon enn de som stemmer tidligere, i og med at de går til valgurnen etter at valgkampen er avsluttet, og de ulike politiske alternativene presumptivt er bedre belyst enn tidligere i prosessen.

Hensynet til tilfredsstillende nivå på valgdeltakelsen tilsier at det finnes en adgang til å forhåndsstemme. Demokratisk ansvarlighet forutsetter at velgerne er informert om den politiske situasjon før stemme avgis, og at forhåndsstemmegivningen ikke strekker seg over for lang tid. Et realistisk system med elektronisk stemmegivning må, som vi senere skal se (kapittel 8), basere seg på at valg fortsatt skal gjennomføres i to faser. Elektronisk stemmegivning i ukontrollerte omgivelser er en aktuell mulighet bare i fase 1.

5.4 Feilkilder ved dagens manuelle valgoppgjør

Feil kan oppstå ved alle valg, enten det gjennomføres manuelt eller elektronisk. Ofte fokuseres det på den – til dels betydelige – risiko en kan løpe ved elektroniske valg, men manuelle prosedyrer er heller ikke uten risikofaktorer. Det er likevel stor forskjell når det gjelder alvorlighetsgraden i de feilene som kan oppstå innenfor dagens velprøvde, papirbaserte valgoppgjør, og et system som inkluderer elektronisk stemmegivning utenfor

godkjent valglokale (jf. vedlegg B). Det er svært sjelden at uregelmessigheter ved valgoppgjør i etablerte demokratier får særlige konsekvenser, for eksempel i form av omvalg. Det er også svært sjelden det fremsettes troverdige anklager om manipulasjon, og det er ikke lett å finne eksempler på at juks av et visst omfang avsløres.

Hensikten med dette avsnittet er å synliggjøre en del av de feilkilder som finnes ved bruk av dagens norske ordning. Vi vil først gi noen eksempler på feil som kan oppstå på ulike trinn av valgprosessen. Deretter redegjør vi kort for formelle klager som har blitt behandlet av Stortingets fullmaktskomité i perioden 1965 til 2005.

5.4.1 Eksempler på feilkilder

Den nye valgloven av 2002 innebar en del praktiske ordninger som skulle bidra til å eliminere tidligere feilkilder, blant annet stemmeseddelkonvolutten og den skjønnsmessige vurderingen ved forkastelse av stemmesedler. Fra og med kommune- og fylkestingsvalget i 2003 opphørte derfor ordningen med stemmeseddelkonvolutt ved ordinært valgting. De nye stemmesedlene skal ikke lenger legges i en konvolutt, men brettes. Erfaringene fra valget i 2003 viste at mange velgere brettet stemmeseddelen feil, så det ble synlig hvilket parti velgeren stemte på. Ved stortingsvalget i 2005 ble denne feilkilden vesentlig redusert. Det antas at feilen vil bli borte etter hvert som velgerne blir vant til ordningen.

Enkelte velgere har også brukt blanke stemmesedler som en slags omslagskonvolutt ved avlevering av stemme. Konsekvensen av dette er at det er den blanke stemmeseddelen som godkjennes, mens velgerens stemme blir forkastet, siden det er den blanke stemmeseddelen som blir stemplet av valgfunksjonæren.

Alle rettelser på stemmeseddelen skal tolkes og godkjennes. Arbeidet utføres i praksis av en valgfunksjonær og vil til en viss grad være utsatt for skjønn og dermed utsatt for feiltolkninger. Den nye valgloven har likevel ført til at færre stemmesedler har blitt forkastet på grunn av formelle feil.

Erfaringer fra valggjennomføringen i 2003 og 2005 viste at flere stemmesedler ble lagt i valgurnen uten stempel. En av feilkildene kan være at velgeren har gått fra valgavlukket direkte bort til valgurnen, uten å manntallsføre og stemple stemmeseddelen først. En annen mulighet er at velgeren har lagt flere stemmesedler i urnen. Det er da kun én av stemmesedlene som får stempel. Det er viktig at valglokalet er hensiktsmessig organisert, og at valgfunksjonærene er tilstrekkelig oppmerksomme.

Sedlene i avlukkene kan byttes om, eller rettes på. En uoppmerksom velger kan ta feil liste og stemme på feil parti eller gi personstemmer til andre kandidater enn tiltenkt.

Når avkryssing skjer manuelt, er det fort gjort å krysse av feil velger i manntallet. Dette oppstår gjerne når det er mange velgere i valglokalet og valgfunksjonæren er stresset.

Når det gjelder klargjøring av stemmesedler for opptelling, er det behov for mottak, registrering, bytting og prøving av stemmesedlene. Mulighetene for å gjøre manuelle feil her er store dersom ikke prosedyrene følges nøyaktig. Stemmesedler kan byttes om eller rotes bort. I forbindelse med opptelling i valglokalet vil det kunne oppstå feil i sorteringen av stemmesedlene. Ved endelig opptelling har man funnet forholdsvis grove sorteringsfeil. Faren for juks fra valgfunksjonærer er størst under klargjøring før telling. Her er det mulighet til å foreta bytting av sedler. Dette krever at man har tilgang til sedler, og for

valgtingsstemmenes del, tilgang til stempel. Men klargjøring skjer i åpne miljøer og med stor risiko for å bli oppdaget.

I forbindelse med forhåndsstemmegivning, institusjonsstemmegivning, hjemmestemmegivning og fremmede stemmer skal stemmeseddelen legges inn i en stemmeseddelkonvolutt som sammen med valgkortet legges i en omslagkonvolutt. Dette skal gjøres umiddelbart etter at velgeren har levert sin stemme. Det kan oppstå feil ved at valgfunksjonæren glemmer å legge ved valgkortet eller ikke benytter omslagkonvolutt. Disse stemmene vil bli forkastet.

Stemmesedler oppbevares fra forhåndstemmegivningen begynner og fram til valgdagen. Stemmesedlene er ofte oppbevart i låste rom eller skap og vil dermed være utsatt hvis det oppstår brann, vannlekkasje, eller juks fra en valgfunksjonær etc. Dette gjelder også institusjonsstemmene, hjemmestemmene og utenlandsstemmene. Postverket eller en intern budtjeneste står ofte for frakt av stemmesedler fra f. eks forhåndsstemmestedene og inn til kommunen sentralt. Stemmesedlene kan også her bli påvirket av ytre omstendigheter eller feil ved budtjeneste eller postverket. I og med at det er forhåndsstemmegivning helt frem til fredag ettermiddag, 2 dager før valgdagen, vil posten ikke ha mulighet til å få frem alle stemmer. Feilsending av forhåndsstemmer vil også forekomme, og kan ikke åpnes i den kommune de er sendt til. Treghet i Posten medfører også at stemmesedler ankommer valgmyndighetene for sent, og dermed blir forkastet. Dette skjedde senest ved stortingsvalget i 2005.

Stemmesedler skal transporteres både fra forhåndsstemmesteder, fra institusjoner, fra hjemsted til enkeltvelgere og fra valglokaler. Transport skal alltid besørges av to personer. Blir disse to enige, kan det foretas bytte av sedler. En utro tjener her vil ha tilgang til sedler, konvolutter, stempel, omslagkonvolutter og forseglingsutstyr.

5.4.2 Formelle klager på valgoppgjøret

Innstillingene fra fullmaktskomiteen inneholder klager fra velgerne og generelle merknader fra fullmaktskomiteen. Det er registrert totalt 90 klager fra velgerne i perioden 1965 til 2005. Disse er stort sett ikke veldig alvorlige i forhold til demokratiske prinsipper. En del av klagene har ikke noe formelt klagegrunnlag. For eksempel er det registrert mange klager på at det ikke lå ute blanke stemmesedler, selv om valgstyrene ikke er forpliktet til dette.

Av klagene fra velgerne dreier 44 seg om forhold før valgdagen, blant disse er 18 klager vedrørende listeforslag og 14 vedrørende forhåndsstemmegivningen. Klagene vedrørende listeforslag dreier seg stort sett om fraksjonsdannelser innad i partiene om hvem som har rett til partinavnet.

Det er klagene som dreier seg om forholdene under stemmegivningen som har mest relevans i vår sammenheng. Det er registrert 42 klager på dette i perioden 1965-2005. Klagene under valget går hovedsaklig på manglende utlegging av stemmesedler og forhold i valglokalet da velgeren skulle stemme. Fire av klagene går på forhold etter valget, antallet er naturligvis lavt siden få av velgerne tar del i opptelling og etterkontroll. Forholdene etter valgene behandles nærmere av komiteen.

Innstillingene fra Stortingets fullmaktskomité inneholder, foruten de formelle klagene og behandlingen av disse, noen generelle merknader. Disse er ganske like fra år til år, og dreier seg hovedsaklig om følgende fem forhold.

- *Valglokalene* har hatt åpent i for kort tid, eller åpningstidene har vært for dårlig kunngjort.
- *Valgfunksjonærer* har fått for dårlig opplæring og de har gjort formelle feil.
- *Stemmesedlene* har ofte vært klebet sammen, papirkvaliteten må forbedres.
- *Møtebøker* har blitt ført mangelfullt og inkonsekvent fra valgkrets til valgkrets.
- Det har vært registrert to tilfeller hvor stemmesedler mangler og har kommet bort i frakt, eller at *transporten* ikke har foregått i tråd med bestemmelsene.

Den mest alvorlige konsekvensen av problemer ved gjennomføring av valg, er at det må holdes omvalg. I den perioden vi har sett på her ble det holdt omvalg etter ett valg: i Buskerud og Troms fylke i 1981. Dette skjedde fordi avviket i antallet feilkrysninger i manntallet var større enn marginen for tildeling av siste mandat (7 stemmer i Troms, og 28 i Buskerud).

5.5 Konklusjon og anbefaling

Vi har i dette kapitlet gått gjennom noen sentrale prinsipper for demokratiske valg, og pekt på hvilke utfordringer bruken av ny teknologi kan representere i denne sammenheng. Prinsippet om hemmelige valg er særlig vanskelig å ivareta i forbindelse med stemmegivning – elektronisk eller per brev – utenfor godkjent valglokale. Det å tillate elektronisk stemmegivning i ukontrollerte omgivelser på valgdagen (fase 2), kommer *klart i strid med ønsket om å gi alle velgere mulighet for hemmelig stemmegivning*. Arbeidsgruppen legger derfor følgende premisser til grunn ved søkningen etter tilfredsstillende tekniske løsninger:

- Valgene i Norge skal fortsatt gjennomføres i to faser, med en periode for forhåndsstemmegivning (fase 1) og et valgting (fase 2). Elektronisk stemmegivning i ukontrollerte omgivelser er kun en aktuell mulighet i perioden med forhåndsstemmegivning (fase 1).

Velgere kan selvsagt utsettes for utilbørlig påvirkning også om stemmegivningen foregår i ukontrollerte omgivelser i fase 1, jf. for eksempel problemet med ”family voting”. Likedan utgjør kjøp og salg av stemmer et mulig faremoment. For å møte problemer av denne typen, legges det opp til et system med en *angremulighet* for velgere som stemmer elektronisk i fase 1, samtidig som tradisjonelle valglokaler opprettholdes, dvs. steder hvor velgere garantert kan avgi en hemmelig stemme selv om de har stemt elektronisk én eller flere ganger tidligere. Tilfredsstillende tekniske løsninger på dette området forutsetter med andre ord:

- Valgtinget bør i overskuelig fremtid gjennomføres på tradisjonell måte med papirstemmesedler. I fase 2 kan det som i dag stemmes bare én gang. Velgere som har stemt *elektronisk* i fase 1, kan avgi (ny) stemme i et valglokale – enten i fase 1 eller fase 2 – og denne stemmen er i så fall tellende.

- Velgere som stemmer *elektronisk* (og bare disse velgerne) kan stemme flere ganger i perioden med forhåndsstemmegivning, og det er den siste stemmen som teller.

Gitt det opplegget som skisseres ovenfor, er det grunn til å tro at alle velgere har god mulighet til å avgi stemme usett og upåvirket – selv om det tillates å stemme (elektronisk) i ukontrollerte omgivelser. Likedan sikrer en seg mot kjøp og salg av stemmer, fordi en potensiell kjøper aldri kan være sikker på at en kjøpt, elektronisk stemme faktisk blir tellende.

Vi anbefaler at det – gitt sikre tekniske løsninger – kun er elektronisk stemmegivning som skal kunne foregå utenfor valglokalet i fase 1. Det åpnes ikke for ytterligere utvidelse av ordningen med brevstemmegivning, selv om denne formen for stemmegivning prinsipielt sett kommer i samme kategori som elektronisk stemmegivning i ukontrollerte omgivelser. Grunnen er at det i et elektronisk system er svært enkelt å håndtere angremuligheter. I et papirbasert (brev), manuelt system vil det være store administrative kostnader forbundet med dette; i det hele tatt er tilbaketrekking av papirstemmer en meget omstendelig prosess. Dette innebærer imidlertid at en må godta en ulikhet mellom de som stemmer elektronisk i ukontrollerte omgivelser i fase 1 og de som stemmer kontrollert i fase 1 eller 2. Angremuligheten er forbeholdt de førstnevnte, og grunnen er ønsket om å hindre utilbørlig påvirkning og kjøp og salg av stemmer (som jo ikke er noe vesentlig problem i kontrollerte omgivelser).

6 Juridiske hensyn

6.1 Innledning

Elektronisk stemmegivning reiser en rekke viktige og fundamentale juridiske spørsmål. Det mest omdiskuterte er som vi har vært inne på spørsmålet om det å avgi stemme elektronisk i ukontrollerte omgivelser i det hele tatt er forenlig med kravet til hemmelig valg. Hvordan skal vi sikre, slik valglovens formålsbestemmelse krever, at velgerne får avgitt stemme hemmelig og uten utilbørlig påvirkning når stemme avgis hjemmefra på egen datamaskin?

Utgangspunktet for diskusjonen i dette kapitelet er hovedpunktet i mandatet om at gruppen skal *"vurdere og forslå hvilke regler og krav som bør stilles til systemer for elektronisk stemmegivning"*. I tillegg er følgende elementer i mandatet særlig sentrale for de juridiske vurderingene:

- problemstillingen "utilbørlig påvirkning" i forbindelse med stemmegivning utenfor valglokalet må vurderes særskilt, jf. også diskusjonen poststemmer (pkt. 7),
- vurdere ev. bruk av et landsdekkende elektronisk manntall, betydningen i forhold til et system der stemmer avgis elektronisk (pkt. 11),
- vurdere betydningen av en overgang fra lekmannskontroll til profesjonalisering; blant annet betydningen for valgsystemet mht kontroll, administrasjon av valg, kompetanse (pkt. 14),
- vurdere ansvarsforholdene ved elektroniske valg, lokalt og nasjonalt (pkt. 15).

I dette kapitlet skal vi gjøre rede for den norske valglovgivningen. Deretter vurderes annen nasjonal lovgivning vi mener har betydning ved innføring av elektronisk stemmegivning. Deretter presenteres de viktigste momentene i internasjonal rett med vekt på den Europeiske Menneskerettighetskonvensjonen (EMK) og Europarådets anbefaling for elektronisk stemmegivning. Til dette hører også de vurderingene av EMKs artikkel 3 som er gjort av Venezia-kommisjonen i lys av elektroniske valg.

Hovedkonklusjonen i kapitlet er at innføring av elektronisk stemmegivning på sikt vil medføre at det må gjøres vesentlige endringer i nasjonal valglovgivning. Arbeidsgruppen antar imidlertid at en slik omfattende lovendring ikke er nødvendig eller ønskelig før det eventuelt innføres mulighet til å avgi elektroniske stemmer på landsbasis eller i stor skala. Innenfor rammene av et forsøksregime vil elektronisk stemmegivning kunne gjennomføres med hjemmel i egne regler om forsøk.

Vår valgordning er utviklet og utformet for å sikre at prinsippene for demokratiske valg imøtekommes. Det er essensielt at disse prinsippene ikke undergraves dersom det introduseres nye måter å avgi stemme på. Et elektronisk system for stemmegivning må derfor være utformet og fungere på en slik måte at det sikrer pålitelighet og sikkerhet i stemmegivningsprosessen. Retten til å stemme hemmelig ved valg er et av de viktigste prinsipper for frie og demokratiske valg. Men som vi skal se, må det i ulike relasjoner innfortolkes visse modifikasjoner, jf. avsnitt 6.5.3.

6.2 Nasjonal valglovgivning

6.2.1 Generelt

Gjennomføring av valg reguleres av lov 28. juni 2002 nr. 57 om valg til Stortinget, fylkesting og kommunestyrer (valgloven). Men hjemmel i loven er det i tillegg gitt utfyllende bestemmelser i forskrift av 2. januar 2003 nr. 0005 (valgforskriften). Grunnloven har dessuten flere bestemmelser som regulerer valg til Stortinget. Valg til Sametinget reguleres av lov av 12. juni nr. 56 om Sametinget og andre samiske rettsforhold (sameloven), samt forskrift av 10. desember 2004 nr. 1641 (samevalgforskriften) gitt med hjemmel i denne lov.

Elektronisk stemmegivning *er ikke tillatt* etter dagens valglovgivning. Vår valglovgivning er basert på at papirstemmesedler skal benyttes ved stemmegivningen; både ved bestemmelser om trykking, gjennomføring av forhåndsstemmegivning og valgtingsstemmegivning, prøving av stemmesedler og opptelling.

Valglovgivningen garanterer på den ene siden for våre viktigste demokratiske rettigheter og fastsetter hovedprinsippene for valgordningen. På den andre siden gir valgloven også bestemmelser av teknisk/administrativ karakter. Det er for eksempel detaljerte regler om den praktiske fremgangsmåten ved valget og om selve valghandlingen, om hvilke oppgaver som ivaretas av ulike offentlige myndigheter og så videre. Selv om denne siden av regelverket også er ment å bidra til oppfyllelsen av de grunnleggende demokratiske prinsippene, er det mange av bestemmelsene som anviser fremgangsmåter og prosedyrer som gjerne kan erstattes av andre.

6.2.2 Valglovens formål

De grunnleggende prinsipper vår valgordning bygger på, kommer direkte til uttrykk i valglovens formålsbestemmelse. Valgloven § 1-1 fastsetter at formålet med loven er å *"legge forholdene til rette slik at borgerne ved frie, direkte og hemmelige valg skal kunne velge sine representanter"* til folkevalgte organ.

I lovens forarbeid pekes det på at *"Vårt demokratiske system bygger på folkestyre, eller det vi kaller et representativt demokrati."* Representanter som velges til Stortinget, fylkestingene og kommunestyrene skal velges av folket direkte. Det innebærer at landets innbyggere har politisk innflytelse gjennom de politikerne de stemmer på ved valgene. Gjennom retten til frie valg sikres at forholdene legges til rette slik at velgeren uhindret får avgi stemme. Videre at velgeren får avgi stemme til det partiet eller den gruppen vedkommende ønsker, uten innblanding eller påvirkning fra offentlige myndigheter eller andre. Prinsippet skal også sikre alle retten til å danne partier, samt å stille liste ved valg. Regelverket skal også sikre at prinsippet om hemmelig valg for den enkelte velger ivaretas. Velgeren skal kunne være sikker på at det ikke offentliggjøres eller på annen måte avsløres hva velgeren har stemt, med mindre vedkommende selv ønsker en slik offentliggjøring.

Formålsbestemmelsen har betydning i flere sammenhenger. Den sier noe om hvilke prinsipper lovens øvrige bestemmelser bygger på. Prinsippene gir velgerne rettigheter. Men det ligger også en forpliktelse i dem ved at valgmyndighetene må legge forholdene til rette for at velgeren kan utøve sine rettigheter. I tillegg vil den ha relevans ved avgjørelser i tolkningsspørsmål. Det innebærer for eksempel at der en bestemmelse gir rom for ulike

fortolkninger, skal den løsningen som ligger nærmest til å realisere lovens formål, fortrinnsvis benyttes.

Prinsippene for valg utfordres dersom det innføres muligheter til å avgi stemme elektronisk. Dette temaet behandles nærmere i kapittel 5 og avsnitt 6.6.

6.2.3 Valgmyndighetene - ansvarsfordeling og kontroll

Kommunal- og regionaldepartementet er overordnet nasjonal myndighet for gjennomføring av valg. Den praktiske tilretteleggingen og gjennomføringen er lagt til den enkelte kommune, og utføres av valgstyret. I henhold til valgloven § 4-1 skal det i hver kommune være et valgstyre som velges av kommunestyret selv.

Lokale valgmyndigheter er ansvarlig for kontroll og godkjenning av listeforslag, trykking av stemmesedler, tilrettelegging av valglokaler og gjennomføring av stemmegivningen. Valgstyret er ansvarlig for mottak av all innenriks stemmegivning. I hvert valglokale i kommunen skal et eget stemmestyre lede gjennomføringen av valget på valgdagen, jf. valgloven § 4-2. Valgstyret oppnevner stemmestyrer som er ansvarlig for mottak av stemmer på valgdagen og stemmemottakere som er ansvarlig for mottak av forhåndsstemmer. Utenriks og på Svalbard og Jan Mayen mottas stemmer av lovoppnevnte stemmemottakere, samt av stemmemottakere oppnevnt av statlige myndigheter. Etter endt stemmegivning på valgdagen skal alle stemmer kontrolleres og telles av stemmestyret/valgstyret, i tillegg til at det foretas valgoppgjør. Kommunestyret foretar formell godkjenning av kommunestyrevalget.

I henhold til valgloven § 4-3 skal det i hver fylkeskommune være et fylkesvalgstyre som velges av fylkestinget selv. Fylkeskommunene har også oppgaver knyttet til tilrettelegging ved fylkestingsvalg og stortingsvalg, som kontroll, godkjenning og trykking av stemmesedler. I tillegg har fylkeskommunen er viktig kontrollfunksjon i forhold til valgoppgjøret ved nevnte valg. Fylkestinget foretar formell godkjenning av fylkestingsvalget. Ved stortingsvalg er riksvalgstyret ansvarlig for å ta stilling til klager, samt å foreta kåring av utjevningsmandatene. Stortinget foretar formell godkjenning av stortingsvalget.

Etter arbeigsgruppens vurdering vil det mest sannsynlig måtte gjøres endringer i ansvars- og myndighetsfordelingen ved valg dersom det innføres elektronisk stemmegivning på landsbasis eller i stor skala. Vi viser blant annet til at det skjer en delvis overgang fra dagens lekmannskontroll til profesjonalisering ved elektronisk stemmegivning. Det må etableres et uavhengig regime for sertifisering av system som brukes ved stemmegivning, jf. kapittel 9. Dette vil måtte få betydning for ansvarsfordelingen. Det er mulig dette på sikt også vil måtte få betydning for godkjenningsansvaret for valgresultatet som sådan.

Arbeidsgruppen legger imidlertid til grunn at dagens ansvarsfordeling stort sett bør ligge fast dersom det igangsettes forsøk. Store endringer på kort sikt anses som lite hensiktsmessige fordi erfaringer fra forsøksvirksomhet på dette området vil utgjøre viktige bidrag med hensyn til å vurdere om og hvilke endringer som bør foretas når det gjelder ansvarsfordelingen.

6.2.4 Om manntallet

Hvem som er stemmeberettiget ved valg fremgår av valgloven §§ 2-1 og 2-2. For å kunne utøve stemmeretten krever loven at velgeren er innført i manntallet. En manntallsoversikt har flere formål. Den skal sikre at det kun er de med stemmerett som får avgitt stemme. Manntallet gir dessuten oversikt over hvilken valgkrets den stemmeberettigede tilhører og dermed hvor stemme skal avgis. Videre skal manntallet sikre at hver stemmeberettiget kun får

avgi én stemme hver. Alle stemmeberettigede skal føres inn i manntallet i den kommunen de var folkeregistrert som bosatt per 31. mai i valgåret.

Manntallet og folkeregisteret benyttes også til kontroll av valgbarhet for kandidatene som stiller til valg.

Valgstyret i den enkelte kommune er ansvarlig for å utarbeide manntall det året det skal avholdes valg, jf. valgloven § 2-3. Manntallet føres på bakgrunn av opplysninger fra folkeregisteret. Valgloven fastsetter derfor at Sentralkontoret for folkeregistrering på en hensiktsmessig måte skal stille til disposisjon for valgmyndighetene opplysninger om hvem som skal manntallsføres i den enkelte kommune, jf. § 2-5. I praksis foregår dette ved at folkeregistermyndigheten inngår avtale med et utenforstående datafirma om distribusjon av folkeregisteropplysninger generelt, herunder også distribusjon til bruk ved utarbeiding av manntall ved valg. Dette datafirmaet skal på bakgrunn av avtalen distribuere både manntall pr. 31.5 og oppdateringer etter 31.5 til kommunene i det året hvor det er valg. Manntallet kan oppdateres helt frem til valgdagen. Oppdateringer kan imidlertid bare skje i særskilte tilfeller, jf. valgforskriften § 1.

Et elektronisk manntall er ikke en forutsetning dersom det gis mulighet til elektronisk stemmegivning i valglokalet. Stemmegivning i ukontrollerte omgivelser krever imidlertid elektronisk kontroll av velgers stemmerett, og det må gjøres mot et elektronisk manntall, jf. rekommandasjonens punkt 39-41. Et elektronisk manntall må inngå i den tekniske løsningen for valgsystemet. Manntallsregisterets kvalitet, konfidensialitet, tilgjengelighet og integritet må sikres, jf. rekommandasjonen punkt 86.

6.3 Annen nasjonal lovgivning av betydning ved innføring av e- valg

Dersom det tillates at stemmer avgis *elektronisk* vil, i tillegg til den ordinære valglovgivningen, en rekke andre lover komme til anvendelse. Vi skal her gjennomgå den viktigste lovgivningen og vurdere hvilken betydning denne får ved innføring av elektronisk stemmegivning. Arbeidsgruppen ser ikke bort fra at også annen lovgivning kan komme til anvendelse. Dette vil blant annet måtte vurderes ut fra hvilke type forsøk som eventuelt skal igangsettes.

6.3.1 Personvernlovgivning ved bruk av elektroniske systemer

Et system der stemmeberettigede ved politiske valg gis anledning til å avgi elektroniske stemmer vil sette krav til sikring av personopplysninger. Et datasystem for elektronisk stemmegivning i ukontrollerte omgivelser krever at stemmeberettigede registreres i et elektronisk manntall og at velgeren identifiserer seg overfor systemet elektronisk. Et elektronisk manntall kan også brukes når stemme avgis i kontrollerte omgivelser. *At* vedkommende velger har avgitt stemme må fremkomme av manntallet. Det må videre etableres en midlertidig kopling mellom velgeren og vedkommendes stemme dersom velgeren skal ha anledning til å stemme på nytt, jf. kapittel 8.

Krav til slik sikring av personopplysninger er regulert i lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven). Loven er gitt for å beskytte den enkelte mot krenkelse av personvernet når personopplysninger behandles elektronisk, jf. § 1. Den angir rammene for krav som stilles og må suppleres med regler gitt i forskrift 15. desember 2000 nr. 1265 (personopplysningsforskriften).

Loven kommer til anvendelse på behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler. Med *"behandling"* av personopplysninger menes enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf §§ 2 og 3.

Arbeidsgruppen legger til grunn at personopplysningsloven får anvendelse dersom det åpnes for elektronisk stemmegivning. Vi legger videre til grunn at regelverket for behandling av *sensitive* personopplysninger skal følges. I henhold til § 2 nr. 8 er en persons politiske oppfatning å anse som sensitive personopplysninger.

Personopplysninger kan bare behandles dersom de rettslige grunnlagene i §§ 8 og 9 er oppfylt. De rettslige grunnlagene er knyttet til informert samtykke, lovhjemmel eller at behandlingen anses nødvendig. Hjemmel for føring av manntall følger av valglovens kapittel 2. Det foreligger imidlertid ikke hjemmel i lov for føring av et elektronisk manntall, men loven setter heller ikke forbud mot slik behandling. Folkeregistret reguleres av lov 16. januar 1970 nr. 1 om folkeregistrering med forskrift. Manntallet vil være en utskrift av deler av folkeregisteret og består ikke av sensitive opplysninger.

I relasjon til personopplysningsloven er det koplingen mellom velger (manntall) og avgitt stemme som er viktig. En slik kopling må anses som behandling av sensitive opplysninger. Krav til en slik kopling fremgår pr. i dag ikke av valglovgivningen. Det må imidlertid kunne legges til grunn at velgeren som avgir stemme elektronisk samtykker i en slik kopling. Dette forutsetter helt klart at velgeren informeres om koplingen før stemme avgis, jf. § 2 nr. 7. I motsatt fall vil det ikke foreligge samtykke, noe som eventuelt nødvendiggjør en lov- eller forskriftshjemmel.

Det foreligger meldingsplikt til Datatilsynet for behandling av personopplysninger. For behandling av sensitive opplysninger krever konsesjon, med mindre behandlingen har hjemmel i lov, jf. § 33 og § 31. Datatilsynet er tilsynsmyndighet, jf. lovens kapittel VIII.

Personopplysningsloven knytter flere vilkår og krav til *"behandlingsansvarlig"* og *"databehandler"*. Behandlingsansvarlig vil i denne sammenheng være aktuell valgmyndighet, jf. § 2 nr. 4. Databehandler er den som på vegne av behandlingsansvarlig behandler personopplysningene, jf. § 2 nr. 5.

Utforming av sikkerhetsstrategi utgjør et sentralt element. Det er valgmyndighetene (den behandlingsansvarlige) som gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet, jf. § 13[45]. I forkant av at det innføres muligheter til å avgi stemme elektronisk må det etableres rutiner som sikrer oppfyllelse av personopplysningslovens og –forskriftens bestemmelser. Dette inngår naturlig også i et arbeid med å utforme et regelsett og kravspesifikasjonen for systemet for elektronisk stemmegivning. For øvrig må dette også ses i sammenheng med de strenge krav som settes i henhold til bestemmelsene i Europarådets anbefaling.

Personopplysningsloven får anvendelse ved behandling av personopplysninger dersom ikke annet fremgår av spesiallovgivningen, jf. § 5. Det kan være aktuelt med særlovsbestemmelser der det ønskes andre eller mer presise løsninger enn personopplysningsloven gir anvisning på.

[45] Se nærmere om dette i Datatilsynets "Veileder om informasjonssikkerhet for kommuner og fylker" TV-202-2005.

I slike tilfeller får de enkelte bestemmelsene i personopplysningsloven anvendelse i den utstrekning ikke annet følger av den særskilte loven som regulerer behandlingsmåten. Valglovgivningen har i dag som kjent ingen slik regulering. Europarådets anbefaling legger imidlertid sterke føringer med hensyn til kvalitet, integritet, konfidensialitet og tilgjengelighet av elektroniske opplysninger som bør legges til grunn ved eventuell elektronisk stemmegivning. Det bør derfor på sikt vurderes om det på valgområdet bør lages særregler i valglovgivningen dersom elektronisk stemmegivning innføres som en permanent ordning. Vi ser det imidlertid ikke som naturlig at et slikt regelsett utformes før elektronisk stemmegivning eventuelt innføres som en permanent ordning eller i stor skala.

Konklusjon: Arbeidsgruppen legger til grunn at personopplysningsloven kommer til anvendelse dersom det åpnes for elektronisk stemmegivning. Alternativt kan valgmyndighetene gjennom valglovgivningen lage særregler for all elektronisk behandling av personopplysninger ved politiske valg.

6.3.2 eSignaturloven

Når en stemme avgis elektronisk, kreves det at velgeren identifiserer seg og at det skjer en autentisering overfor valgsystemet. Systemet må dessuten sikre at velgeren ikke avgir mer enn én godkjent stemme. Når stemme avgis elektronisk i kontrollerte omgivelser, kreves ikke alltid at velgeren identifiseres elektronisk. Dette stiller seg annerledes når stemme avgis i ukontrollerte omgivelser. Her kreves bekreftelse på *hvem som sender* informasjon (autentisering), sikkerhet *mot innsyn underveis* (konfidensialitet), sikkerhet for at elektronisk overført informasjon *ikke endres underveis* (integritet) og sikkerhet for at velgeren *ikke skal kunne benekte at han sendte den (*uavviselighet*)*. Elektronisk signatur reguleres av Lov om elektronisk signatur (eSignaturloven) av 17. juni 2005 nr. 104. Elektronisk signatur er data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode, jf. § 3 nr. 1. Definisjonen omfatter også en bestemt type esignatur basert på PKI-teknologi. Denne signaturen oppfyller kravene ovenfor.

eSignaturloven skal legge til rette for at markedet tilbyr sikre signaturtjenester og -produkter (eksempel på slike er PKI-løsninger som smartkort, bankID, eID o.l.) ved at det stilles krav til kvalifiserte sertifikater, utstedere av sertifikatene og selve signaturfremstillingssystemet, jf. § 2. eSignaturloven får generell anvendelse på alle elektroniske signaturer som brukes i åpne eller lukkede nett. Utgangspunktet er at bruk av elektronisk signatur skal skape tillit mellom ukjente parter som har behov for å vite at den de kommuniserer med er den vedkommende utgir seg for å være. For å sikre denne tilliten mellom avsender og mottaker utstedes signaturen sammen med et tilhørende elektronisk sertifikat av en tredje part; sertifikatutsteder.

Systemet er avhengig av at partene stoler på denne utstederen. Sertifikatutstederen skal blant annet kontrollere identiteten til den som mottar sertifikatet. En nærmere beskrivelse av den tekniske løsningen for slike PKI-basert signaturer finnes i NOU 2001:10 ”Uten penn og blekk”.

En *kvalifisert* elektronisk signatur er ifølge definisjonen i § 3 nr. 3 en avansert elektronisk signatur (se § 3 nr. 2), basert på et kvalifisert sertifikat (se § 4), og fremstilt av et godkjent sikkert signaturfremstillingssystem (se §§ 8-9). Med dagens teknologi vil en avansert elektronisk signatur tilsvare en PKI-basert signatur. Dette kan endres over tid. PKI-teknologi oppfyller de funksjonene som er definert i § 3 nr. 2. For å være en avansert elektronisk signatur kreves således at

1. signaturen entydig kan koples til undertegner (velger),

2. signaturen kan identifisere undertegner (velger),
3. den er laget med midler som undertegner (velger) har kontroll over, og
4. den er knyttet til andre elektroniske data på en slik måte at det kan oppdages dersom disse er endret etter signering.

Det er helt nødvendig at disse kravene blir stilt for signaturer som skal benyttes ved stemmegivning i ukontrollerte omgivelser. Nærmere krav til innholdet i kvalifiserte sertifikater fremgår av loven § 4.

Krav til utstedere av kvalifiserte sertifikater fremgår av lovens §§ 10-15. Et viktig krav for nødvendig tillit til sertifikater er kontroll med undertegners identitet. I henhold til § 13 er den som utsteder kvalifiserte sertifikater ansvarlig for at identiteten til undertegner og ytterligere relevante opplysninger om vedkommende blir kontrollert gjennom sikre rutiner. Kravet til slik identitetskontroll er ytterligere regulert i forskrift om krav til utsteder av kvalifiserte sertifikater § 7. Her heter det at *"identifisering skal skje ved personlig fremmøte"* hos sertifikatutsteder eller representant for denne, med mindre undertegner allerede er identifisert ved personlig fremmøte gjennom eksisterende kundeforhold. Undertegner kan ikke benytte fullmektig.

Loven gir ingen generell rett til å kommunisere elektronisk, men kommer til anvendelse der lovgivningen åpner for elektronisk kommunikasjon. Det heter i § 6 at dersom det i lov, forskrift eller på annen måte er krav om underskrift for å få en bestemt rettsvirkning og disposisjonen kan gjennomføres elektronisk, *"oppfyller en kvalifisert elektronisk signatur alltid et slikt krav."* Bestemmelsen innbærer at hjemmel for å kreve elektronisk signatur ved autentisering ved valg må fastsettes i lov eller forskrift.

Post- og teletilsynet er i forskrift til loven utpekt som tilsynsmyndighet av utstedere av kvalifiserte sertifikater. Datatilsynet er tilsynsmyndighet for enkelte deler av loven (§ 7).

I henhold til § 5 kan Kongen fastsette nærmere regler om hvilke krav som skal stilles til kvalifiserte elektroniske signaturer som brukes ved kommunikasjon med og i offentlig sektor, se kapittel 6.3.3.

Konklusjon: Dersom det skal innføres mulighet til å avgi stemme i ukontrollerte omgivelser, må kravene til kvalifiserte sertifikater i eSignaturloven oppfylles.

6.3.3 eForvaltningsforskriften

Forvaltningsloven fikk i 2001 en ny § 15a som bestemmer at det kan gis forskrift om elektronisk kommunikasjon med og i forvaltningen, herunder nærmere regler om signering, autentisering, sikring av integritet og konfidensialitet. Gjeldende forskrift er fastsatt 25. juni 2004 nr. 988 og trådte i kraft 1. juli 2004 (eForvaltningsforskriften). Forskriften er også hjemlet i eSignaturloven § 5, se kapittel 6.3.2.

Forskriften gjelder for elektronisk kommunikasjon mellom forvaltningen og publikum og for elektronisk saksbehandling og kommunikasjon i forvaltningen, jf. eForvaltningsforskriften § 1. Formålet er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Dette gjøres gjennom detaljerte regler for hvordan den enkelte skal gå frem.

Det enkelte forvaltningsorgan har stor grad av frihet til selv å velge om, og i tilfelle på hvilken måte, det vil legge til rette for slik elektronisk kommunikasjon. Som anført over vil autentisering ved elektronisk stemmegivning i ukontrollerte omgivelser kreve en PKI-løsning. Det må derfor etableres hjemmel for bruk av elektronisk kommunikasjon i lov eller forskrift som regulerer elektronisk stemmegivning. eForvaltningsforskriften kommer da til anvendelse.

Forskriften stiller ikke i seg selv krav til at det skal brukes kvalifiserte elektroniske signaturer. I henhold til § 4 (1) er hovedregelen at den som henvender seg elektronisk til forvaltningen kan gjøre det "uten bruk av sikkerhetstjenester eller –produkter". Det betyr for eksempel at vanlig e-post kan brukes.

Forvaltningen kan imidlertid, basert på regler i § 4 (2), eventuelt basert på hjemmel i lov eller forskrift, stille krav om bruk av slike sikkerhetstjenester som kvalifisert elektronisk signatur. Med sikkerhetstjenester og –produkter menes blant annet løsninger for å oppnå bekreftelse på en persons identitet (PKI som autentiseringsmetode). Definisjon finnes i § 4 (1) bokstav a. Bruk av sikkerhetsløsninger skal være behovstilpasset og basert på forvaltningsorganets sikkerhetsstrategi. Hvilken sikkerhetsløsning som velges, må altså tilpasses til hva som er aktuelt behov, den må ikke være unødig tyngende eller vanskelig å håndtere. Krav til at det skal benyttes en sikkerhetsløsning ved autentisering av velgeren ved elektronisk stemmegivning må altså fremgå av regelverket for slik stemmegivning.

Utforming av en sikkerhetsstrategi er også her gjort til et sentralt element, jf. § 13. Denne vil være grunnlaget for blant annet krav til bruk av sikkerhetstjenester i henhold til § 4. Sikkerhetsstrategien skal utarbeides i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet, jf. § 13 (2). Bestemmelsen angir flere forhold sikkerhetsstrategien som må vurderes, og eventuelt konkretiseres i form av ulike prosedyrer, jf. tredje ledd.

Myndighetene må videre gi anvisning på hvilken løsning som skal benyttes (hvilke produkter) og hvordan dette skal skje, jf. § 4 fjerde ledd. Særskilte krav i denne sammenheng stilles når det skal brukes en løsning der taushetsbelagt informasjon samles, jf. § 5. Et konkret eksempel er Datatilsynets anbefaling om kryptering for overføring av sensitive personopplysninger. Det må legges til rette for bruk av sikre kanaler.

Utover dette vil eForvaltningsforskriften stille en rekke krav når det først er etablert hjemmel for at den kommer til anvendelse. Arbeidsgruppen omtaler ikke disse nærmere her. Vi viser til at det er utarbeidet en veileder til forskriften[46].

Konklusjon: eForvaltningsforskriften bør legges til grunn dersom det åpnes for bruk av en PKI-løsning som autentiseringsmetode.

6.3.4 Straffelovgivningen

Valglovgivningen har ikke egne straffebestemmelser, men eventuelle brudd på enkelte av valglovens bestemmelser blir fanget opp av straffeloven. Bestemmelsene vil også komme til anvendelser dersom det innføres muligheter til elektronisk stemmegivning. Straffelovens kapittel 10 regulerer forbrytelser ved utøvelse av statsborgerlige rettigheter.

[46] Veileder til forskrift om elektronisk kommunikasjon med og i forvaltningen: http://odin.dep.no/fad/norsk/dok/andre_dok/veiledninger/002001-120010/dok-bn.html

I henhold til straffeloven § 105 er det straffbart ved trusler, kjøp, eller løfte om fordel, løgnaktig forespeiling eller ved andre utilbørlige midler å forsøke å få innflytelse over noens stemmegivning. Det samme gjelder forsøk på å avholde noen fra å stemme. Bestemmelsen rammer den som utsetter noen for utilbørlig påvirkning. Forsøk er nok for fullbyrdet forbrytelse, det kreves ikke at velgeren faktisk *har* stemt i mot egen overbevisning på grunn av utilbørlig påvirkning. Som følge av regelen om hemmelige valg vil det sjelden være mulig å skaffe til veie bevis for hvordan velgeren faktisk har stemt. Dette er bakgrunn for kravet om fremskutt fullbyrding, slik at allerede det å forsøke å påvirke en annens stemmegivning på utilbørlig måte rammes.

Etter § 106 er det straff for den som, på grunnlag av avtale, en fordel eller et tilsagn, stemmer på en bestemt måte eller avholder seg fra å stemme. Bestemmelsen omfatter salg av stemmer, og rammer den som mottar en fordel av å stemme på en bestemt måte. Den konkrete stemmegivningen må skyldes den fordelen som mottas eller som er lovet. Bestemmelsen bruker begrepet ”afgiver Tilsagn”. Dette viser at det etter dette alternativet ikke er noe vilkår at det har kommet i stand en avtale, men at det er tilstrekkelig at den stemmeberettigede har tatt initiativet til å ”selge” sin stemme. Initiativ til taktisk stemmegivning ved at man forsøker å få flere med på å stemme på et parti som det anses opportunt å stemme på, er ikke rettsstridig.

§ 107 setter straff for den som ved usannferdig atferd urettmessig skaffer seg eller andre stemmerett eller som tilsniker seg eller andre adgang til deltagelse i valg. Dette kan være manipulasjon med folkeregisteropplysninger slik at man oppnår en stemmerett man ikke har. Det omfattes også om man ved å gi uriktige opplysninger oppnår å stemme, eller om man avgir stemme selv om man vet at man uriktig er innført i manntallet.

- Det er straffbart å forvanske eller forspille valgresultater
- Det er straffbart å tvinge noen til å stemme på et parti mot sin vilje
- Det er straffbart å medvirke til at noens stemmegivning ikke blir tatt med i opptellingen
- Det er straffbart å selge stemmeretten sin
- Det er straffbart å kjøpe noens stemmerett

Videre er det straff for den som rettsstridig får noen til å stemme annerledes enn det vedkommende ønsket, eller avgir en ugyldig stemme eller ”afholdes” fra å stemme, jf. også § 105. Dette kan for eksempel skje ved at vedkommende blir villedet om hvilken stemmeseddel som faktisk avgis. Det samme gjelder uriktig instruksjon om hvordan stemmeseddelen kan endres og tilfeller hvor velgeren forledes til å avgi stemme på en slik måte at stemmeseddelen blir forkastet. «Afholdes» fra å stemme omfatter tilfeller hvor velgeren ved fysiske midler hindres i å komme til stemmelokalet. Skjer det ved psykiske midler mv., reguleres forholdet av § 105. En annen handling som rammes er at det forsettlig gis uriktige opplysninger om stemmetiden slik at velgeren kommer for sent.

I henhold til § 108 er det straff for dem som rettsstridig forvansker eller forspiller valgresultater, eller medvirker til at noens stemmegivning ikke blir tatt med i opptellingen. Forvanskning kan skje ved å erstatte det riktige valgresultatet med for eksempel falske møteprotokoller, eller alternativt ved forsettlig å telle feil eller notere uriktige tall. Bestemmelsen rammer også den som stemmer mer enn én gang ved samme valg, eller legger mer enn én stemme i valgurnen.

Straffelovens kapittel 11 om forbrytelser i offentlig tjeneste og kapittel 33 om forseelser i offentlig tjeneste inneholder også bestemmelser som kan komme til anvendelse. Disse omtales imidlertid ikke nærmere her.

De nevnte straffebestemmelser gjelder som sagt også dersom det innføres rett til å stemme elektronisk. Bruk av datasystemer ved stemmegivningen åpner imidlertid for en helt annen type kriminalitet. Flere straffebestemmelser regulerer datakriminalitet. Arbeidsgruppen finner det ikke formålstjenlig å omtale alle disse i denne rapporten. Vi vil kun nevne at den viktigste og mest sentrale bestemmelse i denne sammenheng er forbudet mot datainnbrudd i straffeloven § 145 annet ledd. Bestemmelsen setter straff for den som "ved å bryte en beskyttelse eller på lignende måte uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller tekniske hjelpemidler." Uttrykket ”data” omfatter all slags maskinlesbar informasjon, for eksempel om personlige, tekniske eller økonomiske forhold.

Både personopplysningsloven, eForvaltningsforskriften og eSignaturloven setter krav til informasjonssikkerhet. Det å la være å beskytte seg mot sikkerhetstruende hendelser er til en viss grad straffbart, jf. personopplysningsloven § 48 og eSignaturloven § 21.

Arbeidsgruppen vil for øvrig vise til at det pågår et arbeid med å vurdere gjeldende straffelovs spesielle del. Vi mener det i denne sammenheng vil være naturlig at også straffebud som berører straffbare handlinger knyttet til valg, gjennomgås. Til dette hører også en vurdering av om eventuell innføring av mulighet til å stemme elektronisk krever nye straffebud.

6.4 Internasjonale forpliktelser

Norsk lov forutsettes å være i samsvar med internasjonal rett. Prinsipper for demokratiske valg gjenspeiles i en rekke internasjonale forpliktelser, som den europeiske menneskerettighetskonvensjonen og Kodeks for god valgpraksis. Begge er utviklet gjennom samarbeidet i Europarådet[47]. Det er i første rekke forpliktelser gjennom samarbeidet i Europarådet som har betydning på valgområdet. Europarådet ble opprettet i 1949 og har 46 medlemsland, deriblant Norge. Den viktigste oppgaven for Europarådet i dag er å verne om menneskerettigheter, demokrati og rettsstatsprinsippet. Samarbeidet har resultert i et nettverk av internasjonale avtaler og konvensjoner. Venezia-kommisjonen, den europeiske kommisjon for demokrati gjennom lovgivning, er opprettet av Europarådet. Den utgir forfatningsmessige analyser, rapporter og publikasjoner. Kommisjonen avgir også uttalelser om fortolking av grunnleggende nasjonale og internasjonale juridiske virkemidler. En annen viktig institusjon gjennom Europarådssamarbeidet er Den europeiske menneskerettighetsdomstolen. Domsstolen kan avgjøre klager med bindende virkning for medlemsstatene.

6.4.1 Den europeiske menneskerettighetskonvensjonen

Den europeiske menneskerettighetskonvensjonen (EMK) fra1950 art. 3 (tilleggsprotokoll) bestemmer at medlemsstatene *”forplikter seg til å holde frie valg med rimelige mellomrom ved hemmelig avstemning, under forhold som sikrer at folket fritt får uttrykke sin mening ved valget av den lovgivende forsamling.”*

Bestemmelsen skal sikre frie og hemmelige valg. I samsvar med praksis nedfelt av Menneskerettighetsdomstolen refererer bestemmelsen seg ikke bare til forpliktelsen om å

[47] www.coe.int.com

holde frie valg, men garanterer også velgers individuelle rett til å avgi stemme og til å stille til valg. Det samme gjelder universell og lik stemmerett for alle. Det betyr at den enkelte velger har individuelle rettigheter i henhold til bestemmelsen. Valg skal gjennomføres på en slik måte at fri stemmegivning sikres. I tillegg skal den sikre at stemmegivningen foregår under slike omstendigheter at stemmesedlene sikres hemmelighold.

I henhold til rettspraksis er ikke rettighetene i art. 3 absolutte; de er gjenstand for underforståtte begrensninger. Medlemsstatene har således muligheter for skjønnsutøvelse når betingelsene for universell stemmerett og valgsystemet fastsettes. Slike begrensninger og vilkår må imidlertid tjene legitime formål.

Det er klart at EMK art. 3 gjelder valg til landets nasjonalforsamling. Om den også omfatter valg til andre folkevalgte organer er i praksis[48] avgjort etter vektlegging av om det aktuelle organ har vidtgående og selvstendige beføyelser. Sannsynligvis vil norske kommuner og fylkeskommuner på grunn av mer begrensede fullmakter falle utenfor (Aall 2004).

6.4.2 Kodeks for god valgpraksis

Kodeks for god valgpraksis fra 2002, fastsatt av Venezia-kommisjonen, gir retningslinjer for gjennomføring av valg i medlemsstatene. Retningslinjene er vedtatt av Ministerkomiteen i Europarådet. Denne kodeksen bygger på "European electoral heritage", som er felles prinsipper for europeiske valg, gjennom retten til alminnelige, like, frie, hemmelige og direkte valg. Denne demokratiske arven består hovedsaklig av internasjonale standarder. I Europa kommer dette til uttrykk gjennom den europeiske menneskerettighetskonvensjonen art. 3.

Kodeks for god valgpraksis forutsetter at det kan tilrettelegges for elektronisk stemmegivning. Retningslinjene fastslår at velgere alltid skal ha muligheten til å avgi stemme i et valglokale, jf. punkt I 3.2 ii. Fra dette utgangspunktet heter det at elektronisk stemmegivning kan aksepteres dersom slik stemmegivning er *sikker og pålitelig*, jf. punkt I 3.2 iv.

I merknadene til retningslinjene fremheves myndighetenes forpliktelser med hensyn til at velgere alltid skal beskyttes mot trusler eller utilbørlig tvang slik at stemme avgis etter egen overbevisning. Det påpekes videre at visse sikkerhetstiltak bør iverksettes for å minimere risikoen for valgfusk, for eksempel ved at velgeren gis anledning til å kontrollere sin stemme umiddelbart etter at den er avgitt. Det heter videre at velgeren skal kunne få bekreftelse på sin stemme. Dette betyr ikke at velgeren skal få en papirkvittering som gjengir innholdet i stemmegivningen. For å legge til rette for verifikasjon og ny opptelling av stemmer kan det sørges for at systemet skriver ut stemmene på papir. Disse må i tilfelle plasseres i en forseglet innretning der stemmene ikke kan ses. Uansett hvilken metode som benyttes skal den sikre konfidensialitet.

Velger må ha mulighet til å korrigere stemmen om nødvendig uten at kravet til hemmelighold brytes. Med dette menes at velgeren må ha mulighet til å endre stemmegivningen der og da, før vedkommende trykker på send-knappen for å avgi stemmen.

Systemet skal være transparent, det vil si at det må være gjennomsiktig i den forstand at det kan kontrolleres om det fungerer som det skal.

[48] Domsstolens avgjørelser 5. juli 1985 (Booth-Clibborn) og 2. mars 1987 (Mathieu-Mohin and Clerfayt)

6.4.3 Rekommandasjon om standarder for elektronisk stemmegivning

Ministerkomiteen i Europarådet vedtok 30. september 2004 en rekommandasjon om juridiske, operasjonelle og tekniske standarder for elektronisk stemmegivning, se vedlegg A. Rekommandasjonen (anbefalingen) er et juridisk instrument som må vedtas enstemmig av medlemsstatene, men som ikke er folkerettslig forpliktende i seg selv. Arbeidsgruppen legger imidlertid til grunn at Europarådets anbefaling skal følges dersom det innføres adgang til å avgi stemme elektronisk. Dens standarder gjøres juridisk bindende gjennom oppfølging i norsk lov eller forskrift.

Europarådet vektlegger at anbefalingen skal bidra til at det utvikles felles europeiske standarder for elektronisk stemmegivning. Alminnelige europeiske standarder er grunnleggende for å sikre at alle prinsippene for demokratiske valg blir respektert også ved gjennomføring av elektronisk stemmegivning, for slik å bygge tillit og tiltro til nasjonale ordninger for elektronisk stemmegivning.

Det er videre viktig å skape samspill (interoperabilitet) i stemmegivningssystemene i de ulike medlemslandene. Regler for interoperabilitet og åpne tekniske standarder innenfor og på tvers av medlemsstatene kan sikre både kombinert og fortsatt bruk av e-stemmegivningssystemer fra forskjellige leverandører og at anskaffelseskostnadene for nasjonale myndigheter reduseres.

Europarådets anbefaling har omfattende bestemmelser og krav til hvordan et system som brukes til elektronisk stemmegivning skal utformes, blant annet hva som kreves for å imøtekomme prinsipper for gjennomføring av valg. Europarådets anbefaling i seg selv utgjør ikke et helhetlig regelverk for gjennomføring av elektroniske valg. Standardene må ses i sammenheng med og suppleres med internasjonale forpliktelser og nasjonal lovgivning som berøres.

Bestemmelsene i Europarådets anbefaling må anses som minimumsstandarder. De juridiske bestemmelsene tar utgangspunkt i de prinsipper vi bygger vårt demokratiske system på, og angir de krav som, i tillegg til prinsipper nedfelt i nasjonal lovgivning, må imøtekommes i det øyeblikk det tillates å avgi stemme elektronisk. De operasjonelle kravene handler om hvilke krav som stilles til både maskinvare og programvare som benyttes ved e-stemmegivning. De tekniske kravene omhandler oppbyggingen og bruken av maskinvare og programvare i e-stemmegivningssystemer, og er ment å skulle garantere teknisk sikkerhet, tilgjengelighet og interoperabilitet i et e-stemmegivningssystem.

6.5 Demokratiske prinsipper for valg – gjeldende rett

Arbeidsgruppen vil i dette avsnittet, med utgangspunkt i valglovgivningen og bestemmelsene i Europarådets anbefaling, drøfte de rettslige kravene som må ivaretas ved en eventuell overgang til elektronisk stemmegivning. De juridiske kravene må suppleres med bestemmelser av operasjonell og teknisk art som fremkommer i rekommandasjonens vedlegg II og III, jf. også denne rapportens kapittel 5, 8 og 9.

6.5.1 Prinsippet om alminnelig stemmerett

Prinsippet om alminnelig stemmerett krever tilrettelegging for at alle velgere skal kunne delta i valg. Valgloven fastsetter i § 8-3 (1) at forhåndsstemmegivningen skal foregå i ”egnet lokale”. Dette stiller krav både til hvilke lokaler som benyttes og til utformingen inne i selve

lokalet. Detaljer gis i valgforskriften § 26. Tilsvarende gjelder for stemmegivning på valgtinget, jf. valgforskriften § 30. Det er særlig lagt vekt på å imøtekomme behov velgere med funksjonshemninger har. God tilrettelegging krever også god utforming av stemmesedlene. I valgforskriften § 3 kreves at disse skal være "lesevennlige". Det er krav til blant annet størrelse på seddelen, farge, skriftstørrelse og utforming med hensyn til rettinger på stemmesedler.

De samme prinsippene må legges til grunn i et elektronisk valgsystem. I Europarådets anbefaling heter det at med mindre måter å stemme på utenfor valglokalet er tilgjengelige for alle, skal de kun tilbys som en ekstra og valgfri stemmegivningskanal, jf. rekommandasjonen punkt 4. Dette for å forhindre at noen velgere holdes utenfor ved at det legges opp til stemmegivning på en slik måte at velgeren i realiteten ikke kan delta. Regelen får betydning ved at det må kreves at alle velgere får lik mulighet til å benytte de kanaler som kan brukes til å avgi stemme elektronisk og ved at ordinær stemmegivning ved papirstemmesedler fortsatt må tilbys.

I et elektronisk valgsystem kan utformingen av brukergrensesnittet sammenlignes med utformingen av stemmesedler ved manuelle valg. Rekommandasjonen krever at brukergrensesnittet i et e-stemmegivningssystem skal være forståelig og lett anvendelig for velgeren, jf. rekommandasjonen punkt 1. Det heter videre i rekommandasjonen punkt 3 at systemet skal, så langt det er praktisk mulig, utformes slik at det maksimerer mulighetene slike systemer kan gi personer med funksjonshemninger. Det må være et mål at en gjør alle stemmegivningskanalene mest mulig tilgjengelige for funksjonshemmede.

Brukergrensesnittet må så langt det teknisk og praktisk lar seg gjøre tilpasses mennesker med ulike funksjonshemminger. Velgere med synshemninger kan for eksempel ikke bruke et rent visuelt stemmegivningssystem, som pekeskjermer, uten spesiell tilrettelegging[49]. Ved utformingen anbefaler vi at retningslinjene som er utarbeidet av Web Content Accessibility Guidelines (WCAG) under programmet Web Accessibility Initiative (WAI) - også kjent som WAI-retningslinjene[50], følges. Dette er også i samsvar med strategi for IKT i offentlig sektor[51].

6.5.2 Prinsippet om lik stemmerett

Prinsippet er grunnleggende og innbærer at hver enkelt velger bare kan få godkjent én stemme. Systemet må garantere at denne registreres og telles. Det forutsetter også at det finnes et system som forhindrer at velger avgir flere tellende stemmer, at samme stemme telles flere ganger, at stemmer forsvinner, eller at stemmer endres underveis i valgprosessen.

Gjennom valglovgivningen ivaretas disse forutsetningene gjennom at velgers rett til å avgi stemme er knyttet til krav om at vedkommende står oppført i manntallet, jf. valgloven kapittel 2. Når stemme avgis kan velgeren avkreves legitimasjon, jf. §§ 8-4 (3) og 9-5 (2), som skal sikre rett identitet. I praksis er det mulig for velgeren å avgi flere stemmer. Det er imidlertid ikke mulig å få godkjent mer enn én stemme. Manuelt system bygger på at når velgeren er avkrysset i manntallet vil vedkommende ikke få godkjent flere stemmer, jf. §§ 10-1 og 10-2. Tilsvarende forutsetninger må sikres i et system hvor stemmer avgis elektronisk. Rekommandasjonen har bestemmelser om at det må utformes et system som forhindrer en

[49] Jf. veileder fra Deltasenteret/Sosial- og Helsedirektoratet: "Selvbetjening for alle?"
[50] http://www.w3.org/WAI
[51] "Strategi for IKT i offentlig sektor 2003-2005" http://odin.dep.no/filarkiv/171428/AAD_IKT.pdf

velger fra å legge flere enn én stemmeseddel i den elektroniske valgurnen. En velger skal kun få avgi stemme hvis det er fastslått at hans eller hennes stemmeseddel ikke allerede er lagt i valgurnen, jf. rekommandasjonen punkt 5. Dette betyr ikke at velgeren ikke kan avgi flere stemmer, men systemet må sikre at hver velger ikke får *godkjent* mer enn én stemme. Det må tilsvarende lages rutiner for å sikre at velgeren ikke får godkjent mer en én stemme når det gjøres bruk av flere stemmegivningskanaler, jf. rekommandasjonen punkt 6. Dette krever rutiner knyttet til manntallet, og vil være tilsvarende som i et manuelt system, der prinsippet sikres gjennom at velgeren kun får godkjent én stemme.

Alle stemmene som er lagt i den elektroniske valgurnen skal telles, og hver stemme skal telles kun én gang, jf. rekommandasjonen punkt 7. Bestemmelsen er identisk med det som gjelder ved ordinær stemmegivning, selv om dette ikke er uttrykt eksplisitt i loven.

Det må lages rutiner for hvordan en på en sikker og pålitelig måte samler sammen stemmer fra flere kanaler og beregner et korrekt resultat, jf. rekommandasjonen punkt 8. Vi viser også til en teknisk beskrivelse i kapittel 8.

6.5.3 Prinsippet om frie og hemmelige valg

Prinsippet om frie valg skal sikre alle stemmeberettigede rett til å gi sin stemme til det partiet/gruppen velgeren ønsker, uten innblanding, tvang eller utilbørlig påvirkning fra offentlige myndigheter eller andre. Dette innebærer en forpliktelse for myndighetene til å legge forholdene til rette i forbindelse med stemmegivningen på en slik måte at rettigheten sikres. Det betyr for eksempel at det må etableres en ordning der velgeren skal ha mulighet til å avgi stemme under slike forhold at vedkommende ikke utsettes for utilbørlig påvirkning. Det må sikres at innholdet i velgers stemme kan holdes hemmelig.

Hemmelige valg kan imidlertid ikke forstås som et absolutt eller helt ufravikelig krav. Som vi skal se kan hensyn til velgeren selv tilsi at det etableres unntak fra kravet. Myndighetene kan heller ikke garantere for at velgeren ikke selv avslører innholdet i sin stemmegivning. Kravet til frie og hemmelige valg er kommet til uttrykk i valgloven gjennom at den krever at velgeren skal avgi stemme i ”enerom og usett”, jf. §§ 8-4 (1) og 9-5 (3). Bestemmelsene gjelder både ved forhånds- og valgtingsstemmegivningen, utenriks og innenriks, og innebærer krav til stemmeavlukker eller egne rom i valglokalene og at velgeren skal være alene når stemme avgis. I forlengelsen av dette gir loven også anvisning på hvem som kan være stemmemottaker. Det gir kontroll over stemmegivningssitasjonen og betyr at stemmer bare kan avgis hos en på forhånd bestemt stemmemottaker.

Vi har ett unntak fra kravet til enerom og usett. Av hensyn til velgere som trenger hjelp i forbindelse med selve stemmegivningen, bestemmer loven at slik hjelp skal gis av valgfunksjonær. Har velgeren alvorlig psykisk eller fysisk funksjonshemming kan vedkommende peke ut en ekstra hjelper, jf. valgloven §§ 8-4 (1) og 9-5 (5). Fra kravet om at stemme skal avgis hos stemmemottaker er det også av hensyn til velgeren gjort unntak. I særlige tilfeller kan velgere bosatt i utlandet, og som ikke har mulighet til å oppsøke stemmemottaker, avgi stemme pr. brev, jf. § 8-2 (3).

Kravet til frie og hemmelige valg må også sikres dersom det innføres muligheter til å avgi stemme elektronisk. Dette anses uproblematisk dersom stemme avgis elektronisk i kontrollerte omgivelser.

Problemer oppstår i det øyeblikk stemmegivningen flyttes ut av det offentlige rom der stemmegivningssituasjonen ikke kontrolleres av valgfunksjonærer. Hemmelighold av stemmen må her i utgangspunktet sikres av velgeren selv. Og det blir ikke mulig for myndighetene å sikre velgerne mot utilbørlig påvirkning. Det kan argumenteres med at utilbørlig påvirkning i forbindelse med stemmegivning er straffbart. Det er likevel et spørsmål om dette er tilstrekkelig med tanke på at myndighetene i henhold til lov er forpliktet til å tilrettelegge for hemmelig stemmegivning uten utilbørlig påvirkning.

Enkeltmenneskets rett til å avgi stemme er et viktig og grunnleggende prinsipp. I rekommandasjonen heter det at organiseringen av elektronisk stemmegivning skal sikre at velgeren fritt får danne og gi uttrykk for sin egen mening, og, der det kreves, personlig får utøve sin rett til å stemme, jf. rekommandasjonen punkt 9. Noen medlemsstater tillater stemmegivningsprosedyrer hvor prinsippet om alminnelig stemmerett gis prioritet over prinsippet om personlig fremmøte. Sistnevnte bestemmelse er ikke aktuell for oss, siden det etter valglovgivningen ikke er tillatt å avgi stemme ved stedfortreder.

Rekommandasjonen punkt 9 setter for øvrig krav til hvordan valget organiseres med hensyn til kravet til hemmelig stemmegivning, jf. også kravet i rekommandasjonen punkt 16. Dette er også et spørsmål om problemet kan avhjelpes ved at det settes inn spesielle tiltak. Vi viser til en særskilt diskusjon rundt problemstillingen i avsnitt 6.6.

Kravet i rekommandasjonen er at elektroniske stemmegivningssystemer skal organiseres slik at hemmeligholdelsen av den enkeltes valg, på ethvert trinn i stemmegivningsprosessen og spesielt i velgerautentiseringen, ikke settes i fare, jf. rekommandasjonen punkt 16. Dette stiller krav til at hemmeligholdelsen må sikres gjennom alle valgprosedyrer: prosedyrene før selve stemmegivningen (som overføring av PIN-koder, eller elektroniske meldinger til velger), under utfyllingen av stemmeseddelen, når stemme avgis, under overføringen av stemmen, og under opptellingen av stemmene. Dette setter spesifikke krav til utformingen av den tekniske løsningen og må komme til uttrykk i kravspesifikasjonen for systemet.

I et manuelt system vil det i et tidsrom være en kopling mellom velgeren og velgerens stemme. Dette gjelder i første rekke for forhåndsstemmer, men i noen få tilfeller også for valgtingsstemmer. Rutinene for hvordan koplingen gjøres er satt opp for best mulig å sikre hemmelighold. Ved forhåndsstemmegivningen skal velgeren legge sin stemmeseddel i en stemmeseddelkonvolutt. Denne legges sammen med valgkort, som inneholder opplysninger om velger, i en omslagskonvolutt som sendes rett valgstyre. Prosedyren er nødvendig så lenge en har en ordning der velgeren har mulighet til å avgi stemme i en annen kommune/utenriks, og stemmen må sendes kommunen vedkommende er manntallsført for godkjenning. For å kunne krysse av i manntallet for godkjent stemmegivning, må valgmyndighetene vite velgers identitet. I et manuelt system vil kontrollen med fysisk atskillelse av omslagskonvolutt og valgkort foretas av minimum to valgfunksjonærer, jf. valgforskriften § 35. En tilsvarende kopling i et elektronisk system vil også være nødvendig dersom det legges opp til at velgerne skal kunne avgi stemme flere ganger/ombestemme seg. Tidligere stemme(r) må da forkastes.

E-stemmegivningssystemet skal garantere at stemmene i den elektroniske valgurnen og stemmene som telles, er og forblir anonyme, og at det ikke er mulig å rekonstruere noen forbindelse mellom velgeren og vedkommendes stemmegivning, jf. rekommandasjonen punkt 17. Bestemmelsen er ikke til hinder for at det på ett gitt stadium i e-stemmegivningsprosessen gjøres en teknisk kopling mellom velgers identitet og stemme, så lenge hemmelighold sikres. Dersom velgeren gis mulighet til å forandre stemmen senere, er det nødvendig å opprettholde

en kopling mellom velger og stemme, inntil tidspunktet for når det ikke lenger er mulig å avgi stemme. I hele denne prosessen må det sørges for hemmelighold av stemmen, det betyr at en stemme må forsegles og forbli forseglet gjennom hele stemmegivningsprosessen, lagringen og tilbaketrekningsprosessen. Men den forseglede stemmen må fortsatt knyttes til en navngitt velger.

I tradisjonelle stemmegivningssystemer holdes som nevnt velgers identitet og stemme fra hverandre ved fysisk atskillelse, noe som lett kan kontrolleres av valgfunksjonærer og valgobservatører. Ved elektroniske stemmegivningssystemer utenfor valglokalene må denne atskillelsen gjøres elektronisk. I tilfelle velgeren kan ombestemme seg, vil det være den sist avgitte stemmen som teller. Denne skal legges i valgurnen når stemmegivningen er avsluttet, og koplingen mellom stemme og velger brytes. Det er kun den godkjente stemmen som skal legges i urnen. Det skal ikke være mulig å rekonstruere denne forbindelsen når stemmen først er lagt i den elektroniske urnen. Elektronisk atskillelse krever spesielle tekniske løsninger som må komme til uttrykk i kravet til spesifikasjon av systemet. Kontroll og godkjenning av systemet utgjør her en viktig forutsetning, jf. kapittel 9.

E-stemmegivningssystemet skal være utformet slik at det forventede antall stemmer i enhver elektronisk valgurne ikke gjør det mulig å knytte resultatet til de enkelte velgerne, jf. rekommandasjonen punkt 18. Til dette hører også med at det må tas forholdsregler som sikrer at informasjon som er nødvendig for den elektroniske prosesseringen, ikke kan benyttes til å bryte hemmeligholdelsen av den avgitte stemmen, jf. rekommandasjonen punkt 19. Nødvendige forholdsregler betyr for eksempel at lagringen av avgitte stemmer gjøres tilfeldig i den elektroniske valgurnen, slik at rekkefølgen stemmene lagres i ikke gjør det mulig å rekonstruere rekkefølgen de ble avgitt i.

Kravet til fritt å kunne bestemme hva en ønsker å stemme på, må også ivaretas gjennom utforming av brukergrensesnittet og gjennom måten velgerne veiledes gjennom e-stemmegivningsprosessen. Den skal være slik at den forebygger en forhastet eller ureflektert stemmegivning, jf. rekommandasjonen punkt 10. Ureflektert i denne sammenheng betyr at velgeren må få tilstrekkelig tid til å tenke gjennom sin stemmegivning før stemme avgis.

Brukergrensesnittet må utformes slik at det ikke er mulig på noen måte å utøve noen form for manipulerende innflytelse over velgeren under stemmegivningen, jf. rekommandasjonen punkt 12. Dette stiller krav til den tekniske løsningen, men også til brukergrensesnittet. Eksempler er lyder som kan assosieres med en spesiell kandidat eller valgmulighet eller pop-opp skjermbilder som fremmer et spesielt valg.

Velgere skal ha mulighet under selve stemmegivningen til å ombestemme seg i prosessen før stemme avgis, eller å avbryte prosessen uten at tidligere valg blir registrert eller gjort tilgjengelig for noen andre, jf. rekommandasjonen punkt 11. Det er bare velgeren som skal ha tilgang til stemmen. Det betyr at systemet ikke skal tillate at den utfylte stemmeseddelen lagres på velgerens personlige datamaskin eller på den innretningen som brukes for stemmegivning, for eksempel for å avgis senere. Ingen andre enn velgeren selv skal ha tilgang til stemmen, verken i selve systemet eller under overføring til valgurnen.

Kravet til frie valg innebærer også rett til å avgi blank stemme, uten å måtte velge noen av de godkjente listeforslagene, jf. rekommandasjonen punkt 13. Samme krav gjelder ved manuell stemmegivning, jf. valgforskriften § 20.

E-stemmegivningssystemet skal gi tydelig tilbakemelding til velgeren når stemmegivningen har vært vellykket og når hele prosessen er fullført, jf. rekommandasjonen punkt 14. Bestemmelsen setter krav til teknisk løsning og brukergrensesnitt, og skal sikre at velgeren vet når stemme er avgitt. Dette er et viktig ledd i å skape tillit til systemet og av hensyn til prinsippet om at enhver avgitt stemme skal telle. Videre må velgeren vite når hele stemmegivningsprosedyren er vellykket gjennomført slik at vedkommende trygt kan bryte forbindelsen/gå ut av avlukket.

Stemmegivningsprosedyren er vellykket gjennomført når den riktige elektroniske stemmen er lagt i en sikker elektronisk valgurne til riktig tid uten at uvedkommende har hatt tilgang til stemmen. I ukontrollerte omgivelser er prosedyren vellykket gjennomført først når stemmen er sendt fra velgerens stemmegivningsmekanisme (personlig datamaskin, telefon, osv), over Internett eller et annet nettverk og har kommet frem til målet, dvs. tjeneren der valgurnen befinner seg. Dersom velgeren skal få avgi elektronisk stemme flere ganger (ev. stemme ved papirstemmeseddel), må det finnes en mekanisme som sikrer at det kun er den sist avgitte stemmen som godkjennes og dermed legges i den elektroniske urnen. Det kan derfor være nødvendig at stemmene legges i en midlertidig urne.

6.5.4 Er det å stemme elektronisk forenlig med kravet til hemmelig valg?

Krav til hemmelig valg innebærer at velgeren skal ha mulighet til å avgi stemme *alene, usett og uten å bli påvirket på en utilbørlig måte.* I valgloven kommer kravet til hemmelig valg til uttrykk på flere måter. Ved tradisjonell stemmegivning gjøres dette ved at en og en velger får gå inn i stemmeavlukket, der stemme avgis usett og uten påvirkning fra andre. Å utsette noen for utilbørlig påvirkning er straffbart, jf. straffeloven kapittel 10.

Prinsippet utfordres dersom det tillates stemmegivning i ukontrollerte omgivelser, dvs. hjemme, på arbeidsplassen, stemmegivning pr. brev eller lignende. I disse tilfellene kontrolleres ikke stemmegivningssituasjonen av en valgfunksjonær, og faren for utilbørlig påvirkning er til stede.

Spørsmålet er vurdert av Venezia-kommisjonen. Uttalelsen fra kommisjonen[52] kom i forbindelse med utarbeidelsen av rekommandasjonen om standarder ved elektronisk stemmegivning. Problemstillingen for kommisjonen var om det å avgi stemme i ukontrollerte omgivelser lar seg forene med EMK. EMK gir velgere en individuell rett til å avgi stemme ved *"hemmelig avstemning"*. Denne retten er knyttet til krav om at myndighetene skal legge til rette for stemmegivning *"under forhold som sikrer at folket fritt får uttrykke sin mening"*.

Problemstillingen er aktuell også ved brevstemmegivning (hos noen kalt postvalg). Brevstemmegivning anses som tradisjonell form for "remote voting", dvs. stemmegivning i ukontrollerte omgivelser. Kommisjonen viser i sin uttalelse til at brevstemmegivning i ukontrollerte omgivelser ("remote voting in an unsupervised environment") er blitt vanlig praksis[53] ved valg i flere medlemsland de senere årene og derfor må defineres som en

[52] CDL-AD (2004)012 Or. Fr. Vedtatt på Venezia-kommisjonens 58. plenumsmøte 2004. http://www.venice.coe.int/docs/2004/CDL-AD(2004)012-e.asp

[53] Fem land tillater brevstemmegivning fullt ut; Tyskland, Spania, England, Irland og Sveits. I Norge er slik stemmegivning kun tillatt i særlige tilfeller av velgere bosatt i utlandet og som ikke har mulighet til å stemme hos ordinær stemmemottaker ved ambassader, konsulat m.m. Utover dette finnes ulike varianter for brevstemmegivning i ca halvparten av medlemslandene som er undersøkt, særlig gjelder dette brevstemmegivning for alle som er bosatt i utlandet. Undersøkelsen, som gjengis i Venezia-kommisjonens uttalelse i CDL-AD (2004) 012, er foretatt av Europarådet blant dets medlemsstater i forbindelse med

europeisk standard. Dette er en *felles* europeisk standard og følgelig lagt til grunn i Venezia-kommisjonens Kodeks for god valgpraksis.

Visse restriksjoner må ligge implisitt i art. 3 ved at bestemmelsen sies å pålegge landene en minimumsstandard for å sikre hemmelighold av stemmene. En slik standard defineres ut fra felles lovgivning og er i seg selv grunnlaget for de retningslinjene som er nedfelt i Kodeks for god valgpraksis. Når det gjelder brevstemmegivning, er kravet i kodeksen av slik stemmegivning bare kan tillates dersom postsystemet er sikkert og pålitelig. Kommisjonen mener at selv om kodeksen ikke inneholder bindende regler, har den nedfelt europeiske standarder som kan påvirke fortolkningen av EMK art. 3.

Når det gjelder elektronisk stemmegivning, viser kommisjonen også til retningslinjene i Kodeks for god valgpraksis der det heter at elektronisk stemmegivning bare skal tillates dersom det er sikkert og pålitelig. Basert på en analyse av brevstemmegivning i ukontrollerte omgivelser, mener kommisjonen lignende standarder kan utvikles ved elektronisk stemmegivning. Elektronisk stemmegivning er ikke generelt tillatt etter menneskerettighetene, men heller ikke utelukket. Aksept vil være avhengig av de juridiske, prosessuelle og tekniske standarder som gjøres gjeldende. Over tid kan det altså utvikles standarder som må anses som sedvane.

Kommisjonens konklusjon er således at elektronisk stemmegivning vil være i samsvar med europeiske standarder og dermed EMK, forutsatt at visse forholdsregler ivaretas når prosedyrer for slik stemmegivning utformes.

Spørsmålet om valghemmelighet og utilbørlig påvirkning er særlig aktuelt i forbindelse med såkalt ”family voting”; hvor et familiemedlem urettmessig utøver innflytelse på et annet familiemedlems stemmegivning. Europarådet vedtok i oktober 2004 en rekommandasjon, 2004(1676), hvor de ber om at Ministerkomiteen lager utkast til et charter om ”electoral equality”. Charteret skal inneholde retningslinjer som tar opp i seg alle nødvendige tiltak for å forby og fjerne ”family voting”. De nevner tiltak som holdningskampanjer, opplæring, sanksjoner mot valgfunksjonærer som tillater slik stemmegivning m.m. Problemstillingen blir imidlertid ikke reist i tilknytning til elektronisk stemmegivning i ukontrollerte omgivelser.

I et par rettssaker (Skottland 1922 og USA 1999), har man kommet til at kravet til hemmelig valg ikke forutsetter at myndighetene skal garantere absolutt hemmelighold. Den enkelte velger har også en del av ansvaret.

Den europeiske menneskerettsdomsstolen har ikke uttalt seg særskilt om spørsmålet. Vi skal kun vise til at når det foreligger lang praksis i mange medlemsland på et bestemt område, har praksisen stor rettskildemessig vekt hos den europeiske menneskerettsdomstolen. Det samme gjelder dersom det finnes en felles europeisk standard på området.

Spørsmålet om elektroniske valg og forholdet til EMK er også diskutert internt i medlemslandene i forbindelse med at det er avholdt ulike forsøk med elektronisk stemmegivning eller ev. innføring av brevstemmegivning.

I England er det anledning til å avgi stemme i ukontrollerte omgivelser ved brevstemmegivning. De har også vært gjennom ulike forsøk med elektronisk stemmegivning i

---

utarbeidelsen av rekommandasjonen for elektronisk stemmegivning. I tillegg innførte Sverige brevstemmegvning som en fast ordning for utenlandsboende fra og med 1.1.2006.

ukontrollerte omgivelser. Engelske myndigheter mener dette er uproblematisk så fremt velgerne har alternative stemmegivningskanaler.

Bob Watt, professor ved University of Essex i England, hevder internasjonale forpliktelser forhindrer elektronisk stemmegivning i ukontrollerte omgivelser (Watt 2002). Han viser til at EMK ikke har bestemmelser som gir mulighet for begrensninger. Watt viser ellers til at brevstemmegivning og elektronisk stemmegivning fører til at hele ansvaret for å sikre hemmelighold overføres til den enkelte velger.

Hans standpunkt imøtegås av andre. Det argumenteres i motsatt retning med at et slikt syn er uttrykk for en rigid fortolkning av regelverket. Vi har mange eksempler på at samfunnsutviklingen endrer innholdet i juridiske begreper over tid. Noen vil også hevde det er urimelig at EMK skal stå i veien for en nyskapning som det å avgi stemme elektronisk (Auer 2005). Auer stiller spørsmål ved om EMKs bestemmelse virkelig skal oppfattes så urokkelig at den setter stopper for en nyskapning som det elektronisk stemmegivning er. Han viser også til at bestemmelsen, særlig i lys av fallende valgdeltagelse, ikke bør stå i veien for modernisering av måter å stemme på.

Auer viser i denne sammenheng til domsstolens fleksibilitet og at den har gitt uttrykk for at "the Convention is a living instrument which must be interpreted in the light of present-day conditions"[54]. Han stiller seg derfor tvilende til om domstolen vil gi uttrykk for en kompromissløs holdning lik den Watt gir uttrykk for.

6.5.5 Vurdering og anbefaling

Retten til hemmelig valg er et grunnleggende prinsipp i vårt demokrati, og må stå fast også dersom det innføres mulighet til elektronisk stemmegivning.

Venezia-kommisjonen mener elektronisk stemmegivning ikke strider mot prinsipper nedfelt i EMK art. 3, forutsatt at visse tekniske forhåndsregler tas. Dette bestrides av noen.

Arbeidsgruppen er enig i at myndighetene vanskelig kan garantere hemmelighold. Dette er heller ikke mulig i et manuelt system. Vi mener likevel ikke at dette er et spørsmål om å garantere hemmelighold, men et spørsmål om hvor langt myndighetene må gå for å *legge forholdene til rette* for å at kravet til hemmelighold sikres på best mulig måte.

Arbeidsgruppen mener at utgangspunktet er klart: Det er ikke mulig for myndighetene å kontrollere verken om velgeren får avgitt stemme hemmelig eller om velgeren utsettes for utilbørlig påvirkning når stemme avgis i ukontrollerte omgivelser. Spørsmålet er da om dette stenger helt for elektronisk stemmegivning i ukontrollerte omgivelser, eller om det er mulig å sette inn tiltak for på annen måte å imøtekomme kravene til hemmelighold.

Feil stemmegivning på grunn av utilbørlig påvirkning har tradisjonelt ikke skapt problemer her i landet. I vår tradisjon står både hemmelighold og det at velgeren ikke skal påvirkes utilbørlig, sterkt. I de senere årene har imidlertid problemstillingen vært mer fremtredende, og var direkte årsak til at regelverket rundt bruk av hjelper i stemmeavlukket ble innskjerpet ved valget i 2005. For det store flertall av velgere vil spørsmålet om utilbørlig påvirkning likevel ikke være en aktuell problemstilling. Hvorfor skal man da si nei til en hensiktsmessig og nyttig ordning, som kun kan skape problemer for et lite mindretall? Til dette er å anføre at

[54] Avgjørelse 18. februar 1999 (Matthews vs. United Kingdom)

retten til hemmelig valg må omfatte samtlige velgere. Det er ikke tilstrekkelig at det kun er oppfylt for flertallet.

I Storbritannia argumenterer man med at kravet til hemmelighold er oppfylt så lenge man opprettholder retten til å avgi stemme i valglokaler. Man kan også argumentere med at det er straffbart å tvinge noen til å stemme i strid med ens egen overbevisning. Så lenge muligheten til å stemme i valglokaler opprettholdes, må velgeren selv sørge for at stemmegivningen skjer der. På den annen side er det vel nettopp tvangen i seg selv som ofte er problemet, og det endres neppe ved at velgeren har et alternativ.

Det er delte meninger om og i hvor stor grad kravet til hemmelighold er forenlig med elektronisk stemmegivning. Spørsmålet er ikke løst internasjonalt. Til syvende og sist vil spørsmålet måtte løses rettslig, nasjonalt eller internasjonalt. Siden rettsstillingen synes såpass uklar, vil også domstolene i en eventuell rettssak måtte legge stor vekt på praksis.

Arbeidsgruppen klare utgangspunkt er at det ikke kan gjennomføres elektronisk stemmegivning i ukontrollerte omgivelser uten at myndighetene legger forholdene til rette for å sikre kravet til hemmelighold og stemmegivning uten utilbørlig påvirkning. Flere forutsetninger er etter vår vurdering således nødvendige før elektronisk stemmegivning kan tillates.

Elektronisk stemmegivning må innføres som et alternativ til ordinær stemmegivning. Stemmegivning med papirstemmesedler må opprettholdes og velgeren må selv få bestemme hvordan vedkommende vil avgi stemme. Dersom det gis mulighet for elektronisk stemmegivning hjemmefra, må velgere som stemmer elektronisk gis mulighet til å ombestemme seg, det vil si stemme på nytt for eksempel i et valglokale for forhåndstemmegivning eller på valgdagen. Det bør dessuten ikke kunne avgis elektroniske stemmer i ukontrollerte omgivelser på valgdagen, siden dette i praksis sterkt begrenser eller eventuelt gjør det umulig for velgeren å stemme på nytt.

Arbeidsgruppen mener Norge per i dag bør kunne ta utgangspunkt i de retningslinjer som er nedfelt i internasjonale regler dersom det innføres elektronisk stemmegivning her i landet. Om det er muligheter for å prøve ut elektronisk stemmegivning vil imidlertid avhenge av om den tekniske løsningen kan gjøre systemet sikkert og pålitelig. Det er ikke tilstrekkelig at grunnleggende prinsipper for valg stadfestes i et regelverk. Prinsippene må implementeres gjennom prosedyrer som sikrer at de oppfylles korrekt. Ved elektronisk stemmegivning gjelder dette ikke minst ulike tekniske prosedyrer, se nærmere om dette i kapittel 8. I tillegg vil et system for godkjenning og kontroll av den tekniske løsningen være av stor betydning. Se nærmere om dette i kapittel 9.

Innføring av elektronisk stemmegivning ved valg vil på sikt medføre at det må gjøres vesentlige endringer i nasjonal valglovgivning. Vi antar at en slik omfattende lovregulering ikke er nødvendig eller ønskelig før det eventuelt innføres mulighet til å avgi elektroniske stemmer på landsbasis eller i stor skala.

Arbeidsgruppen mener det heller ikke er mulig på det nåværende tidspunkt å utforme et konkret forslag til lovgivning som skal regulere elektronisk stemmegivning eller si noe mer konkret om og hvilken annen lovgivning som vil komme til anvendelse. Før en kommer så langt, vil en måtte ta stilling til hvilke forsøk som skal gjennomføres og rammene for slike. Det bør gjerne prøves ut ulike løsninger gjennom forsøk. Hvordan elektronisk stemmegivning

skal gjennomføres, hvilke tekniske løsninger som skal brukes, hvilken betydning slik stemmegivning vil ha i forhold til demokratiske prinsipper for valg osv, må vurderes innenfor et forsøksregime og vil til syvende og sist være med å danne grunnlaget for utformingen av lovgivningen.

Innenfor rammene av et forsøksregime vil elektronisk stemmegivning kunne gjennomføres med hjemmel i egne regler om forsøk. Regelverk for konkrete forsøk vil da kunne reguleres gjennom egen forskrift.

7 Økonomiske og administrative hensyn

7.1 Innledning

I dette kapitlet skal vi se nærmere på økonomiske og administrative hensyn i forhold til elektronisk stemmegivning, med utgangspunkt i følgende punkter i mandatet:

- ”vurdere fordeler og ulemper ved elektronisk stemmegivning vs ordinær stemmegivning” (pkt. 12).
- ”vurdere kostnadselementer ved elektronisk stemmegivning i større skala, på kort og lang sikt, herunder hvilke innsparingspotensial som finnes på kort og lang sikt” (pkt 13).

Innledningsvis redegjøres det kort for enkelte sentrale trekk ved valggjennomføringen i Norge. Deretter vurderes kostnadselementene, både i forhold til gjennomføring av valg i dag og hvilke konsekvenser ulike elektroniske løsninger vil ha for kostnadsutviklingen.

7.2 Gjennomføring av valg i Norge

I Norge gjennomføres valg hvert annet år, avvekslende kommunestyre- og fylkestingsvalg og stortingsvalgsvalg sammen med sametingsvalg. Alle forvaltningsnivåer er involvert i valggjennomføringen. Kommunal- og regionaldepartementet sørger for det nødvendige regelverk, bidrar med veiledningsmateriell overfor valgmedarbeidere, utarbeider informasjonsmateriell og sørger for system for sentral innhenting av valgresultater. Ved fylkestingsvalg og stortingsvalg har fylkeskommunene enkelte oppgaver i forbindelse med gjennomføringen, som for eksempel produksjon av stemmesedler og fylkesvis kontrollopptelling og valgoppgjør. Sametingsvalget følger egne prosedyrer i samsvar med samevalgforskriften, for eksempel produserer sametinget samemanntall, stemmesedler og noe annet materiell til alle kommunene.

Utover dette er alle andre oppgaver i forbindelse med praktiske forberedelser og gjennomføring av valg i Norge lagt til kommunene, med det formelle ansvaret plassert hos valgstyret i den enkelte kommune. Kommunene i Norge er svært ulike når det gjelder antall innbyggere – fra vel 200 innbyggere i Utsira kommune til vel 530 000 innbyggere i Oslo kommune. Selv om alle kommuner må forholde seg til samme lov og forskrift (valgloven med tilhørende forskrift), vil den store forskjellen i kommunestørrelse føre til helt ulike måter å organisere valgarbeid på.

↑*Optisk skanner til opptelling av stemmesedler i Oslo kommune.*

Valgloven og forskrift til loven sammen med veiledningsmateriell utarbeidet av Kommunal- og regionaldepartementet gir en grundig beskrivelse av valgforberedelsenes ulike faser samt gjennomføring av selve valget. Arbeidet kan gjennomføres helt og fullt basert på manuelle arbeidsoperasjoner, noe som praktiseres i de minste kommunene. I noe større kommuner skaffer man seg teknologisk bistand, for eksempel i forbindelse med manntall/ manntallsoppdateringer og valgoppgjørssystem (beregningsprogram – mandatfordeling og kandidatkåring). I de største kommunene tar man også teknologien til hjelp i forbindelse med selve opptellingen ved at endelig opptelling foretas maskinelt ved hjelp av optiske lesere (OMR/OCR – teknologi). Opptellingssystemene kombineres med valgoppgjørssystem som gjør at man får en rask og presis opptelling og et komplett valgoppgjør på relativt kort tid.

I de mindre kommuner vil ofte valgforberedelser og gjennomføring bli håndtert direkte av valgstyret med sekretær. De folkevalgte bemanner også valglokalet/-lokalene. Hvis kommunen har mer enn ett valglokale, skal kommunen velge et stemmestyre med minimum 3 medlemmer til hvert valglokale. De større kommunene skal gjennomføre valg etter samme regelverk, men den organisatoriske/administrative utfordringen blir større. Her gir valgstyret føringer gjennom vedtak, men utfører ikke praktiske valgoppgaver selv.

Kommunene skal organisere et variert mottak av forhåndsstemmer (faste mottaksteder, institusjoner, videregående skoler, eventuelle høgskoler og universiteter samt mulighet for stemmegivning hjemme). Lokaler både til forhåndsstemmegivning og valgting må skaffes og lokalene må rigges. I mange kommuner skal lokalene på valgdagen i tillegg til et stemmestyre også bemannes med valgfunksjonærer som må rekrutteres. Det må organiseres mottak fra lokalene og organiseres en samlet, endelig opptelling.

Den norske valgordningen med velgernes mange muligheter til å avgi sin stemme til ulike tider og på ulike steder samt mulighetene til å foreta rettelser på stemmesedlene, stiller store krav til tilrettelegging i kommunene. Kommunene skal ha kontroll på alle avgitte stemmer, foreta en korrekt registrering av velgerne i manntallet og foreta en korrekt registrering og opptelling av alle stemmesedler med de rettelser som er foretatt. Det er en forventning om at resultatene skal foreligge umiddelbart etter valgdagen. Siden valggjennomføringen er basert på tradisjonelle metoder med papirstemmesedler som utgangspunkt, vil også mye av kontroll- og opptellingsrutinene være basert på tradisjonelle arbeidskraftintensive metoder. Kompleksiteten øker med økende kommunestørrelse. De store kommunene nyter derfor ikke godt av stordriftsfordeler, men har på den andre siden sett nødvendigheten av å ta i bruk moderne teknologi for å opprettholde god kontroll, nøyaktighet og samtidig kunne levere raske resultater. Sett under ett er likevel kostnadene pr. stemme større for store kommuner enn for små.

7.3 Hva koster valg i Norge?

Blant annet på grunn av store variasjoner i kommunestrukturen er det vanskelig å gi et presist bilde av hva gjennomføring av valg totalt sett koster for alle kommunene i Norge. Arbeidsgruppen har undersøkt litt i ulike kommuner. Kostnadsnivået følger generelt kommunestørrelsen. De større kommunene får økte utgifter fordi man velger flere elektroniske løsninger, får behov for mer kompliserte kontrollrutiner og dermed også større bemanning. Større kommuner har også gjennomgående høyere utbetalinger til lønn og honorarer.

Det antas også at det ligger mange skjulte kostnader forbundet med valg i kommunene fordi mye av forberedende valgarbeid utføres av ansatte som i utgangspunktet har andre oppgaver og funksjoner og at avlønning skjer i forhold til primæroppgavene. Det kan også være forskjeller med hensyn til hvordan bruk av interne/eksterne ressurser synliggjøres i budsjett og regnskap for valg i den enkelte kommune.

I Norge har kommunene ansvar for gjennomføring av både kommunestyrevalg, fylkestingsvalg, sametingsvalg og stortingsvalg. Ved fylkestingsvalg og stortingsvalg er fylkeskommunen ansvarlig for trykking av stemmesedler og noe annet materiell til bruk i kommunene. I tillegg foretar fylkeskommunene kontrolltelling av stemmesedlene og valgoppgjør på fylkesnivå. Ved sametingsvalg er Sametinget ansvarlig for trykking av stemmesedler og annet materiell, samt produksjon av samemanntall for den enkelte kommune. Opptelling ved sametingsvalget skjer innenfor landets 13 samedistrikter.

I henhold til de prinsipper som ligger til grunn for utgiftsdekningen ved valg, skal hvert forvaltningsnivå i utgangspunktet bære utgiftene til gjennomføringen av sine respektive valg. Av praktiske grunner er det enkelte mindre modifikasjoner i dette prinsippet.

Kommunenes valgutgifter til lokalvalg dekkes av kommunenes frie inntekter (summen av skatteinntekter og rammetilskudd). Dette betyr at det ikke er øremerkede tilskudd fra staten til dekning av valgutgifter. Det er således ikke mulig å identifisere dette beløpet pr. kommune isolert.

I 2003 ble også utgifter til stortingsvalget innlemmet i inntektssystemet, i motsetning til ordningen tidligere hvor nødvendige utgifter ble dekket etter regning. Dette ble gjort for senke behovet for administrasjon og kontroll både hos kommunene og fylkesmennene. Utgangspunktet for beregningen, da utgifter til stortingsvalget skulle innlemmes i inntektssystemet, ble tatt i nødvendige utgifter kommunene fikk dekket for å gjennomføre EU-valget i 1994. Etter justering for prisstigning og økte utgifter som følge av ny valglov utgjorde beløpet totalt 111,5 millioner kroner. I tillegg ble det lagt inn antatte økte utgifter til gjennomføring av lokalvalg på grunn av den nye valgloven med 5 millioner kroner. Totalt ble det dermed lagt inn 116,5 millioner kroner i tillegg til det som lå i rammen fra før (for lokalvalg).

Ved innlemmingen legges ¼ av beløpet inn i inntektssystemet pr. år. Hvor stor andel den enkelte kommune tildeles, varierer ut i fra de ulike kriteriene satt i inntektssystemet.

Fylkeskommunenes utgifter, i tillegg til det som ligger i rammen, er anslått til 17,2 millioner kroner. Ved innlemmingen legges ¼ av beløpet inn i inntektssystemet pr. år.

I tillegg til dette settes det hvert år av midler over Kommunal- og regionaldepartementets budsjett til dekning av departementets utgifter til valg. Staten dekker blant annet utgifter til følgende (alle valg):

- Gjennomføring av utenriks forhåndsstemmegivning (trykking og distribusjon av valgmateriell).
- Trykking og distribusjon av stemmeseddelkonvolutter og stemmesedler uten kandidatnavn ved forhåndsstemmegivningen.
- Utvikling og drift av elektronisk system for innsamling, bearbeiding, prognostisering og distribusjon av valgresultater.

- Sentrale informasjonstiltak.
- Sametingets utgifter til gjennomføring av sametingsvalg.

Ved lokalvalget i 2003 var det satt av 29 millioner kroner til dekning av utgiftene staten har ved gjennomføring av valg. I 2004 var beløpet 5 millioner kroner og i 2005 31,7 millioner kroner.

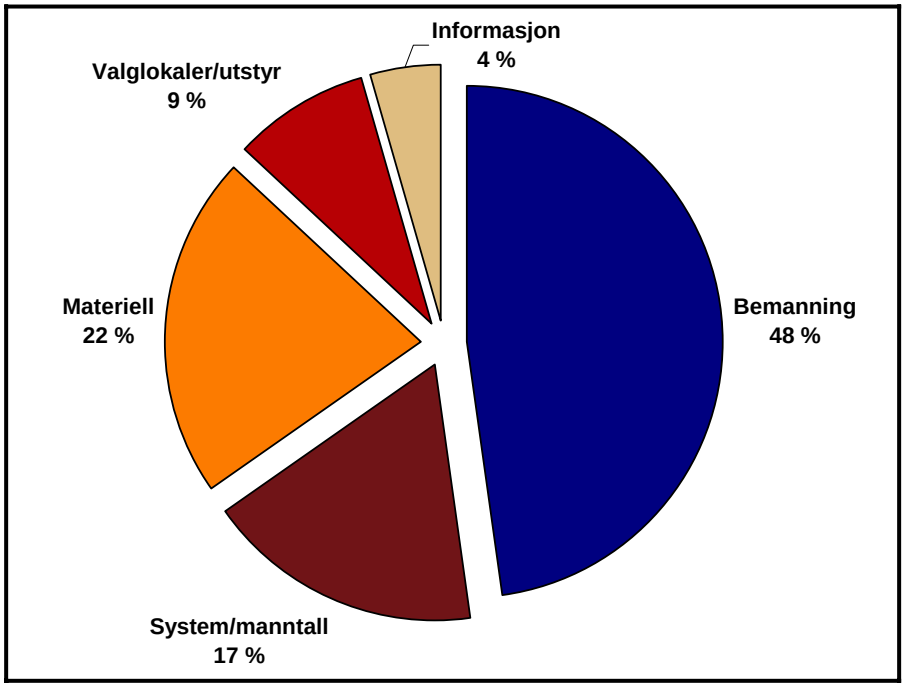
Totalt ble det i forbindelse med beregningene som skulle danne grunnlag for innlemming av valg i inntektssystemet, beregnet at stortingsvalg på landsbasis skulle koste ca 163 millioner kroner. Samme året ble det til kommunestyrevalget avgitt 2 050 000 stemmer. Disse beregningene tilsier en pris på 80 kroner pr. stemme. Kommunenes andel av utgiftene fordelt pr. avgitt stemme utgjør 57 kroner.

For kommunene fordeler kostnadene seg på ulike kostnadsarter i forbindelse med valggjennomføringen. Kostnadene er forsøkt gruppert på følgende måte:

- Bemanning: Kostnadene til bemanning består i hovedsak av ekstra godtgjørelser til de som bemanner valglokalene på valgdagen, enten i form av overtidsgodtgjørelse eller faste satser. I tillegg skjer mye av arbeidet med forhåndsstemmegivningen utenom ordinær arbeidstid (kveldsåpne lokaler, sentralt mottak, prøving av forhåndsstemmer og klargjøring for opptelling), noe som utløser overtidsgodtgjørelse eller andre faste godtgjørelser. Endelig opptelling etter at valglokalene stenger skjer også på kveld og natt, noe som også utløser ekstra bemanningskostnader. Mange kommuner vil kunne dekke en stor del av bemanningsbehovet gjennom omdisponering av egne ressurser. Dette kommer ikke alltid til syne i regnskapene hvis ikke virksomhetene får refundert lønnsutgifter. Enkelte kommuner vil ikke kunne klare å skaffe tilstrekkelig bemanning gjennom intern rekruttering og må derfor ty til innleid arbeidskraft.
- System/manntall: Et stort antall kommuner benytter datasystemer som gir tilgang til elektroniske manntallsopplysninger, slik at kommunene har de nødvendige manntallsopplysningene til bruk under forhåndstemmegivningen og får produsert avkrysningsmanntallet til bruk på valgdagen. Kommunene benytter også systemet til å foreta valgoppgjøret for kommunene og beregninger av endelig valgresultat (lokalvalg). De større kommunene benytter også datasystemer til elektronisk opptelling.
- Materiell (stemmesedler, valgkort): Det skal produseres et betydelig antall stemmesedler. Det er behov for ulike typer konvolutter, skjemaer mv. Det produseres langt større kvanta enn det som isolert sett synes å være nødvendig i forhold til mottatte stemmer. Dette skyldes at det foregår aktiviteter mange steder samtidig og det er kritisk dersom man for eksempel skulle gå tom for stemmesedler til ett parti. Mye av materiellet er særskilt merket for det enkelte valg og må derfor kastes etter valget.
- Det kan være behov for urner og annet materiell i forbindelse med forhåndsstemmegivningen. En større kostnad vil være forbundet med produksjon og utsending av valgkort, for de kommunene som velger å gjøre dette.
- Valglokaler/utstyr: Mye av utstyret som brukes i valglokalene er utstyr som oppbevares fra valg til valg, eller utstyr som allerede finnes der hvor valgtinget avholdes (for eksempel stoler og bord). Det kan være behov for fornyelse av stemmeavlukker, det skal produseres en del henvisningsskilt og andre typer plakater og det er behov for ulike typer rekvisita.
- Informasjon: Kommunene er gjennom valgloven pålagt å gjennomføre enkelte informasjonstiltak i form av konkrete kunngjøringer. Utover dette kan kommunene selv

velge å igangsette ulike informasjonstiltak. Det kan være ulike typer informasjonskampanjer som for eksempel husstandsaviser, oppslag på offentlige steder, utsending av stemmesedler og partiprogram osv.

Diagrammet i figur 7.1 viser hvordan utgiftene fordelte seg i Drammen kommune i forbindelse med kommunestyrevalget i 2003.



Figur 7.1: Utgiftsfordeling i forbindelse med Drammen kommunes gjennomføring av kommunestyrevalget i 2003

De totale kostnadene for Drammen kommune i forbindelse med valget i 2003 er beregnet til kr 2 300 000. Kostnadsfordelingen tar utgangspunkt i kommunens gjennomføring av kommunestyrevalg pluss kommunens ansvar i forbindelse med avvikling av fylkestingsvalget. Tilsvarende beregninger er foretatt for henholdsvis Trondheim og Oslo kommune. Kostnadsfordelingen er også forelagt Steinkjer kommune og Grong kommune som eksempler på mindre kommuner. Disse beregningene og undersøkelse viser at utgiftsfordelingen i det store og hele er lik i kommunene. Variasjonene mellom kommunene har sitt utgangspunkt i valg av tekniske løsninger, nivå på lønn/godtgjørelse, bruk av valgkort eller ikke m.m. Som det er redegjort for tidligere gjør lokale variasjonene også utslag på kommunenes totale kostnader.

Det er vanskelig å foreta en presis kostnadsfordeling mellom stemmegivning på valgdag og forhåndsstemmegivning. Ved stortingsvalget 2005 ble 17,9 % av stemmene avgitt på forhånd. Tar man hensyn til at forhåndsstemmegivningen er mer komplisert både når det gjelder ulike måter å avgi stemmer på og behov for kontrollrutiner m.m., antas det at kostnadene relativt sett er høyere ved forhåndsstemmegivningen enn på valgdagen.

7.4 Økonomisk vurdering i forbindelse med ulike e-valgsløsninger

Av avsnitt 7.3 går det fram at det er to vesentlige kostnadselementer knyttet til valg. Det ene er bemanning som utgjør rundt regnet 50 % av kostnadene. Det andre er materiell som utgjør

over 20 %. Hvis ett av målene med innføring av ny teknologi skal være å forsøke å redusere kostnadene, bør vurderingene i hovedsak være rettet mot disse faktorene. Kommunenes og fylkeskommunenes andel av kostnadene fordelt på disse kostnadsartene utgjør i størrelsesorden 100 millioner kroner.

7.4.1 Elektronisk stemmegivning i kontrollerte omgivelser

Elektronisk stemmegivning i kontrollerte omgivelser vil si at valglokaler utstyres med datamaskiner der velgeren avgir og får sin stemme registrert direkte inn i et datasystem, enten ved lokal lagring på et medium som transporteres til en sentral opptellingsenhet eller via en linje til en sentral opptellingsenhet. Effekten av denne ordningen er at tellefeil vil reduseres og resultatene vil kunne leveres raskere etter at valglokalene stenges.

I prinsippet finnes to alternative løsninger velgeren kan møte i valglokalet. Den ene er at man benytter spesielt utviklet utstyr for elektronisk stemmegivning. Som eksempel på dette kan nevnes de valgomatene som ble benyttet i Norge i forbindelse med forsøk med elektronisk stemmegivning i 2003. Dette var en spesialutviklet enhet der velgerne utførte sine valghandlinger på pekeskjermer (touch-screen). Det andre alternativet er å benytte generelt eller standard datautstyr (tradisjonell personlig datamaskin) der velgeren for eksempel må benytte tastatur og mus for å utføre valghandlingen.

Velgernes tidsforbruk for å avgi stemme
Et avgjørende moment i vurderingen av elektroniske løsninger i valglokalene er hvor lang tid det tar velgeren å avgi sin stemme. Vi har sett en tendens de senere årene til at velgerne bruker lengre tid i avlukkene og foretar flere rettelser på stemmesedlene. Samtidig øker kravene til gjennomstrømming i valglokalene, det vil si at det er mindre aksept for kødannelser i dag enn det var tidligere. Kapasiteten i valglokalene blir derfor en kritisk faktor som må tas alvorlig.

I land der velgeren enten stemmer på en enkelt kandidat eller på et parti, vil det sannsynligvis ikke bety noe for tidsforbruket om stemmen avgis på papir eller elektronisk. Men desto flere valg- eller rettemuligheter velgeren har, desto mer funksjonalitet må bygges inn i de elektroniske løsningene, og det er all grunn til å tro at velgeren dermed vil bruke lengre tid foran maskinen for å prøve ut mulighetene før stemmen endelig avgis. Denne antagelsen bygger blant annet på erfaringene fra forsøkene med valgomater ved kommunestyrevalget i Oslo i 2003. Det ble ikke foretatt særskilte tidsstudier i forbindelse med forsøket, men tilbakemeldinger og observasjoner foretatt i Oslo kommune tyder på at velgerne brukte lengre tid for å avgi stemme ved bruk av valgomat enn hva som er normalt ved tradisjonell stemmegivning.[55]

De tidsobservasjonene som ble gjort i 2003 indikerte et gjennomsnittlig tidsforbruk på 3 minutter pr velger. Med et slikt gjennomsnittlig tidsforbruk vil en valgomat i løpet av en valgdag på totalt 11 timer ha en teoretisk kapasitet på 220 velgere. Da velgertilstrømningen er ujevn med størst tilstrømming mellom kl 16.00 og 20.00, må et valglokale som utelukkende tilbyr stemmegivning med valgomat ha betydelig flere valgomater enn hva denne teoretiske kapasiteten skulle tilsi. En valgomatløsning vi følgelig, i tillegg til behov for investering i

[55] Oslo kommune gjennomførte i forbindelse med kommunestyrevalget i 2003 en brukerundersøkelse med to ulike teknologiske løsninger for elektronisk stemmegivning. I tillegg til selve testen av utstyret ble det også foretatt korte, stikkprøvemessige tidsobservasjoner for å få et inntrykk av velgernes tidsforbruk.

selve utstyret, innebære et behov for flere stemmeavlukker, større valglokaler og muligens også økt bemanning, og derav følgende økte kostnader.

Spesialutviklet utstyr

Som nevnt over ble det benyttet spesialutviklede dataløsninger med pekeskjerm i forbindelse med forsøkene i 2003. Pekeskjermer brukes i dag i mange sammenhenger, eksempelvis er de i stor grad tatt i bruk i forbindelse med innsjekking på flyplasser, der passasjerene foretar handlinger ved å berøre skjermen etter de instruksjoner som gis. Teknologien har sin fordel i den selvforklarende fremgangsmåten og den enkle funksjonaliteten ved at man etter anvisninger berører felt på selve skjermen. Dette bekreftes av tilbakemeldinger i forbindelse med forsøkene i 2003, der det gikk fram at velgerne var positive til løsninger med valgomat med pekeskjermteknologi.

Når det gjelder investering i utstyret til valglokalene, er dette svært vanskelig å estimere. Det må foretas mer detaljerte analyser og eventuelt en prekvalifisering mot utvalgte leverandører før man kan si noe mer presist om dette. I forbindelse med forsøkene i 2003 ble det antydet at en stemmegivningsenhet kostet om lag kr 30 000. Med en prisutvikling på datautstyr slik vi kjenner den, vil det samme utstyret sannsynligvis være langt rimeligere i dag. Hvis man i Norge skulle gjennomføre valg ved hjelp av en slik løsning på bred basis ville det likevel være behov for vesentlige investeringer. Det vil også påløpe kostnader til tilrigging, nedrigging, pakking og lagring av utstyret mellom valg, dette vil kunne utgjøre store beløp. Hvis utstyret skal koples opp med linje til en sentral opptellingsenhet, vil det påløpe ekstra kostnader til etablering av linjer.

Det er vanskelig å vurdere levetiden på utstyret, men man må anta at investeringen vil kunne fordeles over noen valg. Normalt er det relativt kort avskrivningstid på datautstyr.

Med begrenset bruksfrekvens knyttet til valg bare annet hvert år er det dessuten usikkert om det vil finnes leverandører som vil anse det som lønnsomt å stå for utleie.

Standard datautstyr

De vurderingene som er foretatt over i forbindelse med bruk av spesialutviklet utstyr vil også gjelde i forhold til ordinære datamaskin-løsninger. Utgiftene pr. stemmegivningsenhet vil med bruk av standard datautstyr sannsynligvis bli redusert, men slikt utstyr er pr. i dag normalt ikke utstyrt med pekeskjermer. Bruk av utstyr og programvare som baserer seg på tastatur og mus vil ikke være like brukervennlig som pekeskjerm. Dette medfører at velgerne vil bruke enda lenger tid ved maskinen. Da løsningen ikke er utprøvd i Norge basert på gjeldende bestemmelser i norsk valglovgivning, er det imidlertid vanskelig å anslå konkret hvor lang tid velgeren vil bruke, dermed også definere behovet for antall enheter. Det er imidlertid ikke urimelig å anta at velgeren fort vi bruke dobbelt så lang tid foran maskinen i forhold til tradisjonell valghandling med stemmesedler i stemmeavlukker. Med andre ord vil det være behov for å doble antall avlukker. Et stort behov for økt bemanning i tillegg til investering i utstyr vil medføre at denne løsningen ikke blir vesentlig rimeligere enn bruk av spesialutviklet utstyr.

De samme vurderinger om avskrivning som er gjort i forbindelse med pekeskjerm vil også gjelde for bruk av tradisjonell personlig datamaskin. Man kan imidlertid tenke seg at behovet for personlige datamaskiner i forbindelse med valg kan koordineres med kommunenes generelle behov for fornyelse av sine datamaskiner. Dette antas å være en mulig løsning i mindre kommuner med sentralt innkjøp og distribusjon. I store kommuner med store selvstendige enheter vil dette være en svært vanskelig koordineringsoppgave særlig sett i

sammenheng med det store behovet man ville hatt i forhold til valggjennomføringen. Det vil også være vanskelig for kommunene å ta et større antall personlige datamaskiner ut av ordinær drift og stille disse til disposisjon til valggjennomføringen uten at dette får konsekvenser for kommunens øvrige drift.

Økonomisk vurdering
Elektronisk stemmegivning i kontrollerte omgivelser vil også medføre en del besparelser. Blant annet vil utgifter til stemmesedler bli redusert. I tillegg vil det foreligge muligheter for bemanningsreduksjon i forbindelse med enkelte oppgaver i opptellingsprosessen. Foreløpig opptelling i valglokalene for stemmer avgitt elektronisk vil være oppgaver som utgår. Det vil også kunne beregnes besparelser vedrørende utgifter tilknyttet optisk lesing av stemmesedler.

Elektronisk stemmegivning i valglokaler, enten man bruker pekeskjerm eller ordinær personlig datamaskin vil kreve investeringer i utstyr. Da elektronisk stemmegivning tar lengre tid enn stemmegivning etter tradisjonelle metoder vil man måtte utstyre valglokalene med flere elektroniske avlukker, eventuelt etablere flere valglokaler. Det vil påløpe store utgifter til opprigging, nedrigging og lagring av utstyr. Valglokaler må bemannes, og bemanning til bistand og kontroll må økes. Hvordan disse utgiftsøkningene slår ut i forhold til de innsparingsmuligheter som er redegjort for over, vil avhenge av hvordan den enkelte kommune har mulighet til å gjennomføre valget. Elektronisk stemmegivning i valglokaler vil gi nye og endrede utgifter, og ikke nødvendigvis gi en økonomisk effektiviseringsgevinst.

7.4.2 Elektronisk stemmegivning i ukontrollerte omgivelser

Elektronisk stemmegivning i ukontrollerte omgivelser er stemmegivning via for eksempel mobiltelefon, Internett, TV, elektroniske terminaler eller lignende. Slik stemmegivning vil kreve at det offentlige tilrettelegger for stemmegivning ved at nødvendige datasystemer for avlevering av den enkeltes stemme utvikles og gjøres tilgjengelig for velgeren samtidig som det utvikles systemer for mottak og registrering av stemmegivninger (registrering av velgere som har avgitt stemme – manntallsfunksjon) og avgitte stemmer. I sin ytterste konsekvens vil kommunene ikke lenger ha behov for å opprette valglokaler og vil få vesentlige lavere utgifter til bemanning og utstyr. Da velgeren selv vil inneha det nødvendige utstyr for å avgi sin stemme, vil den vesentligste del av utgiftene til denne delen av valggjennomføringen overføres fra kommunene til et allerede eksisterende privat system. I hovedsak vil alt utstyr være eid av privatpersoner (personlig datamaskin, mobiltelefoner, TV etc.) eller private aktører (elektroniske terminaler). Selv om man i Norge har en meget god dekning av nødvendig teknisk utstyr (personlig datamaskin, mobiltelefoner, TV etc.), vil man måtte ta hensyn til for at noen velgere ikke har slik tilgang. Det må derfor også settes opp mulighet til å benytte offentlig utstyr der velgeren kan få avgitt sin stemme. Utgifter til elektronisk manntall, system for elektronisk stemmegivning, elektronisk opptelling, offentlig utplassert utstyr for å avgi sin stemme, informasjonstiltak/opplæring og noe bemanning vil fortsatt være offentlige utgifter.

Det knytter seg stor usikkerhet til kostnadene i forbindelse med elektronisk stemmegivning i ukontrollerte omgivelser. Hovedkostnaden vil her være systemutvikling og implementering. Kostnader forbundet med dette er det vanskelig å anslå uten at man har en konkret kravspesifikasjon som kan prøves i markedet. Kostnadsnivået vil blant annet være avhengig av hvor kompliserte løsninger man ønsker å velge i forhold til for eksempel sikkerhetsnivå.

Stemmegivning i ukontrollerte omgivelser vil, i tillegg til de effektiviseringsgevinster som følger av elektronisk stemmegivning i kontrollerte omgivelser, redusere behovet for valglokaler og bemanning til et meget beskjedent nivå. Dette alternativet vil kunne gi store effektiviseringsgevinster i forbindelse med til bemanning, utstyr og materiell.

7.5 Administrative hensyn

Forberedelse og gjennomføring av tradisjonelt valg i Norge krever i utgangspunktet ingen særskilt formell kompetanse. Det kreves imidlertid kunnskap om og innsikt i de forberedelser og det arbeid som skal gjennomføres frem til endelig valgoppgjør. De formelle kravene skal ivaretas ved å følge valglovens bestemmelser og veiledninger som er gitt av KRD. Administrasjon og gjennomføring av valg krever kunnskap om prosedyrer, rutiner og geografi i den enkelte kommune. Det kreves evne til strukturert arbeid, nøyaktighet og gjennomføringsevne.

Valgloven definerer valgstyrets ansvar i den enkelte kommune. Valgstyret fastsetter kommunens kretsinndeling og hvor stemmegivningen skal foregå. Valgstyret godkjenner listeforslag ved kommunestyrevalg. Ved forhåndsstemmegivningen oppnevner valgstyret stemmemottakere. I de tilfeller kommunen er inndelt i flere kretser, velges det stemmestyrer som administrerer valget på det enkelte stemmested på valgdagen. Valgstyret skal føre kommunens manntall og skal for øvrig overvåke alle deler av valghandlingen.

Selv om valgloven beskriver en tradisjonell, papirbasert valggjennomføring, er det allerede stadig flere kommuner som støtter seg på ulike teknologiske løsninger i arbeidet.

En videre utvikling av teknologiske løsninger vil for kommunene bidra til å forenkle og effektivisere de omfattende manuelle prosedyrene valget i dag består av og redusere de manuelle feilkildene. Teknologien vil også kunne bidra til at man får til et valgoppgjør som er raskere tilgjengelig, med et økt presisjonsnivå. Moderne teknologi vil dessuten kunne bidra til bedre løsninger for velgere som har behov for veiledning på et annet språk enn norsk og velgere med synshemming. Ved for eksempel å tillate stemmegivning over Internett vil valghandlingen dessuten bli bedre tilgjengelig for bevegelseshemmede.

Bruk av moderne teknologi er imidlertid mer kompetansekrevende enn tradisjonelle metoder. Med den norske kommunestrukturen med mange små kommuner, er det ikke sikkert at kommunene innehar tilstrekkelig kompetanse og kapasitet til å ta i bruk teknologien innenfor et såpass begrenset saksområde som valg er. Dette er bekymringsfullt, særlig hvis omfanget av elektroniske løsninger i forbindelse med valg utvides. Det er derfor en viss risiko for at man overlater til leverandørene å fastsette premissene for løsningene og selve valggjennomføringen. I lys av dette er det viktig at det på nasjonalt nivå tilrettelegges for en overordnet koordinering og styring når det gjelder bruk av teknologi ved elektronisk stemmegivning. Staten bør ha ansvaret for utarbeidelse av kravspesifikasjoner og tilrettelegge for sertifiseringsordninger.

I dag brukes det store ressurser på å gjennomføre valgene i Norge. Det bør være en forutsetning at bruk av moderne teknologi reduserer ressursbehovet og ikke øker det. Her viser vi til beregningene av kostnadsfordelingen, der bemanningskostnadene utgjør omtrent 50 % av de totale utgifter til valg. Det langsiktige målet som arbeidsgruppen skisserer, vil være i samsvar med et ønske om å redusere ressursbruken. Forsøksvirksomheten vil imidlertid innebære at man både kompliserer den administrative gjennomføringen og øker

ressursbruken fordi man gjør dette i tillegg til ordinær valggjennomføring. Man kan ikke regne med at kommunene kan ta på seg økte utgifter til å drive forsøk av den typen vi snakker om her. Ønsker man å gjennomføre planmessige og målrettede forsøk, mener arbeidsgruppen at disse også må finansieres av staten.

Arbeidsgruppen forutsetter at elektronisk stemmegivning i ukontrollerte omgivelser må knyttes til muligheten til stemme på nytt, dette for å ivareta kravet om hemmelig valg og forhindre muligheten for utilbørlig påvirkning. Å åpne for muligheten til å stemme flere ganger krever tradisjonelt omfattende administrative prosedyrer for å sikre at velgeren kun får avgitt én godkjent stemme. Så lenge muligheten for å stemme flere ganger avgrenses til kun å gjelde stemmer avgitt elektronisk i ukontrollerte omgivelser, vil de elektroniske løsningene automatisk sørge for at bare den siste avgitte stemmen havner i stemmeurnen. Dersom en velger som har stemt elektronisk ønsker å stemme om igjen på selve valgtinget, må valgfunksjonæren sørge for at det blir sendt en melding til det elektroniske systemet om at velgerens elektroniske stemmer skal annulleres. Arbeidsgruppen har ikke tatt stilling til nøyaktig hvordan dette skal gjøres, men antar at den ekstra arbeidsbelastningen for valgfunksjonærene vil være minimal, ut fra en antagelse om at det ikke vil være mange velgere som vil benytte seg av denne muligheten

7.6 Anbefaling

Elektronisk stemmegivning vil ha en rekke administrative fordeler både ved at presisjonen på valgoppgjøret bedres og at de endelige resultatene vil foreligge raskere. Elektronisk stemmegivning vil også bidra til å redusere en rekke manuelle prosedyrer og kontrollrutiner som i dag er ressurskrevende. Elektronisk stemmegivning i kontrollerte omgivelser vil imidlertid utløse nye kostnader i form av investeringer i nytt datautstyr, riggkostnader samt behov for flere avlukker, eventuelt lokaler med større bemanning enn ved tradisjonelle valg. Arbeidsgruppen antar at det først er ved elektronisk stemmegivning i ukontrollerte omgivelser at man kan forvente å oppnå økonomiske besparelser.

Det vil si at kostnadsnivået vil være minst like stort som i dag så lenge man opprettholder stemmegivning med papirstemmesedler i valglokale. Det er først når antallet velgere som avgir stemmer manuelt synker til fordel for velgere som avgir elektroniske stemmer i fase 1 ved hjelp av eget utstyr i ukontrollerte omgivelser en over tid vil kunne se reduksjon i kostnadsnivå og ressursbehov.

8 Tekniske utfordringer og mulige løsninger

Dette kapitlet går inn på følgende punkter i mandatet:

- gi en oversikt/utredning av ulike måter/system å avgi stemme elektronisk gjennom ulike typer kanaler (Internett, pekeskjerm, SMS, digital-tv m.m.) (pkt. 2),
- peke på fordeler og ulemper ved de ulike systemene/kanalene (pkt. 3),
- gi en vurdering av disse ut fra brukervennlighet og sikkerhet (pkt. 4),
- drøfte og vurdere om det bør tillates elektronisk stemmegivning ved hjelp av Internett-teknologi, både i og utenfor valglokalene (pkt. 5),
- vurdere løsninger for identifisering av velger i forbindelse med elektronisk stemmegivning (smartkort, id-kort e.l.) (pkt. 6),
- vurdere om det bør innføres verifikasjonsløsninger i systemene, og i tilfelle komme med forslag til hvordan slike løsninger kan legges opp (pkt. 9),
- vurdere problematikken åpen kildekode (pkt. 10),
- vurdere ev. bruk av et landsdekkende elektronisk manntall, betydningen i forhold til et system der stemmer avgis elektronisk (pkt. 11).

8.1 Premisser for tekniske løsninger

La oss oppsummere de premissene som etter diskusjonen i de foregående kapitlene må ligge til grunn for de tekniske løsningene.

Tofasevalg
Valgene i Norge skal fortsatt gjennomføres i to faser (kjent som forhåndsstemmegivning og valgtingsstemmegivning), der den første fasen omfatter en stemmeperiode på flere dager, kanskje flere uker eller måneder, og den andre fasen en (eventuelt to) valgdag(er). Mellom de to fasene må det være et tidsopphold som må fastlegges senere.

Elektronisk stemmegivning kun i fase 1
Arbeidsgruppens undersøkelser viser at innføring av elektronisk stemmegivning i kontrollerte omgivelser vil være meget kostbart og gi begrensede gevinster. Det vil være mulig å gjennomføre valgoppgjøret raskere og med mindre bemanning, men kostnadene til utstyr og til håndteringen av dette vil bli vesentlig høyere enn dagens. Det er først i det tilfelle der løsningen bygger på tekniske komponenter som eies og administreres av velgeren selv at man kan se potensialet for innsparinger i valgbudsjettet. Dessuten er det et poeng å beholde et velprøvd tradisjonelt system i fase 2 som sikkerhetsnett i tilfelle man skulle få problemer med elektroniske løsninger i fase 1.

Ingen endringer i prosedyrene for stemmegivningen i fase 2 (på valgtinget)
Velgere som fortsatt ønsker å stemme på tradisjonell måte, skal fortsatt kunne gjøre dette, og på nøyaktig samme måte som før. Elektroniske løsninger må altså utformes slik at de ikke påvirker gjennomføringen av et tradisjonelt valg med papirstemmesedler.

Valg over flere kanaler
De tekniske løsningene må kunne tillate at valg i fase 1 skal kunne gjennomføres over flere kanaler, eksempelvis Internett, mobiltelefon (SMS) og andre kanaler som kan komme i fremtiden.

Flergangsstemmegivning
Det skal være mulig å avgi elektronisk stemme flere ganger, men bare den stemmen som blir registrert sist blir godkjent og vil telle. I fase 2 kan det stemmes bare én gang. En stemme fra de kontrollerte omgivelser i fase 2 vil alltid gå foran eventuelle elektroniske stemmer fra ukontrollerte omgivelser fra fase 1. En elektronisk stemme fra en velger skal altså ikke godkjennes og legges i den elektroniske urnen før det er klarlagt at velgeren ikke har stemt på valgtinget. De som avgir stemme ved papirstemmesedler kan ikke avgi stemme på nytt verken i fase 1 eller fase 2.

Kompromisser må berøre e-velgeren, ikke velgere som stemmer på tradisjonell måte
Hvis det er nødvendig å inngå kompromisser med hensyn til velgernes rettigheter for å få etablert en elektronisk valgløsning, er det e-velgerne som skal berøres, ikke de som bruker papirstemmesedler.

Ved elektroniske valg må e-velgeren i større eller mindre grad gi fra seg personlige opplysninger til valgsystemet, opplysninger som i verste fall kan brukes til å avsløre velgerens identitet. Velgeren er dermed *nødt til å stole på* at systemet behandler disse opplysningene på en korrekt måte, og at det finnes tilfredsstillende sperrer mot å kunne koble innholdet av stemmen med velgeren. Situasjonen er helt analog med manuell forhånds- eller fremmedstemmegivning med en ytre konvolutt som identifiserer velgeren – velgeren er da nødt til å stole på at selve stemmen skilles fra den ytre konvolutten på en måte som ivaretar anonymiteten.

Arbeidsgruppen er imidlertid av den oppfatning at det er fornuftig å akseptere en noe høyere risiko for at velgerens identitet kan bli koblet med stemmens innhold, hvis dette kan høyne sikkerheten for at velgernes stemmer blir korrekt registrert.

Utforming av brukergrensesnittet
I Europarådets anbefaling legges det vekt på at brukergrensesnittet skal ha en høy kvalitet – se Europarådets anbefaling punkt 47 – 50. Dette innebærer blant annet at ved utformingen av brukergrensesnittet må det legges stor vekt på at presentasjonen er nøytral i forhold til valgmulighetene. Stemmegivning ved politiske valg er en oppgave som brukerne utfører med lange mellomrom, derfor må det stilles store krav til brukervennlighet. Brukergrensesnittet bør baseres på WAI-kriteriene[56] som er et sett med retningslinjer for tilrettelegging av nettsideløsninger for funksjonshemmede.

De tekniske løsningene må oppfylle kravene i Europarådets anbefaling
I Europarådets anbefaling Vedlegg III er satt opp en rekke tekniske krav til elektroniske stemmegivningssystemer, og arbeidsgruppen tar som gitt at løsninger må oppfylle disse kravene. I dette kapitlet går vi derfor kun inn på de mest relevante kravene, sett i sammenheng med de øvrige premissene for en teknisk løsning.

8.2 Hva er utfordringene?

Bruk av elektroniske løsninger i stemmegivningen har sine uomtvistelige fordeler, som høy tilgjengelighet, enkelhet i valghandlingen og effektiv opptelling av stemmer. Men elektroniske løsninger bringer også med seg en lang rekke utfordringer. Med utgangspunkt i

[56] Se W3C Web Accessibility Initiative på http://www.w3.org/WAI/

kravene om at valg skal være frie og hemmelige og prinsippet om ”én velger, én stemme” får vi følgende fundamentale utfordringer:

- Sikre at velgeren får avgitt stemme.
- Sikre at ikke velgeren får avgitt mer enn en godkjent stemme.
- Sikre at stemmen holdes hemmelig ved at den ikke kan kobles til velgeren.
- Sikre at stemmen ikke endres eller forfalskes.
- Sikre at avgitte stemmer ikke går tapt.
- Sikre at det ikke introduseres stemmer som ingen velger har avgitt.

Valggjennomføringen i Norge har tradisjonelt en meget høy grad av tillit hos velgerne. Den tradisjonelle valggjennomføringen basert på papirstemmesedler er prinsipielt sett så enkel at alle og enhver kan observere og forstå hva som foregår, slik at valget er åpent for lekmannskontroll. Så snart velgernes stemmer leses og behandles av en datamaskin, må denne lekmannskontrollen erstattes av en tillit til ekspertene – de som har utformet, programmert, testet, kontrollert og sertifisert systemet. Den manglende transparens i valggjennomføringen og bortfallet av en reell lekmannskontroll gjør at det vil kunne reises spørsmål om valgets integritet, og tilliten kan undermineres.

Innføring av ny teknologi i valghandlingen introduserer nye trusler. Selv om dagens manuelle løsninger ikke kan garanteres å være fullstendig uten feil, så er truslene rettet mot manuelle systemer av en slik art at det ville kreve mange uavhengige feil eller et stort antall utro tjenere for å kunne påvirke valgutfallet. I en elektronisk løsning åpnes det for at en enkelt person med tilstrekkelige tilgangsrettigheter kan gjennomføre små endringer i systemløsningen som kan påvirke et stort antall stemmer. Maskinell lagring av avgitte stemmer kan også åpne for omfattende manipulering.

Et elektronisk stemmegivningssystem består i prinsippet av:

- Stemmegivningsklienten – den datamaskinen som velgeren bruker for å kunne avgi stemme.
- Stemmemottakstjeneren – en eller flere datamaskiner som tar i mot og videresender velgernes stemmer.
- En datalinje eller et datanett mellom stemmegivningsklienten og stemmemottakstjeneren.
- Et bakenforliggende system med en eller flere maskiner som tar i mot stemmene fra stemmemottakstjeneren og viderebehandler dem.

Generelt er det slik at det er umulig å garantere at et elektronisk system er fullstendig feilfritt (Schneier 2004). Spørsmålet er hvilket sikkerhetsnivå som er akseptabelt i forbindelse med ulike anvendelser, og hvilke mottiltak som kan settes opp dersom noe skulle svikte. Sikkerhetsproblemene i forbindelse med bruk av Internett er kjent og er belyst i et stort antall kilder. I valgsammenheng finnes det et stort antall evalueringer og sikkerhetsanalyser både for rene Internett-løsninger[57] og for valgomater (spesielt elektronisk utstyr for stemmegivning i

[57] Department of Defence i USA utarbeidet en forsøksløsning for stemmegivning over Internett som var ment til bruk for enkelte militære stasjonert i utlandet ved det amerikanske presidentvalget i 2004. Løsningen ble evaluert av en ekspertgruppe høsten 2003. Fire av ekspertgruppens medlemmer publiserte en egen evalueringsrapport (Jefferson et.al 2004) der de konkluderte med at den utviklede løsningen ikke kunne anbefales. Delgruppens rapport trekker frem angrep rettet mot velgerens datamaskin, sårbarheten i Internett og bruken av spesialutviklet, leverandørkontrollert programvare på tjenerne som de største truslene. Gruppen anbefaler ikke å gå videre med forsøket, og systemet ble da heller ikke tatt i bruk ved valget i 2005. Konklusjonene fra evalueringsrapporten er interessante og relevante, men det er grunn til å understreke at evalueringen gjelder en spesiell versjon av Internettstemmegivning. Det er mulig å bygge løsninger med andre karakteristika og sikkerhetsnivåer.

valglokalet)[58]. Innføring av IT-systemer generelt medfører risiko for programmeringsfeil og teknisk sammenbrudd på sentrale komponenter. Innføring av ny teknologi åpner også for rene brukerfeil som følge av manglende bevissthet eller forståelse.

I vedlegg B oppsummerer vi de viktigste sikkerhetsutfordringene forbundet med elektronisk stemmegivning i ukontrollerte omgivelser. Andre løsninger for elektronisk stemmegivning anses å være vesentlig mindre utsatte for fusk og feil.

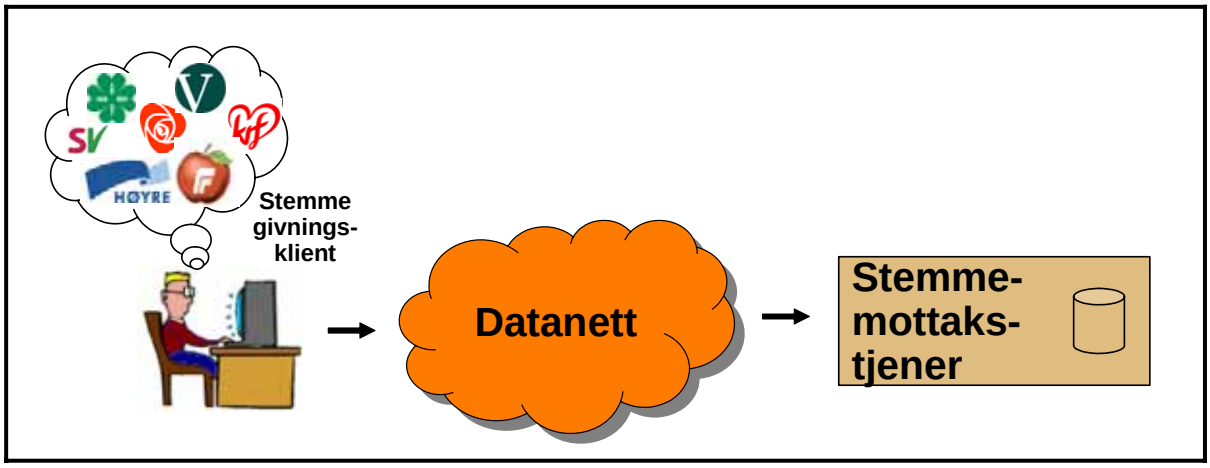
De største tekniske utfordringene ved innføring av elektroniske valg anses å være:

1. Ondsinnet programvare på stemmegivningsklienten.
2. Generell sårbarhet i datanettene, spesielt Internett.
3. Manglende mulighet for omtelling.
4. Innsideangrep, spesielt på stemmemottakstjeneren og de bakenforliggende systemene, med mål å sabotere eller manipulere valgresultatet.

I den videre diskusjon om løsninger er sikkerhet et sentralt aspekt. Vi vil fokuseres spesielt på tiltak som kan beskytte løsningen mot de fire største sikkerhetsutfordringene.

8.3 Løsningsalternativer

Vi skal i dette avsnittet drøfte ulike elektroniske løsninger for selve stemmegivningen, se figur 8-1. Her kan stemmegivningsklienten være alt fra en større datamaskin til en håndholdt enhet som for eksempel en mobiltelefon. Stemmegivningsklienten kan stilles til disposisjon for velgeren på offentlige kontorer og på andre hensiktsmessige steder, eller den kan være en maskin som velgeren disponerer, i yrket eller privat. Stemmemottakstjeneren befinner seg i et sikret miljø hos valgmyndighetene. Det kan være mange slike tjenermaskiner i aktivitet under et valg. Stemmegivningsklient og stemmemottakstjener er forbundet med hverandre gjennom et datanett, som kan være alt fra et lukket lokalnett til det åpne Internett.



Figur 8.1: Stemmegivningsklient og stemmemottakstjener

Vi står her overfor det problemet at det i ukontrollerte omgivelser er umulig å etablere en garantert 100 % sikker overføringskanal ved hjelp av det datatekniske utstyret som vi i dag finner på arbeidsplassene og i hjemmene. Allikevel gjennomfører vi et utall sikkerhetskritiske transaksjoner, som eksempelvis nettbanktransaksjoner, med slikt utstyr. Dette kan vi tillate

[58] Se Rebecca Mercuris publikasjoner om e-valgsløsninger på http://www.notablesoftware.com/evote.html

oss fordi det finnes kontrollmuligheter (vi kan se i kontoutskriften at alt stemmer), og fordi – i nettbanktilfellet – bankene bærer risikoen for eventuelle feil som ikke skyldes nettbankbrukeren. Slike kontrollmuligheter er det ikke mulig å etablere for elektroniske stemmer, fordi innholdet av stemmen skal være hemmelig. Et mulig alternativ er da å duplisere stemmen, slik at vi kan falle tilbake på kopien dersom det skulle reises tvil om behandlingen av originalstemmen. Problemet med dette er at tilstrekkelig sikkerhet i overføringen da må garanteres fra det stedet der velgeren kan konstatere at stemmen er korrekt til det stedet der stemmen kan kopieres. Nettopp her ligger det springende punkt: Hvor høy er "tilstrekkelig sikkerhet", og hvordan skal vi oppnå denne?

8.3.1 Elektroniske løsninger i kontrollerte omgivelser

Ved elektroniske løsninger i kontrollerte omgivelser er det mulig for valgmyndighetene å ha full kontroll over den maskin- og programvaren som benyttes, og datakommunikasjonen kan skje gjennom sikrede datanett – se figur 8-2. Dessuten er det mulig å produsere en lokal logg (for eksempel i form av en papirkopi) med de avgitte stemmene, og utstyret kan utformes slik at hver enkelt velger kan verifisere sin egen stemme. Dermed er det ved behov mulig å etterprøve at stemmene er blitt behandlet korrekt (se også avsnitt 8.7.4). Da er det heller ikke nødvendig å forlange en absolutt sikkerhet for overføringen av stemmer til stemmemottakstjeneren.

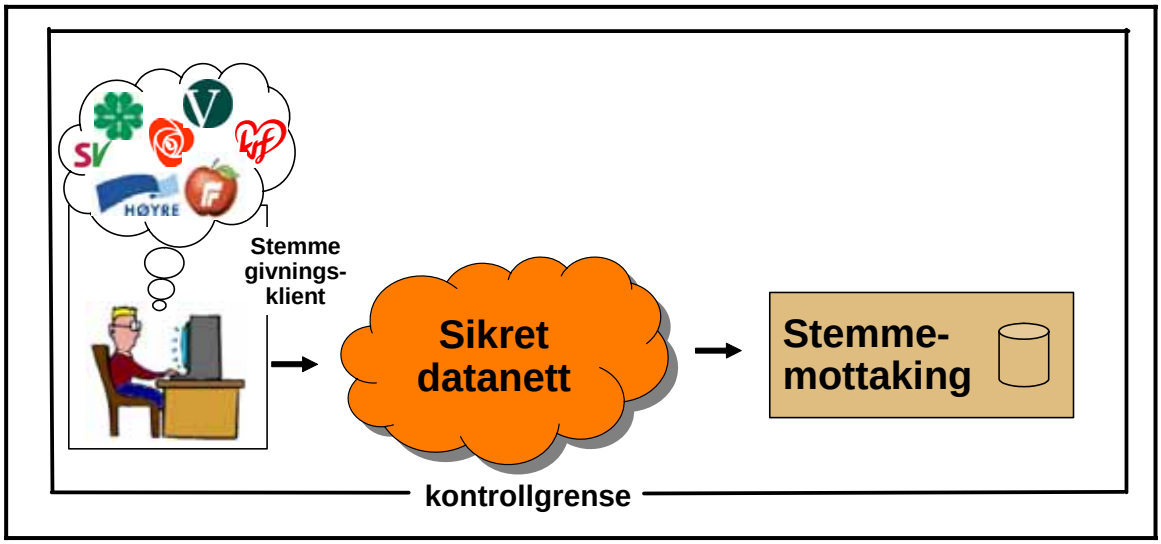
Som stemmegivningsklient kommer fortrinnsvis to løsninger på tale, enten en vanlig personlig datamaskin eller en maskin som er spesialbygd for formålet (såkalt valgomat).

Personlig datamaskin
Som stemmegivningsklient er en personlig datamaskin unødvendig kompleks, og dermed også sikkerhetsmessig betenkelig. Fordelen med den er at den er masseprodusert og dermed billig, det er enkelt å få tak i reserveutstyr, og den kan ev. brukes til andre oppgaver mellom valgene.

Selv om det er en krevende oppgave, så er det i kontrollerte omgivelser ikke umulig å teste og kontrollere systemet så vidt grundig at man kan ha tillit til at det fungerer etter forutsetningene. Dette forutsetter imidlertid at systemløsningen er bygget på en gjennomtenkt systemarkitektur som kan verifiseres. Ved å bruke maskiner med nyinstallert operativsystem kan man også være rimelig sikker på at de ikke inneholder ondsinnet programvare. Eventuelt kan man starte opp maskinen fra en spesiell valg-CD-ROM (se avsnitt 8.3.2).

Valgomat
I kontrollerte omgivelser er spesialbygde stemmemaskiner, såkalte valgomater, et mulig alternativ til bruk av vanlig personlig datamaskin. En valgomat er typisk en datamaskin med spesialtilpasset operativsystem og programvare. Den betjenes vanligvis ved å trykke med fingeren direkte på en trykkfølsom skjerm. Den mest aktuelle varianten vil ha en nettverksforbindelse til en stemmelagringstjener, slik at de avlagte stemmene ikke lagres i maskinen, men sentralt.

Fordelene med slike valgomater er at de er spesialtilpasset for stemmegivning, og at mengden potensielt distraherende momenter er liten i forhold til stemmegivning på vanlig personlig datamaskin med nettleser. Siden all maskin- og programvare er under leverandørens kontroll, er det også relativt lett å verifisere at maskinen ikke er modifisert, angrepet av virus etc.



Figur 8.2: Stemmegivning i kontrollerte omgivelser

Det er dessuten mulig å bygge en valgomatlignende maskin uten å måtte bruke spesielle programvareløsninger. Man kan koble en pekeskjerm eller liknende mot en ordinær personlig datamaskin – fordelen med å slippe mus og tastatur er altså ikke forbeholdt valgomaten. Skillet mellom valgomat og personlig datamaskin er dermed ikke absolutt.

Arbeidsgruppen mener at man bør legge vekt på å bruke de samme programvareløsningene – så langt det er hensiktsmessig – på alle teknologiske plattformer og i både kontrollerte og ukontrollerte omgivelser. Arbeidsgruppen anser derfor en valgomat med spesialutviklet programvare som en blindvei mot en varig løsning, fordi teknologien ikke uten videre kan utnyttes i andre kanaler.

8.3.2 Elektroniske løsninger i ukontrollerte omgivelser

Overgang til stemmegivning i ukontrollerte omgivelser introduserer ikke bare betenkeligheter av demokratisk natur (jf. kapittel 5), men også betydelig større sikkerhetsutfordringer. I ukontrollerte omgivelser bruker velgeren en stemmegivningsklient som valgmyndighetene har liten eller ingen kontroll over, og datakommunikasjonen skjer over offentlige datanett, eksempelvis Internett – se figur 8-3. Vi åpner dermed for angrep utenfra og introduserer en kompleksitet som gjør det svært vanskelig å kunne garantere at valgsystemet til enhver tid fungerer som det skal. Selv en lang serie med vellykkede tester eller reelle valggjennomføringer beviser ingenting, fordi angriperen først kan slå til neste gang. Og fordi vi har et usikkert system mellom velgeren og resten av valgsystemet, er det spesielt vanskelig å sikre at alle avgitte stemmer logges på en sikker måte (se avsnitt 8.5.2).

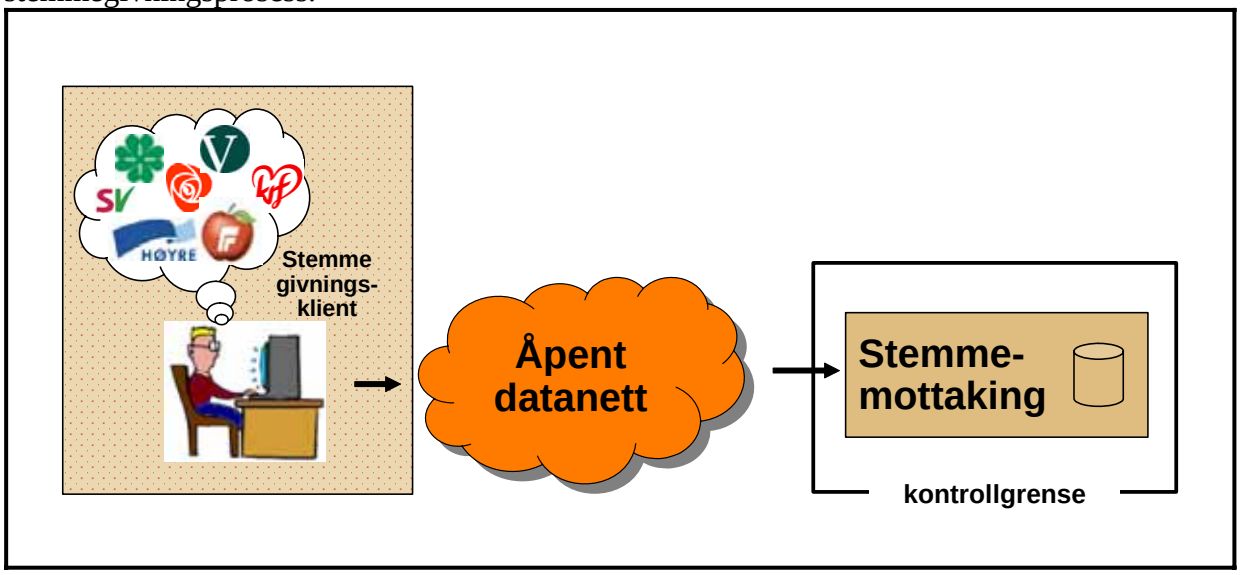
De ekstra utfordringene i ukontrollerte omgivelser kan i prinsippet møtes på to ulike måter:

- Finne fram til alternativt teknisk utstyr hos velgeren med vesentlig høyere sikkerhet enn med dagens utstyr, og bruke sikrere datakommunikasjonskanaler.
- Etablere kommunikasjon mellom velger og valgsystem over parallelle, teknisk uavhengige kanaler, slik at velgeren kan bekrefte eller få bekreftet stemmegivningen.

Dagens teknologi er beheftet med mange svakheter som kan utnyttes for valgfusk. Siden det er et generelt behov for sikre løsninger også i ukontrollerte omgivelser, og det ikke bare i forbindelse med elektronisk stemmegivning, er det all grunn til å tro at problemet en gang i fremtiden vil bli løst ved at det kommer på markedet sikrede elektroniske enheter som ikke

kan "tukles med" ("tamper-free devices"), som enten vil bli benyttet som selvstendige enheter koblet til Internett eller mobiltelefonnettet, eller som tilleggsenheter til personlige datamaskiner og mobiltelefoner.

Inntil vi kommer så langt, er det en mulig løsning å la velgeren utføre stemmegivningen to ganger via to teknisk ulike og uavhengige kanaler (for eksempel personlig datamaskin tilkoblet Internett og mobiltelefon), og la stemmemottakstjeneren godkjenne resultatet bare hvis de to stemmegivningene stemmer overens. Tankegangen her er at sannsynligheten for at samme feil skal oppstå i to helt uavhengige kanaler, er praktisk talt lik null. Imidlertid er det vel tvilsomt om det store flertallet av velgere vil akseptere en så vidt omstendelig stemmegivningsprosess.



Figur 8.3: Stemmegivning i ukontrollerte omgivelser

Personlig datamaskin koblet til Internett
Med ”dagens teknologi” tenker vi fortrinnsvis på en personlig datamaskin tilknyttet Internett. Her er det svakeste leddet uten tvil brukerens personlige datamaskin. Det er i dag altfor lett, uten brukerens vitende, å besmitte slike maskiner med ondsinnet programvare i form av virus, ormer og ”root-kits”. Bruk av antivirusprogrammer og lignende gir dessverre ingen garanti for at all ondsinnet programvare er fjernet.

En annen sårbarhet i elektroniske systemer i ukontrollerte omgivelser oppstår gjennom at stemmemottakstjeneren er tilknyttet et åpent tilgjengelig datanett. Dermed er maskinen utsatt for "hacker-angrep" av ulike typer. Mye av dette går det an å gardere seg mot ved å overvåke trafikken inn mot maskinen. En type angrep som det imidlertid er vanskeligere å gardere seg mot, er såkalte tjenestenekt-angrep ("denial-of-service-attacks"), der maskinen blir angrepet utenfra ved å belaste den med et høyt antall uvedkommende henvendelser. Et opplagt mottiltak er å ha flere stemmemottakstjenere i systemet – å slå ut alle er mye vanskeligere enn å slå ut bare en. Man kan også oppfordre velgerne til å stemme i god tid før fristen går ut for fase 1, slik at det er mulig å forsøke om igjen senere hvis man ikke får kontakt med valgtjeneren. Skulle alt slå feil, har man stadig muligheten for tradisjonell papirstemmegivning i fase 2.

Duplisering av systemer og dataoverføringskanaler kan gi en høy grad av sikkerhet (Selker & Goler 2004). Det er imidlertid en del av systemet det er vanskelig å sikre på denne måten, nemlig behandlingen av dataene fra de er skrevet på tastaturet til de kommer fram på

skjermen. Et eksempel på ondsinnet programvare som er svært betenkelig i valgsammenheng, er programvare som snapper opp brukerens tastetrykk og modifiserer dem på en slik måte at alt ser tilforlatelig ut på skjermen, men at maskinen allikevel sender fra seg helt andre data enn den skulle ha gjort. Dette kan for eksempel brukes til å knytte maskinen opp til en falsk stemmemottakingstjener.

En mer detaljert analyse av de ulike typer trusler mot et Internettbasert valgsystem finnes i vedlegg B. Det finnes dessuten et bredt tilfang av litteratur som belyser svakhetene med hensyn til sikkerhet i dagens Internettarkitektur.

En moderne hjemmedatamaskin med sitt operativsystem, drivere og alle andre programmer er egentlig en altfor kompleks og generell type teknisk utstyr for å gjennomføre enkle, men sikkerhetskritiske transaksjoner, som for eksempel signering av dokumenter og stemmegivning ved valg. Derfor et det slett ikke utelukket at vi i fremtiden vil få se alternativt type utstyr for sikkerhetskritiske anvendelser. Disse kan tenkes å fungere helt uavhengig av hjemmedatamaskinen, men kan også tenkes å utformes som tilleggsutstyr til denne. Arbeidsgruppen vil imidlertid ikke gå inn for å utvikle slike løsninger utelukkende for bruk ved valg. Det må dreie seg om allmenne, utbredte løsninger som også brukes i andre anvendelser som har høye krav til sikkerhet.

Personlig datamaskin med spesialoperativsystem
En mellomløsning er å kjøre en vanlig personlig datamaskin med et eget, sikkerhetssertifisert operativsystem med begrenset funksjonalitet. Operativsystemet kan foreligge på en valg-CD-ROM.
Den største fordelen er at all programkode på CD-rom'en kan verifiseres, og at datamaskinens vanlige operativsystem ikke benyttes. Siden maskinen startes opp med et verifisert og godkjent operativsystem og ikke fra maskinens harddisk, unngår man å starte eventuelle spionprogrammer og lignende på brukerens maskin. Stemmegivningen blir da i prinsippet like sikker som i kontrollerte omgivelser.

For at brukeren skal slippe å konfigurere/installere systemet kreves det også at datamaskinen er koblet til Internett via nettverkskort med dynamisk tildeling av IP-adresser. Dette vil da typisk gjelde hjemmebrukere med ADSL-router. Det er også teknisk mulig at stemmegivningssystemet kan gjenkjenne modem/ISDN kort i maskinen og bruke dette til å koble opp mot et forhåndslagret telefonnummer som gir Internett-aksess kun til den aktuelle stemmemottakstjener.

Ulempene er først og fremst den tekniske kompleksiteten denne løsningen bygger på. Operativsystemet må være i stand til å starte opp og gjenkjenne en god del varianter av konfigurasjoner, hovedsakelig knyttet til hvilken type nettverk/modem/ISDN kommunikasjonskort som er brukt. Utstyr fra forskjellige produsenter trenger ulike støtteprogrammer (drivere) for å kunne kommunisere med stemmegivningssystemet. For å øke sikkerheten ytterligere, kan stemmegivningssystemet sette opp en sikker overføringskanal fra datamaskinen til stemmemottakstjeneren gjennom et i utgangspunktet usikkert nett som eksempelvis Internett (en "Virtual Privat Network"-forbindelse eller VPN-tunnel)

I kontrollerte omgivelser er en slik løsning absolutt gjennomførbar. I ukontrollerte omgivelser er løsningen av flere grunner neppe egnet for bruk i stor skala – den krever at brukeren behersker å starte opp maskinen med ulike operativsystemer, og det spesielle operativsystemet må ha drivere for de ulike varianter av nettilknytninger som kan være

aktuelle. Man må også ta med i vurderingene det støttebehovet som fort kan oppstå når hjemmevelgerne av en eller annen grunn snubler i et problem.

Digital/satellitt-tv
Ulike former for digital-TV kan brukes til å avgi stemme i ukontrollerte omgivelser. En forutsetning her er at det er en toveiskommunikasjon (dvs. en vei tilbake til stemmemottakstjeneren fra ”set-top”-boksen som er koblet til TV-apparatet, enten gjennom samme nett (kabel-TV) eller over for eksempel en telefonlinje (satellitt-TV). Stemmegivning kan da gjennomføres ved hjelp av utvidelser til menysystemet på "set-top”-boksen, og har en del av de samme karakteristika som valgomat-løsningen beskrevet tidligere.

I ”set-top”-boksen må det finnes programvare spesialtilpasset for valg. Boksene kjører egne operativsystemer, og stemmegivningsapplikasjonen må derfor utvikles spesielt for disse. Nye ”set-top”-bokser har Internett-tilknytning og egne nettlesere, og dersom boksens nettleser benyttes for å logge på det Internett-baserte stemmegivningssystemet, er det ingen prinsipielle forskjeller på stemmegivning over digital-TV og vanlig personlig datamaskin.

Det største ankepunktet mot teknologien er at utbredelsen av slikt utstyr forløpig er relativt liten (i forhold til mobiltelefon og personlig datamaskin). Det er heller ikke noe standardisert PKI-løsning tilgjengelig på plattformen, og siden en digital tuner neppe kan kalles en "personlig" enhet, går det heller ikke an å identifisere stemmegiver gjennom TV-abonnementet. Stemmegivning fra sofakroken på en 32 tommers skjerm kan vel heller ikke sies å oppfordre spesielt til "hemmelig valg".

Mobiltelefon
Bruk av mobiltelefon til stemmegivning er i og for seg en interessant mulighet. Generelt blir både selve telefonen og dataoverføringskanalen betraktet som mye sikrere enn en personlig datamaskin koblet mot Internett, ikke minst fordi mobiltelefonnettet er lukket på en helt annen måte enn Internett. Selv om det ikke er utenkelig at uvedkommende på forskjellige måter kan "hacke" seg inn i nettet, er risikoen for dette langt lavere enn angrep på Internett.

En klar ulempe er at skjermen på dagens mobiltelefon er relativ liten. Dette gjør det vanskelig å lage et godt brukergrensesnitt for rettelser, kumuleringer og overføring av slengere. Velgeren må derfor eventuelt akseptere at endringsmulighetene i denne kanalen er begrenset.

Man må også se på hvilke muligheter som foreligger for å skjule innholdet av stemmen – enten ved kryptering i mobiltelefonen, på stemmemottakstjeneren eller ved bruk av ”zero-trust”-løsninger – se neste avsnitt.

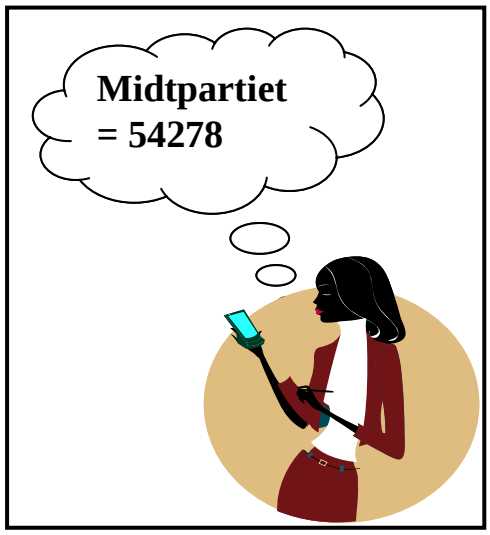
Bruk av mobiltelefon bør på bakgrunn av dette bare være en supplerende elektronisk kanal i tillegg til andre elektroniske kanaler med rikere brukergrensesnitt. Det er imidlertid ikke utenkelig at mobiltelefonteknologien med tiden kan utvikle seg til den type utstyr for sikkerhetskritiske anvendelser som vi har etterlyst tidligere i dette avsnittet.

8.3.3 ”Zero trust”

En løsning som kan være aktuell når stemmegivningsklient og overføringsnett ikke er tiltrodd, er en såkalt ”zero-trust”-løsning. Denne bygger på at velgeren og det sentrale, sikrede systemet for elektroniske valg deler en hemmelighet som de usikre komponentene ikke kjenner til. Konkret kan dette gjøres på den måten at velgeren ikke gir fra seg data til klienten i klartekst, men på kodet form. Eksempelvis kan velgeren istedenfor et partinavn eller

partinavnforkortelse sende en kode, for eksempel et tall. Denne kodingen må være individuell for hver enkelt velger.

Stemmedataene kan overføres helt åpent, siden ingen andre enn velgeren og det sentrale systemet vet hva de betyr. Dette innebærer også at velgeren kan få en kvittering som inneholder de kodede opplysningene fra det sentrale systemet Hvis disse er uendret, kan vi med høy grad av sikkerhet si at stemmen er korrekt registrert og logget på den sentrale systemet.



Utfordringen i en slik løsning er å distribuere de hemmelige kodene fra det sentrale systemet til velgerne (eller omvendt). I de tilfellene der en slik løsning har vært brukt i praksis, har kodene vært tilsendt velgerne pr. post på forhånd. I mer moderne løsninger kan vi tenke oss at kodene oversendes via alternative kanaler (stemmes det over Internett, kan kodene sendes via mobiltelefonnettet) eller på en form som kanalen ikke uten videre kan tolke. For eksempel kan kodene legges inn i bilder som et menneske lett kan tolke, men som et tekstgjenkjenningsprogram vil ha store vanskeligheter med.

Figur 8.4: Stemmegivning med individuelle koder

Når stemmene skal telles opp, må en oversikt over de kodene som sto til disposisjon for hver enkelt velger være knyttet til stemmen. Dette kan gjøres på den måten at både stemme og kodeoversikt i separate prosesser gis en pseudoidentitet som kan avledes fra velgerens identitet, men som ikke kan føres tilbake til ham. En klar ulempe er at denne relativt kompliserte dekodingsprosessen må foregå i en tidskritisk periode etter at urnene på valgtinget er stengt for e-velgere som vil avgi ”angrestemme”.

Et annet viktig spørsmål er om velgerne vil kunne beherske en så vidt komplisert og lite brukervennlig måte å stemme på, spesielt når vi tar i betraktning de mulighetene velgerne har for å gjøre endringer på stemmesedlene. En fremtidsløsning her kan være at kodene produseres ved hjelp av en liten spesiell datamaskin med skjerm der velgeren kan operere på stemmeseddelen i klartekst. Da begynner vi imidlertid å nærme oss den sikre brukerenheten som er omtalt i avsnitt 8.3.2.

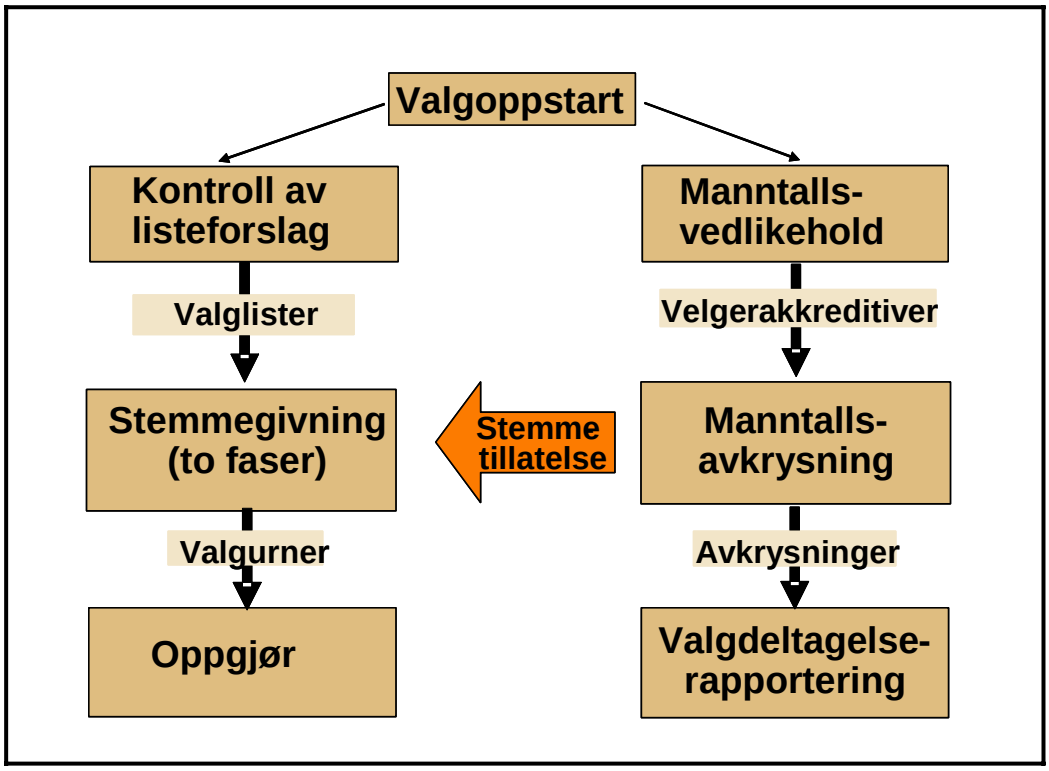
Alt i alt synes de praktiske ulempene med et ”zero-trust”- system såpass store at arbeidsgruppen ikke vil anbefale en slik løsning.

8.4 Én velger, én stemme

8.4.1 Stemmetillatelsen

For at en velger skal kunne avgi stemme, må vedkommende ha en stemmetillatelse. I et tradisjonelt papirbasert valg på selve valgdagen oppstår stemmetillatelsen implisitt ved at velgeren etter å ha legitimert seg og blitt krysset av i manntallet slippes fram til valgurnen – jf. figur 8-5. Det samme prinsippet kan brukes for all stemmegivning i kontrollerte

omgivelser, men ved elektroniske valg må valgfunksjonæren passe på at velgeren ikke stemmer med en annens identitet. Det kan for eksempel gjøres på den måten at velgeren får utdelt en stemmetillatelse i form av et elektronisk lesbart kort som inneholder velgerens identitet og som velgeren kan bruke mot systemet.

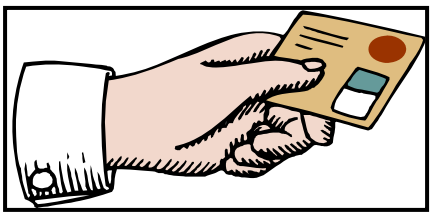


Figur 8.5: Valgprosessen

8.4.2 Elektronisk stemmegivning krever et velgerakkreditiv

Ganske annerledes forholder det seg ved elektronisk stemmegivning i ukontrollerte omgivelser. Da må velgeren ha en eller annen form for velgerakkreditiv (”credential”) som gir vedkommende anledning til å stemme. Akkreditivet skal også forhindre at samme person kan få avlagt mer enn én tellende stemme, se spesielt Europarådets anbefaling punkt 5, 6 og 94.

Velgerakkreditivet kan være alt fra et valgkort med en hemmelig kode til avanserte smartkortløsninger. Vi kan også tenke oss at velgeren kan bruke et generelt personlig identifikasjonskort som brukes også for andre formål enn valg, og at systemet ved oppslag i manntallet gir velgeren anledning til å avlegge stemme.



En velger skal altså kunne legge kun én stemme i valgurnen. Dette kan enten gjøres ved at systemet ved stemmegivning sørger for å gjøre velgerakkreditivet ubrukelig for ytterligere stemmegivninger, eller ved at velgerakkreditivet har et entydig identifikasjonsnummer som kan leses av stemmegivningssystemet.

Figur 8.6: Elektronisk stemmegivning krever et velgerakkreditiv

Den første løsningen forutsetter at systemet på en eller annen måte kan skrive på eller endre velgerakkreditivet. I dette tilfellet må man ta hensyn til at systemet kan gå ned under

stemmegivningen – velgerakkreditivet må derfor endres etter at stemmen er registrert. Dette åpner for fusk, for eksempel ved at velgeren bryter strømmen på sitt utstyr akkurat i det kritiske øyeblikket. I den andre løsningen har systemet oversikt over hvilke akkreditiver som har vært brukt. Hvis et akkreditiv blir forsøkt brukt flere ganger, kan systemet enten avvise forsøket på å avgi stemme, eller ta i mot stemmen og ugyldiggjøre de foregående. Arbeidsgruppen anbefaler den siste løsningen, siden den fjerner mye av problemene forbundet med utilbørlig påvirkning og kjøp og slag av stemmer, og ikke fører til økte kostnader av betydning. En elektronisk stemme kan følgelig ikke legges i den elektroniske valgurnen og manntallet ikke avkrysses før fristen for å kunne avgi stemme om igjen er løpt ut.

I hvilken grad akkreditivets identifikasjonsnummer skal kunne kobles til velgerens identitet, som for eksempel fødselsnummeret, er en interessant diskusjon. For at det skal være mulig å legge inn nye elektroniske stemmer og eventuelt annullere dem på valgtinget, må koblingen mellom stemme og velger være direkte eller indirekte til stede helt til fristen for å kunne avgi stemme om igjen er løpt ut. Vi minner om at det er et ufravikelig krav at en elektronisk stemme skal kunne kalles tilbake ved tradisjonell papirstemmegivning på valgtinget.

La oss se på alternativene.

Stemmegivning med anonymt akkreditiv
En teoretisk mulighet er å anonymisere velgeren fullstendig før stemmen avgis ved at velgeren får tildelt et tilfeldig stemmeakkreditiv og avgir stemme med dette. Velgeren kan få tilsendt eller kan hente et akkreditiv fra et troverdig system, eller kan trekke et akkreditiv fra en bøtte eller lignende. Det er da ingen kobling mellom velgerens identitet og den avgitte stemmen.

Denne løsningen ivaretar i utstrakt grad kravet om velgerens anonymitet. Imidlertid er det en rekke ulemper med denne løsningen. Det må avmerkes i manntallet at velgeren har fått utstedt et velgerakkreditiv. Ytterligere akkreditiver kan ikke utstedes til samme velger, for eksempel hvis velgeren hevder å ha mistet det, fordi dette ville åpne for at samme velger kunne avgi stemme flere ganger med ulike identiteter. Hvis velgeren ønsker å stemme på selve valgtinget, og det er avmerket i manntallet at vedkommende har fått utstedt et akkreditiv, må akkreditivet fremlegges for at det skal være mulig å annullere eventuelle elektroniske forhåndsstemmer. Et anonymt stemmeakkreditiv er heller ikke ønskelig siden det åpner for kjøp og slag av stemmeretten – akkreditivet kan oppfattes som et verdipapir som kan omsettes.

Selv om denne metoden garanterer total anonymitet, er den derfor uaktuell av praktiske og sikkerhetsmessige grunner.

Avledning av akkreditivets identifikasjon fra velgerens identitet
For å begrense antall moduler/komponenter som kjenner stemmegivers reelle identitet kan vi benytte et akkreditividentifikasjonsnummer som er avledet fra velgerens identitet. En isolert del av stemmegivningssystemet eller en såkalt tiltrodd tredjepart brukes da til å generere akkreditividentifikasjonsnummer (pseudoidentiteter) basert på for eksempel på velgerens fødselsnummer. Sender vi samme fødselsnummer inn får vi

samme pseudoidentitet ut, men det er ikke mulig å gå motsatt vei, dvs. å finne fødselsnummeret basert på pseudoidentiteten.[59]

Bruk av pseudoidentitet vil støtte gjentatt stemmegivning, siden det er den samme identiteten som brukes hver gang. Dersom et stemmeakkreditiv knyttet til pseudoidentiteten går tapt, kan et nytt genereres basert på velgers reelle identitet (siden samme pseudoidentitet da vil kunne genereres på nytt).

Hvis velgeren ønsker å stemme på selve valgtinget, og det er avmerket i manntallet at velgeren har fått utstedt et velgerakkreditiv, foreligger to muligheter. Den ene er at velgeren fremlegger akkreditivet slik at pseudoidentiteten kan brukes umiddelbart til å annullere eventuelle elektroniske stemmer. Dersom velgeren ikke kan fremlegge akkreditivet, er den andre muligheten å registrere velgerens fødselsnummer, og la et tiltrodd system beregne pseudoidentiteten på nytt.

Akkreditivet har velgerens identitet
I denne løsningen kjenner stemmegivningssystemet velgerens identitet, men det må være utformet på en slik måte at velgeridentiteten ikke kan koples med stemmens innhold. Dette kan gjøres ved hjelp av "forseglede elektroniske konvolutter" – detaljene er beskrevet i avsnitt 8.4.3.
Dersom velgeren velger å forhåndsstemme elektronisk, må dette avmerkes i manntallet. Velgeren kan i tillegg avlegge stemme på valgdagen, enten ved fremlegging av velgerakkreditivet eller ved å oppgi identitet.

Det enkleste rent teknisk er om velgeren bruker sin reelle identitet (fødselsnummer e.l.) ved stemmegivningen. Selv om disse løsningene krever spesiell oppmerksomhet på utformingen av de sentrale systemene slik at det ikke skal være mulig å kunne koble velgerens identitet med innholdet av stemmen, oppveies denne ulempen av fordelene. En meget viktig fordel er at velgerakkreditivet ikke er påkrevd for å kunne stemme om igjen på valgtinget, og dermed gjør velgerakkreditivet uinteressant som handelsvare for stemmekjøpere.

Arbeidsgruppen anbefaler at man velger den siste løsningen. Vi skal derfor i det følgende anta at velgeren henvender seg til valgsystemet med sin reelle identitet. Spørsmålet er da på hvilken måte valgsystemet skal kunne forvisse seg om hvem velgeren er (identifisering) og at velgeren er den vedkommende gir seg ut for å være (autentisering).

I prinsippet gjøres identifisering og autentisering ved hjelp av:
- Noe velgeren har (pass, identifikasjonskort, smartkort, eID eller lignende).
- Noe velgeren vet (passord, PIN-koder).
- Noe velgeren er (utseende, fingeravtrykk, retinamønster).

Foreløpig er identifisering og autentisering ved hjelp av ”noe velgeren er” (såkalt biometri) for dyrt og for komplisert for utbredt bruk, spesielt på hjemmemaskiner, men dette kan endre seg med den teknologiske utviklingen. Løsningen bør derfor bygge på en kombinasjon av noe velgeren har (eksempelvis et smartkort) kombinert med noe velgeren vet (eksempelvis en PIN-kode). Arbeidsgruppen vil imidlertid fraråde at man innføre egne

[59] Nasjonalt reseptregister hos Nasjonalt folkehelseinstitutt bruker en slik løsning, hvor Statistisk Sentralbyrå er tiltrodd tredjepart og leverer en pseudoidentitet før en resept registreres i registeret. Man kan da samle en persons resepter over tid, men har ikke mulighet til å finne personens reelle identitet.

identifikasjonsmekanismer spesielt for elektroniske valg. Dette vil være kostbart, og kort med PIN-koder kan lett bli gjenstand for kjøp og salg.

Istedenfor anbefaler arbeidsgruppen at man bygger på de offentlig aksepterte PKI-løsningene[60] som er under etablering i Norge. Dette bidrar til å senke kostnadene, gjør at velgeren får færre kort og PIN-koder å holde styr på, og minsker ikke minst faren for kjøp og salg av velgerakkreditiver. En velger vil neppe være villig til å "låne bort" et PKI-kort med tilhørende PIN-koder når låneren kan bruke kortet til mye annet enn bare å avgi stemme.

En PKI-løsning utnytter asymmetrisk krypteringsteknikk. Denne teknikken går ut på at det ved hjelp av en spesiell algoritme dannes et elektronisk nøkkelpar – dvs. to bitmønstre. Den ene nøkkelen brukes til å kryptere en elektronisk melding slik at den blir uleselig. Den eneste måten å få fram den opprinnelige, lesbare meldingen på, er å dekryptere den med den andre nøkkelen i nøkkelparet. Slike nøkkelpar utnyttes gjerne på den måten at den ene nøkkelen ("the public key") er offentlig kjent, mens den andre ("the private key") holdes strengt hemmelig. Hvis A skal sende en melding til B som bare B skal kunne lese, kan A kryptere meldingen med B's offentlige nøkkel. Hvis på den annen side B skal kunne forvisse seg om at en melding virkelig kommer fra A, kan A kryptere den (eller et tall beregnet på grunnlag av den) med sin egen private nøkkel. Dette kalles en *digital signatur*. Hvis meldingen da lar seg dekryptere med A's offentlige nøkkel, kan man ha tillit til at meldingen komme fra A, og ikke fra noen som utgir seg for å være A.

Det å bekrefte at en offentlig nøkkel virkelig tilhører en bestemt person eller organisasjon, gjøres ved hjelp av et *digitalt sertifikat.* Slike sertifikater utstedes ofte av tiltrodde tredjeparter. Eksempelvis kan stemmegivningssystemet gjennom sikkerhetsportalen hos BBS[61] ved hjelp av PKI være sikker på at bruker A faktisk *er* bruker A (eller i hvert fall at den som logger inn har tilgang til bruker A sin elektroniske ID). En mer detaljert fremstilling av dette finnes i NOU 2001:10 Uten penn og blekk, kapittel 3.

I Norge er det lagt opp til at private aktører skal ta seg av utstedelse, validering og vedlikehold av PKI-identiteter. (Dette i motsetning til for eksempel Estland der ID-kort med PKI identitet utstedes i offentlig regi.) Post og Teletilsynet fører tilsyn med tilbydere av såkalte "kvalifiserte sertifikater", og alle slike tilbydere skal være registrert hos Post og Teletilsynet[62]. Tjenester som "MinSide" som etter planen lanseres i første kvartal 2006, kan bidra til at befolkningen etter hvert ser nytten av å anskaffe seg en slik PKI-identitet.

I kravspesifikasjonen for PKI i offentlig sektor er det definert to nivåer for personlige sertifikater: "Person-Standard" og "Person-Høyt". Person-Høyt tilsier at sertifikatet er lagt inn i et smartkort, og krever personlig fremmøte ved utlevering. Ved Person-Standard kan sertifikatet lastes ned i en fil på en personlig datamaskin. Arbeidsgruppen anbefaler at man for elektronisk stemmegivning stiller krav om Person-Høyt.

---

[60] http://odin.dep.no/filarkiv/234033/Kravspek_PKI_v102.pdf er en kravspesifikasjon for PKI i offentlig sektor.

[61] http://www.brreg.no/sikkerhetsportal/ - Formålet med Sikkerhetsportalen er å gjøre det enkelt for offentlige etater og kommuner som ønsker å tilby elektroniske tjenester som krever bruk av elektronisk identitet og signatur til sine brukere. Sikkerhetsportalen skal kunne integrere PKI-løsninger fra flere leverandører, og den skal kunne tilby mulighet for felles pålogging (Single Sign-On) til flere tjenester, enten de er tilgjengelig gjennom Sikkerhetsportalen eller direkte fra ulike etaters eller kommuners nettsider.

[62] Se http://www.npt.no/pt_internet/sikkerhet_teleberedskap/digital_sign/tilbydere.html

Et alternativ er å la mobiltelefonen få en rolle som en sikkerhetsenhet ("trusted device") i kombinasjon med datamaskin-basert stemmegivning. En stor andel av befolkningen har i dag en mobiltelefon med PKI-muligheter innebygd i SIM kortet.[63] Ved innlogging for stemmegivning på Internett kan man få en verifiseringsmelding på sin mobiltelefon. Denne meldingen signeres med den private PKI-nøkkelen i SIM-kortet (ved å legge inn passordet på mobiltelefonen) og velgerens identitet er dermed klarlagt. Dette åpner imidlertid for kjøp og salg av stemmer ved at kjøperen kan avtale med selgeren at han skal godkjenne en slik transaksjon, og stemmegiveren (kjøperen) og velgeren (selgeren) behøver ikke en gang å befinne seg på samme sted. Ved å sende et engangspassord til velgerens mobiltelefon som skal legges inn i stemmegivningsklienten kan man til en viss grad bekrefte velgerens identitet. Det kan også tenkes at man må forhåndsregistrere seg med hvilket mobilnummer en ønsker å avgi stemme med.

8.4.3 Hvordan unngå at stemmens innhold kan kobles til velgeren

Arbeidsgruppen legger opp til at elektroniske stemmer avgitt i ukontrollerte omgivelser skal kunne trekkes tilbake, enten gjennom en ny elektronisk stemme eller ved stemmegivning på selve valgtinget. For å oppnå dette, må hver enkelt elektronisk stemme være koblet til velgerens identitet helt fram til stemmen ikke lenger kan kalles tilbake, men selve stemmen må i hele denne perioden være forseglet. I Europarådets anbefaling punkt 35 heter det at "Informasjon om stemmer og velgere skal holdes forseglet så lenge datamaterialet oppbevares på en slik måte at stemmer og velgere kan knyttes sammen".

Den generelle løsningen på dette problemet er et dobbelkonvoluttsystem, slik som vi eksempelvis kjenner det fra papirbaserte valg i forbindelse med forhåndsstemmegivning og stemmegivning utenfor egen valgkrets på valgtinget. Selve stemmen legges i en indre, anonym stemmeseddelkonvolutt. Denne legges i en ytre konvolutt sammen med valgkortet som er påført velgerens identitet. Ved opptellingen skilles valgkort og stemmeseddelkonvolutt, og stemmeseddelkonvolutten legges i en urne sammen med de øvrige stemmeseddelkonvoluttene.

I et elektronisk valgsystem konstruerer vi et slikt dobbelkonvoluttsystem ved hjelp av asymmetrisk kryptering (se avsnitt 8.4.2) og minst to nøkkelpar – ett for å beskytte selve stemmen (den indre stemmeseddelkonvolutten) og ett for å kunne verifisere at stemmen virkelig kommer fra den angitte velgeren (den ytre konvolutten). Etter at velgeren har gjort sine valg, vil den utfylte elektroniske stemmeseddelen umiddelbart bli kryptert med valgets offentlige nøkkel. Denne krypteringen forsegler altså den indre konvolutten. Stemmen kan kun leses etter dekryptering med den tilhørende private nøkkelen – dette kan betraktes som en åpning av den indre konvolutten. Nøkkelparet genereres av en sikkerhetsmodul like før valgets fase 1 starter. Valgets offentlige nøkkel distribueres til velgerne gjennom programvaren som brukes under stemmegivningen. Den tilhørende private nøkkelen oppbevares i sikkerhetsmodulen og kan kun gjøres tilgjengelig gjennom en prosedyre der et antall personer fra valgmyndighetene må "låse opp" sikkerhetsmodulen ved hjelp av nøkler (fysiske og/eller digitale)[64].

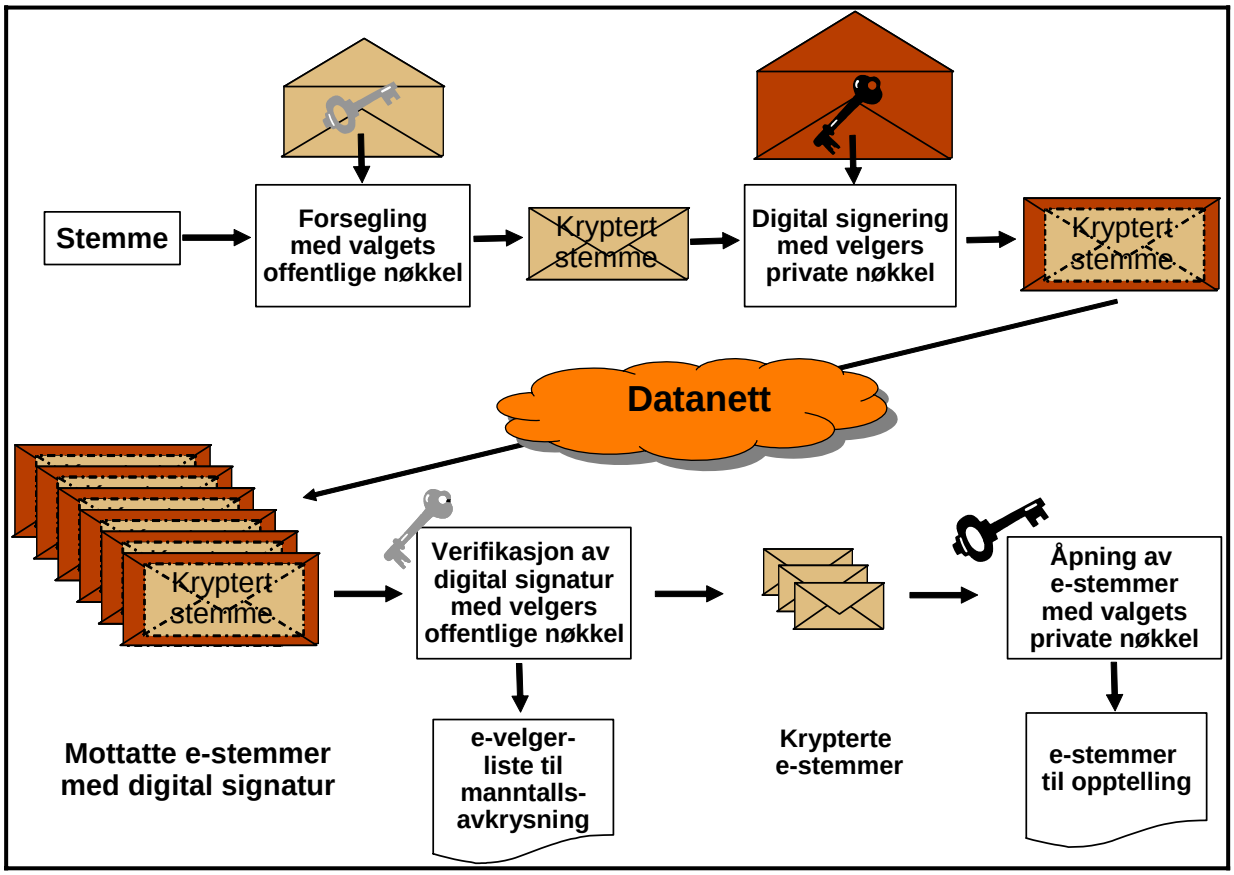
I sammenheng med valg er det i utstrakt grad standardiserte meldinger – det vil si uendrede stemmesedler – som krypteres. Derfor kan vi ikke bruke asymmetrisk kryptering direkte på

[63] Alle SIM-kort fra Telenor Mobil har PKI-funksjonalitet innebygd fra 1. mai 2002

[64] Denne løsningen er identisk med den løsningen som brukes ved elektroniske valg i Estland, se The National Election Committee: E-Voting System – Overview på http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf

uendrede stemmesedler – ellers kunne en innbryter lett få tak i innholdet av stemmen. Vi må innføre noen tilfeldige data i tillegg til den egentlige stemmen. En nærliggende løsning er å bruke hybrid kryptering med en tilfeldig valgt sesjonsnøkkel.[65]

Før den krypterte stemmen sendes av gårde fra stemmegivningsmaskinen, må den imidlertid legges i en forseglet elektronisk ytre konvolutt. Denne konvolutten forsynes med velgerakkreditivets identitet og krypteres med velgerens private nøkkel, det vil si at stemmen gis en digital signatur. Åpningen av den ytre elektroniske konvolutten gjøres ved å dekryptere med velgerens offentlige nøkkel som valgsystemet kan hente enten fra et elektronisk manntall eller fra et nasjonalt PKI-system, alt etter hvilken løsning som velges. På denne måten kan vi verifisere at stemmen virkelig kommer fra den angitte velgeren. Figur 8.7 gir en oversikt over disse prinsippene for sikring av e-stemmer.



Figur 8.7: Prinsipper for sikring av e-stemmer

Forutsetningen for at denne løsningen skal kunne sikre at stemmeinnholdet ikke kan kobles til velgerens identitet, er at ingen som er involvert i valgprosessen skal ha tilgang til både de digitalt signerte e-stemmene og valgets private nøkkel *samtidig*.

[65] I hybrid kryptering brukes symmetrisk kryptering for den egentlige meldingen, det vil si at den krypteres og dekrypteres med samme nøkkel. Denne nøkkelen er imidlertid en tilfeldig valgt engangsnøkkel som overføres fra sender til mottaker ved hjelp av asymmetrisk kryptering. Siden asymmetrisk kryptering krever mer datamaskinkraft enn symmetrisk kryptering, og det er vesentlig mindre arbeid med å kryptere en engangsnøkkel enn en hel melding, kan hybrid kryptering være meget effektivt. Samtidig introduseres det ønskede element av tilfeldighet.

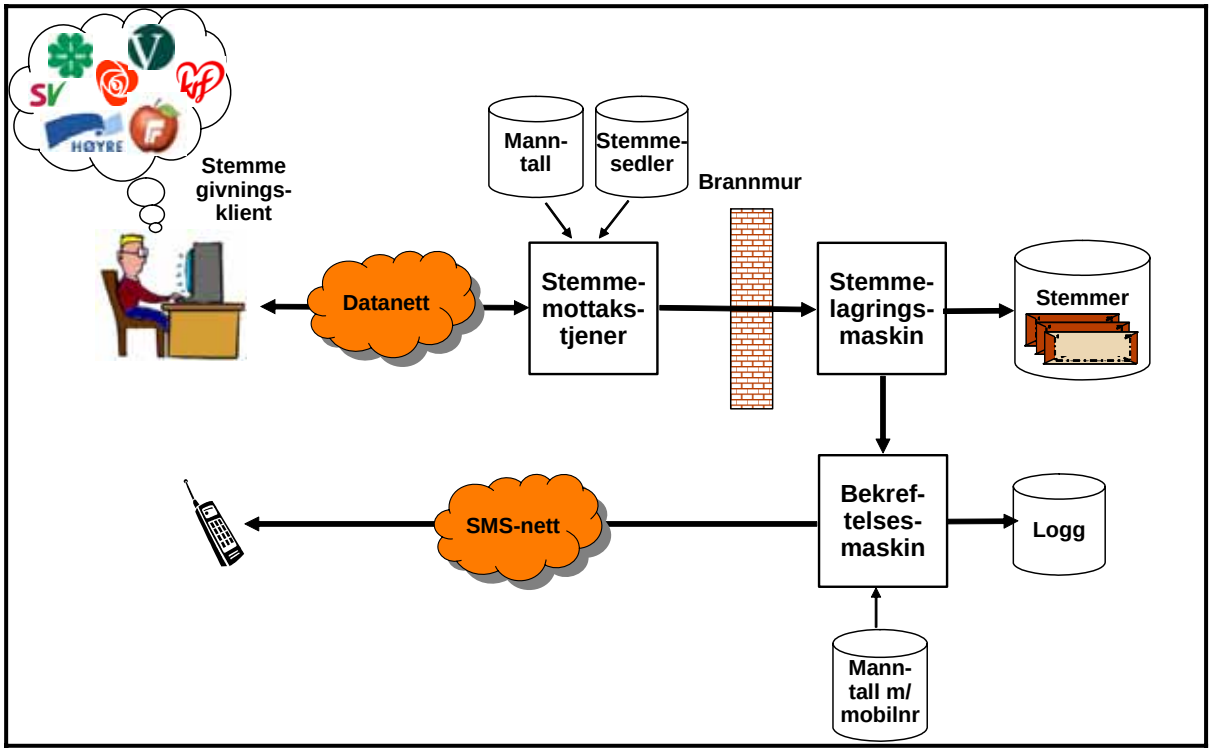
8.5 Valgsystemets funksjonalitet

Det går frem av de foregående kapitlene at arbeidsgruppen anbefaler at papirbaserte og eventuelle elektroniske valgløsninger skal sameksistere i lang tid framover. Derfor er det nødvendig å finne løsninger for å integrere disse to måtene å avlegge stemme på.
I dette avsnittet legger vi fram en skisse for hvordan rutinene rundt et valg med så vel tradisjonelle papirstemmer som elektroniske stemmer kan legges opp. Rutinene er beskrevet ved hjelp av bruksmønstre (Use Cases) i henhold til UML-standarden (Rumbaugh, Jacobson & Booch 2004) [66].

Bruksmønstre er stort sett selvforklarende, men noen ord kan kreve en nærmere forklaring:

- *Aktør*: En bestemt type bruker av systemet – mennesker eller andre systemer som spiller en eller annen rolle overfor systemet, og som har et mål som kan nås ved å utføre bruksmønsteret.
- *Prebetingelse*: Betingelse som må være oppfylt for at bruksmønsteret skal kunne utføres.
- *Postbetingelse*: Tilstand til system og aktør etter at bruksmønsteret er utført.
- *Normal hendelsesflyt*: Hendelsesforløp i et bruksmønster som fører til at aktøren når sitt mål på en enkel måte.
- *Variasjon*: Avvik fra normal hendelsesflyt.

8.5.1 Den elektroniske stemmegivningen



Figur 8.8: Arkitektur for stemmegivningssystemet

Den sentrale funksjonaliteten i ethvert e-valg-system er selve stemmegivningen. Funksjonaliteten som er beskrevet i dette avsnittet bygger på en arkitektur som vist i figur 8.8. Vi ser at stemmemottakstjeneren trenger *lesetilgang* både til manntall og stemmesedler, både

[66] Se også nettstedet http://www.uml.org

for å kunne verifisere at velgeren har anledning til å stemme og for å kunne oversende de riktige stemmesedlene. Stemmemottaksmaskinen sender stemmen videre innover i systemet til stemmelagringstjeneren gjennom en brannmur. Stemmelagringstjeneren skriver den mottatte stemmen ut på et ”write-once”-medium, og sender deretter stemmen videre til bekreftelsesmaskinen.
Av hensyn til sikkerheten må den delen av programvaren som mottar den ferdig modifiserte stemmeseddelen på klienten og sender den videre til stemmemottaksmaskin og stemmelagringsmaskin, være så enkel som overhodet mulig. Denne delen av programvaren må holdes klart atskilt fra programvaren som henter og presenterer stemmesedlene og som tillater velgeren å endre dem, siden kravene til sikkerhet her er mindre, og programmene fort kan bli store og kompliserte.

Bruksmønsterbeskrivelse
Aktør: Velger
Prebetingelse: Velgers maskin med nettleser er klar til bruk
Postbetingelse: Velgers stemme er registrert i stemmedatabasen

1. Velgeren tar kontakt med valgsystemet og identifiserer seg overfor systemet.
2. Systemet verifiserer at velgeren er oppført i manntallet og gir velgeren anledning til å stemme (gir stemmetillatelse). De riktige stemmesedlene presenteres basert på hvilken valgkrets velgeren tilhører.
3. Velgeren velger stemmeseddel, gjør eventuelt endringer og tilføyelser og avgir den ferdige stemmeseddelen til systemet. I et ”zero-trust”-system kan stemmen gis en pseudo-identitet allerede her.
4. Systemet tar i mot stemmeseddelen og lagrer den på et trygt sted inntil opptellingen.
5. Systemet bekrefter overfor velgeren at stemmen er mottatt, fortrinnsvis over en alternativ kanal (for eksempel SMS).
6. Velgeren kontrollerer bekreftelsen og går ut av systemet.

Variasjoner:
2a.
1. Systemet finner ut at velgeren ikke står i manntallet.
Systemet gir melding om dette og avslutter bruksmønsteret.
4a.
2. Systemet finner ut at stemmeseddelen er feilaktig utfylt.
Systemet gir feilmelding og går tilbake til 3.

Denne funksjonaliteten må bygges på en klient/tjener-arkitektur der stemmegivningsklienten betjenes av velgeren og stemmemottakstjeneren tar i mot og videreformidler stemmen til andre deler av det totale valgsystemet. Vi skal i de følgende avsnittene se mer detaljert på hvert enkelt trinn i bruksmønsteret.

Velgeren tar kontakt med valgsystemet og får tilgang ved hjelp av velgerakkreditivet
Brukergrensesnittet bør utformes som en Internett-nettside/webapplikasjon, slik at flest mulig klientplattformer og operativsystemet skal kunne brukes til å avgi stemme. Alternativet er å lage "stemmegivningsprogrammer" som må lastes ned i forskjellige versjoner for PC, Mac, Linux etc, noe som er mindre plattformuavhengig og vesenlig mer kostbart. En klientmaskin skal ikke trenge mer enn en standard nettleser (samt støtte for valgt sikkerhetsløsning) for å avgi stemme.

Velgeren utfører altså første del av bruksmønsterspesifikasjonens punkt 1 ved å starte opp en nettleser og skrive inn den av valgmyndighetene oppgitte nettadresse (URL). Fra tjeneren hentes nå inn en programkomponent som tar seg av den videre dialogen med velgeren. Dette krever at nettleseren er innstilt slik at den kan kjøre slike komponenter.

Deretter skaffer velgeren seg tilgang til e-valg-systemet ved hjelp av velgerakkreditivet, se avsnitt 8.4.2. Gjennom akkreditivet er velgeren automatisk identifisert og autentisert overfor systemet.

Systemet verifiserer at velgeren er oppført i manntallet, henter stemmeseddel basert på valgkrets og gir velgeren anledning til å stemme (gir stemmetillatelse)
Velgerens identitet sendes nå over til stemmemottakstjeneren. Tjeneren slår opp i manntallet og kontrollerer først at velgeren er stemmeberettiget. Hvis dette ikke er tilfelle, returneres en melding om dette til klienten.

Deretter finner tjeneren fram til velgerens valgkrets og returnerer til klienten de stemmesedlene som velgeren har anledning til å velge mellom. Tjenermaskinen må altså ha *lesetilgang* til et elektronisk manntall og en database med stemmesedler. Systemet kan eventuelt splittes på flere tjenermaskiner som hver bare har en viss del av manntallet og stemmesedlene.

Velgeren velger stemmeseddel og gjør eventuelt endringer og tilføyelser og avgir den ferdige stemmeseddelen til systemet
Velgeren velger nå hvilke stemmesedler han vil få vist frem på skjermen og hvilken av dem han vil bruke for å stemme. I denne forbindelse er det viktig at brukergrensesnittet ikke favoriserer enkelte stemmesedler på bekostning av andre.

Velgeren kan deretter gjøre lovlige endringer på stemmeseddelen ved å bruke tilgjengelige input-enheter (pekeskjerm eller taststatur/mus). Kryssing og stryking kan gjøres direkte i listen og slengere fra andre lister kan legges inn via nedtrekksmenyer med de andre partienes lister, søkebokser eller lignende.

Systemet bør kontinuerlig validere de endringene velgeren gjør og feilaktige eller ugyldige endringer avvises med en informativ feilmelding. Stemmesedler som ikke kan godkjennes bør ikke kunne avgis.

Når velgeren har klargjort stemmeseddelen, avgir han stemme ved å klikke på en knapp som starter overføringen av stemmen til stemmemottakstjeneren.

Systemet tar i mot stemmeseddelen og lagrer den på et trygt sted inntil opptellingen
Før overføring legges stemmeseddelen i en forseglet "elektronisk konvolutt" ved at innholdet i stemmeseddelen[67] krypteres med systemets offentlige nøkkel. Dette sikrer at stemmen kun kan leses av den som kjenner systemets private nøkkel. Stemmekonvolutten legges igjen i en forseglet ”ytre konvolutt” ved hjelp av elektronisk signering med velgerens private nøkkel for at systemet skal kunne forvisse seg om at stemmen kommer fra den personen vedkommende utgir seg for å være, og for å kunne trekke stemmen tilbake dersom velger møter opp for å

[67] Stemmen kan enten overføres i sin helhet (alle navn på listen) inkludert velgerens endringer, eller den kan overføres i form av en stemmeseddelidentifikator ("Midtpartiet") etterfulgt av velgerens endringer. Det siste prinsippet vil antagelig senke datamengden som overføres, under forutsetning av at velgerne ikke gjør for mange endringer.

stemme papirbasert på valgdagen. Ytterligere detaljer om denne dobbeltkrypteringen finnes i avsnitt 8.4.

Europarådets anbefaling foreskriver at EML skal brukes som dataoverføringsformat så langt det er tilrådelig. Arbeidsgruppa anser at kommunikasjon mellom stemmegivningsklient og stemmemottak er "intern" kommunikasjon mellom to systemer som logisk hører sammen og etter all sannsynlighet vil leveres av samme leverandør. Dette tilsier at det her kan brukes et vesentlig enklere rådataformat, både for å redusere mengden av overførte data og for – av hensyn til sikkerheten - å kunne gjøre programmene i de to maskinene så enkle som mulig. Stemmemottakstjenerens videre kommunikasjon med bakenforliggende systemer bør imidlertid følge EML formatet.

Stemmemottakstjeneren overfører dobbelkonvolutten umiddelbart til stemmelagrings-maskinen. Denne maskinen skriver dobbeltkonvolutten ned på et ”write-once”-lagringsmedium som inneholder de avgitte stemmene. Denne maskinen er beskyttet av en brannmur. Det er altså bare stemmegivningsklienten og stemmemottaksmaskinen som eventuelt er tilknyttet Internett.

De avgitte stemmene lagres på stemmelagringsmaskinen frem til opptellingsfasen.

Systemet bekrefter overfor velgeren at stemmen er mottatt
Stemmemottakstjeneren sender en melding til en logg- og bekreftelsestjener om at stemme er mottatt fra en bestemt velger. Tjeneren logger på et ”write-once”-medium et det er mottatt en stemme fra en velger med en gitt identifikasjon (men skriver ikke *innholdet* i stemmen i loggen). Etter at stemmen er logget skal tjeneren gi en bekreftelse tilbake til velger på at stemmen er mottatt og registrert – jf. Europarådets anbefaling punkt 14. For å øke sikkerheten kan denne bekreftelsen sendes over en helt annen kanal i tillegg til den stemmen ble sendt over, for eksempel som SMS over mobiltelefonnettet. En slik løsning forutsetter da selvsagt at velgeren har registrert et mobiltelefonnummer i forbindelse med manntallet, eller oppgir dette i forkant av stemmegivningen.

Bekreftelsen kan også forhindre at uvedkommende på en eller annen måte stemmer om igjen med velgerens identitet uten at velgeren får vite om det, ved at det oppgitte mobilnummer automatisk vil brukes til bekreftelse ved ny stemmegivning (telefonnummeret kan bare legges inn en gang og ikke endres).

Et sentralt spørsmål er hvordan velgeren skal kunne ha en viss grad av sikkerhet for at den registrerte stemmen ikke er blitt endret og forfalsket på veien. En mulig løsning er at klienten beregner en ”digital hash” (en tallkode) av den krypterte stemmen før den sendes og viser denne fram på skjermen. Stemmelagringsmaskinen beregner den samme ”digital hash” av den krypterte stemmen og returnerer denne sammen med bekreftelsen. Velgeren kan så kontrollere at de to tallverdiene stemmer overens, altså at kodene er beregnet ut fra samme stemme.

Alternativt kan hele den krypterte stemmen returneres med bekreftelsen. Dersom det er benyttet hybrid kryptering (jf. avsnitt 8.4.3) og klienten har tatt vare på eller fått tilgang til den tilfeldig valgte engangsnøkkelen, kan klienten dekryptere stemmen og vise den fram i klartekst[68].

[68] Forutsatt at klientmaskinen tar vare på engangsnøkkelen, er det faktisk mulig å lage en funksjon som setter velgeren i stand til når som helst å inspisere stemmen slik den er registrert på stemmelagringsmaskinen. Om

Velgeren kontrollerer bekreftelsen og går ut av systemet
Stemmegivningen er dermed avsluttet. Etter dette må det ikke ligge noen data om stemmegivningen på klienten, jf. Europarådets anbefaling punkt 93.

Stemmegivning via SMS?
Alternativt kan vi tenke oss en stemmegivning via SMS. På forhånd må velgeren ha registrert seg og opplyst hvilket mobilnummer han ønsker å stemme fra, og får etter registrering oppgitt en personkode som skal brukes. Velgeren kan da sende "<listenavn> <personkode>" til et gitt telefonnummer. Når stemme-SMS'en mottas av stemmemottakstjeneren verifiseres det at oppgitt tallkode stemmer med det mobilnummeret velgeren har avlagt stemmen fra. Stemmen registreres og det sendes en SMS tilbake med kvittering på at stemmen er mottatt. I en slik løsning er det ikke mulig å foreta rettelser på listen.

SMS-stemmegivningen kan utvides til en flertrinnsprosess der man først sender "STEM <personID>" til et gitt telefonnummer og får tilbake en melding som man må svare på ved å signere den med sin private nøkkel. Nøkkelen er lagret i SIM-kortet og er beskyttet av en separat PIN kode. Stemmemottakstjeneren verifiserer at signaturen er korrekt ved hjelp av velgerens offentlige nøkkel og bekrefter at stemme kan sendes inn. Velgeren kan deretter sende listenavn og få en ny forespørsel om å "signere" valget.

Sikkerheten i løsningen er i en viss grad ivaretatt ved at stemmegivningen er beskyttet av en to-faktor autentisering, dvs. noe velgeren har (mobiltelefon med SIM-kort med PKI-funksjonalitet) og noe velgeren vet (PIN kode for signering).

8.5.2 Logging av stemmer

En meget viktig egenskap ved et valgsystem er at resultatet er etterprøvbart, jf. spesielt Europarådets anbefaling punkt 107 og 108. I et tradisjonelt valg med papirstemmesedler er det bunkene med stemmesedler som gir denne muligheten. Reises det tvil om at opptellingen er korrekt, kan stemmesedlene telles en gang til.

Så snart stemmen avgis elektronisk, er det ikke enkelt å finne en fullgod erstatning for papirstemmeseddelen som sikkerhetsmekanisme. Kravet er at velgeren skal kunne være helt sikker på at sikringsstemmen er absolutt korrekt. Amerikanske valgsikkerhetseksperter har derfor foreslått "valgomater" som i tillegg til å sende fra seg stemmen elektronisk også produserer en papirutskrift som velgeren kan verifisere gjennom et vindu, og som deretter havner i en stemmeurne uberørt av menneskehender (Mercuris valgomat[69]). Et annet forslag går ut på å dele stemmegivningsprosessen i to, slik at hvert av trinnene foregår på to atskilte maskiner (Bruck, Jeffeson & Rivest 2001). Velgeren avgir først stemme på en egen maskin som ikke er tilknyttet noe datanett. Denne maskinen "brenner" stemmen elektronisk på en spesiell elektronisk brikke kalt en "frosk" ("frog"). Så går velgeren til valgfunksjonæren som registrerer innholdet av brikken i valgsystemet, og etterpå slipper brikken i valgurnen. Brikkehaugen utgjør nå sikkerhetskopien. Andre, mer fantasifulle forslag går ut på å lage et sikkerhetsnett ved å videofilme valgomatens tastatur og skjerm, dog slik at velgeren ikke kan gjenkjennes.

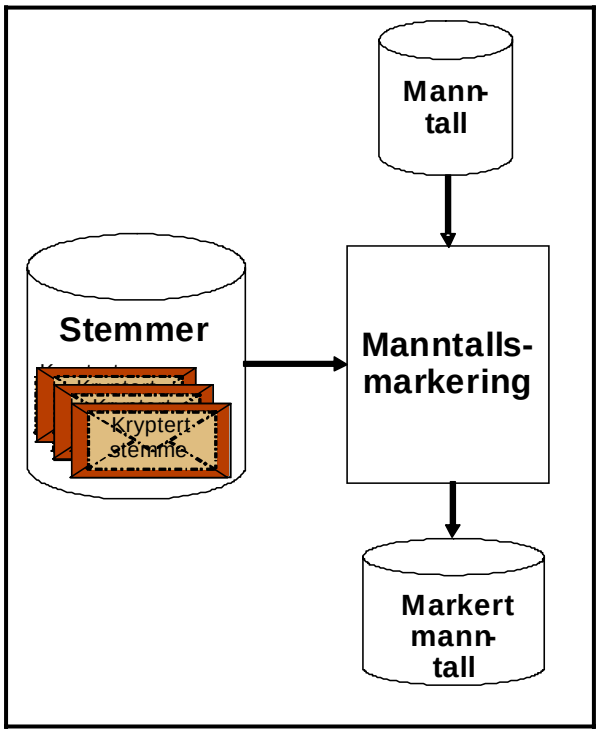
---

dette er en ønskelig funksjon, er diskutabelt: Velgeren kan få en større tillit til at stemmen er riktig registrert, men funksjonen øker også faren for kjøp og salg og utilbørlig påvirkning. Det kan også stilles spørsmål ved om denne løsningen er i samsvar med rekommandasjonens punkt 51.

[69] Se beskrivelse på http://www.notablesoftware.com/evote.html

Slike prinsipper lar seg ikke bruke ved elektronisk stemmegivning i ukontrollerte omgivelser, fordi det ikke er mulig å ha kontroll over sikringskopiene. Istedenfor må stemmene logges på de sentrale tjenermaskinene.

8.5.3 Markering av e-velgere i manntallet etter fase 1



Figur 8.9: Markering av e-velgere i manntallet etter fase 1

For korrekt behandling av velgere som allerede har stemt elektronisk i fase 1 og ønsker å stemme en siste gang på valgtinget, må valgfunksjonærene ha tilgang til den delen av manntallet som gjelder den aktuelle valgkretsen. Manntallet behøver imidlertid ikke å være elektronisk tilgjengelig i valglokalet – en papirutskrift gjør også nytten.
Manntallet som skal brukes på valgtinget må vise om velgeren allerede har stemt elektronisk. Oppdateringen av manntallet med disse opplysningene må gjøres i perioden mellom fase 1 og valgtinget. Dette forutsetter at en troverdig del av systemet kjenner til koblingen mellom velgerakkreditivets identitet og velgerens identitet i manntallet.

Bruksmønster for markering av e-velgere i manntallet etter fase 1
Aktør: Valgmyndighetene

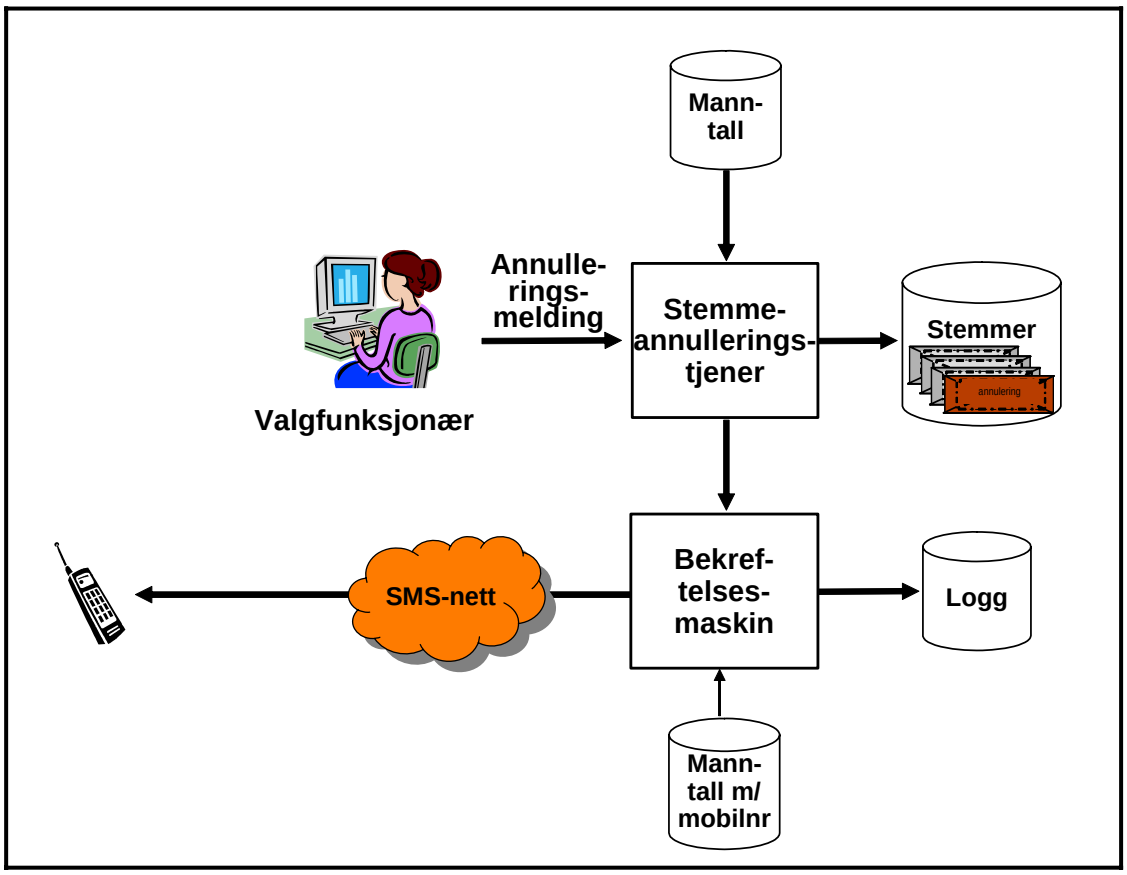
Prebetingelse: Fristen for elektronisk stemmegivning i fase 1 er gått ut
Postbetingelse: Markeringer er satt i manntallet for velgere som har avgitt en eller flere elektroniske stemmer.

1. Valgmyndighetene starter markeringssystemet.
2. Markeringssystemet løper gjennom alle de elektroniske stemmene som ligger i stemmedatabasen og krysser av i manntallet.
3. Markeringssystemet produserer de nødvendige papirutskrifter av manntallet for bruk under valgtinget.
4. Markeringssystemet lager de nødvendige og/eller interessante statistikker.

8.5.4 Annullering av elektroniske stemmer under valgtinget

Hvis en velger som har forhåndsstemt elektronisk vil avgi stemme enda en gang i valglokalet, må valgfunksjonæren sende melding til det elektroniske systemet om at alle stemmer som velgeren har avgitt elektronisk skal annulleres. Hvis det brukes fullstendig frikoblede stemmeakkreditiver, må akkreditivet fremlegges for å få tillatelse til å stemme på valgdagen. Hvis akkreditivets identitet er avledet fra velgerens identitet er dette ikke nødvendig, siden avledningen kan gjøres en gang til. Imidlertid er det enklest å annullere eventuelle stemmer hvis disse er direkte knyttet til velgerens identitet.

Rutinen forutsetter at annulleringssystemet er online tilgjengelig i valglokalet. Dette kan være en kostnadskrevende løsning, og alternativet er at valgfunksjonæren på en eller annen måte formidler til et sentralt kontor at de elektroniske stemmene fra fase 1 skal trekkes tilbake. Hvordan dette skal gjøres i detalj, og om man i så fall skal avvente bekreftelse på annulleringene, har arbeidsgruppen ikke tatt endelig stilling til. Uansett må annulleringssystemet utformes slik at det ikke skal være mulig verken for utenforstående eller for utro valgfunksjonærer å annullere stemmer uten at det er hjemmel for det.
Når en elektronisk stemme trekkes tilbake bør bekreftelse på dette sendes til samme adresse som den opprinnelige stemmebekreftelsen (se avsnitt 8.5.1)



Figur 8.10: Stemmeannullering

Bruksmønster for annullering av elektronisk stemme fra fase 1 på valgtinget
Aktører: Valgfunksjonær, velger

Prebetingelse: Valgfunksjonæren har funnet velgeren i manntallet og konstatert at vedkommende har stemt elektronisk.
Postbetingelse: Elektroniske stemmer er slettet, og velgeren kan nå avgi papirstemme på vanlig måte.

Normal hendelsesflyt:

1. Valgfunksjonæren registrerer identiteten til velgerens medbrakte akkreditiv i annulleringssystemet (pseudoidentitet eller fødselsnummer, alt etter hvilken løsning som er valgt, jf. avsnitt 8.4.2).
2. Annulleringssystemet annullerer stemmene fra fase 1 ved å legge inn en "annulleringskonvolutt" i stemmedatabasen på stemmelagringsmaskinen.[70]
3. Annulleringssystemet skriver også "annulleringskonvolutten" i en logg.
4. Annulleringssystemet bekrefter overfor valgfunksjonæren at alle elektroniske stemmer med denne identiteten er annullert.
5. Annulleringssystemet sender også en melding til velgeren via den samme kanalen som bekreftelsessystemet om at forhåndsstemmene er annullert.

Variasjoner:

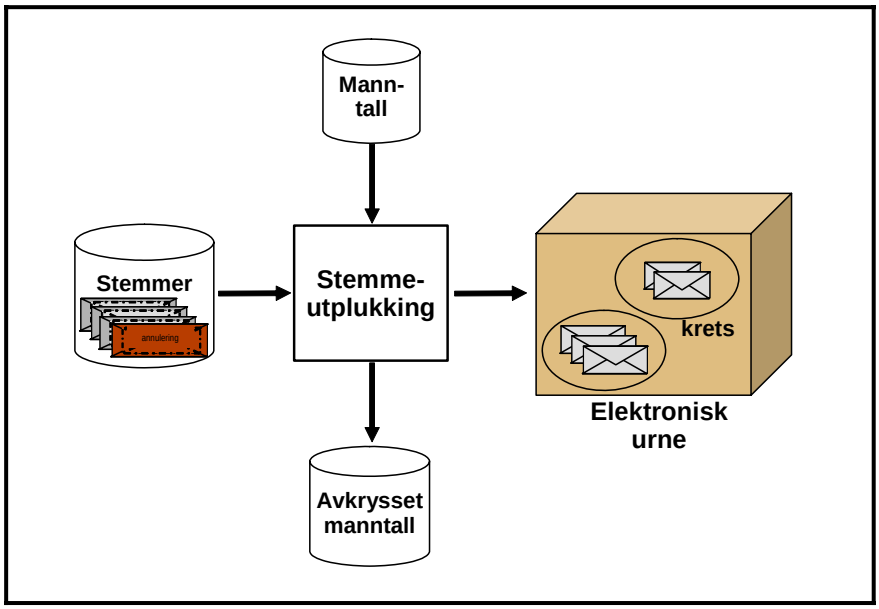
1a. Velgeren har ikke noe akkreditiv, men fremlegger annen legitimasjon med fødselsnummer. Valgfunksjonæren registrerer fødselsnummeret.

3a. Av tekniske grunner kan valgfunksjonæren ikke gis noen bekreftelse. Valgfunksjonæren må da ha tillit til at annulleringssystemet har annullert eller vil komme til å annullere de elektroniske forhåndsstemmene.

8.5.5 Opptelling av elektroniske stemmer

Denne funksjonaliteten består egentlig av to bruksmønstre, ett for å ta ut de gyldige elektroniske forhåndsstemmene, og ett for å telle dem. De to prosessene bør atskilles for å minske faren for at stemmeinnhold kan kobles til velgers identitet.

[70] Dette er bedre enn å slette de elektroniske forhåndsstemmene, eller å markere dem ugyldige. På denne måten kan stemmelageret på stemmelagringstjenere utformes som et "write-once"-medium. Hvilke stemmer som skal være gyldige, bestemmes under opptellingen.



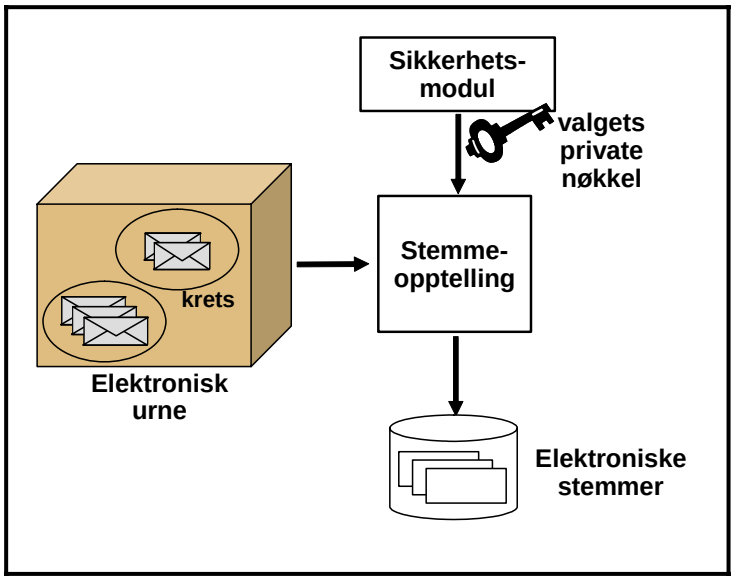
Figur 8.11: Utplukking av gyldige e-stemmer

Bruksmønster for utplukking av gyldige elektroniske stemmer
Aktør: Valgmyndighetene

Prebetingelse: Fristen for å annullere elektroniske forhåndsstemmer under valgtinget er gått ut.
Postbetingelse: Elektroniske forhåndsstemmer i elektronisk "indre konvolutt" er klare for opptelling.

Normal hendelsesflyt:

1. Valgmyndighetene starter utplukk av gyldige stemmer.
2. Utplukkingssystemet sorterer avgitte stemmer (som fremdeles ligger i de ytre elektroniske konvoluttene) på velgerakkreditivets identifikator og på registrert tidspunkt for stemmegivningen.
3. Utplukkingssystemet tar ut bare den siste stemmen for hver av akkreditividentifikatorene. Den siste stemmen kan eventuelt være en "annulleringskonvolutt".
4. Utplukkingssystemet foretar en siste avkrysning av elektroniske stemmer mot manntallet for å fange opp annulleringer under valgtinget og fordeler stemmene på valgkretser. (Hvis en valgkrets har færre enn et visst antall elektroniske stemmer må stemmene, av hensyn til hemmeligholdelse, fordeles i én samlevalgkrets.)
5. Utplukkingssystemet blander de gyldige stemmene.
6. Utplukkingssystemet åpner de ytre konvoluttene ved hjelp av velgernes offentlige nøkler, som må hentes fra manntallet.
7. Utplukkingssystemet skriver de indre konvoluttene på et "write-once"-medium – dette er den "elektroniske urnen". I et ”zero-trust”-system må stemmene gis en pseudo-identitet, hvis de ikke alt har det.
8. Utplukkingssystemet rapporterer at de gyldige elektroniske stemmesedlene er klare for opptelling.



Figur 8.12: Opptelling av gyldige e-stemmer

Bruksmønster for opptelling av gyldige elektroniske stemmer
Aktør: Valgmyndighetene

Prebetingelse: Elektroniske forhåndsstemmer i elektronisk "indre konvolutt" er klare for opptelling.
Postbetingelse: Elektroniske forhåndsstemmer er talt opp og klare for å integreres med papirstemmene.

Normal hendelsesflyt:

1. Valgmyndighetene åpner sikkerhetsmodulen som inneholder valgets private nøkkel.
2. Valgmyndighetene starter opptelling av elektronisk urne.
3. Opptellingssystemet leser valgets private nøkkel og åpner alle de elektroniske indre konvoluttene. I et ”zero-trust” system må kodene dechiffreres ved hjelp av en samling koder med samme pseudoidentitet.
4. Opptellingssystemet lister stemmesedlene på et "write-once"-medium.
5. Opptellingssystemet teller stemmene og produserer for hver valgkrets en rapport som er velegnet for samkjøring med resultatene fra opptellingen av papirstemmene.
6. Opptellingssystemet rapporterer at opptellingen er ferdig.

Man bør tenke nøye gjennom hva man skal gjøre med valgets private nøkkel etter fullføringen av dette bruksmønsteret. Sikkerhetslogger og kopier av velgerstemmer i elektroniske dobbelkonvolutter kan på dette tidspunkt eksistere flere steder i systemet, og med samtidig tilgang til disse loggene og valgets private nøkkel er det mulig å avsløre innholdet av e-velgernes stemmer. Makuleres den private nøkkelen, vil velgernes stemmer forbli uleselige for alltid.[71]

[71] I det estiske elektroniske valgsystemet opereres det med flere nøkkelpar for hvert valg, og velgerens stemme dupliseres og krypteres med den offentlige nøkkelen fra hvert nøkkelpar slik at man har noe å falle tilbake på hvis en av valgets private nøkler skulle gå tapt eller ikke fungere. Ubenyttede private nøkler blir liggende beskyttet i sikkerhetsmodulen.

8.5.6 Oppgjør

Papirbasert stemmegivning vil sannsynligvis utgjøre hovedtyngden av avlagte stemmer i mange valg fremover. De elektronisk avgitte stemmene bør derfor integreres inn i de eksisterende oppgjørssystemer som finnes i kommunene allerede. Dette kan gjøres ved at en "Elektronisk urne" (utskrift) med mottatte elektroniske stemmer for hver kommune sendes den enkelte kommune valgnatten (når det er klart hvem som har valgt å stemme i valglokalet og således overstyre sin elektroniske stemme). Disse stemmene legges så i det ordinære valgoppgjøret som en egen krets eller lignende.

8.6 Manntallet

Vi har i det foregående sett at velgermanntallet spiller en sentral rolle i gjennomføringen av et elektronisk valg, Det er inne i bildet ved gjennomføringen av alle de følgende funksjonene:

- Produksjon av manntallsutskrifter for manuell eller elektronisk forhåndsstemmegivning i kontrollerte omgivelser.
- Produksjon av velgerakkreditiver.
- Presentasjon av stemmesedler basert på valgkrets på stemmegivningsmaskinen.
- Sending av bekreftelse på at elektronisk stemme er registrert (for å finne SMS-nummer eller annen egnet svaradresse).
- Manntallsmarkering etter elektronisk stemmegivning i fase 1.
- Produksjon av manntallsutskrifter for valgtinget.
- Annullering av elektroniske stemmer under valgtinget.
- Utplukking av godkjente elektroniske stemmer (for avkrysning).
- Opptelling av elektroniske stemmer (for å finne velgerens public key).

Noen av disse funksjonene er svært tidskritiske. For eksempel vil det være svært uheldig om manntallet var utilgjengelig under opptellingen av de elektroniske stemmene. Heldigvis er det lite behov for oppdateringer i funksjonene som er nevnt ovenfor, slik at det er enkelt å operere med mange identiske elektroniske kopier av manntallet (såkalt speiling).

I tillegg til de tradisjonelle opplysningene bør det diskuteres om et manntall som skal understøtte elektroniske valg på den måten som er beskrevet i denne rapporten, også bør omfatte velgernes SMS-numre (eller annet egnet svaradresse) og velgernes offentlige nøkler. Arbeidsgruppen har ikke tatt stilling til utformingen av rutinene for eventuelt å få disse tilleggsopplysningene inn i manntallet.

8.7 Overordnede krav til systemarkitektur

I dette avsnittet går vi gjennom arbeidsgruppens forslag til overordnede, prinsipielle krav til systemarkitektur for e-valg-systemer. Kravlisten må ikke betraktes som endelig, og må utdypes og presiseres i en konkret kravspesifikasjon for et e-valg-system.

8.7.1 Samme tekniske løsning overalt

Arbeidsgruppen mener at tekniske løsninger bør utformes slik at de lett kan tilpasses stemmegivning både i kontrollerte og ukontrollerte omgivelser og gjennom ulike tekniske kanaler. Dette forenkler kontroll- og sertifiseringsarbeidet og minsker tekniske barrierer mot endringer hvis de teknologiske og politiske rammebetingelsene endrer seg, Dessuten er det et

poeng at velgerne skal kunne ta med seg erfaringen fra stemmegivning i kontrollerte omgivelser hjem i ukontrollerte omgivelser. Dette betyr altså at også for stemmegivning i kontrollerte omgivelser bør det benyttes utstyr som man kan forvente at velgerne enten allerede har i hjemmet, eller som det er realistisk å forvente at de vil anskaffe seg.

8.7.2 Plattformuavhengige løsninger

Programvareløsningene bør utformes mest mulig plattformuavhengig, slik at de samme løsningene kan gå på maskiner av ulikt fabrikat og med ulikt operativsystem. Dette gjelder dog først og fremst stemmegivningsklienten. Tjenermaskinene vil det være bare et fåtall av, så her kan det være akseptabelt for en programvareleverandør å binde seg til en bestemt plattform.

8.7.3 Datautveksling mellom komponenter skal skje i et standardisert format

Et komplett valgsystem består av et antall relativt frittstående komponenter, eksempelvis manntallsystem, stemmemottakssystem, stemmelagringssystem og opptellingssystem Det er en stor fordel om datautvekslingen mellom disse komponentene skjer i et standardisert format. De ulike komponentene vet da nøyaktig formatet på de data de skal sende og motta, ansvarsfordelingen mellom komponenter blir klarlagt, og det er enkelt å skifte ut en komponent med en annen tilsvarende komponent. Dette er viktig både for å kunne åpne for at ulike komponenter kan produseres og leveres av ulike leverandører, og for å kunne bearbeide de samme dataene i parallell med ulike komponenter (N-versjon-systemer, se avsnitt 8.7.9).

Når data skal overføres mellom komponenter, er det alltid en vurdering i hvilken grad dataene skal være selvbeskrivende, altså inneholde opplysninger om seg selv. Dersom dataene ikke er selvbeskrivende, må alle komponenter som sender og mottar disse dataene, på forhånd vite hvordan de er formatert og hva de betyr. Med selvbeskrivende data kan komponentene i større grad tilpasse seg de dataene som kommer. Det er også mulig å generere de delene av komponentene som mottar og sender data ut fra databeskrivelsene. En ulempe med selvbeskrivende data er at databeskrivelsene ofte gjentas og at det derfor overføres mer data enn strengt tatt nødvendig mellom modulene.

Et etter hvert allment akseptert format for selvbeskrivende data er XML (Extensible Markup Language)[72]. Spesielt for elektronisk stemmegivning er det utviklet en spesialisering av XML, kalt EML (Election Markup Language)[73]. I Europarådets anbefaling punkt 66 til 68 stilles det krav om at datautvekslingen mellom komponenter i et e-valg-system skal skje ved hjelp av standardiserte overføringsformater, nærmere bestemt EML, så sant det lar seg gjøre.

EML er en meget omfattende standard, og det er ikke gjort i en håndvending å konstatere om den er dekkende for norske forhold. Arbeidsgruppen har derfor fått bygd en såkalt prototyp av et komplett e-valg-system for norske valg, der dataoverføringene skjer i samsvar med EML-standarden (Aas 2005). Konklusjonen er at det må foretas noen mindre utvidelser og tilpasninger av EML-standarden (versjon 4.0) for at den skal være dekkende for norske valg. Arbeidsgruppen anbefaler at man snarest tar et initiativ for å få innarbeidet disse endringene i neste versjon av standarden.
Et spesielt forhold ved norske valg er at velgeren har anledning til å endre stemmeseddelen, og dette krever at det må overføres mer data til stemmemottaksmaskinen enn hva som er

[72] Se http://www.w3.org/XML/
[73] Se http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election

vanlig internasjonalt. Kapasitetsbegrensninger i dataoverføringer mellom stemmegivningsmaskin og stemmemottaksmaskin og behandlingskapasiteten i stemmemottakingsmaskinen må derfor vies spesiell oppmerksomhet.

8.7.4 Sikkerhetslogging

Stemmegivningen og alle andre signifikante hendelser i forbindelse med bruken av valgsystemet må logges på en betryggende måte, slik at det er mulig å etterprøve og kontrollere gjennomføringen av valget (jf. Europarådets anbefaling punkt 102 og 103). Dette omfatter sikkerhetskopiering av avgitte stemmer, identifiserte angrep på sentrale komponenter og funksjonalitet, alle aktiviteter utført av valgfunksjonær i forbindelse med valggjennomføringen som oppstart og avslutning av stemmemottak, åpning av elektroniske urner, dekryptering av mottatte stemmer og oppstart av opptelling og beregning. Europarådets anbefaling stiller også krav til beskyttelse av loggen mot angrep (jf. punkt 109)

8.7.5 Sertifisering

Sikkerhetskritiske, spesialutviklede moduler må sertifiseres av akkrediterte sertifiseringsorganer (se kapittel 9 og Europarådets anbefaling punkt 111 og 112). Sikkerhetskritiske moduler som må være gjenstand for inngående inspeksjon må skilles klart fra moduler med lavere krav til sikkerhet. Sikkerhetskritiske moduler må utformes og programmeres så enkelt at man gjennom inspeksjon av programteksten (såkalt hvitbokstesting) kan resonnere seg fram til at de er korrekte. De må ikke bygge på omfattende, uoversiktlige programvarebiblioteker som eventuelt kan inneholde sikkerhetshull.

8.7.6 Løsningene må bygge på velprøvd programvare

I den utstrekning sikkerhetskritiske deler av systemet bygger på programvare fra tredjepart, må denne programvaren være allment utbredt, velprøvd og åpen for inspeksjon. Et eksempel på slik programvare er moduler for kryptering og dekryptering.

8.7.7 Åpen kode?

Bruk av åpen kildekode er en mulig måte å beskytte systemløsninger mot utilsiktet og ondsinnet kode. Tradisjonelle åpne kildekode-prosjekter baseres på et samarbeid om utvikling av funksjonalitet med innspill fra mange ulike aktører. En slik utviklingsfilosofi bidrar til at det blir vanskelig å bygge inn sikkerhetshull og ondsinnet kode. Jason Kitcat var tidligere en forkjemper for bruk av åpen kildekode og kollaborativ systemutvikling for valgapplikasjoner. Han går i en artikkel fra 2004 tilbake på dette standpunktet (Kitcat 2004), men dette er i hovedsak fordi han mener at åpen kildekode ikke påvirker de fundamentale problemene forbundet med elektronisk stemmegivning.

Arbeidsgruppen er av den mening at det ikke er realistisk eller ønskelig å la en sikkerhetskritisk applikasjon som valg bli utviklet som et tradisjonelt åpen kildekode prosjekt. Valget krever en planmessig utvikling med strenge deadlines, klare leveranseforpliktelser og veldefinerte ansvar og roller. Åpen kildekode vil også kunne blottstille viktige sikkerhetstiltak på en uønsket måte.

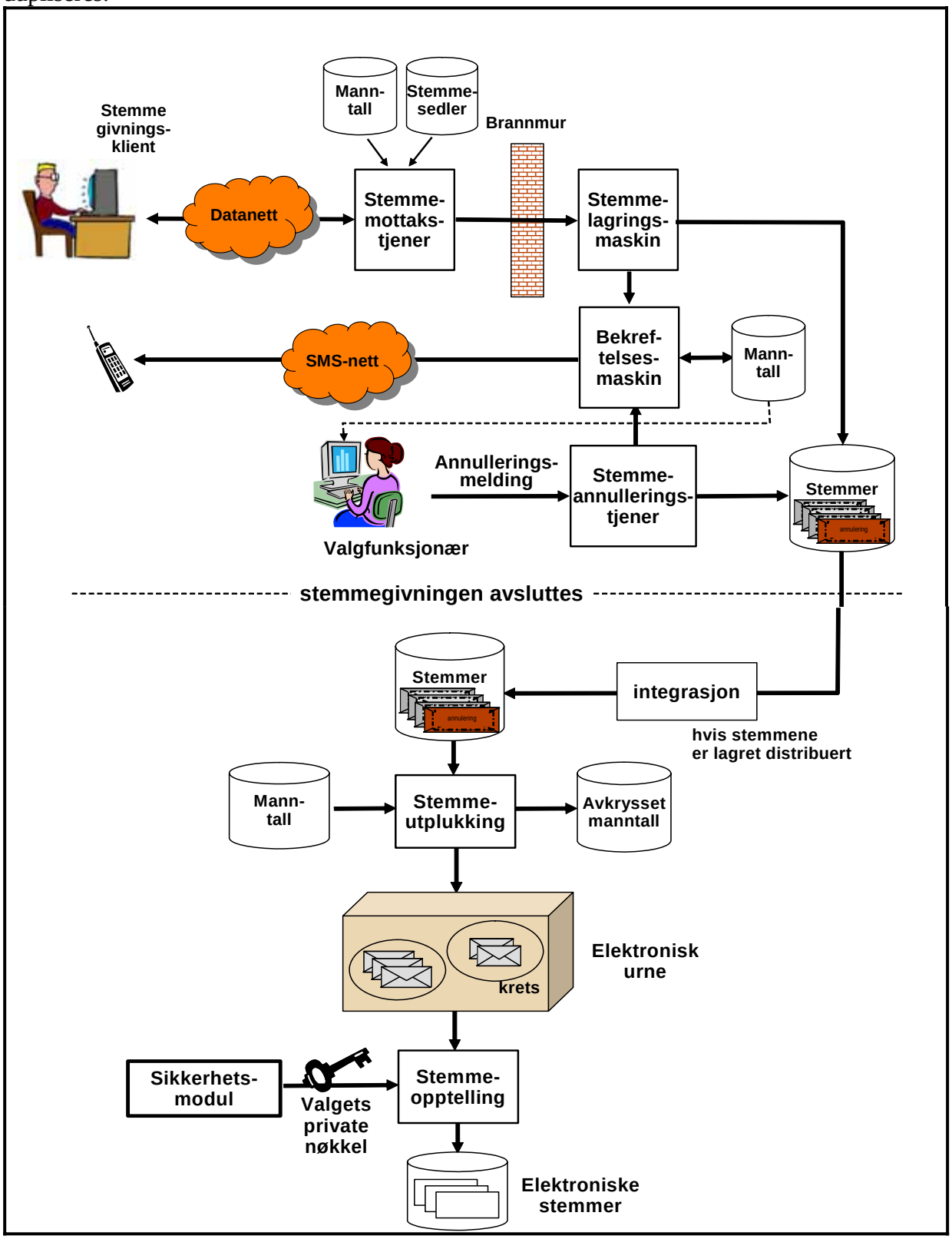
Kravet til verifisering generelt og den skisserte sertifiseringsordringen spesielt gjør imidlertid at det må stilles krav om at kildekoden skal være tilgjengelig for inspeksjon. Dette innebærer at alle leverandører av sentrale komponenter må forplikte seg til å gi tilgang til kildekoden for kontroll og verifisering.

8.7.8 Brukergrensesnittet

Brukergrensesnittet for stemmegivningen er også sentralt, og bør standardiseres eller underlegges strenge spesifikasjoner og retningslinjer (noen slike krav finnes allerede i Europarådets anbefaling, se punkt 61 til 65). Målet må være at grensesnittet er mest mulig likt fra valg til valg, uavhengig av hvilken produsent som har laget det.

8.7.9 Distribuert tjenerstruktur

I figur 8.13 er vist en samlet oversikt over de ulike datamaskinbaserte delsystemene i et stemmegivningssystem som er bygd opp etter de prinsippene som er skissert i dette kapitlet. I dette avsnittet tar vi opp i hvilken grad de ulike sentrale systemene bør distribueres og dupliseres.



Figur 8.13: Samlet oversikt over stemmegivningssystemet

Stemmemottakstjenere
Det er viktig å sikre en høy tilgjengelighet av stemmemottakstjenere. I et nasjonalt, fullt utbygd e-valg-system må det derfor finnes flere stemmemottakstjenere, plassert på ulike geografiske steder. Sannsynligheten for at alle tjenerne blir satt ut av spill på grunn av tjenestenektangrep, tekniske problemer, driftsproblemer, strømbrudd etc. vil da være liten.

Stemmelagringsmaskiner og stemmeannuleringstjenere
Arbeidsgruppen anbefaler at stemmene lagres på én eller et fåtall stemmelagringsmaskiner, hovedsakelig med tanke på sikkerhet og oppetid. Risikoen for avvik og driftsforstyrrelser øker med antall separate lagringssteder. Man må også ta med i betraktningen at i en distribuert løsning kan stemmer og ”annulleringskonvolutter” fra samme velger ligge på ulike maskiner, og disse må samordnes før stemmeutplukkingen. Et valgsystem basert på hundrevis av "elektroniske urner" som samler inn stemmer for senere overføring til opptelling regnes derfor som mindre aktuelt.

Øvrige sentrale systemer
For de øvrige sentrale systemene (stemmeutplukking og opptelling) anbefaler arbeidsgruppen av sikkerhetsgrunner at alle maskiner i prinsippet samles på ett eller et fåtall steder. Dette er prosesser som må skje under overvåkning og med utførlig logging av gjennomførte transaksjoner

Selve maskinvaren og infrastrukturen må utformes slik at det ikke eksisterer noen "single point of failure". Det betyr at alle kritiske komponenter må dupliseres, blant annet med flere nettforbindelser og flere fysiske tjenere som kjører i parallell. Strømforsyningen må sikres. Det er også nødvendig å ha tilgang til reserveinstallasjoner, fortrinnsvis på et geografisk annet sted, for det tilfelle at de sentrale systemene blir satt ut av drift.

For å øke sikkerhetsnivået kan man tenke seg en duplisering av de sentrale løsningene med sikte på å etablere et såkalt N-versjon-system (Liburd 2004). Prinsippet her er at de kritiske prosessene kjøres i parallell på flere maskiner, fortrinnsvis av ulikt fabrikat og med ulike operativsystemer, og med programvare produsert av ulike produsenter med ulike systemutviklingsmetoder. Hvis de parallelle prosessene gir samme resultat, har vi en høy grad av sikkerhet for at resultatene er korrekte. N-versjon-systemer garanterer i utstrakt grad mot utilsiktede feil og bevisst programmerte bakdører i de sentrale systemene. Slike løsninger vil være kostbare, men vil i utstrakt grad kunne forhindre innside-sabotasje og feilaktige resultater som følge av ubevisste feil.

8.8 Anbefaling

- De tekniske løsningene bør utformes slik at de lett kan tilpasses stemmegivning både i kontrollerte og ukontrollerte omgivelser og gjennom ulike tekniske kanaler. Dette forenkler kontroll- og sertifiseringsarbeidet, fjerner tekniske barrierer mot endringer hvis de teknologiske eller polistiske rammebetingelse endrer seg, og gjør at velgerne lett kjenner seg igjen i de nye rammene.
- Mottatte stemmer bør registreres på et ”write-once”-medium slik at det ikke er mulig å slette eller overskrive stemmen.
- Sikkerhetskritiske komponenter må sertifiseres av et uavhengig sertifiseringsorgan.
- For å gjøre programvareløsningene sikre og sertifiserbare, må sikkerhetskritiske komponenter skilles klart fra de øvrige komponentene, og de må utformes og

programmeres så enkelt at man gjennom inspeksjon av programteksten (såkalt hvitbokstesting) kan resonnere seg fram til at de er korrekte.

- Sikkerhetskritiske programvarebiblioteker, for eksempel for kryptering og dekryptering, skal være åpne, alminnelig tilgjengelig og godkjent av sikkerhetseksperter.
- For å muliggjøre hvitbokstesting, må leverandørene gi sertifiseringsorganene fri tilgang til kildekoden.
- Datautveksling mellom komponenter skal skje i et dataformat som spesifisert i EML-standarden, med unntak av datautvekslingen mellom stemmegivningsklient og stemmemottakstjener.
- Velgernes tilgang til valgsystemet bør reguleres gjennom bruk av offentlig godkjente PKI-løsninger på nivå Person-Høyt. Det skal ikke utstedes noe spesielt velgerakkreditiv som skal brukes bare i forbindelse med valg.
- Velgeren bør få kvittering på at stemmen er registrert i det sentrale systemet, fortrinnsvis gjennom en annen overføringskanal enn den som ble brukt for å avgi stemmen.
- For å øke sikkerhetsnivået, bør man vurdere bruk av N-versjon-systemer og duplisering av systemer og lagerenheter.
- Politisk bindende valg bør ikke gjennomføres med teknisk utstyr som er utenfor valgmyndighetens kontroll, før teknologien kan tilby vesentlig større sikkerhet enn i dag.

9 Kontroll og godkjenning av elektronisk stemmegivning

9.1 Innledning

Spørsmålet som behandles i dette kapitlet er hvordan vi best mulig skal sikre at de tekniske løsningene i elektroniske valg er like trygge og pålitelige som dagens manuelle løsninger. Det er særlig tre punkter i mandatet som omhandler dette:

- vurdere betydningen av en overgang fra lekmannskontroll til profesjonalisering; blant annet betydningen for valgsystemet mht kontroll, administrasjon av valg, kompetanse (punkt 14),
- vurdere ansvarsforholdene ved elektroniske valg, lokalt og nasjonalt (punkt 15),
- vurdere hvordan godkjenning av elektroniske system bør foregå (punkt 16).

Selv om de forskjellige kulepunktene framstiller litt ulike momenter, har de det til felles at alle handler om å bevare *tilliten* til politiske valg. Går vi for eksempel i retning av å fjerne lekmannskontrollen, kan vi risikere å rokke ved viktige demokratiske institusjoner nedarvet gjennom mange år med politiske valg i Norge. Betyr dette at ”dataekspertene” skal ta over kontrollen med valg?

Dette er vanskelige og viktige spørsmål. Nedenfor skal vi belyse disse og andre forhold i tur og orden. Vi starter med spørsmålet om elektronisk stemmegivning vil medføre endringer i systemet for lekmannskontroll. Deretter følger et generelt avsnitt om sertifisering. Grunnen er at dette er den løsningen arbeidsgruppen har sett som mest sentral (kanskje den eneste) for å møte utfordringene som er skissert over. Vi går så gjennom de viktigste formene for sertifisering (akkrediterte sertifiseringsorgan, sertifisering av virksomheter og sertifisering av tekniske løsninger). Videre går vi gjennom den norske løsningen med vekt på å utnytte eksisterende ordningene knyttet til informasjonssikkerhet. Så følger et kort avsnitt om behovet for en nasjonal kravspesifikasjon om elektroniske valg. Til slutt fremsettes det en del konkrete anbefalinger.

Hovedkonklusjonen i kapittelet er at en innføring av elektroniske valg vil medføre en delvis overgang fra lekmannskontroll til profesjonalisering. En e-valgsløsning vil få betydning for valgsystemet, både med hensyn til funksjonelle krav, kontrollfunksjonen, administrasjon av valg og kompetanse. Arbeidsgruppen legger imidlertid til grunn at dagens kontroll- og godkjenningsrutiner stort sett bør ligge fast i en forsøksperiode. Store endringer anses som lite hensiktsmessige, men utviklingen av nye løsninger for kontroll og godkjenning bør inngå som en viktig oppgave for den anbefalte prosjektgruppen, jf. kapittel 10. Som en interimløsning bør også denne prosjektgruppen ha godkjenningsansvar for den tekniske løsningen.

9.2 Fra lekmenn til profesjonalisering?

Et system for elektronisk stemmegivning endrer på mange måter forutsetningene for kontroll og godkjenning ved valg. Det er særlig tre forhold som er viktige i den forbindelse. For det første kan det ikke forutsettes at alle kommunene har den *tekniske kompetanse* som skal til for å kontrollere og godkjenne elektroniske stemmegivningssystem. Grunnen er at deler av

valgløsningene er svært kompliserte og tilgangen til IT- kompetanse er en knapp ressurs i mange kommuner.

For det andre medfører elektronisk stemmegivning *endringer i rutinene* for kontroll og godkjenning. Kontrollen er blant annet knyttet manuell kontroll av velgers identitet ved fremmøte, prøving av alle stemmegivninger og stemmesedler, opptelling av stemmesedlene og registrering av rettinger på disse. I dag utføres denne kontrollen av stemmestyrets og valgstyrets funksjonærer. I et manuelt system skal funksjonærer som står for opptelling, bokføre alle resultatene etter detaljerte oppsett fastsatt av departementet. Denne valgprotokollen legges frem for kommunestyret/fylkestinget når disse skal fatte beslutning om valget skal godkjennes eller ikke. Kommunestyret/fylkestinget kan således treffe sin beslutning på grunnlag en protokoll nedtegnet av dem som stod for kontrollen og opptellingen av de fysiske stemmesedlene. I et elektronisk system vil prøvingen av stemmene og selve opptellingen automatiseres. Valgprotokollen vil her utgjøre en utskrift fra valgsystemet. Tilsvarende skjer det en automatisering med hensyn til kontroll av velgers identitet. Automatiseringen av prosessen vil redusere kontrollarbeidet for valgfunksjonærene, men medfører samtidig en tilsløring av valgprosessen i form av begrenset innsyn og tilsyn for lekmenn.

For det tredje fremsettes det i *Europarådets anbefaling* flere konkrete krav til kontroll og godkjenning som arbeidsgruppen slutter seg til. Viktigst av disse er kanskje at e-valgsløsningene ”skal kunne kontrolleres av en uavhengig instans” (punkt 85). I tillegg fremkommer det at medlemsstatene ”skal innføre sertifiseringsprosesser” som tillater at ”alle IT-komponentene kan testes og sertifiseres” i henhold til de tekniske kravene som er beskrevet (punkt 111). Dette betyr at det mest sannsynlig må gjøres endringer i ansvars- og myndighetsfordelingen dersom elektronisk stemmegivning innføres på landsbasis eller i stor skala.

9.3 Om sertifisering

Som illustrert over peker både krav til kompetanse, hensynet til informasjonssikkerhet samt Europarådets Rekommandasjon i retning av en eller annen form for *sertifisering* av e-valgløsninger. Men hva menes egentlig?

Tanken bak sertifisering er at bestilleren (her valgmyndighetene) skal få hjelp fra en ”tiltrodd tredjepart” til å skape tillit. Med ”tiltrodd tredjepart” siktes det til ulike sertifiseringsorganer eller uhildede aktører som kan informasjonssikkerhet godt, og som derfor antas å være best skikket til å vurdere om leverandørene leverer det de lover. Selve sertifiseringen er en typegodkjenning av et produkt eller system basert på en forutgående evaluering (www.sertit.no). Slike evalueringer utføres av dataeksperter (i praksis ofte et anerkjent sikkerhetsfirma) og inneholder konkrete tekniske undersøkelser og tester av om løsningene som leverandører har laget oppfyller de funksjonelle og sikkerhetsmessige krav som settes. Kravene utarbeides vanligvis av myndighetene eller internasjonalt anerkjente standarder. Åpenbart kan slike ordninger ikke garantere at e-valgsløsningene er 100 % sikre, men de kan ved hjelp av adekvate metoder forsøke å identifisere eventuelle sikkerhetshull, kontrollere at resultatene som regnes ut er riktige, at leverandørene er til å stole på, osv. Sertifiseringer kan med andre ord bidra til å redusere risiko for bestilleren av e-valgsløsninger.

Prinsipielt kan vi skille mellom tre forskjellige typer sertifiseringer som arbeidsgruppen mener er nødvendig for å kontrollere systemer for elektronisk stemmegivning:

- Godkjenning av *virksomheter for sertifisering* (akkreditere sertifiseringsorgan).
- Godkjenning av *prosedyrer og rutiner* hos leverandører (sertifisering av virksomheter).
- Godkjenning av *teknisk utstyr og løsning* (sertifisering av produkter).

Det første kulepunktet - godkjenning av *virksomheter for sertifisering* - handler om å finne organisasjoner som er kompetente til å utføre kontroll av andre virksomheter og produkter. På IT- området finnes det flere slike og noen er direkte relaterte til IT- sikkerhet. Godkjente virksomheter omtales gjerne som "akkrediterte sertifiseringsorganer" eller evalueringsfirmaer. Vanligvis er løsningene basert på at det foreligger en klart definert standard; typisk Norsk standard (NS) eller Internasjonal standard (ISO) som vedkommende virksomhet blir sertifisert for. Et eksempel er at evalueringsfirmaet tilfredsstiller kriteriene om prøvetakingslaboratorium etter standarden NS ISO/IEC 17025:2005.[74] Det finnes imidlertid varianter av dette, for eksempel ulike former for "samsvarsvurdering" hvor det ikke foreligger konkrete standarder, men hvor virksomheter antas kompetente til å gjennomføre kontroller og anbefale godkjenninger av virksomheter og utstyr etter nærmere fastsatte kriterier, gjerne basert på en eller annen form for kravspesifikasjon. Dette er en noe mildere form for tiltrodde tredjeparter enn akkrediterte sertifiseringsorgan. For virksomheter som skal teste og sertifisere e-valgsløsninger i andre firmaer, er det selvsagt viktig at de selv kan dokumentere inngående forståelse for både de kravene som stilles og den praktiske gjennomføringen av politiske valg.

Det andre kulepunktet handler om godkjenning av *rutiner og prosedyrer* hos leverandørene (virksomhetssertifisering). Det sentrale er at de virksomhetene som skal levere valgløsninger bør ha gjennomført sertifiseringsprosesser som sikrer at de kravene som stilles til dem, etterleves. Eksempler på krav kan være at leverandørene har beredskapsplaner, klare ansvarsforhold, vaktordninger, rutiner for feilmottak og retting, tilgangskontroll, dokumentasjon, opplæring, etc. Det er videre vanlig å stille krav om at det er gjennomført sårbarhets- og risikoanalyser. Anvendt på elektronisk stemmegivning betyr det at det stilles konkrete krav til at hele eller deler av et valgsystem (i vid forstand) er bygget på en bred gjennomgang av mulige risikoer som kan true en vellykket gjennomføring. Virksomheten skal videre, på grunnlag av risikovurderingen, kunne dokumentere at løsningene er tilfredsstillende beskyttet for å overkomme de risikoer som fremkommer i analysen. Det skal for eksempel være predefinerte grenser for svikt i systemet. Risikoanalysen skal kunne dokumenteres og gjøres tilgjengelig for sertifiseringsmyndigheten. Risikoanalysen eller andre nødvendige krav til potensielle leverandører forutsetter dessuten at det legges til grunn lover og regler som regulerer området, jf. kapittel 6. Leverandørenes rutiner og prosedyrer kan godkjennes i forkant av eventuelle tilbud, og er i prinsippet uavhengig av den tekniske valgløsningen. En virksomhetssertifisering kan kun utføres av godkjente sertifiseringsorganer eller evalueringsfirmaer (jf. punktet over). Dette betyr i klartekst at *valgmyndighetene ikke kan velge leverandører av tekniske valgløsninger som ikke er forhåndsgodkjent.*

Det finnes litt ulike standarder for å godkjenne slike rutiner og prosedyrer hos virksomheter. I tillegg til den foreliggende anbefaling fra Europarådet, er et nærliggende sett av standarder NS-ISO/IEC 17799:2005[75] og ISO/IEC 27001:2005.[76] Begge standardene omtaler styring av

[74] NS-EN ISO/IEC 17025:2005: Generelle krav til prøvings- og kalibreringslaboratoriers kompetanse. Ytterligere informasjon om standarden finnes på nettsidene http://www.standard.no

[75] NS-ISO/IEC 17799:2005: Informasjonsteknologi, administrasjon av informasjonssikkerhet. Ytterligere informasjon om standarden finnes på finnes på nettsidene http://www.standard.no/

[76] ISO/IEC 27001:2005: Information technology -- Security techniques -- Information security management systems – Requirements. Standarden f.o.m. høsten 2005 erstattet Britisk standard (BS) 7799-2. Ytterligere informasjon om standarden finnes på nettsidene http://www.standard.no

”informasjonssikkerhet”. Forenklet kan man si at NS-ISO/IEC 17799:2005 konsentrerer seg om tiltak som skal bedre informasjonssikkerhet. Tiltakene er flerfoldige og relateres til ulike deler av virksomhetene. Standarden gir dessuten nokså klar rettledning når det gjelder etablering av sikkerhetsstrategi, ledelsesinvolvering, ansvarsplassering, fysisk sikring, tilgangskontroll, implementering, drift, avhending, etc. Når det gjelder ISO/IEC 27001:2005 er fokuset mer på selve styringssystemet for informasjonssikkerhet (ISMS – Information Security Management System). Eksempler på elementer i styringssystemene er rutiner for å etablere, drifte, overvåke og bevare samt dokumentere kontroll og ledelse. I tillegg inneholder standarden en liste over sentrale mål og tiltak som skal velges ut som en del av arbeidet med å etablere et styringssystem for informasjonssikkerhet (www.standard.no).

Det tredje kulepunktet handler om godkjenning av *de tekniske løsningene* (produktsertifisering). De viktigste kravene er beskrevet i kapitlene foran og i Europarådets anbefaling. Vi skal ikke gå i detalj på dette her, men kort fremheve en del momenter som er særlig relevante for kontroll og godkjenning. For det første bør det fastsettes konkrete kvalitetskriterier for de enkelte tekniske komponentene som inngår i valgløsningene. På den måten er det mulig å sette et klart skille mellom sikre og usikre komponenter. Videre må løsningene som et minimum verne kildekode mot endringer etter inspeksjon; fysiske tiltak, versjonskontroll, sjekksummer og digital forsegling. Ikke under noen omstendigheter skal det anvendes kritiske tekniske løsninger som ikke er forhåndsgodkjent, og det må føres logg over alle endringer i valgsystemene. Videre må det stilles som et overordnet krav at løsningene skal være transparente. Dette betyr at samtlige komponenter i løsningene skal være tilgjengelige – i det minste for ansvarlige valgmyndigheter og tiltrodde tredjeparter – for kontroll og sertifisering etter behov. Vilkår for tilgang til kildekode skal avklares konkret, og ved endringer av teknisk karakter skal dette dokumenteres og rapporteres til valgmyndighetene. Kort sagt skal de tekniske løsningene sikre stemmenes kvalitet, tilgjengelighet, integritet og konfidensialitet. Endelig skal løsningen også holde stemmene hemmelige og forseglet frem til opptelling. Hvis de er lagret eller formidlet utenfor kontrollerte omgivelser, skal de krypteres. Dette inkluderer å sikre at informasjon om avgitte stemmer og velgerinformasjon skal oppbevares og holdes forseglet så lenge datamaterialet kan kople sammen velgere og stemme.

9.4 Nærmere om sertifiseringsordningene i Norge

Ser vi nærmere på ordningene i Norge, finnes det særlig to forskjellige og delvis komplementære miljøer. Begge miljøene omhandler informasjonssikkerhet, og må slik sett sies å representere kompetente miljøer som i stor grad synes å kunne støtte både leverandørenes og myndighetenes arbeid ved gjennomføring av elektroniske valg i Norge. Dog er det viktig at disse miljøene tilføres fagspesifikk kompetanse på valg, noe som i dag antakelig i hovedsak mangler.

Den ene ordningen er *Norsk Akkreditering* (NA) som er utpekt av Nærings- og handelsdepartementet til å utføre teknisk akkreditering og inspeksjon i henhold til OECDs regelverk om ”God Laboratoriepraksis” (GLP). Akkreditering er ”en offisiell anerkjennelse av en organisasjons kompetanse og evne til å utføre angitte oppgaver i samsvar med gitte krav” (www.akkreditering.no). Ordningen fungerer på den måten at visse virksomheter, etter kontroll og godkjenning av Norsk Akkredittering, blir ”akkrediterte sertifiseringsorganer”. På IT-området finnes det flere slike, men bare tre virksomheter er i dag akkreditert på IT-sikkerhet, og da etter den internasjonale standarden ”Informasjonsteknologi-Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet” (NS-ISO/IEC 17799:2005):

- Det Norske Veritas Certification AS
- Nemko Certification AS
- Teknologisk institutt Sertifisering AS.

Styrken i denne ordningen er kanskje primært styring av informasjonssikkerhet i organisasjoner. Den omhandler god praksis for informasjonssikkerhet og favner nærmest alle aspekter som er viktige for å drive et helhetlig informasjonssikkerhetsarbeid. Enkelte aktører tilbyr også bistand ved utferdigelse av kravspesifikasjoner for bestiller samt andre tjenester relatert til informasjonssikkerhet. Svakheten, slik arbeidsgruppen ser det, er at disse miljøene ikke formelt og eksplisitt er sertifisert til å gjennomføre tekniske analyser, herunder evalueringer av enkeltkomponenter i valgsystemet.

Den andre ordningen er Nasjonal sikkerhetsmyndighet (NSM), og da særlig *Sertifiseringsmyndigheten for IT- sikkerhet (SERTIT).* Bakgrunnen for denne ordningen var at Rådet for IT-sikkerhet (RIS) i 1997 anbefalte å opprette en ordning for nettopp sertifisering av IT-sikkerhet i tekniske produkter og systemer. I dag er SERTIT er en offentlig sertifiseringsmyndighet for IT-sikkerhet, underlagt en tverrinstitusjonell styringskomité bestående av følgende aktører:

- Forsvarsdepartementet (leder)
- Fornyings- og administrasjonsdepartementet
- Justis- og politidepartementet
- Nasjonal sikkerhetsmyndighet
- Datatilsynet
- Norsk Akkreditering
- Abelia
- Standard Norge.

SERTIT, som også er sekretariat for denne styringskomitéen, har som oppgave å utstede sertifikater og sertifiseringsrapporter til så vel private som offentlige aktører. Videre er SERTIT ansvarlig for å lage rammevilkår og regler for sertifisering av IT-sikkerhet i Norge samt påse at reglene følges opp av partene. De er også ansvarlig for å godkjenne private firma som evalueringsfirmaer samt føre tilsyn med disse. Virksomheter som skal fungere som evalueringsfirmaer, må kunne godkjennes etter spesifikke kriterier samt være akkreditert som prøvetakingslaboratorium etter NS-ISO 17025. Firmaene må for eksempel gjennomføre en prøveevaluering for å vise forståelse for standarden *Common Criteria,* og metodikken *Common Evaluation Methodology (*www.sertit.no). SERTIT representerer også Norge i det internasjonale forumet *"Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)".* Dette er relevant fordi anbefalingen fra Europarådet på flere områder er tuftet på og legger til grunn de sikkerhetsmekanismer som nettopp finnes i Common Criteria (CC). SERTIT har godkjent to virksomheter som evalueringsfirma under ordningen:

- NorConsult AS
- SeCode Norge AS

Den viktigste fordelen med SERTIT-ordningen er at virksomhetene også sertifiserer tekniske komponenter. Ulempen er at ordningen langt på vei er basert på et nokså omfattende (og slik sett kostbart) sett av kriterier. Virksomhetene har derfor relativt sett få oppdrag og referanser. Men porteføljen er voksende så vel nasjonalt som internasjonalt. Det finnes dessuten ulike moduler og nivåer som skaper en viss fleksibilitet. Endelig er det vesentlig at dette miljøet kjenner og er oppdatert på de rutinene som har dannet grunnlaget for den

sikkerhetsmetodologi som er lagt til grunn for anbefalingen fra Europarådet (Common Criteria/ ISO/IEC 15408:2005).[77]

9.5 Nærmere om kravspesifikasjon

Uavhengig av om og hva slags sertifiseringsregime som eventuelt velges, er det en grunnleggende forutsetning at det utvikles en eller annen form for "standard" eller kravspesifikasjon for elektroniske valg i Norge.[78] En slik kravspesifikasjon bør knytte sammen de mest relevante dokumenter som er omhandlet i denne rapporten (sikkerhetsstandarder, Europarådets anbefaling, lover og forskrifter, mv.). Innholdsmessig kan slike kravspesifikasjoner variere, men typiske elementer er som følger:

- Funksjonelle krav
  - *Fastsatt i anbefalingen fra Europarådet med forklarende memorandum (se vedlegg A)*
  - *Krav til løsningen slik det fremkommer i den juridiske gjennomgangen, jf. kapittel 6*
  - *Krav til løsningen slik det fremkommer i den tekniske løsningen, jf. kapittel 8*
- Krav til leverandøren
  - *Sertifisert etter NS-ISO/IEC 17799:2005: Informasjonsteknologi, administrasjon av informasjonssikkerhet*
  - *Sertifisert etter ISO/IEC 27001:2005: Information technology -- Security techniques -- Information security management systems – Requirements*
  - *Forhold ved bruk av underleverandører*
  - *Responstid ved feil og brukerstøtte*
  - *Videreutvikling*
  - *Bistand ved ny leverandør (oppkjøp, konkurs, etc.)*
- Krav til leveransen
  - *Opplæring*
  - *Dokumentasjon*
  - *Test av leveransen*
- Krav til versjonskontroll
  - *Endringsrutiner*
  - *Etterprøvbarhet*
  - *Sjekksum, mv.*
- Krav til drift og vedlikehold
  - *Krav til ytelse (tilgjengelighet (oppetid), kapasitetsbehov, tjenestekvalitet)*
  - *Feilmottak og dokumentasjon av feil*

[77] Standarden består av tre deler: I del 1 (ISO/IEC 15408-1:2005) fremkommer en introduksjon samt et generelt rammeverk for evalueringer av informasjonssikkerhet. I del 2 (ISO/IEC 15408-2: 2005) fremsettes en lang rekke funksjonelle krav til sikkerhet i IT-systemer. I del 3 (ISO/IEC 15408-3:2005) fremsettes kravene til kvalitetssikring av løsningene, mv. Ytterligere informasjon om forholdet mellom standarden og rekommandasjonen fra Europarådet finnes i forklarende memorandum til rekommandasjonen. For ytterligere informasjon om ISO/IEC 15408:2005 anbefales sidene til ISO (www.iso.org/http) og Common Criteria (www.commoncriteriaportal.org).

[78] Dette er for eksempel gjort i USA. Utviklingen av en standard for elektronisk stemmegivning har der pågått i flere år i regi av Election Assistance Commission (EAC). I praksis styres arbeidet av en komité (Technical Guidelines Development Committee) som ledes av National Institute of Standards and Technology (NIST). Ytterligere informasjon om standarden og organiseringen av arbeidet finnes på sidene http://vote.nist.gov/. Se også kapittel 4.

  - *Brukerstøtte i ulike faser*
  - *Beredskap (krise – katastrofe)*
- Lokale tilpassinger (opsjoner)
  - *Konkrete aksesspunkter (bygg)*
  - *Infrastruktur*
  - *Integrasjon med eksisterende teknologi*
  - *Vaktordninger, opplæring, etc.*

Listen er langt fra fullstendig, men kun ment som illustrasjoner på enkelte sentrale krav som bør stilles i en norsk kravspesifikasjon for elektronisk stemmegivning. Detaljer må avklares ytterligere og mer konkret. Arbeidsgruppen har dessuten vurdert og anbefalt en teknisk løsning som skal danne grunnlaget for å utferdige et slikt dokument. Vi har imidlertid ikke funnet det hensiktsmessig eller mulig å ferdigstille kravspesifikasjonen innenfor de gitte rammer. For øvrig ser arbeidsgruppen at en slik kravspesifikasjon er helt nødvendig for det videre arbeidet med elektronisk stemmegivning. Tre bruksområder kan fremheves: For det første brukes kravspesifikasjonen av *leverandørene* (systemutviklerne) ved utvikling og for å få godkjent sin virksomhet, underleverandører og de tekniske løsningene. For det andre brukes den av *sertifiseringsorganene* som kriterier for å sertifisere leverandører og tekniske løsninger (ev. gjennomføre samsvarsvurderinger). Og sist, men ikke minst, brukes kravspesifikasjonen av *valgmyndighetene* i forbindelse med anbudsrunden som referansedokument, ev. med lokale opsjoner.

9.6 Anbefaling

Det overordnede spørsmålet som har vært behandlet i dette kapitlet er hvordan vi best mulig skal sikre at de tekniske løsningene i elektroniske valg er trygge. Dette er svært vanskelig, men samtidig vesentlig dersom tilliten til den norske valgordningen skal beholdes. Hovedargumentet er at før et e-valgsystem innføres, og ved visse mellomrom etter innføring, skal en uavhengig instans, utpekt av valgmyndighetene, kontrollere at systemene er i orden og at de nødvendige forholdsregler med hensyn til sikkerhet er tatt hos leverandørene. Dette innebærer følgende konkrete anbefaling:

- Det bør gjennomføres en forhåndsgodkjenning (sertifisering) av personell og virksomheter som på vegne av valgmyndighetene skal godkjenne leverandører og tekniske løsninger for elektroniske valg (akkrediterte sertifiseringsorgan eller evalueringsfirmaer).
- Det bør gjennomføres en forhåndsgodkjenning (sertifisering) av *prosedyrer og rutiner* som leverandører av elektroniske valgløsninger skal ha for å sikre valgløsningene. Ansvarlig for å godkjenne leverandørene er akkrediterte sertifiseringsorgan. Valgmyndighetene skal *kun* anvende leverandører som er godkjent/sertifisert på de kritiske delene av løsningen for elektroniske valg.
- Det bør gjennomføres en forhåndsgodkjenning (sertifisering) av *teknisk utstyr og teknisk løsning*. Utstyr som mangler godkjent/sertifisering bør som hovedregel ikke anvendes i valgløsningen. For kritiske deler av løsningen *skal* sertifisering foreligge.

På denne måten er det mulig å redusere risiko for valgmyndighetene, men det gir ingen garanti. Den anbefalte løsningen vil medføre en delvis overgang fra lekmannskontroll til profesjonalisering. E-valgsløsningen vil slik sett få betydning for valgsystemet, både med hensyn til kontrollfunksjonen, administrasjon av valg og kompetanse. En forutsetning for den

anbefalte løsningen er imidlertid at det utferdiges en god kravspesifikasjon for elektroniske valg i Norge. Inntil det eventuelt foreligger en *de facto* standard for elektroniske valg eller lov og forskrift, skal kravspesifikasjonen klart angi de juridiske, operasjonelle og tekniske krav som fremsettes i anbefalingen fra Europarådet. Den skal også klart identifisere og ivareta de endringer og tillegg til Europarådets anbefaling som er skissert i den anbefalte tekniske løsningen, jf. kapittel 8.

Fremgangsmåten som arbeidsgruppen ser for seg i praksis er at sentrale valgmyndigheter utferdiger kravspesifikasjonen. Det praktiske arbeidet kan imidlertid settes bort til en kvalifisert virksomhet. Hovedtanken er å gjenbruke eksisterende ordninger for sertifisering av virksomheter og tekniske løsninger på området informasjonssikkerhet. Det presiseres at arbeidsgruppen ikke anbefaler at det opprettes noe nytt sertifiseringsorgan spesielt for elektroniske valg. Kravspesifikasjonen bør deretter gjøres tilgjengelig for aktuelle tilbydere av e-valgsløsninger i Norge og utlandet. På denne måten varsles leverandørene om at de må få godkjent sin egen virksomhet, underleverandører og ikke minst de tekniske løsningene, dersom de ønsker å være tjenestetilbyder på det norske markedet. Sertifiseringsorganene får også gjennom kravspesifikasjonen klare kriterier å sertifisere leverandører og tekniske løsninger ut i fra. I et forsøksregime vil valgmyndighetene deretter bruke kravspesifikasjonen som referansedokument ved anbud, eventuelt supplert av lokale opsjoner.

Arbeidsgruppen ser også at oppbyggingen av godkjenningsordningen for elektroniske valg vil ta noe tid og bør inngå som en viktig oppgave for den anbefalte prosjektgruppen, jf. kapittel 10. Som en interimløsning bør også denne prosjektgruppen ha godkjenningsansvar for den tekniske løsningen. Representanter for sertifiseringsmiljøene i Norge bør således være representert i prosjektgruppen, eller i det minste konsultert.

10 Forsøk - plan og rammer

10.1 Innledning

Det overordnede mål for arbeidsgruppens anbefalinger er å gjøre det enklere og mindre kostnadskrevende for velgeren å utøve sine demokratiske rettigheter. Et middel for å oppnå dette er å tilby elektronisk stemmegivning i ukontrollerte omgivelser for alle velgere. I tillegg til økt tilgjengelighet vil elektronisk stemmegivning på sikt bidra til reduserte kostnader i forbindelse med valgavviklingen, og raskere og mer nøyaktig opptelling av stemmene. Det kan innvendes at denne form for stemmegivning vil svekke det preg av høytidelighet som kjennetegner valghandlingen i et tradisjonelt valglokale. I den forbindelse vil arbeidsgruppen understreke at elektronisk stemmegivning kun er ment som et *supplement* til den tradisjonelle måten å avgi stemme på, og at stemmegivning i valglokale vil bestå i overskuelig fremtid. Dette innebærer at velgere som ikke føler seg trygg på teknologien, fortsatt vil kunne stemme på tradisjonell måte. Det kan også pekes på at den utstrakte bruken av forhåndsstemmegivning allerede har bidratt til å endre den tradisjonelle måten å avgi stemme på.[79]

Hvis man skal tillate stemmegivning i ukontrollerte omgivelser – uansett om stemmen avgis elektronisk eller manuelt (for eksempel pr. brev) – har man ikke lenger en garanti for at kravet om hemmelig stemmegivning blir ivaretatt på en tilfredsstillende måte. Det åpnes både for utilbørlig påvirkning av velgeren (*family voting*) og kjøp og salg av stemmer. Ved å tillate velgeren å stemme flere ganger i forhåndsstemmeperioden, og ved å åpne for at velgeren kan stemme på nytt i kontrollerte omgivelser på valgtinget, reduseres denne faren betydelig selv om den ikke forsvinner helt.

Det må videre være en ufravikelig forutsetning for elektronisk stemmegivning i ukontrollerte omgivelser at det legges til grunn strenge krav til sikkerhet, og at det skjer på en måte som ikke svekker velgernes tillit til systemet. Med dagens teknologi er det ikke mulig å garantere en slik sikkerhet. Arbeidsgruppen vil derfor ikke anbefale elektronisk stemmegivning i ukontrollerte omgivelser i fullskala nå.

Det kan likevel tenkes at det vil oppstå et betydelig press i retning av å innføre elektronisk stemmegivning i ukontrollerte omgivelser på et senere tidspunkt Et slikt press kan for eksempel komme som følge av den generelle samfunnsutvikling der IKT tas i bruk på stadig flere områder, fordi det innføres i andre land eller som følge av dramatiske fall i valgdeltakelsen. For å unngå at man havner i en situasjon der elektronisk stemmegivning i ukontrollerte omgivelser blir innført *uten* forutgående utprøving, vil arbeidsgruppen sterkt understreke behovet for en offensiv satsing fra myndighetenes side. Det bør så snart som mulig settes i gang planmessige forsøk og systematisk evaluering.

[79] Ved de tre siste stortingsvalgene er mellom rundt 20 prosent av stemmene avgitt på forhånd. Se figur 5.1

10.2 Hensikten med forsøk

Det er mange grunner til at et det bør gjennomføres omfattende forsøk før man tar i bruk et elektronisk valgsystem som skal være tilgjengelig i ukontrollerte omgivelser. Følgende tre punkter anses spesielt viktig:

- Sikre velgernes tillit til valggjennomføringen.
- Avklare problemstillinger knyttet til mulighet for kjøp/salg av stemmer og utilbørlig påvirkning.
- Etablere tekniske løsninger som dekker fundamentale krav til sikkerhet.

Velgernes tillit til valgsystemet er av stor betydning, ikke bare for valgdeltagelsen, men også for hele vårt demokratiske system. Grunnlaget for tillit er blant annet full forståelse av det systemet som benyttes til å avgi stemmer. Tradisjonell måte å avgi stemme på er enkel, kjent og gjennomprøvd. I vår tradisjon har velgerne derfor stor grad av tillit til valgsystemet. Denne er opparbeidet over lang tid og knyttet til et hvert trinn i valgprosessen. Tilliten til systemet kan imidlertid raskt forsvinne. Det er tilstrekkelig at det sås tvil om systemets virkemåte. I henhold til Europarådets anbefaling punkt 20 skal medlemslandene ”ta forholdsregler for å sikre at velgerne forstår og har tillit til det e-stemmegivningssystemet som benyttes”.

De overordnede forhold forbundet med flytting av valghandlingen fra kontrollerte omgivelser til ukontrollerte omgivelser er diskutert i kapittel 5. Problemstillingene knyttet til utilbørlig påvirkning og kjøp/salg av stemmer er kompliserte og omfattende. Det er stort behov for å evaluere betydningen og konsekvensen av denne type utfordringer.

Dagens tekniske løsninger er etter arbeidsgruppen mening ikke gode nok til at vi kan anbefale generell innføring av elektronisk stemmegivning i ukontrollerte omgivelser på det nåværende tidspunkt. For elektronisk stemmegivning over Internett er det problemer knyttet til sikkerhet på klientmaskinen, dvs. velgerens personlige datamaskin som er den største utfordringen. For andre typer tekniske løsninger som SMS vil det stilles store krav til brukerdialog/grensesnitt, og denne type løsning vil også kreve omfattende utprøvning. Det er også svært viktig at den tekniske løsningen er av en slik art at den sikrer hemmelig valg, og at den sikrer mot tap og manipulering av avgitte stemmer.

Forsøk er viktig for å finne ut hva som fungerer, stimulere til offentlig debatt og ikke minst skape tillit til systemene på sikt. Gjennom forsøk kan løsninger prøves ut i liten skala før ordningen eventuelt gjøres landsomfattende. Det kan være spesielt nyttig å prøve seg fram der hvor omlegginger har omfattende konsekvenser. Tilsvarende er forsøk aktuelt hvor det ikke er kommet fram til klart definerte alternativer, eller det er usikkert hvilken vei en skal gå. Gjennom prøving og feiling samles erfaringer som man kan bruke til nærmere presisering av løsninger. Forsøk kan dessuten ofte skape en mobilisering for endring ved at deltakerne får anledning til å gjøre noe nytt og utvikle gode eksempler. På den måten kan forsøk være med på å overkomme en del motstand, vinne ny kunnskap og berede grunnen for omstilling. Endelig ser arbeidsgruppen det som nødvendig å høste erfaringer med elektronisk stemmegivning gjennom forsøk, som i sin tur kan danne grunnlag for eventuelle lovendringer.

10.3 Plan for forsøksvirksomhet

10.3.1 Organisering

Erfaringene fra forsøk i utlandet har vist at forsøk med elektronisk stemmegivning vil være både omfattende og ressurskrevende. Derfor må det det avsettes betydelige ressurser til både forberedelser, gjennomføring og evaluering av forsøksvirksomheten. Forsøkene bør gå over flere valg, med gradvis utvidelse av funksjonalitet og med trinnvis utprøving av ulike typer ordninger.

Gjennomføring av valg berører grunnleggende prinsipper ved vårt demokrati. Forsøk rundt elektronisk stemmegivning krever således en systematisk utprøving. Dette gir også grunnlag for en planmessig evaluering, noe som er nødvendig i en forsøksprosess over flere valg. Vi ser det derfor som nødvendig at forsøkene initieres og styres sentralt, men med aktiv deltagelse fra involverte lokale valgmyndigheter. Deltagelse fra lokale myndigheter må være basert på frivillighet.

Arbeidsgruppen anbefaler at det settes ned en prosjektgruppe med bred sammensetning som får det overordnede ansvaret for gjennomføringen av forsøket. Prosjektgruppen må ha både valgfaglig, datateknisk og juridisk kompetanse og må underlegges Kommunal- og regionaldepartementet. Før forsøkene starter må det være avsatt tilstrekkelige økonomiske ressurser. I samsvar med det som er sagt ovenfor antar arbeidsgruppen at forsøkene må finansieres sentralt.

10.3.2 Rammer

Forsøk bør gjennomføres i utvalgte kommuner etter sentralt initiativ. Det kan være aktuelt med utprøving overfor bestemte grupper velgere, for eksempel grupper av funksjonshemmede. Forsøkene må imidlertid organiseres slik at kravene til hemmelighold av stemmegivningen ikke krenkes. I denne sammenheng er det viktig å være oppmerksom på at det ikke prøves ut ordninger der det vil bli avgitt for få elektroniske stemmer pr. valgkrets. Dette kan for eksempel være tilfellet med forsøk blant utenlandsboende. Disse velgerne er spredt over hele verden, men stemmen skal sendes og telles opp sammen med andre stemmer i den valgkretsen i Norge vedkommende tilhører (dvs. der vedkommende sist var folkeregisterført som bosatt).

Folkeavstemminger reguleres ikke i valglovgivningen. Kommunene står fritt til å gjennomføre folkeavstemminger og til å fastsette regler for slike avstemminger. En folkeavstemming kan kun være rådgivende, og det er for eksempel ikke krav til at alle stemmeberettigede innenfor aktuelle kommune skal delta. Lokale folkeavstemminger kan derfor ligge vel til rette for utprøving av elektronisk stemmegivning. Arbeidsgruppen vil imidlertid anbefale at slike forsøk inngår i, styres og organiseres av sentrale myndigheter. På denne måten vil forsøkene kunne inngå i en overordnet plan for forsøk knyttet til elektronisk stemmegivning, og dermed komme inn under den planmessige evalueringen for å vinne kunnskap om denne formen for stemmegivning.

Utprøving ved skolevalg vil, som følge av de spesielle forhold som gjør seg gjeldende for slike valg, ha begrenset verdi. Kunnskap fra forsøk i forbindelse med skolevalg er i bare delvis overførbar til ordinære valg. Skolevalg kan imidlertid benyttes til utprøving av enkelte viktige elementer som brukergrensesnitt og kapasitet.

10.3.3 Overordnet plan

Arbeidsgruppen anbefaler at forsøkene gjennomføres i klart avgrensede trinn og med veldefinerte rammer i form av omfang og hensikt. Hvert trinn må bringe forsøkene fremover og gi reelle bidrag, samtidig som at det er en forutsetning at risikoen avgrenses.
Det anbefales at forsøksvirksomheten begynner i kontrollerte omgivelser. I senere trinn tenker vi oss at valghandlingen gradvis flyttes ut i ukontrollerte omgivelser som vist under:

- Kontrollert — Elektronisk stemmegivning i valglokaler eller andre lokaler som er under kontroll av valgfunksjonærer.
- Ukontrollert (i) — Elektronisk stemmegivning i ukontrollerte omgivelser med kontrollert utstyr. Dette innebærer at det distribueres en CD-ROM (eller tilsvarende) med grunnleggende programvare som benyttes til å starte opp velgerens terminal ved valghandlingen. Dette sikrer kontrollert kanal fra velgerens tastatur til stemmemottaksmaskinen og reduserer risikoen for virusangrep på velgerens maskin. En kontrollert kanal muliggjør også en sikker logg/kvitteringsløsning.
- Ukontrollert (ii) — Elektronisk stemmegivning over åpent Internett der standard personlig datamaskin og operativsystem benyttes. Dette omfatter også stemmegivning over andre kanaler som for eksempel SMS. Dette forutsetter at det gjøres betydelige fremskritt i sikkerhetsløsninger for personlig datamaskin og Internett.

Et første trinn som kun prøver ut valgløsninger i kontrollerte omgivelser, vurderes til å gi et for begrenset bidrag, og arbeidsgruppen ønsker derfor å kunne utvide omfanget på første trinn av forsøksvirksomheten gjennom at det tas hensyn til type valg:

- Bindende — Bindende politiske valg som stortings-, sametings-, fylkestings- og kommunestyrevalg. I denne type valg kan valghandlingen være komplisert som følge av omfattende stemmesedler og rettemuligheter. Konsekvensen av feil kan være meget stor. Ved bindende politiske valg må det stilles meget høye krav til sikkerhet i alle ledd.
- Rådgivende — Rådgivende folkeavstemninger og andre ikke bindende valg på lokalt nivå. I denne type valg er konsekvensene ved feil mindre og kravene til sikkerhet noe lavere enn ved tradisjonelle bindende valg.

Tabell 10.1: Overordnet plan for forsøkene

Omgivelser	Type valg	Trinn1	Trinn2	Trinn3
Ukontrollert, ukontrollert maskin (i)	Bindende			
	Rådgivende			
Ukontrollert, kontrollert maskin (ii)	Bindende			
	Rådgivende			
Kontrollert	Bindende			
	Rådgivende			

10.3.4 Oppstart

Ramme
Etablere prosjektorganisasjon og klargjøre for forsøksvirksomhet.

Formål
Det første trinn i forsøksvirksomheten vil omfatte etablering av en prosjektorganisasjon med tilhørende mandat, fremdriftsplan og finansiering. Prosjektgruppen vil starte sitt arbeid med å utarbeide en kravspesifikasjon for elektroniske valg. Denne kravspesifikasjonen bør bygge på eksisterende dokumentasjon og bør dekke følgende sentrale områder (se kapittel 9 for en mer detaljert innholdsfortegnelse):

- Overordnede krav med henvisning til relevante lover og standarder
- Funksjonelle krav, inkludert krav til sikkerhet
- Krav til leverandøren
- Krav til leveransen
- Krav til versjonskontroll
- Krav til drift og vedlikehold
- Krav til lokale tilpassinger (opsjoner).

Prosjektgruppen må også bistå departementet med å utarbeide et forskriftsregelverk for forsøket. Når det gjelder dette er det naturlig at prosjektgruppen foreslår forskriftsbestemmelser som senere vedtas av departementet.

Under oppstarten bør det også inkluderes aktiviteter med henblikk på å etablere et formelt sertifiseringsapparat for valgløsninger. Det anses ikke som gjennomførbart å etablere et fullstendig godkjenningsapparat for forsøksvirksomheten. Ansvaret for sikkerhet og kvalitet vil i forsøksperioden ligge i prosjektgruppen og forutsettes ivaretatt gjennom et omfattende og strukturert testregime.

Tidshorisont
Etter departementets behandling av rapporten bør det innen utgangen av 2006 etableres en prosjektorganisasjon.

10.3.5 Første trinn

Ramme
I første trinn av forsøkene bør det legges opp til å prøve ut elektronisk stemmegivning i kontrollerte omgivelser både for bindende og rådgivende valg. Det anbefales også at det gjennomføres begrensede forsøk på stemmegivning for rådgivende valg i ukontrollerte omgivelser fra en kontrollert velgerterminal, dvs. en klient som er satt opp med programvare

distribuert fra forsøksprosjektet på en egen CD-ROM. I dette trinnet vil det også være naturlig å starte arbeidet med å få etablere et kontroll- og sertifiseringsapparat i samarbeid med mulige godkjenningsmiljøer.

Formål
Hovedformålet vil være å prøve ut brukergrensesnitt, kapasitet/ytelse, brukeraksept og grunnleggende sikkerhetsaspekter med fokus på autentisering (PKI), logging og sikker oppbevaring av avgitte stemmer. Deler av forsøksvirksomheten kan gjennomføres uten direkte tilknytning til valg. Ved valg av forsøksarenaer må det sikres at kravet om hemmelige valg opprettholdes.

Tidshorisont
Første trinn av forsøkene bør være gjennomført innen utgangen av 2009.

10.3.6 Andre trinn

Ramme
I denne fasen av forsøkene bør muligheten for å avgi stemme i ukontrollerte omgivelser fra kontrollert maskin utvides til også å kunne omfatte bindende valg. For rådgivende valg er det også et ønske å prøve ut muligheten for å stemme elektronisk i ukontrollerte omgivelser fra maskin som ikke er kontrollert av valgsystemet. I dette trinnet vil det også være naturlig å etablere et midlertidig kontrollapparat i samarbeid med mulige godkjenningsmiljøer.

Formål
Hovedformålet er å prøve ut valg i ukontrollerte omgivelser i en skala og i et miljø der konsekvensene av feil og fusk er begrenset. Brukeraksept og sikkerhetsløsninger vil igjen stå i fokus. Gjennomføring av utvidet stemmegivning i ukontrollerte omgivelser vil også åpne for evaluering av konsekvensene knyttet til sentrale demokratiske utfordringene: utilbørlig påvirkning og kjøp/salg av stemmer. Gjennom dette trinnet bør det også kunne høstes erfaring med sertifiseringsløsningen. Endelig vil trinn 2 kunne gi vesentlige bidrag ved evaluering av tekniske løsninger.

Tidshorisont
Tidspunkt for gjennomføringen av trinn 2 vil avhenge av resultatene fra trinn1, den teknologiske utviklingen og den generelle samfunnsmessige utviklingen.

10.3.7 Tredje trinn

Ramme
Hvis de to første trinnene er gjennomført på en vellykket måte, og hvis den tekniske utviklingen har gitt løsninger som tilfredsstiller de absolutte krav til sikkerhet, vil man i dette trinnet kunne gjennomføre bindende valg i ukontrollerte omgivelser basert på velgerens egen systemplattform (maskin- og programvare) for et begrenset antall stemmeberettigede. I dette trinnet vil det også være naturlig å etablere en fullstendig sertifiseringsordning.

Formål
Dette trinnet vil gi en fullstendig test av alle forhold forbundet med gjennomføring av elektronisk stemmegivning inkludert juridiske, demokratiske, økonomiske, praktiske og tekniske aspekter. Det forutsettes også at rammene for et sertifiseringsregime (organisering) er på plass og kan evalueres.

Tidshorisont
Tidspunkt for gjennomføringen av trinn 3 vil avhenge av resultatene fra trinn 1 og 2, den teknologiske utviklingen og den generelle samfunnsmessige utviklingen.

10.3.8 Informasjonsopplegg

Informasjonsopplegget vil være en viktig del av hele forsøksregimet. I alle trinnene må det legges vekt på at saklig og relevant informasjon om forsøkene kommer ut til valgfunksjonærer, velgere og media. Vi viser her også til krav nedfelt i Europarådets anbefaling.

10.4 Hjemmel for forsøk

Arbeidsgruppen vil peke på at det etter vår oppfatning finnes hjemmel for forsøk både i forsøksloven og valgloven. Vi tar imidlertid ikke stilling til hva som skal være hjemmelsgrunnlaget for gjennomføring av eventuelle forsøk.

10.4.1 Forsøksloven

Lov 26. juni 1992 nr. 87 om forsøk i offentlig forvaltning (forsøksloven) regulerer forsøk i statlig, fylkeskommunal og kommunal forvaltning.

I henhold til forsøksloven § 3 a kan det godkjennes forsøk med avvik fra gjeldende lover og forskrifter om hvordan myndighetene skal organisere sin virksomhet og løse sine oppgaver. For godkjenning kreves for det første at forsøket tar sikte på å oppfylle de mål som er satt i § 1. For det andre skal forsøket anses forsvarlig og faglig vel underbygget. Ytterligere begrensninger finnes i § 4 hvor det blant annet heter at det ikke kan gis godkjenning som innebærer innskrenking av rettigheter eller utvidelse av plikter som enkeltpersoner har etter gjeldende lovgivning. Etter vår vurdering vil dette klart begrense hvordan forsøk med elektronisk stemmegivning i ukontrollerte omgivelser kan gjennomføres. Elektronisk stemmegivning kan således bare tilbys som et supplement til ordinær stemmegivning. Det må likeledes innføres mulighet til å ombestemme seg og stemme på nytt for de velgere som avgir stemme elektronisk.

Ved gjennomføring av forsøk må det utarbeides et sett regler i forskrifts form til erstatning for de bestemmelser det godkjennes avvik fra, jf. § 5. Slike regler skal i utgangspunktet fastsettes av kommunestyret eller fylkestinget og godkjennes av Kongen. I henhold til lovens § 6 kan Kongen gi nærmere regler om forsøk etter loven, blant annet om antallet forsøksenheter, prosedyrer for utvelgelse av forsøksenheter og forsøksområder, og godkjenning og iverksetting av forsøk.

10.4.2 Om forsøkshjemmelen i valgloven § 15-1

I forbindelse med vedtagelse av den nye valgloven av 2002 kom det inn en ny bestemmelse i § 15-1 om forsøk ved valg. I henhold til § 15-1 (1) kan det gis samtykke til *"forsøk der valg etter denne lov gjennomføres på andre måter enn det som følger av denne lov"*. I henhold til § 15-1 (2) kan Kongen fastsette vilkår for forsøket og bestemme hvilke lovbestemmelser det kan gjøres avvik fra.

Bestemmelsen i § 15-1 kom inn i loven først etter behandlingen i Stortinget og var basert på forslag fra Valglovutvalget. Lovbestemmelsen i seg selv angir ingen begrensninger med hensyn til hva det kan drives forsøk med. Arbeidsgruppen ser det som naturlig at de begrensninger som fremgår av forsøksloven også vil måtte legges til grunn ved forsøk etter valgloven. Særlig viktig er kravet om at det ikke kan drives forsøk som begrenser velgers rettigheter, jf. forsøksloven § 4.

Kongens myndighet etter § 15-1 er i noen tilfeller delegert departementet, jf. kgl.res. datert 14.2.03. Bakgrunnen for en slik todeling er at mange forsøk i forbindelse med valg ofte vil gjelde saker av juridisk, teknisk og praktisk art, der det er lite rom for politiske vurderinger. Slike saker behandles og avgjøres mest hensiktsmessig i departementet. Forsøk som berører de mer grunnleggende prinsippene i valglovgivningen, skal behandles og avgjøres av Kongen i statsråd. I delegasjonsvedtaket heter det at ”Saker som innebærer avvik fra grunnleggende bestemmelser i valgloven skal [ ] avgjøres av Kongen i statsråd.”

Litteraturliste

Ad hoc Touch Screen Task force (2003): Report to the Secretary of State.

Dette er rapporten til gruppen som ble opprettet som en følge av bekymringer knyttet til sikkerheten til DRE-valgutstyr (Direct Recording Electronic (inkludert pekeskjermer)). Gruppens mandat var å drøfte disse bekymringene og komme med en anbefaling. Gruppen identifiserte fire områder for anbefaling: Sikkerhet, papirkvittering, velgeridentifisering, og uavhengig verifisering.

Alvarez, R. Michael og Jonathan Nagler (2001): "The Likely Consequences of Internet Voting for Political Representation", *Loyola Law Review* 34: 1115-1154.

Alvares, Michael og Thad Hall (2004): *Point, Click Vote. The future of Internet Voting.* Brookings Institution Press

Forfatterne argumenterer for mer eksperimentering når det gjelder Internett-stemmegivning. De mener man ikke kan vite hvor gode argumenter for og imot Internett-stemmegivning er om ikke systemene er testet ut i ordentlige valg. De hevder at Internett-stemmegivning bør prøves ut i liten skala, og at de må evalueres på en vitenskapelig måte.

Ansolabehere, Stephen og Charles Stewart (2005): "Residual Votes Attributable to Technology", *The Journal of Politics* 67: 365-389.

Arbetsgruppen for e-röstning og demokrati(2002): *E-Röstning. En antologi.* Ju2002E.

Dette er den første rapporten til den svenske arbeidsgruppen for IT og demokrati. Rapporten er en samling innlegg fra gruppens medlemmer angående elektronisk stemmegivning.

Auer, Andreas (2005): "The European Union and e-voting" i Trechsel, Alexander H. & Fernando Mendez (2005), *The European Union and e-voting : addressing the European Parliament's internet voting challenge*. London: Routledge.

Berinsky, Adam J., Nancy Burns og Michael W. Traugott (2001): "Who Votes by Mail? A Dynamic Model of the Individual-Level Consequences of Voting-By-Mail Systems", *Public Opinion Quarterly* 65: 178-197.

Blais, André og Agnieszka Dobrzynska (1998): "Turnout in electoral democracies", *European Journal of Political Research* 33: 239-261.

Bruck, Shuki, David Jefferson, and Ronald L. Rivest (2001). *A Modular Voting Architecture ("Frogs")* http://theory.lcs.mit.edu/~rivest/BruckJeffersonRivest-AModularVotingArchitecture-doc.pdf

Buchstein, Hubertus (1997): "Bytes that bite: The Internet and deliberative democracy", *Constellations* 4: 248-263.

Bullock, Charles S. og M. W. Hood (2002): "One Person—No Vote; One Vote; Two Votes: Voting Methods, Ballot Types, and Undervote Frequency in the 2000 Presidential Election", *Social Science Quarterly* 83: 981-993.

California Internet Voting Task Force (2000): *A report on the Feasability of Internet Voting*.

Dette er rapporten fra gruppen som ble satt sammen for å utrede mulighetene for å innføre Internett-valg i California. Rapporten slår fast at i Internett-stemmegivning bare må ses på som et alternativ til papirstemmegivning i overskuelig framtid. De foreslår en utviklingsprosess delt inn i to faser. I den

første fasen bør all Internett-stemmegivning foregå i valglokalet for å ha bedre kontroll over teknologien. Deretter i fase to skal stemmegivningen flyttes ut av valglokalet.

Caltech/MIT (2004): *Electronically*. Voting Technology Project Working paper # 12 http://vote.caltech.edu/media/documents/wps/vtp_wp12.pdf.

Castberg, Frede (1947): *Norges statsforfatning. Bind I.* Oslo: Akademisk forlag.

Choe, Yonhyok (1997): *How to Manage Free and Fair Elections. A Comparison of Korea, Sweden and the United Kingdom.* Göteborg: Göteborg Studies in Politics.

Christin, Thomas og Alexander H. Trechsel (2005): *Analysis of the 26th September ballot as held in four Geneva municipalities*. E-Democracy Center. Geneva University.

Christensen, Dag Arne, Rune Karlsen & Bernt Aardal (2004): *På vei mot e-demokratiet? Forsøkene med elektronisk stemmegivning ved kommune- og fylkestingsvalget 2003*. Rapport 2004. Oslo: Institutt for samfunnsforskning.

"Code of Good Practice in Electoral Matters" CDL-AD(2002)023rev http://www.venice.coe.int/docs/2002/CDL-AD(2002)023rev-e.asp

van Dijk, Jan A.G.M (2005): *The Deepening Divide. Inequality in the Information Society.* London: Sage

Drechsler, Wolfgang og Ülle Madise (2004) ”Electronic Voting in Estonia” i Norbert Kersting and Harald Baldersheim (red.) *Electronic Voting and Democracy: A Comparative Analysis*, London: Palgrave Macmillan, 2005, 193-225.
Dette er en gjennomgang av situasjonen i Estland opp til 2002.

e-Voting security study. Issue 1.2 (2002): http://www.samfunnsforskning.no/files/rapp_07.pdf/

The Electoral Commission (2003): The Shape of Elections to Come. A Strategic Evaluation of the 2003 Pilot Schemes. London: The Electoral Commission
Dette er kommisjonens evaluering av forsøkene i 2003. Gjennomgangen av e-valg i Storbritannia i kapittel 4 bygger i stor grad på denne rapporten.

Elklit, Jørgen og Palle Svensson (1997): ”What makes an election free and fair?” *Journal of Democracy* 8 (3): 32-46.

Fairweather, N Ben og Simon Rogerson (2002): *Technical options report*. Centre for Computing and Social Responsibility School of Computing, De Montfort University, Leicester.

Fairweather, Ben and Simon Rogerson (2002): ”Internet Voting – Well at Least it’s Modern” *The Journal of Representative Democracy*, 39.

Franklin, Mark N. (1996): ”Electoral Participation”, i Lawrence LeDuc, Richard Niemi og Pippa Norris, red. *Comparing Democracies: Elections and Voting in global Perspective.* Thousand Oaks, CA: Sage.

Fridtun, Dag (2005): *Tillit til elektroniske valg.* Masteroppgave. Oslo:Universitetet i Oslo, Institutt for Informatikk.

Fund, John (2004): *Stealing Elections. How Voter Fraud Threatens Our Democracy*. San Fransisco: Encounter Books.

Funk, Patricia (2004): "Is there an expressive function of Law? An empirical analysis of voting laws with symbolic fines". Upublisert notat. Stockholm School of Economics. (http://www.hhs.se/NR/rdonlyres/5E4F6B09-D249-46A8-81D2-24F08FDE3D1E/0/PFExpressive_Function.pdf)

Geser, Hans (2004): Electronic Voting in Switzerland, kapittel 6 i Kersting og Baldersheim: *Electronic Voting and Democracy. A Comparative Analysis*, Palgrave, London, 2004.

Geys, Benny (2005). "Explaining voter turnout: A review of aggregate-level research", *Electoral Studies* (under trykking).

Gibson, Rachel (2001): "Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary", *Political Science Quarterly* 116: 561-583.

Internet Policy Intstitute (2001): Report of the National Workshop on Internet Voting: Issues and Research Agenda. Mars 2001.

I desember 1999 utstedet President Clinton et memorandum der han anmodet at the National Science Foundation undersøkte mulighetene for bruk av Internett-teknologi i forbindelse med valg. Som en konsekvens av dette ble det i USA i 2000 arrangert en nasjonal konferanse med dette tema. I sluttrapporten skisseres problemer og en strategi for videre forskning omkring temaet. Som nevnt ovenfor har det enn så lenge kommet lite ut av denne rapporten.

Jansen, Arild & Dag Wiese Schartum (2005): *Informasjonssikkerhet : rettslige krav til sikker bruk av IKT*. Bergen: Fagbokforlaget.

Jefferson, David, Aviel D. Rubin, Barbara Simons og David Wagner (2004): *Secure Electronic Registration and Voting Experiment* (SERVE). Rapport.

Rapporten er en kritisk gjennomgang av sikkerheten knyttet til SERVE (Secure Electronic Registration and Voting Experiment), et Internett basert valgsystem som ble utviklet for det amerikanske forsvarsdepartementet. Rapporten anbefaler at SERVE ikke tas i bruk.

Jones, Douglas W. (2004): "Auditing Elections". *Communications of the ACM* Vol.47, issue 10. ACM Press.

Karlsen, Rune, Bernt Aardal og Dag Arne Christensen (2005): «Elektronisk stemmegivning. De første norske erfaringer». I: Jo Saglie & Tor Bjørklund, red., *Lokalvalg og lokalt folkestyre*, s. 122-141. Oslo: Gyldendal Akademisk.

Karp, Jeffrey A. og Susan A. Banducci (2000): "Going Postal: How All-Mail Elections Influence Turnout", *Political Behavior* 22: 223-239.

Kenski, Kate 2005. "To I-Vote or Not to I-Vote? Opinions About Internet Voting from Arizona voters", *Social Science Computer Review* 23: 293-303.

Kersting, Norbert og Harald Baldersheim (red., 2004): *Electronic Voting and Democrazy. A Comparative Analysis.* London: Palgrave MacMillan

Denne antologien har utgangpunkt i en workshop om elektronisk stemmegivning som fant sted i 2002. Boken er delt inn i tre deler. Den første delen er en introduksjonsdel der hovedspørsmålene angående e-valg diskuteres. Den andre delen består av kapitler som tar for seg e-valg i noen utvalgte land. I del tre inngår kapitler som tar for seg ulike pilotforsøk og holdninger til e-valg.

Kitcat, Jason (2003): "The uncertain nature of elections to come". Response and analysis to the electoral Commission's evaluation of the 2003 electoral pilot schemes and the Government's own response to the evaluation. The free e-democracy project (www.free-project.org).

Denne artikkelen er, som det framgår av tittelen, et svar på kommisjonens rapport, og er spesielt kritisk til at det ikke er gjennomført noen sikkerhetsanalyser under eller etter forsøkene.

Kitcat, Jason (2004): "Source availability and e-voting: an advocate recants".*Communications of the ACM* Vol. 47, issue 10. ACM Press.

Laver, Michael (2004): "Analysing Structures of Party preference in Electronic Voting Data" *Party Politics* 10:521-542

Liburd, Soyini (2004): *An N-version Electronic Voting System.* Caltech/MIT Voting Technology Project Working paper # 17
http://vote.caltech.edu/media/documents/wps/vtp_wp17.pdf

Lijphart, Arend 1997. "Unequal Participation: Democracy's Unresolved Dilemma", *American Political Science Review* 91: 1-14.

Magleby, David B. (1987): "Participation in Mail Ballot Elections", *Western Political Quarterly* 40: 79-91.

McLean, Iain (1989): *Democracy and New Technology.* Cambridge: Polity Press.

Morris, Dick (1999): *Vote.com.* Los Angeles: Renaissance Books.

The National Election Committee: *E-Voting System – Overview*
http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf

Newman, Terry (2003): "Tasmania and the Secret Ballot", *Australian Journal of Politics and History* 49: 93-101.

New York Times (2001): *36 days. The Complete Chronicle of the 2000 Presidential Election Crisis.* New York: Times Books.

Niemi, Richard G. og Paul S. Herrnson (2003): "Beyond the Butterfly: The Complexity of U.S. Ballots", *PS: Political Science & Politics* 36: 317-326.

NOU 2001:10 *Uten penn og blekk.*
http://odin.dep.no/fad/norsk/publ/utredninger/NOU/002001-020005/index-dok000-b-n-a.html

Norris, Pippa (2001): The Digital Divide. Cambridge: Cambridge University Press.

Norris, Pippa (2004a): "E-Voting as the Magic Ballot? The Impact of the Internet on Electoral Particiapation and Civic Engagement." Notat. Boston: John F. Kennedy School of Government, Harvard University.

Norris, Pippa (2004b): "Will New Technology Boost Turnout?" i Norbert Kersting and Harald Baldersheim (red.) *Electronic Voting and Democracy: A Comparative Analysis*, London: Palgrave Macmillan, 2005, 193-225.

Kapitlet diskuterer om stemmegivning via Internett kan øke valgdeltakelsen. Norris diskuterer teknologiske, sosiale og praktiske barrierer, samt analyserer de britiske forsøkene fra 2003. Kapitlet konkluderer med at det er liten grunn til å tro at valgdeltakelsen vil øke ved å innføre Internett-stemmegivning.

Nygård, Beate (2003a): *Frie og rettferdige valg? En normative-empirisk analyse av de første direkte stortingsvalgene i Norge.* Hovedoppgave. Oslo: Institutt for statsvitenskap.

Nødtvedt, Einar (2002): Stemmegivning og informasjons- og kommunikasjonsteknologi. Vedlegg til Ot.prp.nr.45. Rapporten kan leses på http://www.dep.no/krd/norsk/publ/otprp/016001-050016/ved002-bn.html

Bakgrunnen for denne rapporten var et ønske fra Kommunal- og regionaldepartementet om å supplere Valglovutvalgets innstilling med en tilleggsrapport som tok sikte på å analysere muligheter og begrensninger ved bruk av IKT i selve valghandlingen.

Olsson, Anders R (2001): E-röstning – En lägesrapport. Stockholm, IT Kommissionen, Rapport 35/2001.

Denne rapporten er en kartlegging av kunnskapsfronten når det gjelder e-valg skrevet på bestilling av den svenske IT-kommisjonen i 2001. Rapporten gjør rede for hvilke krav som bør stilles til et e-valgsystem, og drøfter argumenter for og i mot e-valg.

Qvortrup, Matt 2005. "First past the Postman: Voting by Mail in Comparative Perspective", *The Political Quarterly* 76: 414-419.

Pratchett, Lawrence (2002): The Implementation of electronic voting in the UK. De Montfort University, University of Essex.

Reynolds, Andrew og Marco Steenbergen (2005): "How the world votes: The political consequences of ballot design, innovation and manipulation", *Electoral Studies* (under trykking).

Rumbaugh, James, Jacobson, Ivar & Booch, Grady (2004): *The unified modeling language reference manual* 2nd ed Boston : Addison-Wesley.

Rønning, Wenche M., Astrid M. Sølvberg og Christin Tønseth (2005): "Voksnes bruk av PC og Internet: Digitale skillelinjer er der fremdeles", *Samfunnsspeilet* (SSB) nr. 3/05 (pp. 21-28).

Røsland, Geir (2004): *Remote Electronic Voting*. Hovedoppgave. Universitetet i Bergen.

Oppgaven tar spesielt for seg kryptering av stemmen ved Internett-stemmegivning

Saby, R.S. (1918): "Absent-Voting in Norway", *American Political Science Review* 12: 296-300.

Schartum, Dag Wiese og Lee A. Bygrave (2004): *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. Bergen: Fagbokforlaget.

Schneier, Bruce (2004): *Secrets and lies : digital security in a networked world*. Indianapolis, Ind., Wiley

Schorn, Heiner (2002): *Säkerhetskrav för internetröstning – en analys av skillnader mellan konception och realisering*, Human IT 1-2/2002, s.163-188.

Selker, Ted & Goler, Jonathan: *The SAVE System: Secure Architecture for Voting*

Shuki Bruck, David Jefferson & Ronald Rivest (2001): *A modular Voting Architecture ("frogs")* Caltech/MIT Voting Technology Project Working paper # 3. http://www.vote.caltech.edu/media/documents/wps/vtp_wp3.pdf

Southwell, Priscilla L. og Justin Burchett (1997):"Survey of Vote-by-Mail Senate Election in the State of Oregon", *PS: Political Science & Politics* 30: 53-57.

SOU 2004:111, Ny vallag.

Sturgis, Daniel (2005): "Is Voting a Private Matter?" *Journal of Social Philosophy* 36: 18-30.

Wand, Jonathan N, Kenneth W. Shotts, Jasjeet S. Sekhon, Walter R. Mebane, Michael C. Herron og Henry E. Brady (2001): "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida", *American Political Science Review* 95: 793-810.

Watt, Bob (2002): "Human Rights and Remote Voting by Electronic Means". *Representation The Journal of Representative Democracy 39 (3).* London: The McDougall Trust.

Westholm, Hilmar (2002): "E-Democracy Goes Ahead. The Internet as a Tool for Improving Deliberative Policies?", i R. Traunmüller og K. Lenk, red. *Electronic Government. First International Conference, EGOV 2002.* Berlin: Springer.

Aall, Jørgen (2004): *Rettsstat og menneskerettigheter.* Bergen: Fagbokforlaget.

Aardal, Bernt (1997): «Valg». I: Øyvind Østerud, Kjell Goldmann & Mogens N. Pedersen, red., *Statsvitenskapelig leksikon*, s. 280-281. Oslo: Universitetsforlaget.

Aas, Patricia (2005): *Evaluating the suitability of EML 4.0 for the Norwegian Electoral System – a prototype approach.* Masteroppgave. Oslo: Universitetet i Oslo, Institutt for Informatikk http://wo.uio.no/as/WebObjects/theses.woa/wa/these?WORKID=28266

Standarder

- NS 7799:2005: Styringssystem for informasjonssikkerhet, beskrivelse med veiledning for bruk.
- NS-ISO/IEC 17799:2005: Informasjonsteknologi, administrasjon av informasjonssikkerhet.
- ISO/IEC 27001:2005: Information technology -- Security techniques -- Information security management systems – Requirements.
- NS-ISO 17025: Akkreditering av prøvings- og kalibreringslaboratorier.
- ISO/IEC 15408-1:2005: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

- ISO/IEC 15408-2:2005: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
- ISO/IEC 15408-2:2005: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements

Vedlegg A Europarådets rekommandasjon Rek (2004) 11

Fra Ministerkomiteen til medlemsstatene om juridiske, operasjonelle og tekniske standarder for elektronisk stemmegivning (e-stemmegivning)

(Vedtatt av Ministerkomiteen 30. september 2004 på det 898. møtet til ministrenes stedfortredere)

Ministerkomiteen,

som tar i betraktning at Europarådets mål er å skape større enhet mellom sine medlemmer for å ivareta og realisere idealene og prinsippene som er deres felles arv,

som bekrefter sin tro på at representativt og direkte demokrati er en del av medlemmenes felles arv og grunnlaget for innbyggernes deltakelse i det politiske liv i det europeiske fellesskap og på nasjonalt, regionalt og lokalt plan,

som respekterer forpliktende ansvar og oppgaver innenfor eksisterende internasjonale instrumenter og dokumenter, så som

- Verdenserklæringen om Menneskerettighetene;
- Den Internasjonale konvensjonen om sivile og politiske rettigheter;
- FNs konvensjon om avskaffelse av alle former for rasediskriminering;
- FNs konvensjon om avskaffelse av alle former for diskriminering mot kvinner;
- Konvensjonen om beskyttelse av menneskerettighetene og de grunnleggende friheter (European Treatise Series “ETS” nr. 5), spesielt protokoll nr. 1 (ETS nr. 9);
- Det europeiske charter for lokalt selvstyre (ETS nr. 122);
- Konvensjonen om datakriminalitet (ETS nr. 185);
- Konvensjonen om personvern i forbindelse med elektronisk databehandling av personopplysninger (ETS nr. 108);
- Ministerkomiteens rekommandasjon nr. R (99) 5 om beskyttelse av personopplysninger på Internett;
- Sluttdokumentet fra OSSE-konferansen om den Menneskelige Dimensjon i København;
- Den Europeiske Unions charter om grunnleggende rettigheter;
- Kodeks for god valgpraksis, vedtatt av Rådet for demokratiske valg i Europarådet og Den Europeiske Kommisjon for demokrati ved lovgivning;

som tar hensyn til at retten til å stemme er et av de primære grunnprinsippene for demokrati og at elektroniske stemmegivningsprosedyrer derfor skal rette seg etter prinsippene for demokratiske valg og folkeavstemninger,

som erkjenner at medlemsstatene, fordi ny informasjons- og kommunikasjonsteknologi i stadig økende grad benyttes i det daglige liv, må ta hensyn til denne utviklingen i sin demokratiske praksis,

som merker seg at deltakelse i valg og folkeavstemninger på lokale, regionale og nasjonale plan kjennetegnes ved lavt, og i noen tilfelle stadig synkende, fremmøte,

som merker seg at noen medlemsstater allerede benytter, eller vurderer å benytte, elektronisk stemmegivning for en rekke formål, herunder:

- å sette velgere i stand til å avgi sine stemmer fra et annet sted enn stemmelokalene i deres valgdistrikt,
- å lette stemmegivningen for den enkelte velger,
- å lette deltakelsen i valg og folkeavstemninger for alle de som har rett til å avgi sin stemme, og spesielt for innbyggere som bor eller oppholder seg i utlandet,
- å utvide tilgangen til stemmeprosessen for velgere som har funksjonshemninger eller har andre vanskeligheter med å være fysisk til stede i valglokalet og benytte ordningene som er tilgjengelige der,
- å øke valgfremmøtet ved å kunne tilby flere stemmegivningskanaler,
- å bringe stemmegivningen i samsvar med den nye samfunnsutviklingen og med den økende bruken av ny teknologi som medium for kommunikasjon og samfunnsengasjement i demokratisk øyemed,
- å gradvis redusere valgmyndighetenes samlete kostnader forbundet med gjennomføringen av et valg eller en folkeavstemning,
- å levere pålitelige valgresultater raskere, og
- å yte velgermassen bedre service ved å tilby flere stemmegivningskanaler;

som er klar over visse sikkerhets- og pålitelighetsproblemer ved spesielle e-stemmegivningssystemer,

som derfor er seg bevisst at det bare er de e-stemmegivningssystemene som er sikre, pålitelige, effektive og teknisk robuste, åpne for uavhengig kontroll og lett tilgjengelige for velgerne, som vil skape den tilliten i folket som er en forutsetning for at elektronisk stemmegivning skal kunne avholdes,

anbefaler, i samsvar med bestemmelsene i artikkel 15.b i Europarådets vedtekter, at regjeringene i de medlemsstatene som benytter eller vurderer å benytte elektronisk stemmegivning, følger paragraf i. til iii. nedenfor, jf. likevel paragraf iv, samt standarder og krav som gjelder de juridiske, operasjonelle og tekniske aspektene ved e-stemmegivning slik de er formulert i vedleggene til denne rekommandasjonen:

i. Elektronisk stemmegivning skal følge alle prinsipper for demokratiske valg og folkeavstemninger. E-stemmegivning skal være like pålitelig og sikker som demokratiske valg som holdes uten bruk av elektroniske hjelpemidler. Dette generelle prinsippet gjelder/innbefatter alle valgsaker, enten de er nevnt i vedleggene eller ikke.

ii. Forbindelsen mellom de juridiske, operasjonelle og tekniske aspektene ved e-stemmegivning, slik den er formulert i vedleggene, skal tas hensyn til når rekommandasjonen anvendes.

iii Medlemsstatene bør vurdere å gjennomgå sin relevante interne lovgivning i lys av denne rekommandasjonen.

iv. Prinsippene og bestemmelsene i vedleggene til denne rekommandasjonen krever imidlertid ikke at den enkelte medlemsstat forandrer de nasjonale valgprosedyrene som måtte gjelde når denne rekommandasjonen blir vedtatt og som må kunne opprettholdes av disse

medlemsstatene når e-stemmegivning blir benyttet så lenge de nasjonale valgprosedyrene følger alle prinsippene for demokratiske valg og folkeavstemninger;

v. for å gi Europarådet et grunnlag for mulig videre handling i forhold til e-stemmegivning innen to år etter at denne rekommandasjonen er vedtatt, anbefaler Ministerkomiteen at medlemsstatene

- gjennomfører jevnlig gjennomgang av sin erfaring med, og sin politikk i forhold til e-stemmegivning, spesielt gjennomføringen av bestemmelsene i denne rekommandasjonen, og
- rapporterer resultatene av gjennomgangen til Europarådets sekretariat, som sender dem videre til medlemsstatene og følger opp e-stemmegivningssaken.

I denne rekommandasjonen benyttes følgende termer og definisjoner:

- autentisering: forsikring om korrekt angivelse av personidentitet eller dataidentitet;
- stemmeseddel: et lovmessig godkjent middel en velger kan benytte for å gi uttrykk for sin stemme;
- kandidat: en valgmulighet som består av en person og/eller en gruppe personer og/eller et politisk parti;
- å avgi stemme: å legge en stemmeseddel i valgurnen;
- e-valg eller e-folkeavstemning: et politisk valg eller en folkeavstemning hvor elektroniske midler benyttes på ett eller flere stadier;
- elektronisk valgurne: elektronisk lagringssted for stemmer som avventer opptelling;
- e-stemmegivning: et e-valg eller en e-folkeavstemning som benytter elektroniske metoder ved stemmegivningen – i det minste ved selve avgivelsen av stemmen;
- e-stemmegivning utenfor valglokalet: e-valg hvor stemmegivningen foretas ved en innretning som ikke er kontrollert av en valgfunksjonær;
- forsegling: informasjonsbeskyttelse som gjør at informasjonen ikke kan brukes eller tolkes uten ved hjelp av informasjon eller metode som kun er tilgjengelig for en spesiell person eller myndighet;
- stemme: uttrykk for velgers valg;
- velger: en person som har rett til å avgi stemme ved et valg eller en folkeavstemning;
- stemmegivningskanal: måten en velger kan avgi sin stemme på;
- valgmuligheter: de muligheter en velger kan velge mellom når en stemme avgis ved valg eller folkeavstemning;
- manntallsliste: liste over stemmeberettigede.

Vedlegg I til Rekommandasjonen

Juridiske standarder

A. Prinsipper

I. Alminnelig stemmerett

1. Brukergrensesnittet i et e-stemmegivningssystem skal være forståelig og lett anvendelig for velgeren.

2. Mulige registreringskrav for e-stemmegivning skal ikke skape hindringer for en velger som deltar i et e-valg.

3. E-stemmegivningssystemet skal, så langt det er praktisk mulig, utformes slik at det maksimerer mulighetene slike systemer kan gi personer med funksjonshemninger.

4. Med mindre e-valgskanaler utenfor valglokalet er alminnelig tilgjengelige, skal de kun tilbys som en ekstra og valgfri stemmegivningskanal.

II. Lik stemmerett

5. Ved ethvert valg og enhver folkeavstemning skal en velger forhindres fra å legge flere enn en stemmeseddel i den elektroniske valgurnen. En velger skal kun ha myndighet til å stemme hvis det er fastslått at hans eller hennes stemmeseddel ikke allerede er lagt i valgurnen.

6. E-stemmegivningssystemet skal forhindre at en velger kan avgi sin stemme gjennom mer enn en stemmegivningskanal.

7. Alle stemmene som er avlagt i en elektronisk valgurne skal telles, og hver stemme avgitt ved valget eller folkeavstemningen skal telles kun én gang.

8. Når elektroniske og ikke-elektroniske kanaler benyttes ved samme valg eller folkeavstemning, skal det finnes en sikker og pålitelig metode for å samle alle stemmene og telle opp det korrekte resultatet.

III. Frie valg

9. Organiseringen av e-valg skal sikre at velgeren fritt får danne og gi uttrykk for sin egen mening, og, der det kreves, personlig får utøve sin rett til å stemme.

10. Måten velgerne veiledes gjennom e-stemmegivningsprosessen skal være slik at de forebygger en forhastet eller ureflektert stemmegivning.

11. Velgere skal ha mulighet til å ombestemme seg på ethvert trinn i e-stemmegivningsprosessen før stemme avgis, eller å avbryte prosessen uten at deres tidligere valg registreres eller gjøres tilgjengelig for noen andre.
12. E-stemmegivningssystemet skal ikke tillate at det utøves noen form for manipulerende innflytelse over velgeren under stemmegivningen.

13. E-stemmegivningssystemet skal gi velgeren en mulighet til å delta i et valg eller en folkeavstemning ved å avgi blank stemme, uten å måtte velge noen av de godkjente listeforslagene.

14. E-stemmegivningssystemet skal gi tydelig tilbakemelding til velgeren når stemmegivningen har vært vellykket og når hele stemmegivningsprosessen er fullført.

15. E-stemmegivningssystemet skal forhindre at en stemme kan forandres etter at den er avgitt.

IV. Hemmelig valg

16. E-valg skal organiseres slik at hemmeligholdelsen av den enkeltes valg, på ethvert trinn i stemmegivningsprosessen og spesielt i velgerautentiseringen, ikke settes i fare.

17. E-stemmegivningssystemet skal garantere at stemmene i den elektroniske valgurnen og stemmene som telles, er og forblir anonyme, og at det ikke er mulig å rekonstruere noen forbindelse mellom velgeren og vedkommendes stemmegivning.

18. E-stemmegivningssystemet skal være utformet slik at det forventede antall stemmer i enhver elektronisk valgurne ikke gjør det mulig å knytte resultatet til de enkelte velgerne.

19. Det skal tas forholdsregler som sikrer at informasjon som er nødvendig for den elektroniske prosesseringen ikke kan benyttes til å bryte hemmeligholdelsen av den avgitte stemmen.

B. Sikkerhetsprosedyrer

I. Åpenhet

20. Medlemsstatene skal ta forholdsregler for å sikre at velgerne forstår og har tillit til det e-stemmegivningssystemet som benyttes.

21. Informasjon om hvordan e-stemmegivningssystemet virker, skal gjøres offentlig kjent.

22. Velgerne skal gis anledning til å innøve enhver ny måte å avgi sin e-stemme på før, og uavhengig av, tidspunktet for avgivelse av en elektronisk stemme.

23. Så langt loven tillater det, skal observatører ha anledning til å være til stede for å observere og kommentere e-valgene, innbefattet opptellingen av stemmene.

II. Kontrollerbarhet og tilregnelighet

24. Komponentene i e-stemmegivningssystemet skal være fritt tilgjengelige, i det minste for ansvarlige valgmyndigheter, for kontroll og sertifisering etter behov.

25. Før et e-stemmegivningssystem innføres, og ved passende intervaller etter innføring, og særskilt etter at det er foretatt forandringer i systemet, skal en uavhengig instans, utpekt av valgmyndighetene, kontrollere at e-stemmegivningssystemet er i orden og at de nødvendige forholdsregler for sikkerhet er tatt.

26. Det skal være mulighet for ny opptelling. Andre forhold ved e-stemmegivningssystemet som kan ha innflytelse på riktigheten av resultatene, skal kunne kontrolleres.

27. E-stemmegivningssystemet skal ikke forhindre delvis eller fullstendig gjentakelse av et valg eller en folkeavstemning.

III. Pålitelighet og sikkerhet

28. Medlemsstatenes myndigheter skal sørge for at e-stemmegivningssystemet er pålitelig og sikkert.

29. Alle mulige forholdsregler skal tas under hele valgprosessen for å unngå muligheten for valgfusk eller uautorisert innblanding som kan virke inn på systemet.

30. E-stemmegivningssystemet skal ha mekanismer som sikrer at tjenesten holdes tilgjengelig under hele e-stemmegivningsprosessen. Det skal være særskilt motstandsdyktig mot funksjonsfeil, havari, og angrep som forårsaker transaksjonskork eller transaksjonsstans.

31. Før et e-valg eller en e-avstemning finner sted skal den ansvarlige valgmyndighet være forsikret om at e-stemmegivningssystemet er ekte og fungerer som det skal.

32. Kun personer som er utpekt av valgmyndighetene skal ha tilgang til den sentrale infrastrukturen, tjenere og valgdata. Det skal være etablert klare regler for slik utpeking. Kritiske tekniske aktiviteter skal utføres av grupper på minst to personer. Gruppenes sammensetning skal forandres jevnlig. Så langt mulig skal slike aktiviteter gjennomføres utenfor valgperioden.

33. Så lenge en elektronisk valgurne er åpen kan autorisert intervensjon som virker inn på systemet kun foretas av grupper på minst to personer. Slik intervensjon skal rapporteres, overvåkes av representanter fra valgmyndighetene og valgobservatører.

34. E-stemmegivningssystemet skal bevare stemmenes tilgjengelighet og integritet. Det skal også holde stemmene hemmelige og forseglet frem til opptelling. Hvis de er lagret eller formidlet utenfor kontrollerte omgivelser, skal de krypteres.

35. Informasjon om avgitte stemmer og velgerinformasjon skal oppbevares og holdes forseglet så lenge datamaterialet kan kople sammen velger og stemme. Informasjon i forbindelse med autentisering skal skilles fra velgers stemmegivning på et på forhånd angitt stadium i e-valget eller e-folkeavstemningen.

Vedlegg II til Rekommandasjonen

Operasjonelle standarder

I. Kunngjøring

36. Et nasjonalt juridisk regelverk for e-valg og e-avstemninger skal gi klare kjøreplaner for alle stadier i valget eller avstemningen, både før og etter valget eller avstemningen.

37. Perioden for elektronisk stemmegivning skal ikke begynne før et valg eller en avstemning er kunngjort. Særskilt gjelder det for e-stemmegivning utenfor valglokalet at perioden for stemmegivning skal defineres og gjøres kjent for publikum i god tid før valget starter.

38. Velgerne skal, i god tid før valget starter og på et klart og enkelt språk, informeres om hvordan e-stemmegivningen er organisert og om alle skritt en velger må følge for å delta og avgi sin stemme.

II. Velgere

39. Det skal finnes et manntall som skal oppdateres jevnlig. En velger skal, som et minimum, kunne kontrollere opplysningene om seg selv i manntallet, og be om rettinger.

40. Muligheten for å lage et manntall i elektronisk form og innføre et system som tar imot søknader om innføring i manntallet elektronisk og, der det er aktuelt, tar imot søknader om å få benytte seg av e-stemmegivning, skal vurderes. Hvis deltakelse i e-stemmegivning krever en egen søknad fra velger og/eller andre tiltak, skal elektroniske og så langt mulig interaktive prosedyrer vurderes.

41. I tilfelle perioden for velgerregistrering og stemmegivning faller delvis sammen, skal det tilrettelegges for formålstjenlig velgerautentisering.

III. Kandidater

42. Det skal vurderes om elektronisk nominasjon av kandidater kan innføres.

43. Kandidatlister som genereres og gjøres elektronisk tilgjengelig, skal også være offentlig tilgjengelig på andre måter.

IV. Stemmegivning

44. Der e-stemmegivningen utenfor valglokalet foregår i valglokalenes åpningstider, er det spesielt viktig at systemet er utformet slik at det forhindrer en velger fra å avgi sin stemme mer enn en gang.

45. E-stemmegivning utenfor valglokalene kan begynne og/eller avslutte før valglokalene åpner. E-stemmegivning utenfor valglokalene skal ikke fortsette etter at valglokalene er stengt.

46. For hver e-stemmegivningskanal skal det etableres støttefunksjoner og veiledningsordninger som er tilgjengelige for velgerne. Ved e-stemmegivning utenfor

valglokalene skal slike ordninger også være tilgjengelige gjennom andre vidt tilgjengelige kommunikasjonskanaler.

47. Måten valgmulighetene presenteres på i innretningen som benyttes til å avgi en elektronisk stemme, skal være upartisk.

48. En elektronisk stemmeseddel som brukes til å avgi en elektronisk stemme skal ikke inneholde noen annen informasjon om valgmulighetene enn de som er helt nødvendige for å avgi stemme. E-stemmegivningssystemet skal hindre fremvisning av andre budskap som kan influere på velgers avgjørelse.

49. Hvis det er bestemt at informasjon om valgalternativer skal være tilgjengelig fra nettstedet for e-stemmegivning, skal denne informasjonen presenteres upartisk.

50. Før det avgis stemme fra et elektronisk stemmegivningssystem utenfor valglokalene, skal velger gjøres eksplisitt oppmerksom på at e-valget eller e-folkeavstemningen de avgir sin stemme til på elektronisk vis, er et virkelig valg eller avstemning. Ved øvelse skal deltakerne gjøres eksplisitt oppmerksomme på at de ikke deltar i et virkelig valg eller en virkelig folkeavstemning. Velgerne skal – når øvelsen fortsetter etter at valget har startet – samtidig gis anledning til å avgi sin stemme gjennom stemmegivningskanalene som er tilgjengelige for dette formål.

51. Et e-stemmegivningssystem utenfor valglokalene skal ikke gi velgeren mulighet til å få et bevis på innholdet i sin avgitte stemme.

52. I spesielt tilrettelagte miljøer med tilsyn skal all informasjon om stemmeseddelen fjernes fra det elektroniske apparatet som er benyttet, enten det er visuelt (for syn), auditivt (for hørsel) eller taktilt (for berøring), umiddelbart etter at stemmeseddelen er avgitt. I stemmelokaler hvor velgeren får papirbevis på sin e-stemme, skal han/hun ikke ha anledning til å vise denne til noen annen person, eller ta beviset med seg ut av stemmelokalet.

V. Resultater

53. E-stemmegivningssystemet skal ikke tillate at antall avgitte stemmer for et bestemt valgalternativ kan avsløres før den elektroniske valgurnen er stengt. Slik informasjon skal ikke avsløres for publikum før stemmegivningsperioden er over.

54. E-stemmegivningssystemet skal hindre at informasjon om avgitte stemmer ved spesielt utvalgte enheter viderebehandles på en måte som kan avsløre enkeltvelgeres avgjørelser.

55. Enhver form for dekoding som er nødvendig for opptelling av stemmer, skal utføres så snart det er praktisk mulig etter at stemmegivningsperioden er over.

56. Representanter fra den ansvarlige valgmyndighet skal kunne delta i opptellingen, og valgobservatører skal kunne være til stede.

57. Det skal føres protokoll over opptellingen av de elektronisk avgitte stemmene, med opplysninger om begynnelsen og avslutningen av opptellingen, og om alle personer som er involvert.

58. Ved eventuelle uregelmessigheter som påvirker de avgitte stemmesedlenes integritet, skal stemmesedlene det gjelder registreres som uregelmessige.

VI. Kontroll

59. E-stemmegivningssystemet skal være kontrollerbart.

60. Konklusjonene som trekkes på grunnlag av kontrollen skal anvendes i fremtidige valg og folkeavstemninger.

Vedlegg III til Rekommandasjonen

Tekniske krav

Utformingen av et e-stemmegivningssystem skal være underbygget med en omfattende gjennomgang av alle mulige risikofaktorer som er forbundet med en vellykket gjennomføring av vedkommende valg eller folkeavstemning. E-stemmegivningssystemet skal, på grunnlag av denne risikovurderingen, være tilfredsstillende beskyttet for å hanskes med de risiki som er fremkommet. Det skal være pre-definerte grenser for svikt i systemet eller kvalitetsforringelse.

A. Tilgjengelighet

61. Det skal tas forholdsregler som sikrer at programvare og tjenester kan brukes av alle velgerne og, om nødvendig, at det gis tilgang til alternative måter å avgi stemme på.

62. Brukere skal trekkes inn i utformingen av e-stemmegivningssystemer, spesielt for å identifisere begrensninger og for å teste brukervennligheten på alle trinn i utviklingsprosessen.

63. Når det er nødvendig og mulig skal brukere få tilgang til ytterligere hjelpemidler, som for eksempel spesielle brukergrensesnitt eller andre tilsvarende ressurser, som for eksempel personlig assistanse. Brukervennlige hjelpemidler skal i så stor grad som mulig tilfredsstille retningslinjene i Web Accessibility Initiative (WAI).

64. Ved utvikling av nye produkter skal kompatibiliteten til eksisterende produkter tas hensyn til, deriblant produkter med teknologi som er utviklet for å hjelpe funksjonshemmede.

65. Presentasjonen av valgmulighetene skal være optimal for velgeren.

B. Interoperabilitet (samspill mellom tekniske løsninger)

66. Åpne standarder skal benyttes for å sikre at de forskjellige tekniske komponentene eller tjenestene i et e-stemmegivningssystem, muligvis fra forskjellige kilder, fungerer sammen.

67. I øyeblikket er EML (Election Markup Language) en slik åpen standard, og for å garantere interoperabilitet skal EML benyttes, så sant det lar seg gjøre, i e-valg og e-avstemnings-applikasjoner. Tidspunktet for innføring av EML er opp til medlemsstatene selv. Den EML-standarden (med støttedokumentasjon) som gjelder når denne rekommandasjonen er vedtatt, er tilgjengelig på Europarådets webside.

68. Ved tilfeller som krever spesielle valgdata eller avstemningsdata skal det benyttes en lokaliseringsprosedyre som imøtekommer slike behov. Denne vil gjøre det mulig å utvide eller begrense informasjonstilgangen og likevel forbli kompatibel med den opprinnelige versjonen av EML. Anbefalt prosedyre er å bruke strukturerte skjemaspråk "structured schema languages" og mønsterspråk "pattern languages".

C. Systemdrift
(for den sentrale infrastrukturen og klienter i kontrollerte omgivelser)

69. De ansvarlige valgmyndighetene skal publisere en offisiell liste over programvare som benyttes for e-valget eller e-avstemningen. Medlemsstatene kan av sikkerhetsmessige grunner utelukke fra listen den programvaren som benyttes for databeskyttelse. Som et minimum skal listen opplyse om programvare som benyttes, versjoner, installasjonsdato og en kort beskrivelse. Det skal etableres prosedyrer for jevnlig installering av oppdaterte versjoner og korrigeringer av relevant programvare for databeskyttelse. Det skal til enhver tid være mulig å sjekke stemmegivningssystemets beskyttelsesstatus.

70. Systemansvarlige skal utforme en prosedyre for uforutsette hendelser. Backup-systemene skal overholde samme standarder og krav som originalen.

71. Tilstrekkelige backup-rutiner skal være på plass og alltid tilgjengelige for å sikre at e-valget går greitt. De ansatte som er involvert i driften skal i henhold til prosedyrene som er utformet av de ansvarlige valgmyndighetene være klare til å gripe raskt inn.

72. De utstyrsansvarlige skal benytte spesielle prosedyrer for å sikre at stemmegivningsutstyret og bruken av det tilfredsstiller kravene gjennom hele stemmegivningsperioden. Backup-tjenestene skal jevnlig forsynes med overvåkningsprotokoller.

73. Før et valg eller en folkeavstemning skal utstyret sjekkes og godkjennes i henhold til en protokoll som er ført av de ansvarlige valgmyndighetene. Utstyret skal sjekkes for å sikre at det tilfredsstiller de tekniske spesifikasjonene. Resultatene av kontrollen skal videresendes til de ansvarlige valgmyndighetene.

74. Alle tekniske operasjoner skal underkastes en formell kontrollprosedyre. Større forandringer på sentralt utstyr skal varsles.

75. Sentralt e-valg-utstyr skal plasseres på et sikkert område og området skal overvåkes under hele valget eller avstemningen for å sikre mot enhver form for innblanding av enhver art. Under hele valget eller avstemningen skal det foreligge en redningsplan for fysisk katastrofe. Alle bevarte data etter valget eller folkeavstemningen skal dessuten lagres på en sikker måte.

76. Ved eventuelle episoder som kan true systemets integritet, skal systemansvarlige straks melde fra til de ansvarlige valgmyndighetene, som vil ta de nødvendige skritt for å redusere eventuelle skader. Graden av mulig skade som er meldepliktig skal på forhånd spesifiseres av valgmyndighetene.

D. Sikkerhet

I. Generelle krav
(med referanse til tiden før, under og etter avstemningen)

77. Det skal tas tekniske og organisasjonsmessige forholdsregler for å sikre at ingen data går ugjenkallelig tapt i tilfelle av sammenbrudd eller feil som påvirker e-stemmegivningssystemet.

78. E-stemmegivningssystemet skal beskytte enkeltmenneskets privatliv. Manntallsregistret som er lagret eller formidlet i systemet skal alltid være konfidensielt.

79. E-stemmegivningssystemet skal utføre regelmessige kontroller for å sikre at delene fungerer i henhold til de tekniske spesifikasjonene og at tjenestene er tilgjengelige.

80. E-stemmegivningssystemet skal regulere adgangen til tjenestene, avhengig av brukeridentitet og brukerrolle, til de tjenestene som er avtalt for den spesielle brukeren eller rollen. Brukerautentiseringen må være i orden før avstemning kan foretas.

81. E-stemmegivningssystemet skal beskytte autentiseringsdata slik at ikke-autoriserte instanser ikke kan misbruke, få tak i, forandre eller på annen måte få kunnskap om alle eller noen av disse data. I ukontrollerte miljøer anbefales autentisering som bygger på kryptografiske mekanismer.

82. Velgere og kandidater skal identifiseres på en måte som gjør at den enkelte velger eller kandidat holdes klart atskilt fra alle andre personer (unik identifikasjon).

83. E-stemmegivningssystemet skal generere pålitelige og tilstrekkelig detaljerte observasjonsdata slik at valgobservatører kan utføre sine oppgaver. Tidspunktene for generering av observasjonsdata skal til enhver tid kunne kontrolleres på en sikker måte. Data-autentisitet, -tilgjengelighet og -integritet skal opprettholdes.

84. E-stemmegivningssystemet skal ha pålitelige synkroniserte klokker. Klokken skal være presis nok til at tidsangivelser for logg og observasjonsdata opprettholdes, i tillegg til at tidsfristen for registrering, nominasjon, stemmegivning og opptelling er overholdt.

85. Valgmyndighetene har det overordnete ansvar for at systemet er i henhold til disse sikkerhetskravene, som skal kunne kontrolleres av en uavhengig instans.

II. Krav som gjelder før stemmegivningen starter.
(og krav til data som videresendes til selve avstemningen)

86. Manntallsregisterets og kandidatlistens autentisitet, tilgjengelighet og integritet skal bevares. Datakilden skal autentiseres. Forskrifter som gjelder databeskyttelse skal respekteres.

87. Det skal være mulig å stadfeste at kandidatnominasjonen og, om det kreves, kandidatens eller den ansvarlige valgmyndighetens bekjentgjøring av nominasjonen, har funnet sted innenfor den fastsatte tidsfristen.

88. Det skal kunne stadfestes at velgerregistreringen har funnet sted innenfor den fastsatte tidsfristen.

III. Krav som gjelder under selve stemmegivningen.
(og krav til data som videresendes etter at valget er gjennomført)

89. Integriteten til data som er innkommet fra perioden før avstemningen starter (for eksempel manntallsregister og kandidatlister), skal bevares. Datakilden skal autentiseres.

90. Det skal sikres at e-stemmegivningssystemet presenterer velgeren for en autentisk stemmeseddel. Ved e-stemmegivning utenfor valglokalet skal velgeren informeres om hvordan det kan stadfestes at det er etablert en forbindelse til den offisielle tjeneren, og at velgeren står overfor en autentisk stemmeseddel.

91. Det skal kunne stadfestes at en stemme er avgitt innenfor den fastsatte tidsfristen.

92. Det skal være tilgjengelig tilstrekkelige metoder for å sikre at systemet velgeren benytter for å avgi sin stemme kan beskyttes mot ytre påvirkning som kan endre stemmegivningen.

93. Gjenstående informasjon om velgerens stemme eller skjermvisning av velgerens valg skal ødelegges etter at stemmen er avgitt. Ved e-stemmegivning utenfor valglokalet, skal velgeren opplyses om hvordan spor av stemmegivningen kan slettes i innretningen som er benyttet til å avgi stemme.

94. E-stemmegivningssystemet skal først sikre at en bruker som prøver å avgi sin stemme er stemmeberettiget. Systemet skal autentisere velgeren og sikre at det riktige antall stemmer, og bare det, avgis fra den enkelte velger og lagres i den elektroniske valgurnen.

95. E-stemmegivningssystemet skal sikre at velgers avgjørelser er korrekt representert i den avgitte stemmen, og at en forseglet stemme er avgitt i den elektroniske valgurnen.

96. Etter at den elektroniske stemmegivningsperioden er over, skal ingen velger ha mulighet til å få tilgang til e-stemmegivningssystemet. Muligheten for å registrere e-stemmer må imidlertid være åpen i en periode som er tilstrekkelig til å ta hensyn til eventuelle forsinkelser i selve transaksjonen.

IV. Krav som gjelder etter at stemmegivningen er avsluttet

97. Integriteten til data som er innkommet fra selve stemmegivningsperioden (for eksempel stemmer, manntallsregister, kandidatlister) skal opprettholdes. Datakilden skal autentiseres.

98. Opptellingen skal telle stemmene nøyaktig. Stemmeopptellingen skal kunne gjøres på ny.

99. Valgurnens tilgjengelighet og integritet og resultatet av opptellingen skal opprettholdes i e-stemmegivningssystemet så lenge det er påkrevd.

E. Kontroll

I. Generelt

100. Kontrollsystemet skal utformes og implementeres som en del av e-stemmegivningssystemet. Det skal være kontrollinnretninger på forskjellige nivåer i systemet: på det logiske nivå, det tekniske nivå og på applikasjonen.

101. Punkt-til-punkt-kontrollen av e-stemmegivningssystemet skal innbefatte logg, hjelpeprogram for overvåking og hjelpeprogram for verifikasjon. Kontrollsystemer som tilfredsstiller egenskapene i II -V nedenfor skal derfor benyttes for å imøtekomme disse kravene.

II. Logging

102. Kontrollsystemet skal være åpent og omfattende, og rapportere fortløpende om potensielle problemområder og farer.

103. Kontrollsystemet skal registrere tider, hendelser og handlinger som innbefatter:

a. all stemmegivningsrelatert informasjon, deriblant antall stemmeberettigede, antall avgitte stemmer, antall ugyldige stemmer, opptelling og gjenopptelling, osv.,

b. alle angrep på den operasjonelle delen av e-stemmegivningssystemet og på data-kommunikasjonens infrastruktur,

c. systemfeil, funksjonsfeil og andre trusler mot systemet.

III. Overvåking

104. Kontrollsystemet skal gi muligheten til å overvåke valget eller avstemningen og verifisere at resultatene og prosedyrene er i henhold til gjeldende juridiske bestemmelser.

105. Uautoriserte personer skal ikke ha tilgang til kontrollinformasjon.

106. Kontrollsystemet skal sikre at velgerne til enhver tid forblir anonyme.

IV. Verifikasjon

107. Kontrollsystemet skal gi mulighet til å kryss-sjekke og verifisere at e-stemmegivningssystemets operasjoner er korrekte og resultatene er nøyaktige, til å avdekke valgfusk og til å bevise at alle opptelte stemmer er autentiske og at alle avgitte stemmer er telt.

108. Kontrollsystemet skal gi mulighet til å verifisere at e-valget eller e-avstemningen har tatt gjeldende juridiske bestemmelser til følge, der målet er å verifisere at resultatene utgjør nøyaktig de autentiske stemmene.

v. Annet

109. Kontrollsystemet skal beskyttes mot angrep som kan korrumpere eller forandre loggen eller la loggen gå tapt.

110. Medlemsstatene skal ta tilstrekkelige forholdsregler for å sikre at all informasjon en utøvende kontrollperson får, forblir konfidensiell.

F. Sertifisering

111. Medlemsstatene skal innføre sertifiseringsprosesser som tillater at alle IKT-komponenter (Informasjon og Kommunikasjons-Teknologi) kan testes og sertifiseres i henhold til de tekniske kravene som er beskrevet i denne rekommandasjonen.

112. For å styrke internasjonalt samarbeid og unngå dobbelt arbeid, skal medlemsstatene vurdere om deres respektive institusjoner, hvis de ikke allerede har gjort det, skal slutte seg til relevante internasjonale organisasjoner som oppretter avtaler om gjensidig anerkjennelse, som for eksempel organisasjonen EA (European Cooperation for Accreditation), IAF (International Accreditation Forum) og andre instanser av liknende art.

Vedlegg B Sikkerhetsutfordringer

1 Overordnet trusselbilde

Bruk av elektroniske løsninger i stemmegivningen har sine uomtvistelige fordeler, som høy tilgjengelighet, enkelhet i valghandlingen og effektiv opptelling av stemmer. Men elektroniske løsninger bringer også med seg en lang rekke utfordringer. Med utgangspunkt i kravene om at valg skal være frie og hemmelige og prinsippet om ”én velger, én stemme” har vi følgende fundamentale utfordringer:

- Sikre at velgeren får avgitt stemme.
- Sikre at ikke velgeren får avgitt mer enn en godkjent stemme.
- Sikre at stemmen holdes hemmelig ved at den ikke kan kobles til velgeren.
- Sikre at stemmen ikke endres eller forfalskes.
- Sikre at avgitte stemmer ikke går tapt.
- Sikre at det ikke introduseres stemmer som ingen velger har avgitt.

For hver av disse seks hovedutfordringene er det forsøkt identifisert sentrale trusler, knyttet til:

- Stemmegivningsklienten (klient)
  - Virus
  - Programmeringsfeil
- Dataoverføring/nettløsning (overføring)
  - Manglende sikkerhet i nettet
  - Falsk tjener (Man-in-the-Middle)
- Sentrale tjenermaskiner (tjener)
  - Tjenestenekt (Denial-of-Service)
  - Innside angrep på tjener
  - Sabotasje
  - Uautoriserte stemmer
  - Feil i tjenerprogramvare
- Generelle trusler
  - Teknisk sammenbrudd
  - Menneskelige feil

Utfordringene og truslene er samlet i matrisen på neste side. Den anslått største trusselen i hver kolonne er markert med en stor X (i fet skrift), eksempelvis anser vi at virusangrep på klientmaskinen primært vil kunne medføre at velgerens stemme blir ”stjålet”, men at det også er fare for at velgeren ikke får stemt, at hans stemme blir røpet eller at den blir slettet/ikke blir registrert.

I dette vedlegget beskrives de forskjellige truslene, samt en skisse til hvordan disse kan møtes.

Tabell 1: Trusselmatrise

	Trussel	Velgeren får ikke stemt	Velgeren får avgitt mer enn én godkjent stemme	Velgerens stemme blir røpet	Velgerens stemme går tapt	Velgerens stemme blir forfalsket/endret	Falske stemmer
Klient	"Virus" angrep på klient	x		x	x	**X**	
	Programmeringsfeil klient	x			**X**		
Overføring	Manglende sikkerhet i dataoverføring			**X**	x	x	
	Falsk tjener (Man-in-the Middle)	x		x	x	**X**	
Tjener	Tjenestenekt (DOS)	**X**					
	Innsideangrep på tjener			x	x	x	**X**
	Datainnbrudd		**X**		x	x	**X**
	Sabotasje	**X**			x		
	Feil tjener-programvare	x	x	x	**X**		
Generelle	Teknisk sammenbrudd	**X**			x		
	Menneskelige feil	x		x			

2 Trusler rettet mot stemmegivningsklienten

Virusangrep på klient

Et system for stemmegivning over Internett forutsetter utstrakt bruk av standard maskin og programvare for at det skal kunne fungere etter hensikten. Dagens basis software på personlige datamaskiner har vist seg å være meget sårbar for fiendtlige angrep. De siste par årene har antallet ondsinnede angrep eksplodert, og mange av dem utnytter svakheter, såkalte sikkerhetshull, i programvaren. Informasjon om slike sikkerhetshull spres raskt, og det er ikke alltid leverandøren som oppdager dem først. Det medfører at også de med onde hensikter har kjennskap til hvilke programmer som kan utnyttes på hvilken måte.

En angriper kan utnytte sikkerhetshull på flere måter, ikke bare gjennom å lage virus eller ormer som kan være med på å forstyrre gjennomføringen av det elektroniske valget. Denne type aktivitet kan bidra til at tilliten til det elektroniske valgsystemet blir svekket hos velgerne.

Denne type angrep utgjør en betydelig og mangeartet sikkerhetsrisiko. Truslene rettet mot klienten inkluderer blant annet:

- Generelle virusprogrammer som angriper harddisk og som kan stoppe maskinen.

- Spyware, dvs. programvare som overvåker brukerens inntasting av data.
- Såkalte trojanere som tar over deler av maskinen og får den til å oppføre seg i strid med brukerens interesser og oppfatning uten at denne selv er klar over det.
- Funksjonalitet som manipulerer data på disk og i overføring.

Det oppdages nye trusler hver dag, og sikkerhetshull i standard programvare vil være en løpende utfordring.

Det finnes pr. i dag ingen måte å sikre seg 100 % mot denne typen utfordringer. En delløsning på problemet er å oppfordre alle involverte parter til å installere sikkerhetsoppdateringer så snart de er tilgjengelige. Dersom man ikke har anledning til å installere sikkerhetsoppdateringer for et sikkerhetshull som har blitt kjent – dette kan for eksempel være fordi oppdateringen ennå ikke er tilgjengelig – kan man vurdere å endre enkelte konfigurasjonsinnstillinger. Dette kan være med på å hindre at hullet blir utnyttet på det gitte systemet, eller begrense skadeomfanget.

En måte å kunne garantere rene klientdatamaskiner vil være å starte maskinen fra en spesialversjon av operativsystemet distribuert på CD-ROM. Dette er imidlertid en kostbar og komplisert løsning som ikke vil kunne benyttes av alle velgere. Denne type løsning stiller krav til velgerens maskinutrustning og kompetanse og kan på denne måten ekskludere potensielle brukere.

Programmeringsfeil på klient
All programvare kan inneholde feil og dette inkluderer også klientprogramvaren i stemmegivningssystemet. I en sikkerhets- og tidskritisk applikasjon som valg vil programfeil primært kunne bidra til at velgerens stemme går tapt. Programmeringsfeil kan også bidra til at velgeren ikke får avgitt stemme. Som for all annen programvare kan man beskytte seg mot denne risikoen ved å gjennomføre omfattende, kontrollerte tester.

3 Trusler rettet mot stemmemottakstjener og sentrale maskinressurser

Tjenestenekting (Denial-of-Service – DoS/DDos)
Tjenestenekting innebærer at en tjeneste er utilgjengelig over lengre tid uten at det er en del av planlagt nedetid, for eksempel for vedlikehold. Målrettede tjenestenektingsangrep blir gjennomført ved at flere tusen maskiner (eksempelvis i et såkalt *Botnet*) samtidig bombarderer en tjenestemaskin (målet) med trafikk. Mange nettbaserte tjenester har bare kapasitet til å håndtere normal bruk, og er ikke skalert til å håndtere de ekstreme trafikkmengdene som følger av et tjenestenektingsangrep. Denne typen overbelastningsangrep forventes å bli vanligere og mer sofistikerte. Dette innebærer at beskyttelsen mot denne typen angrep må bedres og videreutvikles.

I forbindelse med elektronisk stemmegivning kan et tjenestenektingsangrep – avhengig av angrepets omfang – medføre at valgsystemet blir helt eller delvis blokkert under hele eller deler av valgets gjennomføringsfase. Tjenestenekt-angrep vil kunne resultere i at velgeren ikke får avgitt sin stemme.

Løsningen på problemet kan være å
- avslutte e-valget før valgdagen. Dette vil alltid gi velgerne en mulighet til å avgi stemme i valglokalet hvis e-valget skulle være sperret.

- planlegge for et trafikkvolum som langt overskrider den forventede trafikkmengden i forbindelse med gjennomføringen av det elektroniske valget.
- sørge for å ha oppdaterte sikringsmekanismer og oppfølging av patching, både av virksomhets- og hjemmemaskiner, kan begrense skaden av virus/ormer.
- sikre ventuelle svake punkter (single-points-of-failure) for den elektroniske valgløsningen med redundans gjennom backup-tjenere. En angriper kan omdirigere sitt angrep til det nye systemet, men dette øker risikoen for å bli oppdaget og gjør det vanskeligere å lykkes med et ev. angrep.
- ha rutiner for å flytte nettsidene som skal benyttes ved det elektroniske valget til andre IP-adresser dersom et angrep skulle ramme systemet.

Innsideangrep på tjenerprogramvare
For å kunne gjennomføre et valg vil det måtte utvikles spesiell programvare på tjener for å håndtere sentrale funksjoner i valghandlingen. I litteraturen er ondsinnet programvare på tjenere lagt inn av innsidere ansett som en stor trussel. Denne type ondsinnet kode er vanskelig å avdekke og har potensielt store konsekvenser ved at den kan bidra til at mange stemmer blir endret, lagt til eller slettet.

Arbeidsgruppen mener at dersom det skal benyttes spesialutviklet programvare, produkter eller systemer må disse sertifiseres etter nasjonale og/eller internasjonale regler. Disse gir formell dokumentasjon på at det elektroniske valgsystemet er testet og tilfredsstiller gjeldende koder, standarder og/eller direktiver (se kapittel 9).

Datainnbrudd (hacking)
Datainnbrudd innebærer å skaffe seg uautorisert tilgang til dataressurser. Bakgrunnen kan være alt fra personlig ærgjerrighet til hærverk eller ønske om å manipulere valgutfallet. Selv om et elektronisk valgsystem forutsettes å være oppdatert og riktig satt opp, kan en angriper utnytte sårbarheter som ennå ikke er kjent eller utbedret. Eksempler på slike svakheter kan være dårlige passord eller brukere som har lastet ned ondsinnet programvare, for eksempel virus som installerer *bakdører* på infiserte maskiner.

Datainnbrudd vil primært åpne for at velger avgir mer enn en stemme. I tillegg kan det medføre at velgerens stemme røpes, at den slettes eller i verste fall at en eller flere stemmer endres.

Det finnes ulike tiltak, men det er vanskelig å sikre seg 100% mot denne typen angrep Løsningsforslag for å minske sannsynligheten for datainnbrudd i forbindelse med elektroniske valg kan være:
- Jevnlige søk etter sårbarheter og kontroller av egne systemer for å avdekke sikkerhetshull som inntrengere kan utnytte.
- Sørge for å holde seg informert om kjente sårbarheter i programvare og installere sikkerhetsoppdateringer for relevant programvare (*patching*).
- Overvåkning og filtrering av trafikk ved hjelp av systemer for inntrengingsdeteksjon (IDS) kan avdekke forsøk på innbrudd.
- Integritetskontroll av viktige konfigurasjons- og systemfiler kan avdekke uautoriserte endringer som kan tyde på innbrudd.
- De ansvarlige for å gjennomføre valget og drifte systemet må gjøres kjent med og få opplæring i sikkerhetsrutiner, for eksempel retningslinjer for valg av passord og regler for installering og kjøring av programvare.

Sabotasje
Tekniske løsninger er sårbare for bevisst sabotasje rettet mot sentrale ressurser som datalagre og prosessorer. Angrepene kan også rettes mot strømforsyning og fysiske lokaler. Denne typen angrep vil kunne forhindre velgeren fra å avgi stemme, og vil også kunne slette eller manipulere avgitte stemmer.

For å sikre seg mot denne type trusler er det nødvendig å etablere løsninger med høy fysisk sikring av sentrale komponenter, det må bygges inn redundans i løsningen slik at hvis det finnes back-up hvis sentrale komponenter faller ut. Strømforsyningen bør sikres med UPS løsninger.

Feil i tjenerprogramvare
Som for klienten vil det også for tjeneren være en risiko at det ligger uoppdaget feil i koden. Dette kan i verste fall sette hele valget i fare ved at et stort antall stemmer går tapt. Programmeringsfeil på tjener kan også medføre at velgeren ikke får stemt. Igjen er omfattende og strukturerte tester samt verifikasjon av kode gjennom inspeksjon mulige måter å redusere denne trusselen.

4 Trusler rettet mot dataoverføringen

Svikt i sikkerhet ved overføring
Dataoverføring over et åpent system som Internett medfører en risiko for at andre kan få uautorisert tilgang i velgerens stemme, og i verste fall slette eller manipulere denne. For å gardere seg mot denne type trussel kan man eksempelvis benytte strenge krypteringsrutiner og garanterte sikkerhetsprotokoller (for eksempel https).

Man in the Middle/Domenenavnsystemet (DNS)
Det må tas i betraktning at svindel kan forkomme i form av falske tjenere, for eksempel ved at en annen kan utgi seg for å være den offisielle tjeneren ved å foreta ulovlige endringer i DNS eller ved å benytte et domenenavn som til forveksling ligner den offisielle tjeneren (Man-in-the-Middle).

Falsk DNS-informasjon kan medføre at trafikk styres feil slik at den originale stemmeseddelen blir slettet, erstattet eller at det blandes inn forfalskede stemmesedler. Det er således viktig å sikre at informasjonen i DNS kommer fra riktig kilde. Problemene med å få verifisert hvem som har registrert DNS-informasjon vil medføre en mulighet for å registre falsk informasjon og for eksempel utgi seg for å være noen andre enn den man er.

Et annet problem er at velgeren ikke vil får tilgang til domenenavnsystemet (DNS) dersom dette forstyrres. Uten DNS kan ikke en gitt nettsideadresse oversettes til IP-adresser som Internett benytter for å styre trafikken til rett sted. Unormal belastning på DNS forårsaket av at en – i ondsinnet hensikt – stiller gjentatte forespørsler i store mengder til DNS kan også medføre at normal DNS-tjeneste ikke kan opprettholdes. Dette kan medføre at stemmegiveren ikke får tilgang til e-valgssystemet (jf. pkt. om tjenestenekt).

For å beskytte mot Man-in-the-Middle angrep kan man innføre en digital signatur på stemmeseddelen slik at det være mulig å få verifisert hvem som har avgitt stemme. Det er imidlertid viktig at denne ikke svekker stemmens konfidensialitet.

Det må også etableres sikkerhets/kvitteringsløsninger som vanskeliggjør angrep. Dette kan innebære at velgeren får en kvittering via en alternativ kommunikasjonskanal (SMS, Internett,

digital-TV), eller løsninger som ligner på den som er valgt i Genève der velgerens valgkort inneholder omfattende kontrollinformasjon som inngår i dialogen mellom velgerens maskin og den sentrale stemmemottaksmaskinen.

5 Generelle trusler

Teknisk sammenbrudd
Kontinuerlig tilgang til IT-systemer og Internett er viktig i forbindelse med gjennomføring av et elektronisk valg. Det må derfor forutsettes at alle sentrale deler av infrastrukturen som skal benyttes er robust og sikker. En fullstendig fysisk beskyttelse av Internett vil imidlertid være en uoverkommelig oppgave. Dette skyldes dels nettets komplekse struktur og dels de kostnadene som knytter seg til de ulike sikringstiltakene. Fysisk beskyttelse i denne sammenheng er definert som alle sikringstiltak rettet mot infrastrukturens fysiske deler så som kabelforbindelser, radioutrustning, koblingspunkter, sentrale ressurser mv.

Hvilket behov for sikkerhet som foreligger, avgjøres av hva som er definert som akseptabel risiko og gjeldende normer for sikkerhet. I arbeidet med sikkerhet vil prinsippet om sikkerhetsmessig lønnsomhet være til stor hjelp.

Å sørge for akseptabel risiko er en omfattende oppgave. Det er både mange ressurser (utstyr, systemer, informasjon, personale m.m.) og informasjonsbehandlingsprosesser å sikre. Og det er ikke nok å sikre for eksempel et system når det er satt i produksjon, men det må sikres i sine ulike livsløpsfaser, fra design og utvikling til produksjon og til og med ved avhending. Også for andre ressurser må sikkerhet ivaretas i hele livsløpet.

Det arbeides kontinuerlig med å utvikle bedre løsninger på problemene knyttet til fysisk sikring. I forbindelse med gjennomføring av elektronisk stemmegivning må det stilles klare krav til Internett leverandørene (ISPene) som omfatter blant annet:

- Krav om jevnlig risikovurdering.
- Krav om kontinuerlig oppgradering av teknologi og rutiner for å ivareta et akseptabelt nivå av motstandsdyktighet i forhold til aktuelle trusler.
- Krav om at det foreligger dokumenterte beredskapsplaner.
- Krav om at det er redundans i infrastrukturen.

Manglende bevissthet hos brukerne
En av de største truslene – og utfordringene – knyttet til gjennomføring av elektroniske valg er svikt i og/eller manglende bevissthet om IT-sikkerhet hos den enkelte velger. Personlige datamaskiner som ikke er tilstrekkelig beskyttet kan kapres og utnyttes som plattformer for overbelastnings- og virusangrep mot den infrastrukturen som benyttes i forbindelse med gjennomføringen av det elektroniske valget. Et overbelastningsangrep mot kritiske deler av infrastrukturen kan få konsekvenser for gjennomføringen av det elektroniske valget. Det er derfor en viktig forutsetning at velgerne tar ansvar for sin for sikkerheten i sitt eget miljø. Problemet med dette er imidlertid at sikkerhetsproblemene relatert til IT-bruk i dag er ofte så komplekse at før velgeren kan ta sine forholdsregler må det forutsettes at velgerne har fått den nødvendige forståelse og kunnskap om problemene han eller hun står overfor.

For at et elektronisk valg over Internett skal bli sikrere må velgernes bevissthet og holdning til sikkerhet på Internett forbedres. Dette er tids- og resursskrevende. Tilnærmingen en kan ha er for eksempel å gjennomføre en informasjonskampanje i forkant av valget hvor man blant annet orienterer om hvordan det elektroniske valget skal gjennomføres i praksis, hvilke sikkerhetsmekanismer som er innbygget i systemarkitekturen og hvilke

sikkerhetsforanstaltninger som man forutsetter at den enkelte velger selv skal ha foretatt i forkant av og under et elektronisk valg. For å kunne nå ut til alle forutsettes det at det materialet som skal sendes ut er relativt detaljert med gode illustrasjoner og beskrivelser av valgprosessen.

Mennesker opptrer som kjent ikke alltid logisk og forutsigbart, og det kan derfor være vanskelig å forutse og kontrollere deres oppførsel. Velgerne, og de som skal bygge, drifte og vedlikeholde det elektroniske valgsystemet, er mennesker; og den menneskelige faktor er derfor noe man må ta hensyn til ved design av det elektroniske valgsystemets og utforming av regler og rutiner for bruk av dette.

Utilsiktede hendelser kan i teorien inntreffe hvor som helst. Det er derfor vanskelig å etablere varslingssystemer og -rutiner som kan fange opp alle disse hendelsene. Dette medfører at utilsiktede hendelser avdekkes senere enn tilsiktede handlinger, og dette gjør det mer komplisert å reparere skaden. I tillegg er nødrutiner og beredskapsplaner normalt etablert med tanke på forventede hendelser. Sikkerheten må i stor grad være basert på at velgerne selv tar ansvar for å overholde regler ved bruk av det elektroniske valgsystemet. Med økt antall brukere øker også sannsynligheten for at noen bryter reglene, enten med overlegg eller ved et uhell, og med økt omfang øker også konsekvensene.

Vedlegg C Erfaringer fra andre land - studieturer

1 Storbritannia

Dato: 18. - 20. november 2004
Storbritannia har iverksatt et omfattende arbeid med å modernisere valggjennomføringen. I dette arbeidet er e-valg sentralt, også når det gjelder muligheten til å stemme i ukontrollerte omgivelser utenfor valglokalet. I Storbritannia er elektronisk stemmegivning er del av et større moderniseringsprosjekt. De har en langsiktig strategi og pilotforsøkene er en del av strategien for å komme dit. Storbritannia har en flerkanaltilnærming til stemmegivning.

For å få et mer inngående bilde av erfaringene knyttet til elektronisk stemmegivning, møtte arbeidsgruppen den engelske valgkommisjonen (*The Electoral Commission)* og de sentrale valgmyndigheter i departementet (*Office of the Deputy Prime Minister).*

I tillegg møtte arbeidsgruppen John Borras, som leder arbeidet med å utvikle Election Markup Language (EML) i Storbritannia. EML er sentralt i Europarådets rekommandasjon om elektronisk stemmegivning.

Fordi man i Storbritannia har prøvd ut en lang rekke ulike måter å avgi stemme elektronisk, har vi valgt å redegjøre nærmere for dette i kapittel 4.

2 Sveits

Dato: 26. – 28.november 2004
I Sveits gjennomføres det 4 til 6 valg i året. De fleste er folkeavstemminger, men hvert 4. år holdes det proporsjonale valg til de representative organene. Delvis som følge av de hyppige valgene har landet lenge slitt med kraftig fall i valgdeltakelse. For om lag 10 år siden innførte 25 av landets 26 kantoner derfor brevstemmegivning. I 2003 stemte ca. 2/3 av alle de stemmeberettigede på denne måten.

For å opprettholde de positive resultatene med brevstemmegivning, valgte myndighetene i Sveits i 1999/2000 å videreutvikle løsningen til også å gjelde Internett-valg. Utviklingen var motivert ut i fra et ønske om å tilpasse valghandlingen det moderne informasjonssamfunnet. De ønsket dessuten å gjøre valghandlingen bedre tilgjengelig for handikappede, ungdom og sveitsere som bor i utlandet. Bare i Genève alene utgjør sistnevnte gruppe om lag 10 % av velgerne.

For å kartlegge potensialet for e-valg ble det dessuten gjennomført flere empiriske studier. Undersøkelsene viste at Internett-avstemming hadde betydelig støtte i befolkningen. I følge et representativt utvalg ønsket 66 % av innbyggerne muligheter til å stemme på Internett. Også de fleste politiske partiene og administrative ansatte var for e-valg (Geser 2004:80).
Med dette som utgangspunkt etablerte den sveitsiske stat et prosjekt for elektronisk stemmegivning i 1999. Det ble gjennomført forsøk i tre kantoner; Genève, Zürich og Neuchatel. Om lag 80 % av utgiftene med forsøkene ble finansiert av sentrale myndigheter.
Arbeidsgruppen hadde tre møter under studieturen. De møtte Michel Chevallier og Michel Warynski fra Chancellerie d'etat Genève som presenterte elektronisk stemmegivning i Genève, Daniel Brändli fra Bundeskanzelei, Bern, og tilslutt Laurent Girard fra Hewlett Packhard om presentasjon av sikkerhetsløsning, teknologi og prosedyrer.
I tillegg besøkte arbeidsgruppen et valglokale på valgdagen og overvar åpningen av den elektroniske urnen. Turen ble avsluttet med en pressekonferanse i Genève rådhus.

3 USA

Dato: 30.april - 5. mai 2005
Studieturen til USA var den mest omfattende av studieturene. De personer og organisasjoner gruppen møtte er presentert sammen med et kort referat i punktene nedenfor.

Electionline.org
Electiononline.org er en upolitisk og upartisk organisasjon som arbeider med informasjon om valg, valgordninger og valgreformer i USA. Organisasjonen het opprinnelig Election Reform Information Project. Organisasjonen finansieres av en uavhengig stiftelse (PEW).

Under møtet ble det vist til at valglovgivningen i USA er sterkt desentralisert, ikke bare til delstatsnivå, men helt ned til County-nivå. Spenningene gjør seg gjeldende på tre ulike områder: 1) sentrale vs. lokale myndigheter, 2) tilgjengelighet vs. integritet og 3) sikkerhet vs. rettferdighet i forbindelse med opptelling og omtelling.

Help America Vote Act (HAVA)-loven som ble vedtatt etter presidentvalget i 2000, gir imidlertid de føderale myndighetene en viss mulighet til å påvirke utviklingen gjennom økonomiske støtteordninger til dem som vil implementere de føderale anbefalingene. Det er imidlertid et problem at det er frivillig å følge standardene.

Internasjonal lovgivning i forbindelse med valgordninger har så godt som ingen innflytelse i USA, og det eksisterer flere tusen ulike tekniske valgsystemer i landet. Pennsylvania alene har for eksempel 5-6 ulike systemer. Dette er en konsekvens av den desentraliserte valglovgivningen i USA. Flere stater mener at de gamle stemplingsautomatene (punchcard) fremdeles er billigst og sikrest. Generelt sett er det lite forskning på valg i USA, og særlig Internett-valg.

National Institute of Standards and Technology (NIST)
National Institute of Standards and Technology (NIST) utarbeider standardiseringskriterier for valgsystemer og sorterer under Handelsdepartementet.

Under møtet ble det redegjort for arbeidet med å utarbeide standarder for elektroniske valgløsninger både med hensyn til maskinvare og programvare, på oppdrag fra EAC (HAVA-penger). Dette illustrerer hvordan USA for første gang har valgt å finansiere en harmonisering av valgløsninger og forsøksregimer. Standardene er imidlertid ikke obligatoriske, men rådgivende for de respektive valgmyndighetene. Første versjon av standarden ble levert i 2005. I versjon 2 utvikles ytterligere detaljer, og denne er planlagt ferdig i 2008. Selve sertifiseringen av de ulike løsningene foretas av private, akkrediterte (godkjente) testlaboratorier, og betales av leverandørene selv. Prisen anslås til ca. 60 000 dollar. Dette er et ambisiøst arbeid med blikk også mot fremtidige tekniske løsninger. 37 stater har allerede signalisert at de går inn for å følge de standarder og anbefalinger som NIST kommer med. EML (Election Markup Language) inngår i disse standardene. Selv om valgsystemer har sin egenart sammenlignet med andre systemer, ble det fremholdt at en god del sikkerhetsprosedyrer har samme karakter. Når det gjaldt forsøket på Internett-valg (SERVE), ville de se nærmere på en del av de gode ideene i dette opplegget, slik at man ikke kaster barnet ut med badevannet. Det er et mål at standarder for Internett-stemmegivning kan innarbeides i versjon 3 av standardene.

Det er viktig å være oppmerksom på at ”papirkvitteringer” (paper trail) er frivillig for de stater som velger å følge standardene fra NIST /EAC. NIST håpet å kunne etablere avtaler med opp mot tolv forskjellige ITA'er (Independent Testing Authorities), men forutsatte at det ble minst to. NIST foretrekker å bruke ”guidelines” fremfor ”standards”. Her var det ikke krav om papirkvitteringer, men nødvendigheten av to uavhengige lagringsmedier (dvs. at papir kan være den andre), ble understreket.

United States Election Assistance Commission (US EAC)
US EAC ble opprettet i kjølvannet av HAVA-lovgivningen (se ovenfor), og arbeider særlig med utarbeidelse av retningslinjer for valgsystemer og valgprosedyrer, med særlig vekt på standarder for testing og sertifisering. Det sistnevnte skjer i nært samarbeid blant annet med NIST (se ovenfor).

HAVA-loven nevner eksplisitt at EAC skal sørge for at det blir foretatt en egen studie av Internett-stemmegivning. Dette er ennå ikke blitt gjort, men blir kanskje gjennomført i 2006. Foreløpig har EAC ikke tatt standpunkt til stemmegivning på nettet.

Angående forholdet mellom EAC of Federal Election Commission (FEC), ble det påpekt at FEC hadde ”feil” navn, ettersom dette organet kun har ansvar for reguleringer knyttet til finansiering av valgkamper. Når det gjelder klager knyttet til valget, og ivaretakelsen av føderale valglover, skjer dette i Justisdepartementet. EAC har overtatt ansvaret for utvikling og vedlikehold av standarder for stemmesystemer fra NASED (National Assosciation of Election Directors). Standardene (eller retningslinjene) gjelder både elektroniske (DRE) og optiske (OMR) løsninger.

Federal Voting Assistance Program (FVAP), Department of Defence
Federal Voting Assistance Program forvalter *Uniformed and Oversees Citizens Absentee Voting Act (UOCAVA).* 6,5 millioner amerikanere er omfattet av denne loven.

I forbindelse med Gulfkrigen ble det fra og med valget i 1990 anledning til å sende stemmesedler pr. fax, og senere også via e-post. For 2004-valget hadde man planer om å prøve ut et opplegg for stemmegivning via Internett (SERVE-prosjektet). Dette prosjektet ble som nevnt stoppet. FVAP mener at SERVE er så sikkert som det går an å få det i dag. De innrømmer imidlertid at de hefter betydelig risiko ved nettapplikasjoner. FVAP understreket at man må veie risikomomentene mot fordelene ved å bruke et slikt opplegg. Uansett var Internett-stemmegivning ment å være et alternativ til konvensjonell stemmegivning, og ikke det eneste tilgjengelige.

Foreløpig har SERVE-prosjektet kostet 22 millioner dollar. FVAP var ansvarlige for et forsøksprosjekt i 2000 der det ble avgitt 84 tellende stemmer over Internett. Selv om SERVE er lagt på is inntil videre, er FVAP optimistiske med hensyn til å finne frem til akseptable løsninger for stemmegivning via Internett. Uansett er behovet stort for en forbedring av dagens løsning basert på postgang både for registrering og for stemmegivning.

D.C. Board of Elections and Ethics
D.C. Board of Elections and Ethics er den lokale valgmyndighet i Washington DC. Under møtet ble det redegjort for den praktiske gjennomføringen av valg i 142 valgdistrikter i Washington DC.

I Washington blir to ulike teknologiske løsninger tatt i bruk: dels en optisk leser der velgeren selv mater inn sin ferdig utfylte stemmeseddel, og dels en trykkfølsom pekeskjerm der velgeren trykker på sine utvalgte kandidater og tar stilling til diverse folkeavstemningstemaer. De har 160 scannere og 162 touch-screen maskiner (m/voters card). Det er ingen nettverksløsninger valgdistriktene imellom.

Ved siste valg benyttet omtrent 2/3 den optiske leseren, mens ¼ brukte pekeskjermen. Pekeskjermløsningen gjør det mulig å tilby velgeren informasjoner på sitt eget språk, og det er en tendens til at flere og flere benytter seg av denne løsningen. Hvis minst 5 prosent av velgerne i et valgdistrikt har et annet morsmål enn engelsk, har de krav på å kunne bruke sitt eget språk i valggjennomføringen.

Kapasiteten på pekeskjermmaskinene er ca. 700 velgere pr. dag, den optiske leseren kan håndtere mange flere (mer enn tre ganger så mange). Det ble påpekt at det var viktig med regelmessig vedlikehold av maskinene. Pekeskjerm-maskinen kostet ca. $5000, mens den optiske maskinen kostet rundt $6000.

To ulike system gjør at opptellingen blir mer komplisert enn den hadde vært med bare ett. Det var også noen problemer med valgmedarbeidere som var redde for å benytte utstyret.

Professor Aviel D. Rubin, Information Security Institute, Johns Hopkins University.
Professor Rubin er en velkjent kritiker av e-valg og medforfatter av rapporten som torpederte SERVE-prosjektet. Rubin vedgikk selv at han er negativ til det meste når det gjelder elektronisk stemmegivning. Satt på spissen hevdet han at ”anything electronically should not be trusted.”

Rubin hevdet at alt som skjer ved hjelp av datamaskiner og nettet er usikkert, og at de fleste dataeksperter (computer scientists) var enige med ham. Han mente at Norge kanskje lå noen år etter utviklingen i USA når det gjaldt (mis)tilliten til Internett-løsninger, og spådde at vi ville se et dramatisk fall i handel på nettet når det ble avdekket tilstrekkelig mange vellykkede tilfeller av svindel.

Angående e-valg la Rubin stor vekt på gjennomsiktighets (transparency) argumentet. Han mente at alle sikkerhetsforanstaltninger for elektroniske valg ville bidra til mindre gjennomsiktbarhet for den vanlige velger, og dermed skape grunnlag for mistillit til systemet. Når det gjelder overføring av stemmer via nettet, var han derimot ikke bekymret, forutsatt gode kryperingsalgoritmer.

Hovedproblemene ligger ifølge Rubin i hjemme-datamaskinen, og var meget klar på at Windows ikke var egnet som plattform for kritiske applikasjoner. Han sa også at det vil være variasjon i trusselbildet fra nasjon til nasjon, men han hadde ikke sett nærmere på utenlandske løsninger som for eksempel forsøkene i Genève eller Storbritannia. Rapporten om SERVE-prosjektet var ikke enstemmig, men en mindretallsrapport. Rubin la stor vekt på størrelsesproblemet når det gjaldt sikkerhet knyttet til elektroniske valgløsninger. Mens tradisjonell valgavvikling kan betraktes som ”retail”, dvs. at det er bare mulig å jukse i enkeltlokaler, står man overfor helt andre utfordringer når en person kan påvirke valgresultatet ved en Internett-løsning, dvs. et ”wholesale” (”engros”) problem.

University of Maryland
Dette møtet fant sted på bakgrunn av den rolle Dr. Dan C. Mote (President, University of Maryland), Dr. Paul Herrnson & Dr. Richard M. Schum, spilte i forbindelse med Internet Policy Institutes (IPI) Workshop on Internet Voting i 2000. Dr. Mote var formann for denne konferansen og Dr. Schum er en av to forfattere av oppsummeringsrapporten.

Denne ”workshopen” konkluderte med at Internett-valg ikke var realiserbart på kort sikt og la fram en liste med flere interessante forskningsprosjekter som burde gjennomføres. På direkte spørsmål om hvordan det var godt med disse prosjektene sa de at svært lite, eller ingenting, var gjennomført. Dr. Mote understreket at temaet for den nevnte konferansen ikke hadde vært Internett-stemmegivning, men bruk av ulike elektroniske hjelpemidler i forbindelse med gjennomføring av valg. Dr. Schum minnet om at problemet ikke bare var faktiske inngrep av uvedkommende i valggjennomføringen, men også at for eksempel terrorister etter valget kunne hevde at de hadde påvirket valget, uten at de faktisk hadde gjort det. Uansett ville dette kunne undergrave tilliten til systemet. I følge Schum hendte det noe med USA etter valget i 2000 og etter 9. september, som har hatt innflytelse på den politiske beslutning vedrørende e-valg. Dr. Herrnson minnet også om at man i USA hadde en lang tradisjon med uvedkommende påvirkning, valgfusk og lav valgdeltakelse Tilliten til valgsystemet var derfor i utgangspunktet ikke særlig høy. Hans reaksjon på Internett-stemmegivning var at ”it’s so far away.” Dr. Herrnson var ellers involvert i flere forskningsprosjekter knyttet til brukervennligheten (usability tests) av ulike valgomatløsninger. Etter å ha testet over 6000 maskiner og gjennomført 1500 feltstudier konkluderer de blant annet med at papirkvitteringer (paper trails) ikke øker tilliten til e-valgløsningene.

Association for Computing Machinery (ACM)

Association for Computing Machinery (ACM) er en internasjonal forening av dataeksperter med 80 000 medlemmer.

ACM har engasjert seg i debatten om e-valg fordi de avdekket at kravene til kvalitet i funksjonalitet og utviklingsmetode var strengere for spillemaskiner (gambling) enn for valgsystemer. Policyen er relativt generell, men understreker behovet for en uavhengig, verifiserbar alternativ lagring. Det legges også vekt på at valgsystemer skal utvikles og testes etter gode ”ingeniørprosesser”. ACM har en rent teknisk tilnærming til spørsmålet om e-valg. I forhold til nåværende teknologi er Internett-stemmegivning ikke aktuelt. Det ble likevel understreket at ACMs utspill eller notat – som et stort antall medlemmer hadde sluttet seg til via nettet! – ikke gjaldt Internett-stemmegivning per se, men ulike andre elektroniske løsninger (primært DREs). Det ble i den forbindelse nevnt at ”if done properly, internet voting may be used”.

4 Estland

Dato: 14. - 16. oktober 2005
Estland hadde parlamentsvalg høsten 2005 hvor velgerne kunne stemme elektronisk i forhåndsstemmeperioden. Denne varte fra sjette dag kl 09.00 til fjerde dag kl 20.00 før valget. Det var 1 060 000 stemmeberettigede totalt, rundt 496 336 benyttet seg av stemmeretten, herav ble 9000 stemmer avlagt elektronisk.

Arbeidsgruppens hadde møter med National Election Committe og programvareleverandøren Cybernetica, og var tilstede i valglokalet på valgdagen.

Cybernetica er leverandøren av programvaren for gjennomføring av e-valg over Internett. Vi møtte Monika Oit, leder av avdelingen for Information security og Arne Anspern, Development manager. Firmaet har 80 ansatte. Firmaet er sprunget ut av Estlands satsing på å bygge opp kompetanse på datasikkerhet. Den akademiske delen finnes ved universitetet i Tartu, den kommersielle delen til en stor grad i Cybernetica. Firmaet fikk leveransen av e-valg-systemet i konkurranse med andre estlandske firmaer. Internasjonale leverandører synes ikke å ha vært i bildet.

Orienteringsmøtet hos National Electoral Committee om valget, og da spesielt e-valg-delen fant sted i parlamentsbygningen, Riigikogu. Tilstede var besøkende fra hele Europa - et sted mellom 40 og 50 personer, dels journalister, dels fagpersoner som er involvert i ulike valgprosjekter i hjemlandet. Innledere var lederen for National Election Commitee, Heiki Sibul, og sekretariatsmedlemmene Epp Maaten og Ülle Madise.

Vedlegg D Gjennomgang av innstillinger fra Stortingets fullmaktskomité 1965-2005

Dette vedlegget tar for seg innstillingene fra fullmaktskomiteen om fullmaktene i perioden 1965 til 2005. Vedlegget er delt opp i to deler, 1. klager fra velgerne og 2. komiteens merknader. Klagene er sortert i forhold til klager som gjelder forhold før, under eller etter valgdagen. Komiteens behandling av klagen nevnes kort og angis med 'K:' og er skrevet i kursiv. I enkelte av klagene fra 1997 har departementets uttalelse også blitt tatt med. Dette er det eneste året departementets uttalelse er tatt med i innstillingene. Dette er angitt med 'D:' og står også i kursiv. Del 2 inneholder fullmaktskomiteens merknader etter hvert valg. Disse er også ordnet etter å gjelde forhold før, under eller etter valgdagen.
Til slutt følger en oppsummering.

Del 1 Klager fra velgerne

1 Før valget

1.1 Listeforslag

1973: Partiet Kvinnenes Frie Folkevalgte klager over at enkelte valgstyrer har strøket kandidater fra listen deres uten at tillitsmannen har gitt sitt samtykke. Dette har de gjort fordi kandidatene ønsket det selv. *K: Anmoder regjeringen om å få spørsmålet utredet. Saken har ikke hatt innvirkning for valgutfallet.*

1981: Klage fra SV-medlem over SVs listeforslag. *K: Komiteen er kommet til 'under tvil' at fylkesmannens godkjennelse av listen skal aksepteres.*

1981: På SV-listen for en kommune sto kandidat nummer 13 oppført med feil bosted. Klager mener at dette kan ha ført til at velgerne forvekslet vedkommende med en annen av samme navn. *K: Partiets stemmetall tatt i betraktning er det usannsynlig at dette har hatt utfall for valget.*

1981: Klage fra medlem av Fredspartiet over godkjennelse av listeforslag. Klageren mener den ikke burde vært godkjent. *K: Kan ikke gi klageren medhold.*

1985: Klage fra Frie Folkevalgte om listenominasjonen. *K: Kan ikke gi klageren medhold.*

1989: Frie Folkevalgte klager over at listen deres i Rogaland ble vraket. *K: Riktig av fylkesvalgstyret å vrake listen.*

1989: Frie Folkevalgte og Fredspartiet klager over at listen deres i Kristiansand ble vraket. *K: Riktig av fylkesvalgstyret å vrake listen.*

1989: Miljø og Solidaritet klager over at listen deres ble vraket. *K: Riktig av fylkesvalgstyret å vrake listen.*

1993: Klage fra FrP-medlem om nominasjon. Det ble holdt nytt nominasjonsmøte uten at de fikk skyss- og kostgodtgjørelse. *K: Det ligger utenfor Stortingets oppgave å ta stilling til dette.*

1993: Strid angående listeforslag hos Pensjonistpartiet. *K: Fylkesvalgstyrene har ikke truffet feilaktig avgjørelse om hvilken liste som skal godkjennes.*

1993: Leder for Stopp Innvandringen fikk ikke sendt inn listeforslag innen fristen pga sykehusopphold. *K: Listeforslaget godkjennes ikke fordi det kom inn for sent.*

1997: Klage på fremgangsmåten ved FrPs nominasjon i Oppland. *K: Partiene er ikke pålagt å ordne nominasjonene sine på noen bestemt måte. Klagen avvises.*

2001: Seks klager vedrørende behandling av listeforslag fra Det Liberale Folkepartiet, Sørlandslista, NKP, Miljøpartiet De Grønne, Politiske Parti og Tverrpolitisk Folkevalgte. Klagene er meget omfattende, og dreier seg om fraksjonsdannelser innad i partiene om hvem som har rett til å representere partinavnet. *K: Ingen av dem kan føre til omvalg. Det henvises til ellers departementets slutninger i disse sakene.*

1.2 Valgkamp

1973: Klage på at ikke lister for de små partiene, KKF, NDP og Ensliges Parti ble sendt ut sammen med de andre til stemmeberettigede i Ålesund kommune. *K: Ordningen bør omfatte alle lister.*

1989: Pensjonistpartiet og Felles Framtid fikk ikke tilsendt manntall fra hele fylket. *K: Det er blitt gjort feil, men dette har ikke hatt noe å si for utfallet av valget.*

1993. Klage fra Fridomspartiet mot EF om at partiet ikke fikk tilsendt manntallsavskrift. *K: Ansvarshavende i valgstyret kritiseres for dette bruddet på valgloven § 7. Partiet fikk totalt så få stemmer at det ikke hadde noe å si for valgutfallet likevel.*

1993: Klage fra Harald Trefall, Fedrelandspartiet om at Fedrelandspartiet ikke fikk delta i skole-, TV-debatter, eller valgmøter i militæret, samt manglende beskyttelse mot fysisk vold fra politiske motstandere. *K: Valgloven inneholder ikke regler om hvem som deltar i debatter. Når det gjelder voldsutøvelse er ikke slike lovbrudd 'av den art at de etter valgloven kan føre til ugyldig valg.'*

1997: Pensjonistpartiets valgkamp på Karl Johan forstyrret av konsert. *D: Dette er et ordensproblem det er opp til politiet å ta seg av. K: Enig med departementet.*

2005: Troms RV ber komiteen vurdere om FrPs aksjon om refundering av bensinpenger er i samsvar med valgreglene i Norge. *D: Valgkamp faller utenfor valgloven. R: Riksvalgstyret slutter seg til.*

1.3 Forhåndsstemmegivning

1.3.1 Velger har ikke fått avgi stemme

1977: Klage fra kaptein om at 14 forhåndsstemmer fra mannskapet har blitt forkastet fordi stedsangivelsen på konvoluttene var 'om bord'. *K: Dette er i tråd med reglene*.

1985: Kona til klageren ble lagt inn på sykehus etter at forhåndsstemmegivningen var ferdig der, og fikk ikke stemt. *K: Det er ikke gjort feil i forhold til valgloven, men komiteen understreker at sykehus bør holde forhåndsstemmegivningen så nært opp til valgdagen som mulig*.

1989: Klage fra mannskap på båt over at de ikke fikk forhåndsstemt. *K: Det er beklagelig at valgmateriell ble sendt ut for sent til at mannskapet på skipet fikk avholdt stemmegivning. Komiteen kjenner ikke til om andre skip var i samme situasjon. Kommunaldepartementet bør være oppmerksomme på dette ved neste valg.*

1993: Sykehusinnlagt fikk ikke avgitt stemme fordi han fikk feilaktig informasjon om når stemmeavgivningen ble avholdt på sykehuset. *K: Kan ikke regnes som brudd på valgloven*.

1989: Klage fra velger bosatt på Ibiza om å ha mottatt noe informasjon om hvordan han skal stemme. Ansatt ved ambassaden i Madrid sa over telefon 11/9 at han måtte ha kommet til ambassaden i Madrid for å stemme. *K: Viser til Utenriksdepartementets uttalelse*.

1997: Klager ble satt inn i fengsel 4. september, og de hadde avholdt forhåndsvalg der to dager før. Klager hadde ikke avgitt forhåndsstemme før han ble satt inn. Fikk ikke mulighet til å avgi stemme. *D: Forhåndsstemmegivningen i fengselet fant sted i tråd med reglene. Klageren hadde mulighet til å forhåndsstemme før han ble satt inn. K: Enig med departementet*.

1997: Klager fikk ikke stemt fordi Posten (landpostbudet i Porsanger militærleir) hadde gått tom for stemmesedler. *D: Brudd på valgloven. K: Enig med departementet, men det er ikke sannsynlig at feilen har hatt innflytelse på valget.*

2005: Velger mener at rutinene for forhåndsstemmegivning bryter med prinsippet om hemmelig valg, fordi valgkort legges sammen med stemmen. *D: Ingen regler er brutt. Klagen får ikke medhold. R: Riksvalgstyret slutter seg til.*

1.3.2 Annet

1981: Medlem av valgstyret i Lebesby kommune påklager at valgstyret ikke hadde oppnevnt forhåndsstemmemottakere ved de tre institusjonene i kommunen. De som tok i mot forhåndsstemmer ved institusjonene har ikke vært oppnevnt av valgstyret. *K: Stemmene som ble tatt i mot ved institusjonene skal ha vært forkastet. Det skal dreie seg om ca 10 stemmer, og disse kan ikke ha hatt utfall for resultatet*.

1985: Klager krever nytt valg fordi friske mennesker sperres inne på sykehus. *K: Klageren tar opp forhold som ikke valgloven berører*.

1997: Klager mener fremgangsmåten ved forhåndsstemmegivningen på Posten er i strid med prinsippet om anonymt valg fordi den åpne stemmeseddelkonvolutten leveres i konvolutt sammen med valgkortet hans. *D: Valgloven er fulgt. K. Enig med departementet*.

1997: Klager forhåndsstemte i et annet fylke enn bostedsfylket. Han oppdaget etterpå at han hadde stemt med stemmeseddel beregnet for det fylket han stemte i. Er redd for at stemmen forkastes. *D: Har prøvd å få tak i klageren uten å lykkes. Hvis partiet han stemte på også stiller liste i Oslo er det "mest sannsynlig" at den ikke er blitt forkastet. K: Enig med departementet*.

1997:Valgstyrets leder og sekretær i Lebesby kommune bestemte når og hvor forhåndsstemmingen på de tre institusjonene i kommunen skulle skje uten å snakke med resten av valgstyret. Klagen framsettes av et annet valgstyremedlem. *D: I strid med valgloven, men klagen er ikke fremstilt skriftlig og avvises på formelt grunnlag. K: Enig med departementet*.

2001: SV drev valgkamp utenfor Posten da klager skulle stemme. *D: SVs plassering av stand er i strid med valglovens § 34. K: Enig med departementet. Postens ansvarlige kritiseres, men bruddet på valgloven tyder ikke på å ha hatt innflytelse på valgutfallet.*

2001: Dement kvinne stemte ved hjelp fra ansatt på institusjon. Barna til kvinnen mener stemmen burde bli forkastet. *D: Ingen kommentar fra stemmemottaker at kvinnen var sjelelig svekket. K: Enig med departementet*.

1.4 Manntall

1973: Klage fra velger over kjennelse vedrørende manntallet. *K: Enig med valgstyret*

1973: Velger klager over utelatelse fra manntallet i Karasjok kommune. *D: Klagen tas til følge, og velgeren blir manntallsført i Karasjok. K: Enig i at klagen tas til følge*.

1977: Klager flyttet i august og meldte umiddelbart fra om flytting. På valgdagen var verken han eller ektefelle manntallsført i hjemkommunen. *K: Velger burde selv sjekket manntallet mens det lå ute i tiden før valget.*

1997: Klager mener han burde vært manntallsført i Asker, men står oppført i Oslo. *D: Klageren er folkeregistrert i Oslo, og står i riktig manntall. K: Enig med departementet*.

1997: Klagere har vært bosatt i utlandet i over ti år og søkte ikke om å bli manntallsført før fristen gikk ut, fordi det sto feil tidsfrist på søknadsskjemaet de fikk utlevert ved konsulatet. *D: Korrekt av valgstyret å avslå klagernes søknad. K: Enig med departementet, men mener det er uheldig at skjemaet hadde feil dato. Komiteen kjenner ikke til andre tilfeller av dette problemet, så det er ikke sannsynlig at det har hatt noe å si for valgresultatet*.

1.5 Annet

1973: Klage fra Norges Demokratiske parti om at de er utelatt i valgmateriell tilsendt skip. *D: Partiet ble ikke tatt med fordi det kun stilte liste i to fylker, mens partiene som ble presentert i valgmateriellet skal være landsomfattende. K: Selv om departementet ikke er forpliktet til å ta inn små lister i materiellet bør informasjonen de gir være fullstendig. Partiet kunne allikevel ikke fått noe mandat.*

1989: Klage over at NN er valgt til leder i valgkretsen. *K: Klagen er ikke begrunnet*.

2 Under valget

2.1 Valglokalet

1973: Et valglokale gikk tom for Senterparti-stemmesedler. Dette ble oppdaget kl 18.15, og nye stemmesedler var på plass ca kl 18.40. Stemmegivningen ble stoppet i mellomtiden. *K: Det er begått feil, men kan ikke under noen omstendigheter ha påvirket utfallet.*

1973: Klager hevder det ikke var stemmeseddel for Anders Langes Parti i lokalet. Valgstyret sier at det ikke kan ha vært tilfelle og at de hadde full kontroll over bordet med stemmesedler. *K: Klagen kan ikke 'foranledige noen forføyning' jf. § 51.*

1973: Klage fra Anders Langes Parti om utlegging av stemmesedler. Ved inngangen til valglokalet sto et bord med stemmesedler. Her lå ikke alle partiers stemmesedler, deriblant manglet ALP. Valgstyret sa at bordet ikke hadde noe med valgavviklingen å gjøre. *K: Uheldig plassering av bord. Forholdet 'antas å ikke ha hatt innvirkning på valgutfallet'.*

1981: Sauda kommune hadde valgting kun mandag, og hadde kunngjort at det var mulig å forhåndsstemme fram til klokken 13 lørdag. Stemmestyret ble oppringt klokken 15 lørdag med beskjed om at de i følge loven måtte ha åpent for forhåndsstemming også søndag. Kunngjøringen om muligheten for dette ble slått opp på lensmannskontoret på lørdag. Klageren mener dette er for dårlig informasjon. *K: Dette kan ikke sees som tilstrekkelig kunngjøring. Det har allikevel ikke rammet så mange at det har hatt betydning for utfallet av valget.*

1981: Klager fant ikke RVs liste i valglokalet og kontaktet stemmestyret. De sjekket at riktig antall stemmesedler var der. Klager fant fortsatt ikke RVs liste, og stemte blankt. Stemmestyret mener alle stemmene lå ute. *K: Umulig å avgjøre om stemmestyret eller klager har rett i sin påstand. Stemmestyret burde ha gitt velgeren en blank stemmeseddel der han kunne håndskrevet partinavnet.*

1985: Det manglet stemmesedler i avlukket for partiet klageren skulle stemme på. *K: 'Beklageleg', men stemmestyret kan ikke klandres.*

1985: Det manglet stemmesedler i avlukket for partiet klageren skulle stemme på. *K: Valgstyret skal påse at alle stemmeseddelbunkene ligger hver for seg. Klagen fører ikke til noe.*

1985: Klage på vegne av tre psykisk utviklingshemmede velgere hvis stemmer ble behandlet annerledes enn andres. *K: Klagen tilbakevises. I følge andre som var med forløp det korrekt.*

1993: Stemmesedler for Fedrelandspartiet lå skjult under andre stemmesedler (fremmet i to kommuner). *K: Valgfunksjonærene må rydde i stemmesedlene så alle er synlige.*

1993: Blindeforbundet hadde ikke sendt ut lapp med Felles Framtids partinavn i punktskrift. Denne var ment å klistres på boksen med stemmesedler. *K: Det er ikke gitt uttrykkelige regler om valgmyndighetenes behandling av slike merkelapper. Komiteen mener at hvis det er et parti som ikke har slik merkelapp, bør ingen ha det. Det er ikke opplyst om flere partier manglet lapp med blindeskrift. Det er ikke sannsynlig at denne feilen har hatt utfall på valgresultatet.*

1997: Klage på manglende utlegging av blanke stemmesedler. *D: Å ikke legge ut blanke stemmesedler er i tråd med forskriftene. K: Enig med departementet.*

1997: Klage på manglende utlegging av blanke stemmesedler. Måtte spørre valgfunksjonær om stemmeseddel. *D: Å ikke legge ut blanke stemmesedler er i tråd med forskriftene. Vil se nærmere på denne forskriften. K: Enig med departementet.*

1997: Klage på manglende utlegging av blanke stemmesedler. *D: Å ikke legge ut blanke stemmesedler er i tråd med forskriftene. Vil se nærmere på denne forskriften. K: Enig med departementet.*

2005: Manglende stemmesedler i stemmeavlukket. Klager mener at stemmesedler manglet i flere avlukker, valgkomiteen hevder at det ikke var så utbredt. *D: Uansett omfang er dette "ikke feilfri" valggjennomføring, men det antas at dette ikke påvirket valgresultatet. R: Riksvalgstyret slutter seg til.*

2005: Manglende stemmesedler i stemmeavlukket. *D: Dette er "ikke feilfri" valggjennomføring, men det antas at dette ikke påvirket valgresultatet. R: Riksvalgstyret slutter seg til.*

2005: To klager på at det var mulig for andre å se inn i stemmeavlukket. *D: Plasseringen av stemmeavlukkene synes noe manglefull med hensyn til å sikre hemmelige valg. Klagene tas allikevel ikke til følge. R: Riksvalgstyret slutter seg til.*

2005: Klager følte ubehag ved at valglistene lå på et bord midt i lokalet, og ikke inne i avlukkene. *D: Denne prosedyren er ikke i direkte strid med reglene, men er lite egnet til å ivareta kravet om hemmelig valg. R: Riksvalgstyret slutter seg til.*

2.2 Stemmeprosedyren

1977: Klager og kone ble ikke henvist til avlukke for å legge stemmeseddel i konvolutten. *K: Det burde de ha blitt.*

1981: 'Stemmestyret er satt sammen av søsken og svogere, og dette er etter vanlig praksis inhabilitet.' *K: 'Påklagede forhold er ikke lovstridig'.*

1985: Klage på vegne av psykisk utviklingshemmede som skulle ha blitt fulgt inn i stemmelokalet. *K: Klagen tilbakevises pga misforståelse. Det forløp korrekt.*

1985: Klager måtte hente stemmeseddel på langbord midt i lokale som ikke var avskjermet. 'Alle' kunne se hvilken seddel hun tok. Fikk ikke opplyst at det lå sedler inne i avlukkene. De lå meget uryddig. *K: Feil at bordet ikke var avskjermet.*

1989: Velger fikk beskjed av valgfunksjonær at han ikke kunne forandre på stemmeseddelen, noe som ikke er riktig. *K: Klageren kjente til reglene og ble ikke forhindret fra å stemme slik han ønsket.*

1989: Klage over utlegging av stemmesedler i valglokalet på bord uten skjerming. *K: Det er viktig at bordet med stemmesedler er avskjermet, i samsvar med reglene om dette. Valgstyret kritiseres.*

1993: Klager er utilfreds med stemmeavviklingen i valglokalet. Han må hente stemmeseddel i ett avlukke før han krysses av i manntallet, og etterpå gå inn i et annet avlukke for å legge stemmeseddelen i konvolutt. I det første avlukket må en valgfunksjonær 'kikke inn med jevne mellomrom for å se om det er klart til nestemann'. Dette kan føre til at valgfunksjonæren ser hvilken seddel en velger. Han liker heller ikke å måtte gå med stemmeseddelen i løse luften for å krysses av i manntallet. *K: Prosedyren er ikke i strid med lov eller forskrift, men komiteen 'anmoder departementet om å overveie endring av lov eller forskrifter*.'

1993: Valget i Oslo: Som nødprosedyre da systemet for elektronisk avkryssing i manntallet brøt sammen måtte velgeren legge stemmeseddel sammen med valgkort i stemmekonvolutten. Klager mener dette strider mot prinsippet om hemmelig valg. For øvrig ni innbyrdes uavhengige klager lik denne. Også klage fra velger som ikke fikk stemt pga 'stor kø og tidspress'. *K: Nødprosedyrene er godkjent av departementet og ikke klagegrunnlag. Flertallet i komiteen mener at det er stor margin ved mandatsfordelingen i Oslo. De dokumenterte feilene kan ikke påvirke fordelingen. Et mindretall i komiteen ønsker omvalg.*

1997: Klager fikk ikke lagt stemmeseddelen ned i spalten på urnen, fordi urnen var for full. Valgfunksjonæren tok av lokket på urnen og la konvolutten ned i urnen. Klager mener det er uansvarlig at ikke urnen er forseglet. *D: Valgloven inneholder ingen bestemmelse om at urnen skal være forseglet mens stemmegivningen pågår. K: Enig med departementet*.

1997: I valglokalet lå ikke stemmesedler i avlukkene, men på et langbord med skjermvegg. Det var ikke tilsyn med hvor mange velgere som var bak skjermveggen. *D: Det er lov å ha stemmesedlene på langbord, men en valgfunksjonær burde sett til at det ikke oppholdt seg flere enn én bak skjermen. K: Enig med departementet*.

1997: Klage på at urnen i valglokalet ikke var forseglet. *D: Valgloven inneholder ingen bestemmelse om at urnen skal være forseglet mens stemmegivningen pågår. K: Enig med departementet.*

2005: Klage fra velger som ikke sto i manntallet, selv om hun har bodd i kommunen i 9 år. *D: Klageren er folkeregistrert i en annen kommune. R: Riksvalgstyret slutter seg til*.

2005: Stemmeurne var kun forseglet med hengelås og tråd. Klager fikk ikke stemmen tilbake fra valgurnen da hun ba om det. Klager mener også hun burde ha skrevet under på en liste om at hun hadde stemt. *D: Det er ikke fastsatt regler om hvordan forseglingen av valgurnen skal være. Stemmestyret har ikke brutt noen regler i denne saken. R: Riksvalgstyret slutter seg til*.

2005: Klager krever omvalg fordi valggjennomføringer strider med EMK på flere punkter: Stemmeurnene var uplombert, valgsedlene var åpne (ikke lagt inn i konvolutt), flere velgere gikk sammen inn i stemmeavlukket, velgerne måtte ikke signere i manntallet eller legitimere seg, antall opptalte stemmer tilsvarer ikke stemmer som var krysset av NN klager også på at hans klage på kommunestyrevalget og ordførervalget i 2003 ble avvist, og bes om at denne tas opp igjen. *D: Behandler klagene punkt for punkt, og konkluderer med at gjennomføringen er i tråd med gjeldende lovgivning. Når det gjelder uoverensstemmelse med antall stemmer og*

antall kryss spesifiseres ikke dette med antall. I Oslo var avviket 19. Klagen tas ikke til følge. Klagen på valgene i 2003 avvises. R: Riksvalgstyret slutter seg til.

2005: Klager er syns- og hørselshemmet, og må ha bistand i valglokalet. Hennes ledsager fikk ikke være med inn i valglokalet uten at også en valgfunksjonær var tilstede. Dette ble en stressfaktor for velgeren. Hun mener også at valgfunksjonæren villedet henne til å avlegge feil stemme. *D: Departementet beklager at det har oppstått misforståelser, men kan ikke se at valgfunksjonæren har handlet i strid med regelverket. Velger kan ikke bytte stemme etter at stemmen er avgitt. R: Riksvalgstyret slutter seg til.*

2005: Ordningen med brettbare stemmesedler fører til at valget ikke blir hemmelig. Klager mener hun ikke har fått nok informasjon om valgprosedyren. *D: valgloven er fulgt, og informasjonen i forkant av valget har vært god. R: Riksvalgstyret slutter seg til.*

2005: Klage på at det ikke er mulig for hjemmesittere å kontrollere om noen har stemt i deres navn. Ny teknologi gjør systemet uoversiktlig, og "samfunnet er gjennomsyret av korrupsjon". *D: Det er ikke dokumentert at det er skjedd noe uregelmessig i tråd med klagerens påstander. R: Riksvalgstyret slutter seg til.*

2005: Klage på manglende plombering av valgurne. Plomberingsutstyret kunne ikke brukes, og valgurnen med 103 stemmer sto i et låst rom natten mellom første og andre valgdag. Leder av komiteen hadde nøkkelen. *D: Det som skjedde er ikke i samsvar med loven, men det antas at det ikke har påvirket valgresultatet. R: Riksvalgstyret slutter seg til.*

2.3 Avviste velgere

1977: Ansatte i Forsvaret fikk ikke anledning til å stemme fordi de hadde militærøvelse. Valgstyrets formann sier at valglokalet hadde opp fra klokken 10-13 og 15-20 valgdagen. Øvelsen begynte klokken 18.30. *K: Valgmyndighetene har ikke ansvar i dette forholdet.*

1989: På telefon til kommunen fikk førstegangsvelger beskjed om at hun kunne stemme i kommunen hun jobber. Da hun kom til stemmelokalet fikk hun vite at hun ikke kunne det allikevel. *K: "Uheldig" at hun fikk feil informasjon.*

1989: Klager med kone ble avvist i stemmelokalet fordi det var stengt. Han hadde hørt uriktige opplysninger om åpningstider i lokalradioen. *K: Ingen merknader, klagen fører ikke til noe.*

1997: Klager var allerede krysset av på å ha avgitt forhåndstemme da hun skulle stemme på valgdagen. Nekter for å ha forhåndsstemt.. *D: Det er lite sannsynlig at noen kan ha stemt på vegne av velgeren. Klagen avvises. K: Enig med departementet.*

1997: Klage på at et avlukke i valglokalet var under demontering klokken 19.55 valgdagen. Støy og "anmasande stemning" i lokalet. Stemmesedlene lå på langbord uten beskyttelse mot innsyn. Klager mener valgfunksjonæren som sto ved bordet fulgte med på hvilken stemmeseddel han tok. Klager ble ikke vist til avlukket, og la stemmeseddelen i konvolutten ved bordet. *D: Påklagede forhold er sterkt kritikkverdige, men ikke noe tyder på at velgeren ikke fikk stemt det partiet han ønsket. K: Enig med departementet.*

2.4 Valgagitasjon på valgdagen

1989: Velger klager på radioinnslag i NRK Telemark på valgdagen hvor en valgfunksjonær uttaler seg om hvilke bunker av stemmesedler som har minket og ikke. *K: Slikt må ikke hende. Komiteen ber departementet følge med på dette området og se om det er 'grunn til å utfylle lov eller forskrifter'.*

2001: Det hang et oppslag om korrigert FrP-liste i valglokalet på valgdagen. Klager mente dette var ulovlig valgagitasjon. *D: Klagen kom ikke skriftlig til departementet og ble behandlet, og avslått, av valgstyret på stedet. K: Enig med departementet, i tillegg mener komiteen at denne listen ikke kan regnes som lovstridig valgagitasjon*.

3 Etter valget

3.1 Opptelling

1977: Mannskap på båt forlanger omvalg fordi valgutfallet ble korrigert to ganger. *K: Forholdet har ikke hatt innvirkning på valgutfallet.*

1989: I en kommune hvor to av fire stemmeberettigede til sametingsvalget hadde avgitt stemme, ble det telt opp fem stemmer til sametingsvalget. *K: Utlegging av stemmesedler må gjøres på en oversiktlig måte*.

3.2 Transport

1997: Transport av urner skal ikke ha forgått i henhold til bestemmelsene. To stemmestyremedlemmer var ikke tilstede under hele frakten. *D: Departementet kan ikke se bort fra at urnenes innhold kan ha blitt endret, men det er lite sannsynlig siden de ikke hadde forseglingsutstyr. K: Anser det som "kritikkverdig at rutinene ikke ble fulgt". Er ellers enig med departementet.*

Del 2 Komiteens øvrige merknader

1 Før valget

1.1 Manntallet

1965: Forhåndsstemmer har blitt vraket fordi velger ikke sto oppført i manntallet.

1977: I et ’meget lite antall’ kommuner har manntallet ligget ute for få dager I flere tilfelle har innkalling kommet på et meget tidlig tidspunkt, som juni og april. Hvis denne innkallingen ikke gjentas, er dette ’lite tilfredsstillende’. Uttrykket ’betimelig tid’ i valgloven bør presiseres av departementet.

1981: I noen kommuner har manntallet ligget ute noen dager for lite.

1981: Noen valgstyrer har kunngjort når valgtinget er utenfor det tidsrommet som er fastsatt.

1985: Fremmede stemmer og forhåndsstemmer har blitt vraket fordi velgeren ikke står i manntallet. I Akershus: ’ganske mange’ feil. Grunnene til feil i manntallet skal være omlegging til nytt system for folkeregisterajourhold.

1989: Fremmede stemmer og forhåndsstemmer har blitt vraket fordi velgeren ikke står i manntallet. Velgerne må få bedre informasjon om hvilken kommune de er manntallsført i.

1993: 771 forhåndsstemmer og 4214 fremmede stemmer er blitt forkastet pga velgeren ikke står i manntallet. Velgerne må få bedre informasjon om hvilken kommune de er manntallsført i.

1997: Komiteen oppfordrer departementet om å overveie å endre loven om at nordmenn bosatt i utlandet må søke om å stå i manntallet hvis de har bodd i utlandet i mer enn ti år.

2001: Forhåndsstemmer er blitt forkastet fordi velgeren ikke sto i manntallet selv om originalt valgkort lå med stemmen. Det er ’overraskende for komiteen at slikt kan skje.’

2005: Valgtingsstemmer er blitt forkastet fordi velgeren ikke sto i manntallet der de møtte opp på valgdagen. Komiteen foreslår at valgkortet inneholder informasjon om hvor personen er manntallsført, evt skyve frysningsdatoen fra 31. mai og nærmere valgdagen.

1.2 Forhåndsstemmegivningen

1965: Det virker som stemmemottakeren ”ofte” gjør feil. Komiteen oppfordrer departementet om å vurdere å forenkle det som skal skrives på omslagskonvolutten.

1969: ’En rekke’ forhåndstemmer er blitt forkastet pga manglende utfylling på konvolutten. I enkelte tilfeller kan det tyde på at det har manglet omslagskonvolutter.

1973: Mange stemmer forkastes fordi punktet om legitimasjon som skal fylles ut av stemmemottaker ikke er fylt ut korrekt.

1973: 3,18 % ble forkastet. De feil det finnes flest av er: ikke angitt sted og dato, stemmesedler fra andre valgdistrikter, mangelfull legitimasjon fra stemmegiver.

1973: Ved forhåndsstemming ved sykehus o.l. forekommer det flere stemmer hvor stemmemottaker har anført "utilregnelig" eller "manglende stemmeførhet". Komiteen mener man bør være meget varsom med å nekte noen å avgi stemme eller forkaste en stemme på denne måten.

1977: Det er blitt forkastet en del forhåndsstemmer pga velgeren ikke sto i manntallet eller fordi velgeren stemte på valgtinget. Noen er også forkastet pga feil hos stemmemottakeren. ’En forenkling av hele forhåndsstemme-instituttet synes ønskelig’.

1981: Feil ved omslagskonvolutten har ført til flere forkastelser enn i 1977.

1981: Det synes å være behov for en grundigere forhåndsvurdering mht hvem som får være stemmemottaker.

1981: Omslagskonvoluttene har hatt for lite lim.

1981: De som hjelper funksjonshemmede med forhåndsstemmegivning har i noen tilfelle kun skrevet sitt eget navn på omslagskonvolutten. Dette fører til forkasting.

1985: Stemmesedler er vraket pga feil/ikke omslagskonvolutt.

1985: En valgkrets brukte manntallet fra nabovalgkretsen og krysset av da velgere fra nabokretsen kom for å stemme. Manntallet ble levert tilbake dagen etter, da det var valg i den aktuelle kretsen.

1985: Fremmede stemmer i en kommune ble i løpet av valgdagen transportert til aktuell krets og stemmestyret krysset av i manntallet der, dette skal valgstyret gjøre.

1985: Det er nok til å vrake forhåndsstemme hvis stemmemottaker har strøket ordene ’ved full sans og samling’ på stemmekonvolutten. Komiteen mener at dette bør grunngis mer omstendelig.

1985: Det ble vraket for mange stemmesedler, de som ligger sammen med partibrosjyre/blank stemme burde vært godkjent. Hvis det står A med ring rundt bør denne stemmen komme Arbeiderpartiet til gode.

1985: Stemmer har blitt vraket på grunn av ’velger var psykisk utviklingshemmet’. Dette er feilaktig vraking.

1989: Stemmer har blitt vraket fordi stemmemottakeren har gjort formelle feil. Det er viktig at forhåndsstemmer sendes på den raskeste måten og i god tid før valgdagen. Stemmemottakere må ikke samle opp stemmer over lengre tid og sende dem inn samlet. Det bør vurderes kortere tidsfrist for forhåndsstemming utenfor kommunene man er manntallsført. ’ Komiteen finn det uheldig at reglane er slik at mange førehandsrøyster som blir avgjevne på lovleg tidspunkt, må vrakast fordi dei likevel kjem for seint fram til veljaren si heimkommune’.

1993: Stemmemottakere ved forhåndstemmegivning gjør for mange feil. Velgerens underskrift mangler på omslagskonvolutt, det ikke er brukt omslagskonvolutt, eller ikke ført nummer på konvolutten. Komiteen foreslår å ha to stemmemottakere i stedet for én, og det må vurderes nøye hvem som blir stemmemottaker. Stemmesedler for et annet fylke enn der velgeren er registrert har feilaktig blitt forkastet av en del stemmestyrer. Disse skal godtas hvis partiet stiller til valg i velgerens hjemkommune. Komiteen 'savner oversikt' over hvor mange forhåndsstemmer som er blitt vraket fordi de ble sendt inn for sent, men 'spredte inntrykk tyder på at antallet slike tilfelle er betydelig også i år'. Forhåndsstemmer må sendes så de kommer fram i tide, og må ikke samles opp over tid og sendes samlet.

1997: Posten har mottatt forhåndsstemmer for første gang. Komiteen har i det store og hele et positivt inntrykk av ordningen. Totalt 1398 forhåndsstemmer forkastet i år, mot 1934 i 1993. Ikke alle partier har vært representert i den bunken med stemmesedler som har vært delt ut til velgeren. En alvorlig feil.

2001: Det var 'ulike typer' feil ved stemmeseddelsettene. Feilene ble oppdaget underveis i forhåndsstemmeperioden. Posten satte i gang kontrolltiltak da de ble oppdaget.

2005: Mange stemmesedler ble forkastet fordi de kom for sent fram til valgstyrene. Komiteen mener det kan være grunn til å justere disse innsendingsfristene noe.

2 Under valget

2.1 Åpningstidene til valglokalet

1965: Enkelte valgstyrer har hatt åpningstider som er lovstridige.

1985: Komiteen har merket seg at 'nokre få valstyre' har satt åpningstiden til mindre enn fem timer.

1985: 'Nokre valstyre' har vært for tidlig ute med å kunngjøre tid og sted for valgtinget.

1989: Komiteen har lagt merke til at 'nokre få' valgkretser har hatt kortere åpningstid enn fem timer på mandagen, noe som er i strid med valgloven. Komiteen vil innskjerpe at lovreglene om åpningstider følges.

1993: Ett valglokale hadde ved stemmeavviklingen kun åpent 11-13, hvilket er i strid med loven. 'Enkelte andre' valglokaler hadde åpent kun fra 9-14 hvilket ikke er i strid med loven, men kan skape problemer for velgere som er i arbeid. Meldinger i media om at valglokalene er stengt i en kommune kan føre til at velgere tror det er stengt i deres kommune selv om det ikke er det.

1997: Meldinger i media om at valglokalene er stengt i en kommune kan føre til at velgere tror det er stengt i deres kommune selv om det ikke er det. Departementet bør vurdere hensiktsmessigheten i at kommunene har så stor valgfrihet i å bestemme åpningstidene.

2.2 Valgfunksjonærer

1989: Det er svært uheldig at stemmer blir forkastet på grunn av formelle feil som stemmemottakeren gjør. 'Ein del' valgstyrer har ikke sendt materiellet til Stortinget.

1993: Komiteen reiser spørsmålet ’om de riktige personer alltid utpekes til stemmestyremedlemmer’ på grunn av formelle feil som fører til forkastelse av stemmer. Komiteen foreslår å utvide åpningstiden eller ha flere valgfunksjonærer på grunn av kødannelser under stemmeavgivningen enkelte steder.

1997: Det er gjort formelle feil som kunne vært unngått om valgfunksjonærer og stemmestyre fikk bedre opplæring. Særlig de som åpner stemmeseddelkonvoluttene må få opplæring i hvordan de behandler konvolutter med to stemmer.

2001: Det er gjort formelle feil som kunne vært unngått om valgfunksjonærer og stemmestyre hadde fått bedre opplæring.

2.3 Stemmesedler

1965: Valgstyrene må passe på at de til enhver tid har nok stemmesedler og omslagskonvolutter.

1969: Det har kommet inn klage fra velger om at Senterpartistemmesedler ikke var lagt ut. ’Har ikke hatt noe å si for valgutfallet.

1969: Inkonsekvens i valgdistriktene i behandlingen av stemmesedler hvor det var kysset av på feil sted (eks på høyre side av kandidatens navn når det riktige er til venstre) Noen er blitt forkastet, andre godkjent.

1969: Håndskrevne stemmesedler har for det meste blitt godkjent. Eks. ’jeg stemmer høyre’. Noen har blitt forkastet, eks. ’Bondepartiet’.

1973: Enkelte valglokaler er dårlig utstyrt.

1973: Inkonsekvens blant de ulike valgstyrene i behandlingen av stemmesedler som er skrevet på av stemmegiveren. Enkelte valgstyrer har godkjent alle, mens andre ikke har godkjent noen.

1977: Et ’relativt stort’ antall stemmesedler har blitt forkastet fordi velgeren har benyttet valglister fra andre valgdistrikter. Dette har særlig forekommet i forhåndsstemmegivningen. Det bør vurderes som disse kan godkjennes i fremtidige valg.

1977: Det bør vurderes om det er grunn til å opprettholde reglene om særmerking.

1989: Det er blitt vraket stemmer der det i konvolutten i tillegg til stemmeseddelen lå en blank stemme. Disse burde ikke ha blitt vraket. Stemmeseddelen til stortingsvalget skal også godkjennes hvis det feilaktig ligger en stemme til sametingsvalget i konvolutten i tillegg. Det er blitt forkastet håndskrevne stemmesedler til eksisterende partier. Komiteen mener disse ikke bør forkastes hvis det er ’uten rimelig tvil’ hvilket parti det skal stemmes på.

1993: Stemmestyrene bør holde det ryddig i stemmebunkene for å sikre god oversikt og at ikke sedlene er blandet sammen. Reglene om utlegging av stemmesedler i valglokalene bør vurderes endret. Stemmesedlene bør ligge inne i avlukkene. Papirkvaliteten på stemmesedlene bør bedres for å unngå flere stemmesedler i samme konvolutt.

1993 Vraking av stemmer:
I kommuner hvor det ble avholdt stortingsvalg og ekstraordinært kommunestyrevalg samtidig inneholdt 'ganske mange' stortingsvalgskonvolutter stemmesedler til begge valgene eller bare til kommunestyrevalget. Komiteen mener at stemmeseddelen til stortinget bør godkjennes i disse tilfellene.

I kommuner hvor det holdes stortingsvalg og sametingsvalg legges stemmesedler til sametingsvalget i konvolutt for stortingsvalget. Disse forkastes.

'Et forholdsvis stort antall' fremmede stemmer måtte forkastes fordi det ikke er brukt stemmeseddelkonvolutt. Stemmestyret bebreides. Noen stemmer er blitt forkastet fordi omslagskonvolutten ikke er blitt klebet igjen. I andre tilfeller har de ikke blitt forkastet. Komiteen mener det er riktig å forkaste slike stemmer.

Etiketter med punktskrift for blinde som var ment for boksene med stemmesedler ble brukt som stemmesedler. Noen steder forkastet, andre steder godkjent. 'Uklart' i forhold til valgloven om disse stemmene bør vrakes eller ikke.

1997: Det har blitt telt opp for mange stemmesedler i forhold til tallet på avgitte, godkjente stemmer. En grunn kan være at de har klebet seg sammen. Etiketter med punktskrift for blinde som var ment for boksene med stemmesedler ble brukt som stemmesedler. Noen steder forkastet, andre steder godkjent. For komiteen er det 'ikke opplagt riktig' å forkaste disse stemmene. Komiteen ber departementet vurdere hva som bør gjøres for å legge bedre til rette for blinde og svaksynte.

2001: Papirkvaliteten på stemmesedlene bør forbedres for å unngå sammenklebing.

2005: Det er uheldig at det enkelte steder har manglet stemmesedler i valglokale på valgdagen.

2005: Manglende stempling av stemmesedler er hovedårsaken til at stemmesedler forkastes.

3 Etter valget

3.1 Opptelling

1969: Enkelte stemmestyrer har mangelfull protokollføring. Komiteen har drøftet tidspresset.

1977: Det ble feilplassert en tellekonvolutt med 50 SV-stemmer i bunken til Arbeiderpartiet. Feilen ble oppdaget under fintellingen, med andre ord etter at resultatet av grovtellingen var offentliggjort.

1977: Enkelte 'meget få' valgstyrer unnlater å regne tomme stemmekonvolutter som forkastede stemmer og får unøyaktigheter i oppgjøret.

1981: Det er telt opp for mange stemmer, antakeligvis pga sammenklebing av stemmesedler.

1985: 'Stort sett tilfredsstillande'. Føring av møtebøker er også stort sett tilfredsstillende. 'Nokre' valgstyrer protokollerer feil tomme og vrakede stemmer.

1985: I Oslo er møtebøkene så feil ført at det 'ikkje er mogeleg for nemnda å foreta ei reell etterprøving av valet i Oslo.'

1989: Problem med sammenklebing av stemmer. Valgfunksjonærene må være påpasselige med å sjekke at det bare er en seddel i konvolutten. Det har blitt regnet flere stemmesedler fra samme konvolutt. 'Komiteen understrekar på nytt at slike feil kan vere svært alvorlege, og at alt som kan gjerast for å få dei bort, må gjerast.'

1993: I noen kommuner er det store differanser på avkryssede og opptalte stemmer. Det opplyses at en grunn kan være sammenklebing av stemmesedler. Papirkvaliteten på stemmesedlene bør forbedres.

1997: Det har blitt telt opp for mange stemmesedler i forhold til tallet på avgitte, godkjente stemmer. En grunn kan være at de har klebet seg sammen.

2001: Det er blitt telt opp for mange sedler i forhold til avgitte stemmer. Det opplyses at en grunn kan være sammenklebing av stemmesedler. Papirkvaliteten på stemmesedlene bør forbedres. Tidspress under opptelling må ikke gå ut over hensynet til et riktig resultat.

3.2 Transport

1993: Det manglet ca 700 stemmer fra Nordtvedt krets i Oslo, uten at dette hadde noen sammenheng med sammenbruddet i systemet for elektronisk avkryssing i manntallet. Noen forklaring på 'denne miséren' finnes ikke, men en teori går ut på at en urne med sedler er blitt kastet.

1997: Flere fylkesvalgsstyrer har kritisert måten valgstyrene har pakket valgmateriell på ved oversendelsen til fylkesvalgstyret. 'Flere fylkesvalgstyrer' bemerker at pakkene bare var forseglet med tape, 'til dels dårlig tape.'

2005: Enkelte kommuner i Oppland manglet forsegling på sine forsendelser til fylkesvalgstyret. Komiteen understreker at ansvaret for forskriftsmessig forsegling av valgmateriell må innskjerpes.

3.3 Møtebøker

1965: Stedvis mangelfull føring av møtebøker, men det som faktisk er ført inn er 'klanderlaust'. Det som mangler er sted og tid for stemmegivningen, underskrift av mottaker, ikke krysset av for framvist legitimasjon. Stedsangivelsen 'i sjøen' kan ikke godkjennes.

1973: Er ikke ført så godt som ønskelig. Mangelfullt mange steder. Skjemaene bør gjøres mer oversiktlige.

1977: Bykommunene avgir ikke så oversiktlige valgoppgjør som er ønskelig.

1981: Det er nødvendig at fylkesvalgsstyrer sender alt materiell omgående.

1981: 'Ganske mange' valgstyrer blander sammen protokollføringen av forkastede stemmegivninger og forkastede stemmesedler.

1981: En del valgstyrer fører ikke møtebøker som de skal.

1989: ’Ganske mange’ av møtebøkene er ikke førte i samsvar med formularet, dette gjør kontrollen ’vanskeleg, i nokre tilfelle umogeleg.’ Det trengs mer rettledning til valgstyrene om hvordan de skal føre møtebøkene.

1993: Komiteen finner det uheldig at formularet ikke inneholder oppfordring til protokollering av alle forkastningsgrunner til stemmesedler. Det er fortsatt feil og mangler ved føring av møtebøkene, og at valgstyrene må ha mer informasjon om dette.

1997: Erfaringen fra årets valg viser at føring av møtebøker er svært uensartet. Noen har tilrådd at valgstyrets møtebok blir forenklet.

2001: Har blitt ført feilaktig eller mangelfullt. Valgfunksjonærer må få grundig opplæring i hvordan denne føres.

2005: Har blitt ført feilaktig eller mangelfullt. Valgfunksjonærer må få grundig opplæring i hvordan denne føres.

4 Annet

1977: Innkalling til valgtinget har ved ’en rekke tilfelle’ skjedd på et noe sent tidspunkt.

1981: Omvalg i Buskerud fylke: 38 forhåndsstemmer har ikke blitt forkastet, men skulle vært det. Det var 22 flere stemmesedler enn avkryss i manntall. Det har altså blitt godkjent 60 stemmer flere enn det skulle vært. Marginen for tildeling av siste mandat var på 28 stemmer. Feilene kan ha hatt innvirkning på tildeling av det siste mandatet og det må holdes omvalg, jf.. lovens § 51.

1981: Omvalg i Troms fylke: Det er godkjent i alt 14 stemmer mer enn det skulle vært. KrF vil tape siste mandat hvis stemmetallet reduseres med mer enn 7 stemmer. Høyre vil kunne ta siste mandat i konkurransen med KRF hvis de fikk mer enn 25 stemmer til. Komiteen kan ikke utelukke muligheten av at disse 14 uriktig godkjente stemmene har falt slik på partiene at KrFs siste mandat står i fare. Det må holdes omvalg.

1985: Kringkasting: ’Fleire’ nærradiostasjoner kringkasta valgresultatet før valglokalene stengte.

1989: Utjevningsmandat: Det skiller bare 185 stemmer fra at Akershus skulle fått det ene utjevningsmandatet i stedet for Oslo. Komiteen har merket seg at ved opptelling var det 250 flere opptelt stemmer enn utdelte stemmekonvolutter.

1993: Problemene ved valggjennomføringen i Oslo: Straks etter at man klokken 9 på valgdagen tok i bruk elektronisk avkryssing i manntallet, fant det sted et nettverkssammenbrudd som ut over dagen rammet samtlige stemmelokaler. Nødprosedyren som ble satt i gang gikk ut på at stemmemottaker krysset av i papirmanntall. Velgeren fikk en rød konvolutt som valgkort og stemmeseddelkonvolutt med stemmeseddel skulle legges oppi. Det ble registrert 529 forkastede stemmer i Oslo kommune. Enkelte velgere kan ha latt seg skremme ved å delta i valget pga frykt for manglende anonymitet. Det var i praksis mulig for velgere å avgi dobbelt stemme hvis man først hadde blitt krysset av elektronisk. Ved

etterkontroll ble det registrert 12-15 slike dobbeltstemmer, men man kan ikke si med sikkerhet om dette er med intensjon fra velgeren. Et mindretall i komiteen (4 mot 12) ønsket omvalg i Oslo pga problemene i stemmeavgivningen der.

1993: Tekst på valgkortene: Teksten på valgkortene kan gi inntrykk av at velgeren må ha med valgkortet for å få stemt på valgdagen. Dette kan ha ført til at velgere som har mistet valgkortet sitt har unnlatt å stemme.

1997: Tømming av urne: På Trysil ble innholdet fra en urne som ble tømt blandet med ubrukte stemmeseddelkonvolutter. Noen velgere fikk utdelt stemmeseddelkonvolutt med innhold fra den tømte urnen. Komiteen påpeker at det er svært viktig at innholdet fra tømte urner oppbevares på et sikkert sted.

2001: Offentliggjøring av valgresultater Offentliggjøring av valgresultater på www.nrk.no før kl 21 valgkvelden. Skal ikke forekomme.

2001: Informasjon til innvandrere: Komiteen har lagt merke til at innvandrere har vært i villrede om hvordan prosessen foregår. Viktige ledd i prosessen er annerledes enn i deres hjemland. Departementet bør vurdere om det er behov for mer informasjon.

2005: EDB-systemer: Det har oppstått problemer i flere fylker der de har brukt EDB-baserrte opptellingsystemer. Et eksempel på feilkilde er at rettinger ble utført i papirmøtebok, og EDB-systemet ble ikke oppdatert på samme måte. Komiteen ber om at de eksisterende EDB-systemenes egnethet vurderes, likeledes valgmedarbeidernes opplæring på området.

Del 3 Innstillingene fra fullmaktskomiteen 1965-2005: Oppsummering

Innstillingene fra fullmaktskomiteen inneholder klager fra velgerne og generelle merknader fra fullmaktskomiteen. I dette kapitelet er både klager og merknader sortert i kategoriene før, under og etter valgdagen. Det er registrert totalt 90 klager fra velgerne. Disse er stort sett ikke veldig alvorlig i forhold til demokratiske prinsipper. En del av klagene har ikke noe formelt klagegrunnlag. For eksempel var ikke stemmestyrene forpliktet til å legge ut blanke stemmesedler, selv om mange velgere klaget på dette.

Klager fra velgerne
Av klagene fra velgerne dreier 44 seg om forhold før valgdagen, blant disse er 18 klager vedrørende listeforslag og 14 vedrørende forhåndsstemmegivningen. Klagene vedrørende listeforslag dreier seg stort sett om fraksjonsdannelser innad i partiene om hvem som har rett til partinavnet. Disse klagene er omfattende og er viet mye plass i innstillingene. Når det gjelder klagene vedrørende forhåndsstemmegivningen er det syv som dreier seg om at velgeren ikke har fått avgi stemme. Blant disse klagene er det to klager som omfatter mer enn én person, for eksempel ble alle forhåndsstemmene fra et mannskap på båt forkastet på grunn av feil stedsangivelse på stemmekonvolutten i 1977.

Det er klagene som dreier seg om forholdene under stemmegivningen som har mest relevans for elektronisk stemmegivning. Det er registrert 42 slike klager i denne tidsperioden. Klagene under valget går hovedsaklig på manglende utlegging av stemmesedler, og forhold ved valglokalet da velgeren skulle stemme.

- Problemet med manglende utlegging av stemmesedler forsvinner med innføring av valgomat eller stemmegivning over Internett.
- Klager på forhold i valglokalet er av forkjellig karakter. Støy i valglokalet og valgagitasjon utenfor valglokalet forbedres ikke med bruk av valgomat.
- Det er registrert syv klager på at stemmesedlene lå på et bord midt i lokalet som ikke var skjermet for innsyn. Dette problemet vil kunne løses ved å ta i bruk valgomat og stemmegivning over Internett.

Ved valget i Oslo i 1993 ble det brukt elektronisk manntall. Da dette systemet brøt sammen ble det tatt i bruk nødprosedyrer hvor stemmeseddel og valgkort ble lagt i samme konvolutt. Det kom inn ti klager som gikk på at nødprosedyrene var i strid med prinsippet om hemmelig valg. Disse ble avvist fordi nødprosedyrene ble gjennomført i tråd med bestemmelsene. Fire av klagene går på forhold etter valget, antallet er naturligvis lavt siden få av velgerne tar del i stemmetelling og etterkontroll. Forholdene etter valgene behandles nærmere av komiteen.

Merknader fra komiteen
Merknadene er ganske like fra år til år, og dreier seg hovedsaklig om disse punktene:

- Åpningstider: Åpningstidene til valglokaler har blitt kunngjort for sent, eller for tidlig. Noen valglokaler har holdt åpent i for kort tid.
  - Kommentar: Dette problemet løses ikke med bruk av personlig datamaskin/valgomater i valglokalet, men problemet forsvinner ved Internett-stemmegivning.
- Valgfunksjonærer: Komiteen påpeker ofte at valgfunksjonærer får for dårlig opplæring og de gjør formelle feil. Dette gjelder også stemmemottakere ved forhåndsstemming.
  - Kommentar: Ved bruk av personlig datamaskin/valgomater i valglokalene vil valgfunksjonærer fortsatt trenge opplæring, kanskje mer enn før. Ved Internett-stemmegivning blir valgfunksjonærer i dagens forstand overflødige.
- Stemmesedler: Er ofte klebet sammen, papirkvaliteten må forbedres. Stemmeseddelbunkene må holdes ryddige. Stemmesedler til kommune- og fylkestingsvalg må holdes hver for seg.
  - Kommentar: Problemet forsvinner med personlig datamaskin/valgomat og stemmegivning over Internett.
- Konvoluttregnskapet går ofte ikke opp, dette henger sammen med sammenklebede stemmer og tidspress. Møtebøker føres mangelfullt og inkonsekvent fra valgkrets til valgkrets.
  - Kommentar: Kan forbedres med personlig datamaskin/valgomat og stemmegivning over Internett.
- Transport: Det har vært registrert to tilfeller hvor stemmesedler mangler, eller at transporten ikke har foregått i tråd med bestemmelsene.
  - Kommentar: Ved bruk av personlig datamaskin/valgomat vil stemmene også måtte transporteres, enten manuelt eller elektronisk. Dette kan også medføre problemer.

Omvalgene i 1981
Den mest alvorlige konsekvensen av problemer ved gjennomføring av valg, er at det må holdes omvalg. I den perioden vi har sett på her ble det holdt omvalg etter ett valg: i Buskerud og Troms fylke i 1981. Det var feil ved forhåndsstemmegivningen og opptellingen som førte til omvalg.

Vedlegg E Ordliste

Asymmetrisk kryptering	Kryptering basert på et nøkkelpar, der den ene nøkkelen benyttes til kryptering og den andre til dekryptering. Utnyttes valigvis på den måten at den ene nøkkelen er offentlig mens den andre holdes hemmelig.
Autentisering	Mekanisme for bevis av påstått identitet – at man er den man utgir seg for å være.
Autorisering	En prosess som innebærer å gi tillatelse til å bruke bestemte IT-ressurser.
Backup	Sikkerhetskopi
Biometri	I forbindelse med autentisering: Måling av fysiske egenskaper ved en person (typisk karakteristika ved fingeravtrykk, farge på regnbuehinne).
Brannmur	En samling av komponenter som er plassert mellom to nettverk, og som tilsammen har følgende egenskaper: - all trafikk fra innsiden til utsiden, og motsatt, må passere gjennom brannmuren - kun autorisert trafikk, som definert i lokalt oppsett, vil kunne passere gjennom brannmuren - brannmuren er selv immun mot inntrenging.
Brukergrensesnitt	Samlingen av hjelpemidler som mennesker (brukerne) anvender for å samhandle med en gitt maskin, fysisk enhet og/eller datamskinprogram (dvs. et system). Typiske eksempler er tastatur, mus, skjerm, høyttalere og skjermbilder og effekten av å bruke disse enhetene på bestemte måter.
Buffer/overflytproblemer	At data skrives inn i hukommelsen utenfor det området som er avsatt for formålet. Kan skyldes rene programmeringsfeil eller manglende kontroll av inndata i programmet.
Dataintegritet	En sikkerhetsmekanisme som gjør det mulig å oppdage om data har blitt endret på en uatorisert måte eller pga. feil.
Digital signatur	Et dataelement som følger en elektronisk melding eller et dokument, og som binder dokumentet til et individ, en maskin eller et datasystem. Det tillater mottakeren å bevise hvor dokumentet kommer fra, og om dokumentet er forfalsket. Dataelementet genereres ved først å kjøre en hash-funksjon med utgangspunkt i dokumentet som skal signeres, og deretter kryptere med den private nøkkelen til den som skal signere. Sikkerheten i en digital signatur er dermed avhengig av at man kan stole på at den private nøkkelen kun er kjent av den rettmessige eier.
Digitalt sertifikat	En elektronisk legitimasjon for eieren av en privat og en tilhørende offentlig nøkkel som viser at den offentlige nøkkelen tilhører vedkommende.
Domenenavnsystem (DNS)	Tjeneste i Internett som oversetter URLer (som www.odin.no) til IP-adresser (som 195.225.0.230).
Duplisering	Kopiering, brukes ofte om å lage flere elektroniske eksemplarer av de samme dataene, eller å transportere de samme dataene flere

	ganger eller over parallelle kanaler.
EML	Election Markup Language, XML-basert markeringsspråk for formatering av data som skal overføres mellom moduler i et elektronisk valgsystem.
”Family voting”	Stemmegivning der noen familiemedlemmer blir utilbørlig påvirket av andre familiemedlemmer.
Hacking	Slangpreget betegnelse på å gjøre små endringer i datamaskinprogrammer. Brukes ofte i negativ betydning, og da om endringer som gjøres av uautoriserte personer med uhederlige hensikter.
Hash-algoritme	En matematisk funksjon som med utgangspunkt i en større mengde data genererer et bitmønster med et bestemt antall biter. En hash-funksjon generer alltid samme bitmønster for de samme data.
Hvitboks-testing	Testing av et programsystem basert på resonnering og formelle bevis. Krever tilgang til programkoden. Motsatsen er svartboks-testing, der man bare tester programsystemets funksjonalitet sett fra utsiden.
Ikke-benekting (uavviselighet)	Sikkerhet for at en som har sendt en melding gjennom et informasjonssystem ikke kan benekte eller avvise at det er vedkommende som har foretatt denne handlingen.
Infrastruktur	Grunnleggende strukturer og systemer som er nødvendige for en organisasjon, en samling av organisasjoner eller et land for å fungere på en effektiv måte.
Integritet	se dataintegritet
IP-adresse	Fireleddet adresse for en maskin tilknyttet Internett, eksempelvis 195.225.0.230.
Klientsystem	System som bruker tjenester fra et annet system (kalt tjenersystem).
Konfidensialitet	Sikring av at kun autoriserte personer får tilgang til informasjon.
Kryptering	Å forvanske en tekst (eller et bitmønster) til en uleselig, uforståelig såkalt chiffertekst som bare kan dekrypteres ved hjelp av en krypteringsnøkkel.
Krypteringsnøkkel	Et spesielt bitmønster som brukes som inndata til programmer for kryptering og dekryptering.
Mellommannangrep (”Man in the middle attack”)	Angrep basert på at noen (mellommannen) kobler seg inn i en elektronisk dialog mellom A og B og later som om man er B overfor A og A overfor B.
N-versjon-system	Programsystem som skal gi høy grad av sikkerhet ved at at de samme dataene behandles i parallell av N ulike undersystemer og resultatene sammenliknes. Avviker resultatene, foreligger en feil. Kan betraktes som en spesiell form for redundans.
Optisk leser	Utstyr som leser trykte og skrevne tegn, evt. strekkoder, fra papir og omsetter disse dataene til bitmønstre.
Phishing	Forsøk på å lure brukere til å oppgi sensitive data ved å utgi seg for å være en tillitsverdi organisasjon eller myndighet.
PKI (Public Key Infrastructure)	Public Key Infrastructure. En samling av sikkerhetstjenester, sikkerhetskomponenter og aktører som gjør det mulig å benytte digitale signaturer i stor skala.

Redundans	Duplisering av teknisk utstyr, programmer eller data. Brukes for sikrings- og kontrollformål.
Reviderbarhet	Reviderbarhet angår evnen til å avdekke hendelser og handlinger og knytte disse til bestemte subjekter.
Secure Sockets Layer (SSL)	Protokoll for autentisering og kryptering av nettverkskommunikasjon opprinnelig utviklet av Netscape. Den mest brukte protokollen for å opprette sikre nettverksforbindelser over Internett.
Smartkort	Plastkort i kredittkortstørrelse med en liten innebygd datamaskin.
Sporbarhet	Et prinsipp i offentlig forvaltning som sikrer at behandlingen av en sak kan rekonstrueres i ettertid. Det skal være mulig å etterspore hva som har skjedd (audit trail).
Stemmeakkreditiv (credential)	Et bevis på at velgeren er hvem vedkommende gir seg ut for å være.
Stemmetillatelse	Et bevis på at velgeren har rett til å avgi stemme ved det aktuelle valget.
Symmetrisk kryptering	Kryptering basert på at samme krypteringsnøkkel brukes både for kryptering og dekryptering.
Sårbarhet	Sårbarheten til et system er et uttrykk for de svakheter og mangler som finnes i systemet og spesielle omstendigheter som øker sannsynligheten for at trusler vil materialisere seg i en sikkerhetshendelse (eksempler på spesielle omstendigheter kan være størrelse, kompleksitet, at mange aktører er involvert, geografisk spredning, hyppige endringer og utsatt beliggenhet).
Tilgjengelighet	Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.
Tjenestenektangrep (”Denial of Service attack”)	Angrep mot et nettsted i form av forespørsler for å gjøre det vanskelig for andre brukere å oppnå kontakt med tjenesten som ønsket rammet. I verste fall kan dette føre til at det angrepne nettstedets tjenere vil bryte sammen. Slike angrep kan innebære bruk av flere kraftige datamaskiner (evt. et nettverk av datamaskiner) samtidig.
Trojansk hest	Ondsinnet programvare forkledd som et legitimt program.
Uavviselighet	Se ikke-benekting
UPS	Uninterruptable Power Supply – utstyr som sørger for at strømforsyningen opprettholdes selv om den normale strømforsyningen skulle falle ut.
Virus	Selvkopierende ondsinnet programvare som sprer seg selv fra datamaskin til datamaskin.
VPN	Virtual Private Network – programvare som gir muligheten for å opprette sikre datakommunikasjonskanaler gjennom en offentlig tilgjengelig, ofte usikker datanettinfrastruktur som for eksempel Internett.
”write-once”-medium	Lagringsmedium der data som er lagret, ikke kan overskrives eller slettes.
XML	Extensible Markup Language. Standard måte å kode elektroniske dokumenter på slik at det er mulig å gjenkjenne innholdselementer og formater som dokumentet består av.